INSTITUTO SUPERIOR DE ENGENHARIA DO PORTO
MESTRADO EM ENGENHARIA INFORMÁTICA




Controlo de acesso móvel

JOÃO PEDRO BANDEIRA GONÇALVES MAGALHÃES
Outubro de 2015

POLITÉCNICO
DO PORTO

isep Instituto Superior de Engenharia do Porto

Departamento de Engenharia Informática

Controlo de acesso móvel

João Pedro Bandeira Gonçalves Magalhães

Dissertação para obtenção do grau de Mestre em Engenharia Informática

Área de Especialização em Arquiteturas, Sistemas e Redes

Orientador: Alexandre Manuel Tavares Bragança

Versão Provisória

Porto, 20 de Outubro de 2015

Dedicatória

Quero agradecer a toda a minha família mas em especial aos meus pais por todo o apoio e força que me deram durante todo o meu percurso académico e principalmente nesta fase final do Mestrado. Agradeço também a todos os meus amigos e colegas que me acompanharam durante este percurso académico em especial aqueles com quem tive a oportunidade de trabalhar de perto e os que partilharam o meu sentimento enquanto desenvolviam a sua própria tese. Por fim, gostaria de agradecer ao meu orientador pelo apoio prestando durante estes meses de trabalho e por toda a dedicação que teve comigo no desenvolvimento deste projeto.

Resumo

O mercado de *smartphones* tem vindo a crescer massivamente nos últimos anos, bem como a diversificação das suas funcionalidades no dia-a-dia de cada pessoa. O mercado aberto de aplicações para estes equipamentos também tem sofrido uma forte evolução o que permite uma maior qualidade e competitividade pela apresentação de produtos. O conceito de casas inteligentes está cada vez mais presente e é algo que as pessoas se estão a acomodar de forma gradual. Para acompanhar tal feito, é necessário desenvolver as capacidades dos equipamentos que estas pessoas mais usam para que estes possam dar resposta a estas necessidades. Para o caso atual irão ser estudadas as fechaduras inteligentes.

Os sistemas comercializados atualmente, são tipicamente sistemas proprietários e apresentam algumas limitações ou faltas (ex: ao nível da segurança, incapacidade de abranger um largo número de dispositivos móveis ou mesmo ao nível do preço). Neste contexto, e com base na caracterização das soluções de controlo de acesso atuais, foi estudada a viabilidade de, usando uma abordagem assente em tecnologias não proprietárias (i.e., abertas), desenvolver soluções de controlo de acesso com características comparáveis com os sistemas proprietários actuais e, eventualmente, ultrapassando os limites e falhas identificados. Dadas estas premissas o sistema de controlo de acesso móvel pensado envolve um computador BeagleBone Black e a tecnologia sem fios Bluetooth. Este sistema permite a fácil integração do computador com qualquer *smartphone* atual e é dotado de fortes características de segurança e privacidade. O sistema foi concebido inicialmente para ser implementado em fechaduras de portas mas com possibilidade de expansão para outros equipamentos. Além disso, o sistema permitirá também o acesso a terceiros após a devida autorização do dono.

Palavras-chave: Fechaduras inteligentes, Bluetooth, controlo de acesso, *smartphone*, BeagleBone Black, open source.

Abstract

The smartphone market has seen a massive growth in utilisation in the past few years, as well as in its functionalities in people's everyday life. The open market of applications for these equipment as been on the rise too, which allows for more competitive and quality product presentation. The concept of smart homes is even more present and people are getting used to that in a progressive manner. To keep up with such events, it is necessary to develop the equipment's capacities so that these can give response to those needs. For the given case the smartlocks will be studied.

Nowadays, marketed sistems are typically proprietary systems and come with some faults (e.g.: security, unable to reach a large number of devices or even in terms of price). In this context, and with the current characterization of the existing access control solutions, it was conducted a study of the feasibility of, using an approach based on non proprietary technologies (i.e. open source), develop a solution of access control with characteristics comparable with current proprietary systems and, eventually, overcoming the mentioned limits and faults. Given these assumptions, the mobile access control system would involve a BeagleBone Black computer and the Bluetooth wireless technology. This system allows an easy integration between the computer and any current smartphone and it's gifted with strong security and privacy characteristics. The system was developed in an initial phase for door locks but it can be expanded to further solutions. Furthermore, this system will also allow the access by third party users after proper owner authorization.

Keywords: Smartlocks, Bluetooth, access control, smartphone, BeagleBone Black, open source.

Índice

Lista de Figuras

Lista de Tabelas

Capítulo

1 Introdução

Neste capítulo são apresentados alguns conteúdos de modo a contextualizar o leitor e facilitar a leitura sobre o tópico que será apresentado neste documento. Além do âmbito do mesmo, é explicada a metodologia utilizada para o desenvolvimento e escrita desta tese, assim como as questões mais relevantes que dela advêm. Mais que isso, são apresentados os objetivos do projeto e a fonte de motivação do mesmo. Por fim, é apresentada um visão geral sobre a estrutura do documento.

1.1. Contexto

Dando continuidade à rápida e crescente expansão da tecnologia no quotidiano populacional, chegou a vez dos nossos lares serem "invadidos" pela automatização e informatização. As casas inteligentes e a *Internet of Things* não são um tópico novo mas nos últimos anos têm vindo a ter maior destaque nos media devido aos melhoramentos que as soluções existentes têm vindo a apresentar e às soluções novas que nascem no mercado todos os dias com o objetivo de melhorar cada aspeto das nossas vidas diárias, por mais insignificante que este seja. Quando se menciona algo como "tecnologia recente" ou "novo dispositivo", as pessoas tendem a pensar imediatamente no preço. Afinal de contas, é um dos fatores que mais influencia a compra de equipamentos eletrónicos. Isto porque, com novos equipamentos vêm novas tecnologias, tecnologias estas que por vezes são únicas (i.e. proprietárias) e daí advém o elevado preço.

O mercado do controlo de acesso, mais concretamente, as fechaduras inteligentes tem vindo a crescer rapidamente e encontra-se num estado em que múltiplas empresas se encontram a desenvolver as suas próprias soluções em busca do domínio deste mesmo mercado. Existem soluções interessantes, outras menos comuns, soluções com alguns erros e certamente muitas com muita hipérbole. O que se tem vindo a notar também é a padronização do preço num limite bastante elevado, o que torna este tipo de soluções restritas a certas classes sociais.

Por fim, existe ainda a lenta expansão das tecnologias para lá das fronteiras do país de origem, o que torna a adoção destas um processo demorado e tedioso.

Internet of Things (IoT)

A *Internet of Things* é uma visão. Um visão que se encontra a ser construída neste momento e que irá desempenhar um papel muito significante no futuro. É algo bastante real e em que muitas pessoas dedicam o seu tempo a trabalhar sobre previsões e conceitos à volta do tópico. Este cenário assume-se como algo que irá ligar pessoas, animais e objetos (i.e. "*things*") e permitir a transmissão de dados sem necessidade de qualquer interação de humano para humano ou humano para computador. Esta comunicação é realizada através das tecnologias sem fios e o desenvolvimento da especificação IPv6 foi um passo enorme para a continuidade do trabalho sobre a *Internet of Things*. Este grandioso avanço poderá garantir um endereço virtual para praticamente cada objeto ou ser vivo atualmente existente. Ligados a este tema surgem outras preocupações como a privacidade e soberania [1] de dados e a segurança mas que se encontram fora do âmbito deste projeto.

Apesar do conceito só ter sido batizado em 1999, é algo que já se encontra a ser estudado há décadas. A primeira "coisa" a pertencer a este mundo foi uma máquina de vendas de Coca-Cola na Carnegie Melon University no início dos anos 80 (Wigmore, 2014). Os programadores conseguiam ligar-se à máquina através da Internet e verificar se existia uma bebida fresca disponível antes mesmo de se deslocar até ela.

Controlo de acesso móvel

Quer seja um local físico, quer seja um sistema informático ou um outro qualquer exemplo em que exista a necessidade de controlar quem acede a quê e quando podem aceder, deve-se implementar um sistema de controlo de acesso. O controlo de acesso trata-se da autenticação e autorização a um determinado local, instalação ou outro sistema através de diversos meios. Meios estes que têm vindo a evoluir e a tomar diversas formas ao longo do tempo e de acordo com o sistema a controlar. Desde os típicos torniquetes aos guardas que mantém certas instalações seguras já foram mais que provadas que são soluções com falhas e que por vezes envolvem custos desnecessários. O controlo de acesso móvel trata-se então da aplicação destas validações através de um dispositivo móvel (ex.: telemóvel, tablet, pulseira ou relógio). A grande vantagem na utilização do controlo de acesso móvel está na possibilidade da criação de sistemas homogéneos, escaláveis e facilmente adaptados aos mais variados ambientes em que estes possam ser aplicados e com os diversos requisitos de segurança.

Com o aumento da mobilidade da força de trabalho nas empresas, algo que também se

[1] A soberania de dados é o conceito de que toda a informação convertida e armazenada em formato digital está sujeita às leis do país em que se encontra fisicamente localizada.

tem vindo a notar e que, neste momento é praticamente um *facto standard*, é a utilização do dispositivo pessoal em ambiente empresarial. A este fenómeno dá-se o nome de BYOD ("Bring Your Own Device" – traga o seu próprio dispositivo). Esta situação por vezes não é o ideal para a segurança interna mas é algo que as empresas podem tirar partido de modo a reduzir os seus recursos financeiros e que vêm a auxiliar neste contexto de controlo de acesso móvel.

Fechaduras inteligentes

As *smartlocks*, ou fechaduras inteligentes, são fechaduras eletromagnéticas desenhadas para realizar operações de bloqueio e desbloqueio através de um dispositivo autorizado. Estas usam um canal de comunicação sem fios e uma chave criptográfica para realizar o processo de autenticação e autorização. São também capazes de monitorizar acessos e enviar alertas de diferentes eventos ou outros estados críticos relativos ao estado da fechadura. Como todas as fechaduras convencionais, estas também são constituídas por duas partes essenciais: a fechadura e a chave. Porém, neste caso, a chave não se trata de uma chave física mas sim de um *smartphone* com os recursos necessários para poder comunicar com a fechadura e transmitir mensagens de forma a conseguir o seu controlo à distância e, possivelmente, de forma automática. Este tipo de fechaduras são bastante úteis pois permitem que os donos da *smartlock* possam fornecer acesso a terceiros através de uma aplicação móvel desenhada para o efeito. Esta autorização permite às pessoas acederem à fechadura indicada através da mesma aplicação por um determinado período de tempo ou vezes de utilização e com a possibilidade de revogação de autorização a qualquer altura. Algumas fechaduras possuem módulos Wi-Fi o que permite a monitorização da fechadura, do seu estado e de outras características da mesma através de uma aplicação web. Outras fechaduras possuem (ainda) Bluetooth Smart e SSL para efetuar as comunicações.

1.2. Âmbito

De modo a comparar as fechaduras eletrónicas inteligentes, será necessário definir os meios de comparação pela qual os seus produtos irão ser avaliados e estes podem ser descritos pelos seguintes fatores:

- "Chaves" e gestão de acessos
- Mecanismo de bloqueio/desbloqueio
- Comunicação
- Segurança
- Bateria e falhas de energia

- Instalação
- Design

Estes fatores foram idealizados para um produto que nasce no seio de empresas essencialmente B2C, ou sejam, as soluções que desenvolvem são diretamente vendidas aos consumidores finais. Logo, além das especificações técnicas que as fechaduras apresentam, serão avaliados outros parâmetros de âmbito mais generalista como a instalação e o design. Será também realizada uma primeira visão geral a todas as fechaduras escolhidas para este estudo.

1.3. Metodologia de trabalho

Segundo o trabalho proposto e o objetivo deste projeto, pode-se concluir que esta tese se enquadra na metodologia *Design Science Research* (Vaishnavi/Kuechler, 2004), pois se propõe a criar um novo modelo para fechaduras eletrónicas inteligentes baseado em tecnologias *open-source*. Esta metodologia é um conjunto de técnicas e perspetivas analíticas para realizar investigação no campo dos sistemas de informação. A *Design Science Research* assume a criação de um artefacto, seja este um modelo, um método, uma construção ou uma instanciação de algo. Sendo que, o que for produzido deverá ser depois sujeito a uma avaliação de modo a determinar se existiu ou não inovação no artefacto ou, caso seja algo já existente, se existiu algum tipo de melhoria, seja esta qual for. Dependendo do artefacto podem existir melhorias a nível de processos, algoritmos, metodologias, entre outras. Tanto os métodos de investigação como os de avaliação devem ser de teor científico e rigoroso de modo a manter a coerência em investigações do mesmo género e adotar as exigências estabelecidas pelo método.

1.3.1. Questões de pesquisa

O problema das fechaduras convencionais está certamente resolvido com as crescentes soluções no mercado de fechaduras eletrónicas inteligentes. De uma maneira ou de outra, estas apresentam características que, melhor ou pior, resolvem a situação de abertura de portas à distância, concessão e revogação de acesso a terceiros, entre outras. A solução a que se pretende chegar deve conseguir manter as características básicas que as soluções existentes oferecem e, possivelmente, melhorar algumas delas. No entanto, a pergunta que esta tese pretende responder é a seguinte:

Questão principal: "Seria possível e viável construir um sistema de fechadura eletrónica usando componentes *open-source*?"

Esta é a principal questão desta tese e é a que me proponho a responder no final deste documento. A partir desta questão, surgem outras, direta ou indiretamente, relacionadas que

se designam por subquestões:

SQ-1: "Quais os requisitos funcionais de uma fechadura eletrónica?"
SQ-2: "Quais os requisitos não funcionais de uma fechadura eletrónica?"
SQ-2.1: "Quantos canais de comunicação devem estar disponíveis?"
SQ-2.1.1: "Quais os preferenciais?"
SQ-3: "Qual o hardware necessário para uma fechadura eletrónica?"
SQ-4: "Qual o software necessário para uma fechadura eletrónica?"

As duas primeiras subquestões poderão ser respondidas ao analisar as soluções de mercado atuais e avaliar os conceitos básicos de uma fechadura eletrónica no seguinte capítulo. Sendo que a SQ-2 será completada no terceiro capítulo deste documento, assim como as subquestões 2.1 e 2.1.1. As subquestões 3 e 4 serão abordadas conforme os requisitos apresentados na SQ-1 e, eventualmente na SQ-2, pois o que é pretendido é que seja encontrada uma solução que vá de encontro com a definição básica de fechadura eletrónica inteligente, sem descurar as características das soluções atuais. Além disso, serão estudadas e apresentadas várias alternativas no que toca a *hardware* e *software* e realizada uma comparação entre estas, sendo que dela resultará uma conclusão e uma escolha.

1.4. Objetivos

Ao responder às perguntas apresentadas anteriormente, este projeto espera contribuir em dois aspetos. O primeiro será fornecer um detalhado estudo das atuais soluções de fechaduras eletrónicas no mercado e uma análise de todos os seus aspetos técnicos e não técnicos, de modo a conseguir realizar uma comparação entre todas elas. Esta comparação permitirá a qualquer interessado em adquirir qualquer um destes produtos ou a qualquer pessoa da área obter as informações necessárias para uma escolha informada. Desta comparação irão também surgir conclusões que permitirão estudar e projetar uma solução baseada em tecnologias não proprietárias e facilmente implementáveis por qualquer pessoa interessada no tópico e com o mínimo de conhecimentos técnicos, sendo este definido como o segundo aspeto dos objetivos.

1.5. Motivação

A motivação para o desenvolvimento deste trabalho surge da crescente importância que os *smartphones* têm vindo a obter no quotidiano dos cidadãos e da sua expansão de utilidade através do crescente e aberto mercado de aplicações existente para os diversos sistemas operativos. A massificação do uso do *smartphone* é algo que está a acontecer no presente e continuará a crescer ao longo do futuro, logo é necessário dotar os atuais sistemas que nos rodeiam para que estes sejam capazes de interagir e lidar com tais modificações. Adicionalmente, acredito que os

mercados de *hardware* e *software* são bastante mais valiosos quando aplicados num contexto *open-source*. Apesar dos possíveis ganhos financeiros com tecnologias proprietárias, estes são facilmente ultrapassáveis pelos ganhos da partilha de conhecimento e desenvolvimento de soluções conjuntas.

1.6. Estrutura da dissertação

A presente dissertação encontra-se divida em seis capítulos, cada um com as suas subdivisões em secções. O presente capítulo serve como introdução ao tópico e como contexto para o leitor. O segundo capítulo analisa e descreve as soluções atuais de mercado, realçando as suas características mais importantes enquanto são realizadas comparações entre elas. No terceiro capítulo são apresentadas as tecnologias estudadas a nível de *hardware* e do canal de comunicação. Após apresentadas as possibilidades de cada uma das componentes, são avaliados os candidatos e todas as suas características, havendo uma decisão e justificação final para a escolha das tecnologias utilizadas. No capítulo seguinte, é descrita toda a solução desta tese abordando detalhes técnicos sobre a segurança, a aplicação móvel e o mecanismo de fechadura. Por fim, no quinto e final capítulo, é realizada a análise de resultados e conclusões finais. Existindo uma comparação com as fechaduras já abordadas e validando os resultados de acordo com a metodologia utilizada. Posteriormente, é feito um resumo das questões de pesquisa e descrito o possível desenvolvimento futuro.

1.7. Sumário

Neste capítulo foi dada uma introdução sobre o tema da tese em questão, assim como apresentados e explicados alguns tópicos para contexto da mesma. Dada a metodologia de trabalho, foram também identificadas as questões de pesquisa e as questões de literatura essenciais, assim como os objetivos desta tese. Por fim, foi apresentada a motivação para o desenvolvimento de um trabalho deste género e divulgada a estrutura do documento.

Capítulo

2 Soluções atuais

O presente capítulo tem como objetivo descrever os principais produtos de controlo de acesso da atualidade de forma a identificar as características destes e chegar a uma classificação que permita avalia-los. As fechaduras eletrónicas inteligentes possuem diversas características e o utilizador terá que se ambientar a manusear cada uma destas. O controlo remoto é certamente algo desejável numa fechadura eletrónica, não só pela facilidade de conceder acesso mas acima de tudo pela revogação de acesso à distância à nossa propriedade. Uma outra característica fundamental é o registo e alertas de acessos ou mudanças de estado na fechadura, não só a existência destes mas o formato em que nos são fornecidos (e-mail, SMS, plataforma web, etc.). Por fim, e possivelmente a mais complexa, é a compatibilidade e instalação da fechadura. Não só a nível de *hardware* mas também a nível de tecnologias utilizadas no desenvolvimento de cada solução.

Este capítulo encontra-se dividido em várias secções, na qual cada uma destas representa uma característica a ser avaliada e tomada em conta para a avaliação final. Em cada secção serão avaliadas todas as fechaduras e no final será feito um balanço geral.

Nota: Os padrões de avaliação de instalação e design foram única e exclusivamente obtidos através de comentários e opiniões online.

2.1. Visão global

Para o presente documento irão ser avaliadas 6 fechaduras. Existem muito boas soluções atualmente mas as que se seguem foram escolhidas pela sua maturidade, características e preço como padrão do mercado. Cada vez mais empresas estão a competir para serem a barreira inteligente entre nós e as nossas casas. Algumas requerem a substituição integral da fechadura existente, enquanto que outras são facilmente integradas com a atual. Existem ainda outras características que tentam diferenciar as soluções de maneira a conseguirem alguma vantagem comercial, como abertura através do toque na fechadura ou através da simples aproximação

da porta. Segue-se um resumo das fechaduras a serem avaliadas:

	País de origem	Disponibilidade	Preço	Plataformas
August	EUA	EUA e Canadá	$249,99	Android, iOS e Web
Danalock	Dinamarca	Mundial	$179	Android, iOS e Web
Goji	EUA	Mundial	$278	Android e iOS
Haven	EUA	Mundial	$219	Android, iOS e Web
Lockitron	EUA	Mundial	$99	Android, iOS e Web
UniKey	EUA	Mundial	$219	Android (beta), iOS e Web

Tabela 2.1.: Sumário de fechaduras a analisar

A primeira fechadura trata-se da **August Smart Lock** [1], esta declara-se como o sistema que redefine o controlo de acesso a nossa casa de uma maneira simples, segura e social. Esta fechadura eletrónica foi especialmente desenhada para mecanismos de bloqueio de cilindro único e vem preparada com alternativas energéticas caso algo não corra como esperado. Este produto tem vindo a receber bons comentários por parte das revistas e analistas tecnológicos. Esta fechadura é sem dúvida a mais elegante de todas elas, graças ao toque de design de Yves Behar. O bloqueio circular de alumínio escovado substitui o antigo mecanismo de bloqueio de cilindro único, e é possível ser controlada e gerida a partir de um dispositivo iOS, Android, ou aplicação web. A August avisa quando certas pessoas entram e saem de casa, e permite também emitir chaves digitais ilimitadas a terceiros, personalizando para exatamente quanto tempo estes terão acesso, em que dias, ou mesmo entre que horas. O bloqueio utiliza a tecnologia de baixa energia Bluetooth para reconhecer quando um dispositivo com uma chave digital está próximo. Não há necessidade de retirar o dispositivo e aproximá-lo da fechadura. A August também vem com a funcionalidade de desbloqueio automático (funcionalidade atualmente em verão *beta*).

A **DanaLock** [2] foi facilmente incluída nesta listagem como sendo a única aposta no mercado Europeu. Nascida de uma empresa Dinamarquesa, esta fechadura assume-se como a verdadeira e original fechadura inteligente para as nossas propriedades. Utiliza a tecnologia de ponta Bluetooth LE e *Z-Wave* o que permite uma facilidade e personalização de uso da mesma muito grande. Esta fechadura tem ainda a particularidade de, durante a sua instalação, ser conectada a sistemas de terceiros (hotéis, lares, etc.) e permitir, deste modo, a integração com os sistemas de registos de entradas e saídas. Esta fechadura também se adapta ao cilindro atual e é apenas montada do lado de dentro da porta. Uma das funcionalidades que a Poly-Control (fabricante da fechadura) tenta utilizar como destaque no mercado é a "*knock-to-unlock*" (bater para desbloquear). Esta funcionalidade permite ao utilizador bater no ecrã do telemóvel (como se estivesse a bater à porta) e, caso o padrão de batimento esteja correto, a porta abre-se. Por fim, este fechadura leva também pontos de vantagem no que toca a compatibilidade, visto que

[1] `http://august.com/`
[2] `http://danalock.com/`

oferece múltiplas versões da mesma fechadura. Não só em termos de *hardware* (mecanismos europeus, americanos e escandinavos) como também a nível de *software*, o que permite uma fácil adaptação do preço às necessidades de cada cliente.

A **Goji** [3], marca registada da Bielet Inc., desenvolve sistemas de controlo de acesso sofisticados e visualmente agradáveis de modo a fornecer total controlo sobre a nossa propriedade através de um dispositivo móvel. Tal como muitas das outras fechaduras, também esta tem uma característica que a destaca no mercado: campainha inteligente. Isto significa que não só permite o controlo da fechadura em si mas também permite, em tempo real, saber quem está à nossa porta através de fotografias enviadas para o dispositivo. Uma outra característica bem anunciada deste produto é o seu suporte ao cliente que afirma estar disponível a qualquer altura e até mesmo permitir o desbloqueio remoto da porta como acontece em determinados automóveis hoje em dia. Apesar de ser uma excelente comodidade para alturas em que o *smartphone* falha, esta poderá apresentar-se como uma grande fraqueza e vista pelos consumidores como uma possível falha de segurança. Por outro lado, esta fechadura é complacente com a UL [4]

Por fim surge a verdadeira diferenciação de mercado, a **Haven** [5]. Esta pode não ser considerada uma *smartlock* mas faz certamente parte do mundo do controlo de acesso. Eliminando completamente o conceito de fechaduras e todos os problemas que delas advêm, a Haven é uma pequena placa instalada no chão ao longo da porta de forma a bloquear de maneira bastante eficaz os arrombamentos. Esta placa funciona como uma base mecânica que se eleva de modo a prevenir a abertura da porta e pode ainda baixar-se automaticamente em caso de emergência. Dado que se encontra do lado seguro da divisão e do facto de não existir qualquer tipo de *hardware* do lado de fora da porta, esta diminui significativamente as falhas de segurança e possíveis tentativas de destruição da fechadura. Como grande contrapartida, está obviamente toda a instalação que advém deste sistema ligeiramente mais complexo. No entanto, esta desvantagem pode facilmente ser ignorada com o facto de este sistema de controlo de acesso permitir também a integração com outros sistemas inteligentes já presentes na casa, como por exemplo: ligar a televisão, acender as luzes ou mesmo pré-aquecer o forno. Todo este conceito foi baseado num conjunto de acontecimentos reais que levaram a uma série de assaltos por forçar as fechaduras (técnica conhecida como "*lock bumping*") e arrombamentos de portas.

De seguida, temos a **Lockitron Bolt** [6]. Com a Lockitron Bolt, é possível conceder acesso imediato à família, amigos e clientes, a casa ou à empresa, a partir de qualquer lugar do mundo utilizando apenas um *smartphone* com acesso à Internet. O Lockitron Bolt conecta qualquer dispositivo iOS ou Android diretamente via Bluetooth Low Energy. Graças à tecnologia propri-

[3] `http://gojiaccess.com/`
[4] Underwriters Laboratories (UL) é uma empresa americana de consultoria e certificação de segurança mundial. Esta fornece serviços relacionados com segurança a nível de certificação, validação, testes, inspeção, auditoria, aconselhamento e treino.
[5] `http://havenlock.com/`
[6] `http://lockitron.com/`

etária Sense™, o Lockitron Bolt consegue desbloquear a porta assim que a pessoa se aproxima desta. Esta foi também das primeiras fechaduras no mercado a nascerem do *crowdfunding* e a versão inicial da fechadura não substituía nenhum mecanismo de fecho da porta mas trabalhava sim sobre o atual. Isto significava que o número de portas compatíveis com esta fechadura eletrónica era um pouco mais pequeno em comparação com as outras. A versão atual, requer que o utilizador substitua por completo todo o mecanismo de bloqueio da porta, à similaridade dos competidores. O preço inicial também sofreu alterações estabelecendo-se neste momento como o mais baixo do mercado. Esta fechadura oferece ainda outras capacidades como a sua API aberta que permite a configuração e expansão de funcionalidades da fechadura aos mais variados dispositivos.

A **UniKey** [7], também conhecida como Kevo, nasce da parceria entre a Unikey e a Kwikset & Weiser e apresenta-se como um dos maiores competidores do mercado atualmente. Esta fechadura destaca-se pela diferente abordagem no conceito de instalação da mesma. Ao contrário de muitas outras, esta fechadura substitui por completo a fechadura atual e é instalada tanto do lado de dentro como do lado de fora da porta. Este sistema permite aos fabricantes introduzir a característica do toque para abrir. Com um simples toque na fechadura, este deteta se um *smartphone* autorizado se encontra próximo e automaticamente fornece acesso à propriedade. Este sistema não só permite saber se alguém se aproximou mas também de que lado da porta está de modo a evitar possíveis falhas de segurança. Este feito é atingido através de tecnologia proprietária que se encontra de momento *patent-pending*. Ainda assim, os fabricantes desta poderosa fechadura conseguiram desenvolver um sistema resistente aos mais rigorosos testes da indústria, incluindo provas de colisões e anti *lock picking*.

2.2. "Chaves" e gestão de acessos

A maior parte das fechaduras aqui apresentadas funciona através de chaves eletrónicas ou *eKeys*. Estas chaves podem ser emitidas/enviadas por parte do dono da casa através do seu dispositivo móvel ou através de uma plataforma web. Associadas as estas chaves podem estar tempos de utilização, isto significa que os detentores dessas mesmas chaves só as poderão utilizar em determinados dias e determinadas horas. Além das restrições temporais, as chaves podem ainda ter um tempo de validade definido. Isto permite que os donos das propriedades estabeleçam uma data limite de utilização da fechadura, bastante útil em situações de alugueres esporádicos como se verifica na altura das férias. Além de todo este acesso restrito e controlado, existem ainda todo um registo por cada ação efetuada. Quer seja de bloqueio da porta, quer seja de desbloqueio, todas as ações são registadas num servidor externo ou localmente na fechadura para posterior consulta. Para as fechaduras que oferecem, como sistema de *backup*, uma chave física tradicional, existe ainda a possibilidade de registar os acessos utilizando esta

[7] `http://unikey.com/`

mesma chave.

A utilização de *smartphones* tem vindo a crescer de ano para ano e cada vez mais estes são enviados com as mais recentes tecnologias do mercado. Porém, as empresas que atualmente fabricam estes dispositivos de controlo de acesso não querem esperar que os seus consumidores possuam um *smartphone* ou que este tenha as mais recentes tecnologias disponíveis. Para isso, foram desenvolvidos pequenos dispositivos chamados *key fobs* que permitem um tipo de interação com a fechadura mais básico que o *smartphone* mas capaz de cumprir os requisitos mínimos de bloqueio/desbloqueio da porta. Este dispositivo só se encontra disponível em algumas das soluções.

Figura 2.1.: *Key fob* (Uniforms)

Como pode ser verificado na imagem, estes pequenos dispositivos são muito práticos e podem ser utilizados como porta chaves. São também ideais para crianças e idosos que ainda não possuam qualquer tipo de *smartphone* ou cuja compreensão/utilização do mesmo não seja suficiente para manusear a aplicação necessária.

A **August smarlock** vem, como referido anteriormente, preparada para interagir com aplicações móveis e web. Estas aplicações permitem a gestão de todos os dispositivos/utilizadores que possam interagir com a fechadura. Para adicionar um novo utilizador, basta inserir o número de telemóvel da pessoa (manualmente ou através da lista de contactos) e esta receberá um convite para descarregar a aplicação. Durante este processo, o dono da fechadura define também o nível de acesso do convidado e o tipo de acesso. Existem dois níveis de acesso:

- *Owner* (Dono):
  - Pode convidar/remover outros donos
  - Pode modificar as configurações da fechadura
  - Pode convidar/remover convidados
- *Guest* (Convidado):
  - Não pode convidar outros convidados
  - Não pode modificar as configurações da fechadura

Quanto aos tipos de acesso, existem três tipos de acesso:

- Acesso permanente - Os convidados têm acesso ilimitado, mas o dono pode modificar ou remover a qualquer altura

- Acesso recorrente - Os convidados têm acesso com base num horário recorrente, ex.: os convidados têm acesso às segundas, terças e sextas entre as 19h00 e as 23h00.
- Acesso temporário - Os convidados têm acesso limitado com base num prazo, ex.: os convidados têm acesso entre hoje às 10h00 e amanhã às 11h00

Após fornecer acesso às pessoas desejadas é possível, então, iniciar o processo de monitorização de cada uma das fechaduras. Este processo é possível graças ao registo constante da fechadura sobre toda e qualquer atividade que seja executada. Neste registo também é guardada a pessoa que a executou, bem como a data e hora do acontecimento. Além de todos estes registos, também é possível receber notificações em tempo real sobre todas estas atividades. Também esta fechadura trabalha sobre o conceito de *eKeys*, o que significa que o dono da fechadura pode enviar convites para qualquer pessoa com um *smartphone* para que esta consiga aceder ao interior da sua propriedade.

Um pouco à semelhança da anterior, está a **Danalock** que também permite o controlo de acesso temporário por parte de terceiros. No entanto, e tendo por base a falta de informação tanto no website como no guia da aplicação móvel, não existe qualquer modo de revogação de acesso. Este fator pode tornar-se determinante de qualquer decisão devido à falha de segurança que representa. Adicionalmente, o tipo de acesso em comparação com a **August** é muito básico, sendo que apenas permite a definição de data e hora de início e de fim e não oferece qualquer personalização a nível temporal para os acessos. Por fim, quando alguém utilizar a a aplicação para abrir a **Danalock** não deve ser esperada nenhuma notificação dado que esta não fornece qualquer tipo de alerta para esta.

Para superar estes dois competidores anteriores, surge então a **Goji**. Esta pequena fechadura inteligente assume-se como um verdadeiro concorrente a ter em conta. A gestão de acessos é baseada em contas (i.e. à base de email) e através desta é possível convidar qualquer pessoa a quem desejemos fornecer acesso. Acesso este que, à semelhança da **August**, pode ser personalizado. No entanto, não oferece tantas opções. Permite apenas definir data de início e fim, dias da semana recorrentes e horas de acesso. Ao contrário da **Danalock**, esta fechadura permite editar ou eliminar todas as *eKeys* que foram emitidas a qualquer momento. Durante o processo de emissão de uma *eKey* para alguém, existe uma opção que permite requerer o envio de notificações quando esta for utilizada. Sendo que, independentemente desta definição, todos os acessos são registados nos servidores da empresa para consulta a qualquer momento. Por fim, deve ser notado que esta é uma das fechaduras que oferece a possibilidade de utilização de *key fobs*. Estas *key fobs* podem ser adquiridas separadamente e também funcionam com o mesmo sistema de acesso temporário limitado que os *smartphones*.

No seio de tantas soluções, a **Haven** é a que menos se adequa ao conceito de chaves e fechaduras. Com a sua abordagem única, esta empresa poderá revolucionar o mercado. Esta solução oferece a aplicação móvel para os mercados iOS e Android, assim como a habilidade de envio de *eKeys*. No entanto, apesar de mencionar a possibilidade de definição de data de

validade, não especifica em que condições estas podem ser partilhadas. Assegura também que as *eKeys* podem ser revogadas a qualquer altura. Dada a falta de informação devido ao ciclo de vida deste produto, não é possível determinar se este fornece registos de atividades ou notificações em tempo real de acesso à propriedade. Em semelhança à **Goji**, também esta oferece *key fobs* para facilmente desbloquear este dispositivo.

A **Lockitron** é uma fechadura que segue bastante a linha da **August**. Apresenta-se como uma forma social de fornecer acesso a terceiros por parte da aplicação móvel e tem características muito comuns. Ambas as aplicações desta fechadura (iOS e Android) estão preparadas para responder a 100% a todos os requisitos. O envio de *eKeys* pode ser realizado a partir da lista de contactos do telemóvel ou através da ligação com as redes sociais. Esta última, permite uma muito maior flexibilidade por parte da fechadura no que toca a transmissão de chaves. Nesta transmissão, é possível definir uma data de início e uma data de fim. A identificação do utilizador pode ocorrer tanto por e-mail como por número de telemóvel. Apesar de, como a **Danalock**, não oferecer um método de personalização do tempo de acesso à fechadura a **Lockitron** permite a definição de papéis ou níveis de acesso quando se está no processo de criação de uma chave nova. Esta solução oferece mais um nível de acesso do que a **August**, que pode ser verificado na listagem seguinte:

- *Owner* (Dono):
  - Pode convidar, editar ou remover qualquer pessoa exceto eles próprios
  - Pode criar, editar ou remover chaves de qualquer pessoa exceto eles próprios
- *Admin* (Administrador):
  - Pode convidar, editar ou remover convidados
  - Pode criar, editar ou remover chaves de convidados
- *Guest* (Convidado):
  - Apenas pode abrir e fechar a fechadura

A definição de níveis de acesso ou envio de *eKeys* para terceiros é ilimitada. Em relação aos registos, também esta fechadura guarda todos os registos de atividades ocorridas em relação a uma fechadura. Isto inclui, bloqueios e desbloqueios, mudanças de configurações e gestão de utilizadores. Cada vez que ocorre uma destas operações de bloqueio ou desbloqueio da fechadura, é emitida uma notificação para o dono da mesma. O sistema de notificações funciona inclusive com chaves mecânicas. Esta fechadura não oferece qualquer tipo de suporte para *key fobs*.

Quando se fala da **UniKey**, fala-se de um dos maiores concorrentes no mundo das fechaduras eletrónicas. E no que toca a chaves e controlo de acesso, possui tantas características como as da vizinha **Goji**. Permite o envio de *eKeys* para qualquer pessoa, sendo que é possível escolher entre três tipos de chaves diferentes para distribuir:

- *Anytime* (A qualquer hora): Esta chave pode ser utilizada a qualquer hora e qualquer dia. É considerada uma chave permanente mas pode ser facilmente transformada numa chave *Scheduled*;
- *Guest eKey* (Convidado): Este tipo de chave pode ser emitido a qualquer altura e permite o acesso à propriedade durante 24 horas. Após essas 24 horas, quer a chave tenha sido utilizada ou não, expira;
- *Scheduled* (Programado): Permite um acesso restrito em tempo e dias mas nunca expira. Pode também ser transformada a qualquer altura numa chave *Anytime*.

Estas chaves são sempre geridas pelo dono da fechadura. O dono é a pessoa que instalou a fechadura e é o único que a pode eliminar caso seja necessário. No entanto, este pode definir um outro nível de acesso para administradores. Estes conseguem gerir outros administradores e chaves disponíveis. Qualquer destes acesso pode ser temporariamente desativado ou eliminado de vez. Existe ainda um outro pormenor que diferencia esta fechadura de todas as outras. A **UniKey** coloca um pequeno entrave ao limitar o número de chaves emitidas. Quer seja por questões logísticas, quer seja por questões de segurança, só podem ser emitidas 5 chaves *Anytime* ou *Scheduled*. Recentemente foi decidido que as chaves *Guest* seriam ilimitadas. Apesar desta limitação, a empresa oferece a possibilidade de adquirir novas *eKeys* pelo preço (e como compras *in-app*) de $1,99. Apesar de todas estas possibilidades, também está à disponibilidade dos clientes a tradicional chave mecânica. Sendo que, na compra da fechadura são oferecidas duas destas chaves.

Tal como a concorrência, também esta fechadura oferece um registo completo sobre todas as atividades ocorridas em cada fechadura. Sejam estas ações eletrónicas ou mecânicas. Além disso, estão disponíveis notificações em tempo real sobre a utilização da fechadura e, novamente, tanto para ações eletrónicas como mecânicas. Por fim, a **UniKey** também vem preparada para suportar *key fobs*, existindo um *key fob* por cada fechadura adquirida.

Sumário

Finalizada a primeira secção sobre a análise das soluções atuais, podemos concluir que quase todas as fechaduras se estabeleceram num padrão em relação às chaves e gestão de acesso das mesmas. Algumas preferem uma abordagem ligeiramente diferente mas que é possível ser resumida no quadro seguinte:

	August	Danalock	Goji	Haven	Lockitron	UniKey
Envio de "eKeys"	✓	✓	✓	✓	✓	✓
Key fob	✗	✗	✓	✓	✗	✓
Notificações de acesso	✓	✗	✓	✗	✓	✓
Registo de atividade	✓	✓	✓	✓	✓	✓

Tabela 2.2.: Sumário de: "chaves" e gestão de acesso

2.3. Mecanismo de bloqueio/desbloqueio

Os mecanismos de bloqueio e desbloqueio existentes nas fechaduras são o que mais as diferenciam da concorrência no mercado e é o fator que recebe mais atenção no que toca a inovações que possam ajudar no sucesso da empresa. É também a característica que vai estar em constante execução e teste por parte dos clientes. Existe imenso escrutínio sobre estes processos, logo têm de ser eficientes e eficazes na sua execução. Um dos fatores que sofre mais críticas nos comentários online e críticas aos produtos é a rapidez destes, ou a falta dela. Muitas das fechaduras declaram que vieram para mudar a forma como as portas se abrirão no futuro, afirmando que não existirá mais a perda de tempo à procura das chaves ou a desembaraçar os porta chaves. No entanto, com a intervenção da tecnologia esta veio a constituir uma outra barreira devido às comunicações entre a fechadura e o dispositivo.

A **August smarlock** possui um mecanismo de bloqueio/desbloqueio dentro dos *standards* da indústria. Possui a muito polémica característica de bloqueio/desbloqueio automático através da proximidade, que permite a uma pessoa desbloquear a porta ao se aproximar pelo lado de fora e bloquea-la ao se afastar. O que deixa muitos consumidores preocupados, pois dado que se trata do acesso ao seu lar, têm algumas dúvidas em relação à capacidade de detetar de que lado da porta se encontra o dono da casa. Estas dúvidas surgem da situação em que um estranho toca à campainha e caso o dono se aproxime para verificar a identidade da pessoa que se encontra do lado de fora ou caso passe perto da porta por outra qualquer razão, a porta se possa desbloquear automaticamente. Esta característica também se encontra presente na **Danalock**. Após a definição da localização da fechadura, a aplicação define um raio de segurança que ativará o bloqueio/desbloqueio automático por proximidade. No entanto, também esta abordagem possui problemas de segurança. Imaginando que, após sair de casa e trancar a porta, a pessoa se afasta do perímetro de segurança mas por qualquer razão necessita de voltar atrás sem chegar a entrar dentro de casa, a fechadura desbloquear-se-á automaticamente. Esta representa uma forte falha de segurança para qualquer pessoa. De modo a fornecer alternativas e deixar de fora esta opção de bloqueio/desbloqueio automático, a **Danalock** fornece uma característica única que permite o desbloqueio da porta com o simples toque no ecrã do telemóvel. Esta pequena batida funciona com o ecrã desligado mas a aplicação a executar em

segundo plano. Ao ativar esta característica, é possível executar a operação de desbloqueio sem o aborrecimento de desbloquear o ecrã, abrir a aplicação, selecionar a fechadura e tocar para desbloquea-la. Quem também achou por bem implementar o bloqueio/desbloqueio automático foi a **Goji** e a **Haven**. Com a ligeira diferença de que, como estas oferecem *key fobs*, também estes funcionam da mesma maneira para a operação em causa. Ora, tendo em conta as falhas de segurança apontadas anteriormente e o público alvo a quem as *fobs* se destinam, o resultado pode tornar-se num verdadeiro pesadelo sem confiança alguma sobre os estado das fechaduras. De modo a melhorar a situação e fornecer alternativas como a **Danalock**, a **Haven** criou um sistema de pedal que funciona para abrir a porta e imediatamente colocar a base em modo seguro mal a porta de feche. Este é um processo completamente mecânico o que funciona bastante bem e sem qualquer tipo de atrasos. É também um processo idealmente pensado para situações de emergência em que a saída da habituação é urgente e atrasos em sistema eletrónicos para abertura do único meio de saída são intoleráveis. Este tipo de abordagem tido em conta pela **Haven** traz todo um problema não pensado anteriormente e que provavelmente muitas das outras soluções não consideraram. O que foi sim considerado foi o problema dos mecanismos de bloqueio/desbloqueio automáticos pela **UniKey**. Com um sistema proprietário (patente pendente) e a instalação da fechadura em ambos os lados da porta, esta empresa oferece um sistema inteligente que possibilita a deteção da localização do utilizador com muito mais detalhe e desta forma prevenir desbloqueios indesejados. O que esta fechadura oferece também é um sistema completamente inovador que permite ao utilizador, com um simples toque na fechadura, bloquear ou desbloquear a mesma. Este sistema é único no mercado e surge como alternativa ao bloqueio/desbloqueio automático por proximidade. Isto é, mais uma vez, graças à dupla instalação da fechadura no interior e exterior da porta que permite ter sensores no exterior que, não só detetam o toque humano, mas que também fazem a verificação de proximidade de um dispositivo móvel autorizado. Também como tecnologia proprietária surge a *Sense™*, por parte da **Lockitron**. Esta tecnologia surge no mesmo âmbito do bloqueio/desbloqueio automático por proximidade. *Sense™* trata-se apenas do sistema de descoberta da fechadura automaticamente por proximidade, pois a característica pode ser ativada em dois modos:

- *Sense Notifications*: este modo apenas alerta para o facto de existir um fechadura nossa na proximidade pela simples emissão de uma notificação para o telemóvel;
- *Proximity Unlock*: este modo é o que permite executar as mesmas ações de desbloqueio automático que as outras soluções oferecem. O que é possível neste é, definir um limiar de formar a calibrar a aplicação e melhorar assim a sua performance nestes casos.

Ora, depois de tanto descrever os processos de bloqueio e desbloqueio por proximidade existe ainda uma outra situação que estas fechaduras se depararam e rapidamente solucionaram que é este mesmo processo mas à distância. Para tal, as fechaduras deixam de confiar

na base de comunicações atual de Bluetooth e passa a incluir outra tecnologia na equação: o Wi-Fi. Muitas das soluções originais não vinham preparadas para receber este tipo de característica como a **August** e a **Lockitron**. Para tal, estas duas empresas criaram dispositivos externos como base de suporte para as respetivas fechaduras que é descrito na próxima secção deste documento. Todo o acesso à distância é realizado através de uma plataforma web que comunica diretamente com a fechadura.

Sumário

Com a secção atual finalizada, foi possível verificar que, novamente, as fabricantes de fechaduras eletrónicas inteligentes tendem a estabelecer características muito próximas umas das outras. No entanto, é precisamente neste fator que tentam aplicar a maior diferenciação e criar aspetos que as tornam únicas como o bater para abrir da **Danalock** ou o toque na fechadura da **UniKey**. Apesar do que a **Haven** oferece como mecanismo de abertura ser completamente único, não é algo que possa ser aplicado a todas as fechaduras como padrão de comparação e logo não é listado no seguinte sumário:

	August	Danalock	Goji	Haven	Lockitron	UniKey
Proximidade local aplicação móvel ou *key fob*	✓	✓	✓	✓	✓	✓
Tocar (fechadura) para bloquear/desbloquear	✗	✗	✗	✗	✗	✓
Bater (smartphone) para bloquear/desbloquear	✗	✓	✗	✗	✗	✗
Bloquear/desbloquear à distância	✓	✓	✓	✓	✓	✓

Tabela 2.3.: Sumário de: mecanismos de bloqueio/desbloqueio

2.4. Comunicação

As comunicações entre a fechadura e o dispositivo é um dos fatores com maior importância. É necessário que exista a compatibilidade necessária entre as tecnologias utilizadas e o mercado atual de dispositivos. É também necessário que as comunicações sejam realizadas de forma rápida e eficaz.

As comunicações dos dispositivos entre as fechaduras **August** são efetuadas através de Bluetooth Low Energy (BLE). Esta fechadura apesar de efetuar as comunicações numa base de BLE, também suporta a utilização de Wi-Fi. Por sinal, toda a configuração inicial da fechadura é executada através de Wi-Fi. No entanto, este suporte a Wi-Fi é limitado. Caso alguém queira aceder à fechadura eletrónica à distância, terá que adquirir um dispositivo extra chamado *Connect*.

Figura 2.2.: August Connect (August)

Este pequeno dispositivo oferece aos seus utilizadores a capacidade de interação com a fechadura à distância através de uma aplicação web. Deve ser colocado numa qualquer tomada, preferencialmente perto da fechadura, e é possível executar qualquer ação também possível quando perto desta. O método de comunicação passa pelo *smartphone* aceder à Internet e enviar os comandos para a *Connect* que por sua vez, estando ligado ao router de casa, os envia para a fechadura. O facto deste dispositivo permitir o acesso à distância, também acarreta algumas preocupações de segurança, pois não existe a necessidade do smartphone se encontrar ligado à mesma rede Wi-Fi. Isto significa que, qualquer pessoa, através do roubo de credenciais poderá aceder ao interior da casa. Com um maior leque de opções surge a **Danalock**, que oferece dois estilos de fechadura: uma equipada com BLE e outra com BLE e *Z-Wave*. *Z-Wave* é uma tecnologia sem fios que opera na banda 908.42MHz e é relativamente recente no mundo da *IoT*. Por trás desta tecnologia está a *Z-Wave Alliance* que de momento ostenta mais de 1000 dispositivos diferentes e compatíveis entre si que permite uma maior facilidade na automatização das casas. Com a versão, *Z-Wave* a **Danalock** pode então ser operada em qualquer lugar no mundo através de um *gateway* Z-Wave utilizando a Internet. Caso o utilizador prefira trabalhar *offline*, (operar a fechadura diretamente do *smartphone* sem utilização de uma ligação ao servidor) pode simplesmente alterar o modo desta. Sem revelar muito sobre as comunicações que utiliza, a **Goji** menciona apenas que funciona com Bluetooth e Wi-fi. O interessante neste caso é que o controlo à distância também é realizado através da aplicação móvel e não por uma aplicação web. Caso exista alguma falha na rede, a aplicação conseguirá comunicar com a fechadura e validar as chaves de acesso, no entanto não serão enviadas atualizações até que o sistema seja colocado novamente *online*. Caso a fechadura se encontre mais de duas horas em modo *offline*, o dono receberá uma mensagem de texto a alertar para o facto. No que toca a comunicações, a **Haven** não se deixa ficar para trás. Oferece as já conhecidas soluções de Bluetooth em conjunto com Wi-Fi mas pondera no futuro oferece suporte para Z-Wave. O que este tipo de tecnologias combinadas oferece é um largo suporte para os mais variados dispositivos ou sistemas existentes ou futuros de nossa casa. O que isto significa é que não só poderão ser automatizadas atividades em função de determinadas ações (ex.: o aquecimento

liga, as persianas fecham, as luzes e a televisão acendem assim que a fechadura se desbloqueia a certa hora do dia), como também poderão ser realizadas comunicações de emergência para sistemas interligados (ex.: em caso de arrombamento, efetuar chamada para a empresa de segurança ou polícia). A acompanhar mais uma vez de perto a sua rival **August**, a **Lockitron** passa por oferecer o controlo de acesso total à distância também com base num dispositivo externo.

Figura 2.3.: Bolt Bridge (Lockitron)

Chama-se *Bridge* e é possível comunicar com este aparelho através da plataforma web que a empresa oferece. Este aparelho funciona na mesma base que o *Connect*. Estando ligado à Internet de casa, pode enviar depois todas as comunicações diretamente para a fechadura. Mas este tipo de controlo não fica por aqui, as comunicações são bidirecionais e as capacidades destes dispositivos externos expande para receber notificações em tempo real de tudo que acontece com a fechadura. Por fim, temos a **UniKey** que, apesar de ser um concorrente de peso, não demonstra possuir uma grande vantagem no que toca às comunicações. É capacitado de Bluetooth 4.0 (BLE) e Wi-Fi mas apresenta uma característica peculiar. Dos tipos de "chaves" e métodos de acessos descritos na secção anterior desta fechadura, as "chaves" de convidados e as de acesso temporário requerem uma ligação à Internet. Apesar da possível inconveniência que isto possa acarretar, é um excelente ponto de vista dado que doutra forma não seria possível verificar se os acessos ainda se encontravam válidos.

Sumário

Após avaliar as comunicações entre fechaduras e dispositivos de cada uma das soluções, foi possível verificar a capacidade de adaptação de cada uma delas e a consciência de como não só mercado de fechaduras mas todo o mercado de *IoT* se encontra em constante estado de evolução.

	August	Danalock	Goji	Haven	Lockitron	UniKey
Bluetooth Low Energy (BLE)	✓	✓	✓	✓	✓	✓
Wi-Fi	✓	✓	✓	✓	✓	✓
Z-Wave	✗	✓	✗	✗	✗	✗

Tabela 2.4.: Sumário de: comunicação

2.5. Segurança

Esta pode muito bem ser a característica mais importante a ser analisada. No final de contas, estamos a falar de dispositivos que permitem ou não a entrada no local onde qualquer pessoa se deve sentir 100% segura. Quanto à segurança, esta pode ser avaliada através de duas perspetivas, a segurança física e a segurança lógica. Na segurança física as fechaduras devem apresentar elementos robustos, tolerantes a falhas e resistentes a qualquer tipo de condição meteorológica (dado que poderão estar em contacto com o exterior). Na segurança lógica, é onde será aplicado maior nível de esforço para existir a certificação de que não ocorre nenhuma quebra de segurança. Todas as comunicações e dados armazenados devem ser encriptados e não deve existir nenhum tipo de "código mestre" ou algo que possa ser facilmente roubado de modo a obter acesso ao interior da propriedade.

Apesar da importância de avaliação desta secção, a sensibilidade do tópico torna a obtenção de informações muito difícil e em alguns casos mesmo impossível. No entanto, existem outros casos que foi possível obter informações bastante interessantes.

A segurança digital da **August** é considerada igual à do mercado bancário online. No entanto, já foram executadas algumas auditorias de segurança que comprovaram que existem algumas falhas atualmente. De modo a comprovar estas falhas, foi descarregada a versão Android da aplicação e descompilado o código fonte de modo a conseguir analisar os factos. Existem alguns ficheiros de configurações armazenados no dispositivo que estão encriptados, no entanto, depois de verificar alguns ficheiros .java da aplicação, foi possível encontrar a chave de encriptação dos mesmos.

```
// Decompiled by Jad v1.5.8e. Copyright 2001 Pavel Kouznetsov.
// Jad home page: http://www.geocities.com/kpdus/jad.html
// Decompiler options: braces fieldsfirst space lnc

package com.august.util;

import android.content.SharedPreferences;
import android.content.res.AssetManager;
import com.august.app.App;
import com.august.app.DebugSettings;
import java.io.ByteArrayInputStream;
import java.io.ByteArrayOutputStream;
import java.io.UnsupportedEncodingException;
import java.util.Properties;
import java.util.UUID;

// Referenced classes of package com.august.util:
//            LogUtil, Data

public class Settings
{

    private static final String ENC_KEY = "August#@3417r";
    private static final LogUtil LOG = LogUtil.getLogger(com/august/util/Settings);
    public static final String SIZE_SUFFIX = "*size*";
    public static final String STR_ACCESS_TOKEN = "API_ACCESS_TOKEN";
    public static final String STR_DEBUG_SETTINGS = "DEBUG_SETTINGS";
    public static final String STR_INSTALL_TOKEN = "API_INSTALL_TOKEN";
    public static final String STR_PUSH_ALERTS = "PUSH_ALERTS";
    public static final String VERSION_SUFFIX = "_v1";
    static Settings _instance = null;
    DebugSettings _debugSettings;
    Properties _encryptedProps;
```

Figura 2.4.: Chave AES *hardcoded*

Durante estas auditorias foi também descoberto que o processo de encriptação envolvia o padrão de criptografia AES em modo ECB. O que estes ficheiros de configuração encriptados contêm são os números de telemóvel, emails, UUIDs das fechaduras, etc. Após a análise da fechadura, foi analisada a API. Embora a maioria dos *endpoints* não fosse muito revelador, existia um em particular que não verificava que o utilizador a executar a ação era um dono válido da fechadura, quebrando assim o quarto ponto (*Insecure Direct Object References*) do top 10 de falhas de segurança estabelecidos pela OWASP. A partir deste momento, qualquer atacante sabendo o UUID da fechadura, poderia efetuar um pedido à API para se adicionar a ele próprio como convidado e obter acesso indevido à casa. Numa outra análise ao produto foi também detetada uma grave falha de segurança. Quando o utilizador instalou a fechadura, esta não se encontrava calibrada com o buraco de entrada do fecho. Esta situação fez com que, ao emitir uma ordem de bloqueio para a fechadura, esta, e após cerca de 3 tentativas falhadas de trancar a porta, considerasse que a fechadura se encontrava trancada. Demonstrando essa mesma situação através da aplicação móvel. Apesar da dificuldade de conseguir equiparar todas as fechaduras universalmente disponíveis, esta demonstra-se uma falha enorme de software no que toca a validações de operações de bloqueio e desbloqueio da fechadura.

Em relação à segurança física da fechadura, não existe qualquer relatório sobre a sua es-

tabilidade e atual segurança. As únicas especificações disponíveis são o facto de esta fechadura não substituir a fechadura atual mas sim sobrepor-se a esta e, precisamente por esta especificação, não existe qualquer tipo de reconhecimento sobre o interior e o exterior da porta por parte da aplicação móvel.

Ao analisar o nível de segurança da fechadura **Danalock**, não foram encontradas quaisquer auditorias ou testes de penetração para testar a segurança da fechadura. No entanto, foi possível obter a informação de que esta, como muitas outras, utiliza um nível de segurança digital equiparável ao da segurança bancária.

Mais um vez, e de acordo com os seus pares, a **Goji** oferece um nível de segurança digital semelhante ao das instituições bancárias. Quanto à segurança física da fechadura, um especialista em fechaduras (Towne, 2014), afirma que a fechadura que é enviada pela Goji não é tão segura como afirmado no site da empresa e que existem opções mais seguras no mercado. A fechadura utilizada é uma KW1, pertencente à empresa Kwikset, que cujas chaves não ultrapassam os 5 pins. O que este especialista nota também, é que analisando as afirmações de que esta fechadura oferece um nível de segurança físico máximo e a fechadura de 5 pins que oferecem na realidade, podemos concluir que existe alguma hipérbole em relação à mesma.

Em relação à segurança da **Haven** à que realçar a sua segurança física em primeiro lugar. Com a sua distinta nova abordagem, esta fechadura cria imensas barreiras a qualquer intruso que deseje forçar a sua entrada. Estando instalada na base da porta, esta previne ou reduz drasticamente o número de arrombamentos dado que requer uma força muito maior e, dependendo do tipo porta, pode mesmo tornar-se impossível. O facto de que esta se encontra instalada unicamente do lado seguro da porta, faz com que não exista qualquer tipo de contacto com o exterior e reduz para 0% o nível de acesso que um intruso poderá ter sobre a fechadura do lado exterior. Apesar da sua forte e corajosa aposta na segurança física da porta e devido a toda a atenção estar precisamente concentrada neste aspeto, não foram encontradas quaisquer conclusões em relação à segurança digital da mesma. Apesar de ser a fechadura com melhor segurança física no mercado, caso não exista o mesmo nível de empenho e profissionalismo aplicado à vertente digital, esta fechadura pode mesmo perder todo o seu preciosismo.

A **Lockitron** é uma das empresas mais maduras no mercado e sabe como lidar com segurança. No site da empresa, numa página dedicada exclusivamente a segurança [8], estes afirmam aplicar fortes medidas de segurança contra intrusos. Afirmam que todas as suas aplicações públicas estão fortalecidas contra ataques XSS, MITM, injeções de código, ataques *replay* e que rapidamente solucionam qualquer vetor de ataque emergente. Todo o tráfico das plataformas web da Lockitron é acedido ou redirecionado através de HTTPS, além das informações mais sensíveis relativas ao produto e seus clientes serem fortemente encriptadas nos servidores que estão protegidos por *firewalls* e monitorizados constantemente. Estes disponibilizam ainda a sua chave PGP para quem quiser manter as suas comunicações com a empresa seguras. Em

[8] `https://lockitron.com/security`

relação à segurança física da fechadura em si, a mais recente versão, a Bolt, vem constituída de melhores materiais e num formato mais robusto mas não foram encontrados relatórios sobre a sua durabilidade e resistência.

No que toca à segurança da **Unikey**, esta pode ser vista de dois prismas: um é a fechadura em si, que é proveniente das fechaduras Kwikset e por outro, é a tecnologia Kevo da Unikey que reside no interior da fechadura. Tal como mencionado anteriormente, a *Underwriters Laboratories* realiza testes para verificar o quão resistente é uma fechadura e a Unikey ganha a categoria mais elevada. Resistente à maior parte dos tipos de técnicas que intrusos utilizam para entrar dentro de uma propriedade, esta fechadura ganha alta fama no mercado. Em relação à força da fechadura, a American National Standards Institute (ANSI) e Builders Hardware Manufacturers Association (BHMA) atribuem à fechadura Kwikset 925 existente na Unikey o Grau 2 (de três possíveis [9]), o que apesar de não ser o mais elevado grau, ainda pode aguentar com bastantes pancadas e exibições de força sem se partir. Apesar de todas estas qualificações, existem críticos que afirmam ter quebrado a fechadura em meros segundos, utilizando apenas uma chave de parafusos, um martelo e uma outra ferramenta comum a serralheiros. A segurança digital desta fechadura é considerada uma das melhores no mercado, utilizando metodologias e técnicas equiparadas à da segurança militar. Além disso, tem tecnologias proprietárias que permitem adicionar uma camada de segurança extra quando se trata de verificar de que lado está o utilizador para a abertura automática da porta. Apesar de tudo isto, não foi possível encontrar mais fundamentos em relação à segurança digital da mesma.

Sumário

Após uma análise geral sobre a segurança das fechaduras eletrónicas, foi possível verificar que o mercado existente atualmente não deve ser considerado 100% seguro. Dado ser um assunto sensível, existe muito pouca informação de interesse sobre o tópico mas nesta secção foi possível verificar que as fechaduras estão sujeitas a diversos tipos de falhas de segurança, como:

- **Roubo do telemóvel** - sem qualquer tipo de proteção a nível do dispositivo, qualquer ladrão que consiga obter acesso ao telemóvel poderá aceder ao interior da propriedade;
- **Roubo de credenciais** - dado que a maior parte destas fechaduras funciona através de um sistema de contas centralizado, qualquer pessoa que obtenha acesso às credenciais da vítima (por *shoulder surfing*[10], *social engineering*[11], ou outra qualquer técnica maliciosa) pode, ela própria, descarregar a aplicação e utilizar a fechadura como se fosse o dono

[9] `http://www.buildershardware.com/bhma-standards/grade-levels`
[10] Ato de espiar alguém enquanto a pessoa lida com materiais cuja informação é sensível. Ex.: multibanco, computadores ou outros dispositivos eletrónicos.
[11] Manipulação psicológica aplicada a determinadas pessoas para que estas realizem determinada ação ou divulguem determinada informação.

- *Ataques a redes sem fios* - dado que todas as fechaduras trabalham com tecnologias sem fios, todas elas estão sujeitas a qualquer tipo de ataque proveniente das mesmas.

Para concluir, podemos afirmar que todas estas soluções existentes trazem mais conveniência do que segurança. Apesar de toda a inovação e desenvolvimento existente em torno de qualquer uma das hipóteses, a segurança deveria manter-se em primeiro lugar no que toca a soluções tecnológicas e, principalmente, soluções tecnológicas do teor de segurança doméstica, como é o caso.

	August	**Danalock**	**Goji**	**Haven**	**Lockitron**	**UniKey**
Nível de segurança digital	Segurança bancária	Segurança bancária	Segurança bancária	Desconhecido	Segurança bancária	Segurança militar
Segurança física	Não especificado	Não especificado	Não especificado	Instalada unicamente do lado seguro da porta	Não especificado	À prova de *picklocking* e *bump-proof*
Subsituição de fechadura atual	✗	✗	✓	✓	✗	✓
Reconhecimento de exterior/interior	✗	✗	✗	✗	✗	✓

Tabela 2.5.: Sumário de: segurança

2.6. Bateria e falhas de energia

Como fator menos discutido mas provavelmente dos mais críticos no mercado das fechaduras eletrónicas, temos a energia. Afinal de contas, é que faz operar tanto a fechadura em si como o dispositivo que a controla. Partindo deste ponto, as empresas têm então que garantir que pelo menos os donos são capazes de entrar em casa em caso de falta de bateria no dispositivo e na fechadura em si.

Em relação à bateria, a **August** vem equipada com quatro pilhas AA o que permite que esta se mantenha sempre ligada, independentemente de qualquer falha de energia na casa. Tem uma autonomia estimada entre 6 e 12 meses. É possível consultar o nível de bateria na aplicação móvel e também são emitidos alertas para o utilizador quando esta se encontra num nível demasiado baixo. Para o caso de ser o telemóvel a ficar sem bateria e apesar de não ser bem visível, a **August** afirma que pode ostentar as tradicionais chaves como método de recurso à falta de energia. No caso da **Danalock**, esta vem equipada com uma bateria de iões de lítio. Esta pode parecer como uma solução preocupante dado que não existe opção de recurso de energia. No entanto, a *Poly-Control* assegura que esta é capaz de durar até dois anos. De qualquer forma, a aplicação móvel está preparada para mostrar o nível de bateria da fechadura e emitir alertas quando esta se encontra num nível crítico. Também esta fechadura oferece

recurso à utilização da tradicional chave em caso de falha completa por parte da mesma ou da aplicação. Muito semelhante a esta fechadura está a **Goji**, cuja fonte de energia também é uma bateria de iões de lítio e tem como opções de recurso às falhas de energia da fechadura as clássicas chaves. No entanto, e como mencionado na breve descrição inicial desta fechadura, ela apresenta uma opção de recuperação em caso de falha de energia do telemóvel bastante peculiar. Dado o seu apoio ao cliente constante, com um simples telefonema para este departamento eles conseguem abrir a porta à distância. São desconhecidos os passos de segurança que o pessoal que lida com este tipo de situações é obrigado a cumprir de forma a evitar técnicas como *social engineering* mas, de qualquer forma, esta pode apresentar-se como uma falha e preocupação grave para os donos deste tipo de fechaduras. Caso mais nenhum telefone esteja ao alcance num momento de falta de bateria do dispositivo que possui a chave, é sempre possível utilizar um dos *key fobs* mencionados anteriormente. De seguida, temos a solução mais afastada do tradicional conceito de fechadura eletrónica, a **Haven**. Possivelmente a melhor fechadura a nível de recuperações de energia, esta tem como fonte de energia principal uma bateria recarregável Lipo 5000MAH de 3.7V. Apesar de desconhecida a autonomia desta, a empresa afirma que a bateria poderá ser recarregada mais de 350 vezes. Em caso de falhas de energia por parte da fechadura, esta vem equipada com múltiplas soluções redundantes para certificar que é possível entrar a qualquer altura. Quando o nível de bateria atinge os 10%, notificações de alerta começarão a ser enviadas para o dono da fechadura. Assim que o nível começa a aproximar-se dos 5%, a fechadura entra num modo local que apenas permite ligações Bluetooth. Finalmente, mesmo que o dispositivo atinja os 0%, e assim que tal acontecer este entra num estado de hibernação de apenas permite ligações Bluetooth locais e de 15 em 15 minutos através de uma bateria redundante. Tal como noutros fatores apontados anteriormente, mais uma vez a **Lockitron** aproxima-se da sua concorrente **August**. Trabalha com quatro pilha AA que podem durar até seis meses. Como método de recuperação em caso de falha de energia do telemóvel, é possível utilizar chaves físicas graças à sua Key Match™ que permite manter as atuais chaves tradicionais. Esta fechadura possui ainda um modo de poupança de energia (*Power Save*) que permite reduzir o consumo desta. Esta configuração pode ser alterada a qualquer momento e funciona por reduzir o número de verificações realizadas através de Wi-Fi, passando estas para verificações diárias em vez múltiplas vezes ao dia. Finalmente, a **UniKey** optou por também fabricar a sua fechadura com quatro pilhas AA que deverão durar cerca de um ano. Quando a bateria atinge um nível crítico, a fechadura começa a emitir sinais sonoros e luminosos para alertar os utilizadores. Além disso, são enviadas notificações para o *smartphone*. Como mecanismo de recuperação em caso de falha de bateria do telemóvel, é possível utilizar tanto as *key fobs* como as tradicionais chaves mecânicas.

Sumário

A nível de bateria e falhas de energia, apesar de umas usarem pilhas e outras baterias

incorporadas, todas as fechaduras se aproximam de um padrão. Todas fornecem mecanismos de recuperação mas soluções como a **Haven** destacam-se positivamente. O seguinte quadro permite comparar mais facilmente este fator:

	August	Danalock	Goji	Haven	Lockitron	UniKey
Bateria	✓	✓	✓	✓	✓	✓
Recuperação de energia	✓	✓	✓	✓	✓	✓

Tabela 2.6.: Sumário de: bateria e falhas de energia

2.7. Instalação

A instalação dos equipamentos é levada a cabo pelos clientes, logo deve ser um processo simples e fácil. Deve, também, existir um grande suporte para a verificação da compatibilidade das fechaduras com as portas dos clientes, não só para a facilidade de escolha no momento da compra mas também para evitar situações de insegurança como descrito na secção de segurança da fechadura **August**.

A instalação da **August** passa pela substituição da parte de dentro da fechadura e não requer qualquer tipo de mudança no exterior desta. A embalagem vem com pequenos adaptadores que permitem o ajuste a grande parte das fechaduras mais modernas. É então na instalação que a **Danalock** brilha. Esta fechadura vem em três formatos: formato norte-americano, europeu e escandinavo. Este tipo de método de venda é bastante importante dado que todas as outras fechaduras nasceram nos EUA, o que restringe bastante a expansão das mesmas por falta de compatibilidades com as fechaduras do resto do mundo. Também esta fechadura passa pela substituição do *hardware* interior da mesma sem alterar de qualquer forma o exterior desta. A **Goji** passa exatamente pela mesma abordagem que estas duas fechaduras anteriores, substituição do interior da fechadura pelo equipamento fornecido e manter o exterior completamente intacto. De notar que, as fechaduras ao serem ativadas pela primeira vez devem estar na posição desbloqueada. Possivelmente pela sua abordagem mais única, a **Haven** poderia ser considerada como a mais complexa de instalar. No entanto, provou, mais uma vez, a sua distinção pela facilidade de montagem. Esta solução possui dois métodos de instalação:

- **Método 1**: utiliza uma fita adesiva especial (*3M™ VHB™ Tape*) desenhada para substituir pregos e parafusos. Trata-se de uma solução amovível e que não deixa qualquer marca ou resíduo no chão. Após a aplicação da fita, é só colocar a base **Haven** e pressionar;
- **Método 2**: utiliza uma solução mais permanente. Leva quatro pinos de metal para prender a fechadura à base da porta.

As características únicas desta solução removeram um conjunto de incertezas em relação à compatibilidade da atual fechadura. Independentemente da largura da porta, esta so-

lução funcionará na perfeição. A única preocupação neste caso, será mesmo a altura a que a fechadura se eleva. Caso a base da porta se encontre a uma altura superior à da **Haven** (aproximadamente 4cm) em relação ao chão, a empresa fornecerá prontamente tubos de subida sem qualquer custo adicional. Mais uma vez, a **Lockitron** aproxima-se da concorrência nos métodos de instalação sendo que também esta passa pela substituição da parte interior da fechadura. Finalmente, e já mencionado anteriormente, a **UniKey** decidiu tomar uma abordagem diferente. Esta fechadura assume a substituição de todas a fechadura atual, o que significa que é instalada tanto por dentro como por fora. Graças a este tipo de instalação, a empresa pode e assume a **UniKey** como uma fechadura extremamente segura, sendo mesmo imune a técnicas de abertura comuns como *picklocking* e *bump*.

Sumário

Após analisar todas as fechaduras, podemos concluir que praticamente todas elas assumem o mesmo tipo de instalação com a exceção da **Haven** e **UniKey**. No geral, foi possível comprovar que todas estas possuem uma instalação considerada fácil para o utilizador comum.

2.8. Design

O design é algo meramente indicativo, dado que a análise que se tenta estabelecer neste documento é de foro técnico. No entanto, cada design deve ser pensado ao pormenor dado que é um mercado praticamente intocado à décadas. É algo que irá estar presente permanentemente nas casas dos clientes e num dos casos, do lado exterior da porta. De seguida, demonstram-se as opções tomadas pelos concorrentes.

Este tem sido um dos pontos mais aclamados nas diversas revisões *online* que a **August** amealhou até ao momento. Considerando que um dos fundadores é Ives Behar [12] e líder da equipa de design do produto, esta vem com acabamentos futuristas em formato de cilindro que, pode ou não, ser considerado um pouco volumoso para a entrada de nossa casa. Esta oferece ainda quatro acabamentos diferentes: prateado, cinzento escuro, champanhe e vermelho.

[12] Premiado designer suíço, e um dos mais aclamados eco-designers do mundo

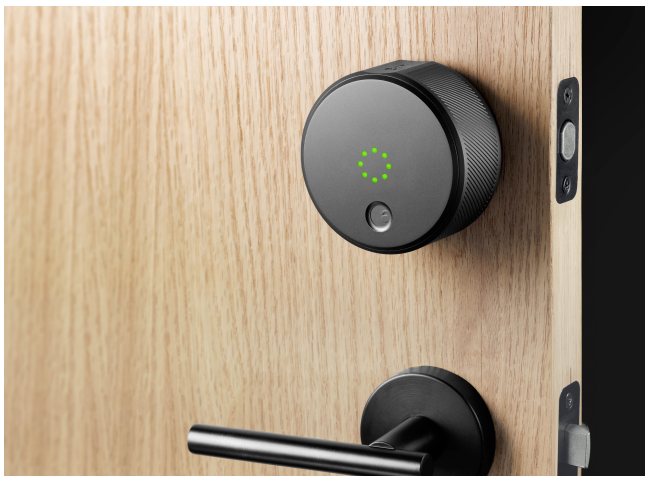

Figura 2.5.: August *smartlock* (August)

A **Danalock** tem um aspeto menos volumoso que a **August** mas um visual menos polido e não tão acabado. Possui um botão central e luzes led de indicação. Esta fechadura combina a elegância e o minialismo do design Dinamarquês com uma luneta de alumínio que funciona tão bem como é discreta.

Figura 2.6.: Danalock (Danalock)

Com um aspeto não tão tradicional está a **Goji**. Que apresenta um design mais futurista tanto no interior como no exterior. Esta fechadura é descrita como tendo um design lustroso e sofisticado que encaixará bem em qualquer lar. No lado exterior possui ainda um ecrã led que permite mostrar mensagens tanto aos donos da fechadura como a pessoas que toquem à campainha.

Figura 2.7.: Goji (Goji)

Como já mencionado inúmeras vezes antes, a **Haven** é sem qualquer dúvida a mais inovadora no que toca ao design. Com uma base preto fusco com dimensões de 7.62 x 76 x 2 cm, esta solução reconsidera todo o aspeto interior e exterior de qualquer porta existente.

Figura 2.8.: Haven (Haven)

De seguida, temos a **Lockitron** que possui um design muito semelhante aos dispositivos Apple - os *iPods*. Esta fechadura já sofreu algumas alterações em relação ao design inicial e de momento possui um aspeto mais elegante. Esta está disponível para venda em dois acabamentos: preto e branco e bronze polido.

Figura 2.9.: Lockitron (Lockitron)

Mais modesta e discreta está a **UniKey**, cujo exterior é praticamente igual ao de uma fechadura tradicional o que trás um aspeto mais convencional. No entanto, o interior da fechadura é um pouco robusto e pode ser considerado abusivo. Quanto aos acabamentos, esta fechadura oferece latão polido, cetim níquel e bronze veneziano.

Figura 2.10.: UniKey interior (Unikey)

Figura 2.11.: UniKey exterior (Unikey)

Sumário

No geral, todas as fechaduras possuem um design apelativo e prático. Algumas um pouco mais robustas que outras mas nenhuma que possua um design que impeça de alguma maneira o bom manuseamento da fechadura e utilização de todas as funcionalidades.

2.9. Ciclo de vida dos produtos

A **August** foi fundada por Jason Johnson e Yves Behar em Maio de 2013 e desde então que tem sido muito bem sucedida. Quando a *startup* se lançou no mercado não tinha a capacidade que achava ter para suportar todos pedidos que chegaram até eles. Esta empresa conseguiu-se erguer-se graças a alguns *angel investors* que não tiveram dúvidas em relação ao valor desta fechadura, amealhando cerca de $15 milhões de dólares. Estes investidores passavam por empresas como Maveron, Cowboy Ventures, Industry Ventures, Rho Ventures e SoftTech VC. Em Janeiro do presente ano, a empresa apresentou o seu dispositivo de expansão de acesso - a *Connect*. Passados quase dois anos do seu lançamento, em Março de 2015, esta empresa conseguiu obter mais $38 milhões de dólares de uma série de investidores como Qualcomm Ventures e Comcast Ventures, lideradas pela Bessemer Venture Partners. Durante todo o processo não foi divulgada a quantia pela qual a empresa foi avaliada. Para o futuro, Johnson acha determinante a empresa manter-se focada num objetivo - "tal como todas as empresas de desenvolvimento de *hardware*" - e diz também que o dinheiro será utilizado para desenvolvimento de mais produtos que encaixarão diretamente na **August**.

A única empresa que não nasceu no meio do mundo tecnológico americano, a **Danalock**, certamente teve o seu momento de publicidade nas revistas tecnológicas quando nasceu em Outubro de 2014 pela empresa familiar Dinamarquesa Poly-Control.

A **Goji** nasceu de uma campanha de *crowdfunding* na plataforma Indiegogo em Agosto de 2013, criada pelo espanhol Gabriel Bestard-Ribas. A sua campanha tinha como objetivo os $120 mil dólares e em apenas dois meses conseguiu um apoio de 261%, amealhando assim $313.457 dólares por parte de 1253 pessoas. Claramente este objetivo foi muito bem sucedido e muitas pessoas acreditaram no projeto. Esta empresa nasce no seio do mundo tecnológico de São Francisco, Estados Unidos.

Tal como alguma da concorrência, também a **Haven** optou pelo *crowdfunding* para tentar emergir neste mercado competitivo mas desta vez na plataforma Kickstarter. Originaria de Nashville, Tennessee (EUA) esta empresa iniciou a campanha em Setembro de 2014 com um objetivo de $150 mil dólares. Pouco mais de 1 mês depois, a campanha foi encerrada não tendo esta atingido o seu objetivo. Ficou-se pelos $116.298 dólares de 469 apoiantes. A partir desse momento, a Haven está até à data a aceitar pré encomendas do produto e espera conseguir iniciar o processo de envio no Outono de 2015.

Quanto ao caso da **Lockitron**, esta tem uma história bastante interessante. Após dias de preparação e de estudo sobre outras campanhas de *crowdfunding*, os fundadores, Cameron Robertson e Paul Gerhardt, decidiram lançar a sua própria campanha na plataforma Kickstarter a 19 Setembro de 2012. Ora, para enorme espanto destes, no dia 20 do mesmo mês a empresa de *crowdfunding* lançou um artigo no seu blog (Chen/Strickler/Adler, 2012) declarando que eles "não são uma loja". Imediatamente no dia a seguir, dia 21 de Setembro de 2012 a campanha foi rejeitada da plataforma. Após uma troca de e-mails com um dos co fundadores da Kicks-

tarter, um firme "Não" foi a única resposta que obtiveram. A razão aparente pela qual estes empreendedores foram rejeitados, residia no facto do projeto em causa se enquadrar na categoria de "melhoramentos para a casa" e a Kickstarter não era o local adequado para eles. Sem outras alternativas, os fundadores começaram a trabalhar em alternativas. Decidiram utilizar o serviço de pagamentos da Amazon e receber pré encomendas diretamente do website deles. Os clientes eram informados constantemente sobre o estado do desenvolvimento do produto e o dinheiro só era cobrado nos cartões de crédito assim que a unidade estivesse pronta a ser enviada. Tudo isto foi concretizado em pouco mais de uma semana após a rejeição da Kickstarter. As 24 horas que seguiram ao lançamento desta campanha própria foram nada mais do que chocantes para os dois promotores. Milhares de pessoas viram a dedicação destes em relação ao produto que estavam a tentar lançar para o mercado e decidiram apostar, juntando assim $150 mil dólares. No entanto, a dedicação deste jovens ainda não tinha acabado. Em Janeiro de 2015, decidiram mudar completamente o produto que estavam a produzir e abandonar completamente o design atual. Esta foi uma mudança muito arriscada mas bem sucedida, sendo que todos os apoiantes da campanha que ainda não tinham recebido a sua fechadura até à data, iriam receber a nova versão sem qualquer custo adicional. De momento, a Lockitron consegue assumir-se no mercado como um grande concorrente e ao preço mais competitivo.

A **UniKey** pode muito bem parecer como a melhor concorrente aqui apresentada, provavelmente porque foi uma das primeiras a surgir no mercado, no ano de 2011. O seu inventor, Phil Dumas, cujo passado envolve trabalho em segurança biométrica na Sequiam Corp, decidiu candidatar-se ao programa americano televisivo do canal ABC "Shark Tank". Esta pôde-se tornar numas das histórias de sucesso do programa ao amealhar $500 mil dólares por 40% da empresa entre dois investidores. Na verdade, o promotor precisava de um pouco mais e depois do programa ir para o ar em Abril de 2012 conseguiu mais $1.1 milhões de dólares, totalizando assim o investimento na empresa em $1.6 milhões de dólares. Em Janeiro de 2013, a empresa juntou-se à Kwikset [13] e à sua fechadura Bluetooth Kevo. Esta junção permitiu que a **UniKey** trouxe-se a sua tecnologia para os produtos já existentes da Kwikset. Neste momento a empresa foca-se em expandir para o mercado da hospitalidade oferecendo soluções para unidades hoteleiras como características completamente inovadoras. A **UniKey** fará com que as experiências em hotéis e unidades semelhantes sejam muito mais agradáveis ao fornecer alertas para os clientes através da aplicação móvel para quando o quarto estiver pronto e, claro, o acesso a este através de uma aplicação móvel.

2.10. Sumário

Neste capítulo foi possível, em primeiro lugar, obter uma perspetiva geral sobre as principais fechaduras do mercado. Além de identificar os seus pontos mais fortes e pontos mais

[13] Fabricante de fechadura eletrónicas e líder de mercado na segurança caseira.

fracos, foi possível perceber como cada uma destas fechaduras nasceu e qual o seu potencial de crescimento. Dados os oito aspetos em que foi realizada esta análise, foi possível responder às primeiras subquestões deste documento:

SQ-1: "Quais os requisitos funcionais de uma fechadura eletrónica?"

- Bloqueio/desbloqueio da fechadura através de um dispositivo móvel
- Registo de bloqueios/desbloqueios
- Transmissão de chaves eletrónicas

SQ-2: "Quais os requisitos não funcionais de uma fechadura eletrónica?"

- Segurança
- Baixos consumos de bateria por parte da aplicação
- Rápido processamento no bloqueio/desbloqueio da fechadura

Como conclusão desta análise às diversas fechaduras eletrónicas, foi possível notar que muitas destas confiavam um múltiplas tecnologias como canal de comunicação entre o dispositivo e a fechadura. No entanto, foi também possível estabelecer que na maior parte dos casos a utilização de mais do que uma tecnologia para o canal de comunicação advinha de funcionalidades muito específicas ou com casos de uso específicos e não da necessidade para o seu funcionamento básico. O que nos remete à subquestão 2.1:

SQ-2.1: "Quantos canais de comunicação devem estar disponíveis?"

Apenas um. Esta situação é justificada com a natureza do projeto e no âmbito em que este se enquadra. Numa primeira fase, este projeto deverá ter as funcionalidades básicas com o mínimo indispensável, ou seja, sem *hardware* desnecessário para o seu funcionamento. Além disso, reduzindo o número de canais de comunicação reduz diretamente o número de ameaças e possíveis falhas de segurança no sistema. Dada esta resposta, fica em aberto a resposta de seguimento à pergunta em questão (SQ-2.1.1) que será respondida no seguinte capítulo ao abordar as tecnologias utilizadas neste projeto.

Capítulo

3 Tecnologias estudadas

Este capítulo visa estudar e avaliar as possíveis características da solução apresentada nesta tese. Será, portanto, efetuada uma análise sobre qual/quais as plataformas em que deve ser desenvolvida a plataforma móvel, que tipo de *hardware* utilizar para a construção da fechadura e por fim, qual o meio(s) de comunicação entre ambos. Serão analisadas várias possibilidades e efetuadas as comparações entre todas elas de modo a determinar quais as mais adequadas para pertencer a este projeto. Para o projeto em questão, é suficientemente importante o estudo e escolha do canal de comunicação entre o dispositivo da fechadura e o dispositivo móvel, pois será este que estará encarregue de enviar todas as informações e instruções para a fechadura. Além disso, é importante conhecer o meio pela qual vamos estar a transmitir informações tendo em conta os avanços tecnológicos da atualidade e as conhecidas quebras de segurança em muitos deles.

3.1. *Hardware*

Esta secção pretende dar foco ao tipo de *hardware* utilizado para o projeto. O que era pretendido era essencialmente um micro computador capaz de armazenar informações relativas à fechadura e seus visitantes, bem como efetuar qualquer processamento a nível criptográfico que fosse necessário para garantir a segurança das chaves eletrónicas e dos processos de bloqueio e desbloqueio da fechadura. Para tal, foram analisadas duas alternativas: o **Raspberry Pi** e o **BeagleBone Black**.

3.1.1. Raspberry Pi

O *Raspberry Pi* é um pequeno (do tamanho de um cartão de crédito) computador de baixo custo desenvolvido pela fundação Raspberry Pi sediada no Reino Unido. Este computador rapidamente se tornou numa série de pequenos computadores, todos com o mesmo tamanho,

mas ostentando especificações diferentes. Foi criado com o intuito de oferecer a qualquer pessoa, mas principalmente a crianças, a capacidade de aprender, desde muito cedo, a programar e desenvolver capacidades com linguagens como *Scratch* e *Python*. Este computador tem a capacidade de se conectar a um monitor externo, teclado e rato e ser utilizado como outro qualquer computador *desktop*. O Raspberry Pi original é baseado no chip Broadcom BCM2835 que inclui um processador ARM1176JZF-S 700MHz e vinha originalmente com 256MB de memória RAM. Nos modelos posteriores (B e B+) esta memória sofreu um aumento para 512MB. A fundação oferece distribuições Debian e Arch Linux para *download* gratuito. Existem ferramentas disponíveis para programação em *Python* como linguagem de programação principal mas também existe suporte para BBC Basic, C, C++, Java, Perl e Ruby.

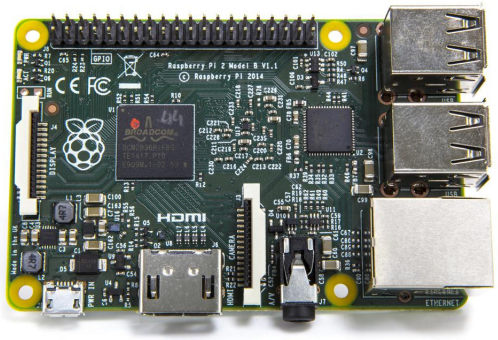

Figura 3.1.: Raspberry Pi (Hut)

Especificações

Estas especificações são referentes ao mais recente modelo, lançado em Fevereiro de 2015, o Raspberry Pi 2 modelo B:

- SoC [1] Broadcom BCM2836;
- CPU de 900MHz quad-core ARM® Cortex-A7
- Placa gráfica Broadcom VideoCore IV @ 250 MHz
- Memória de 1GB (partilhada com a placa gráfica)
- 4 portas USB 2.0
- Input de vídeo conector de interface da câmara de 15 pinos MIPI
- Potência de 800mA (4.0W)

[1] System on a chip

- Fonte de alimentação através de Micro USB 5V
- Peso de 45g

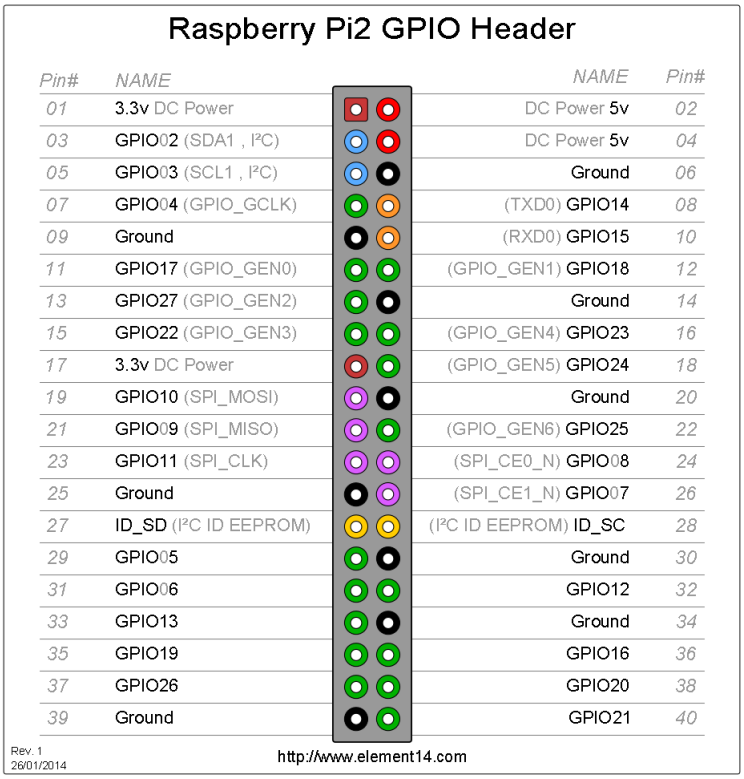

Figura 3.2.: Raspberry Pi 2 GPIO header (Element14)

Acessórios

A fundação Raspberry Pi disponibiliza diversos acessórios para estender algumas das capacidades originais do computador. Estes acessórios, assim como o próprio Raspberry, não só estão disponíveis para compra no site da fundação (https://www.raspberrypi.org) mas também em parceiros como Allien [2], Element14 [3] e RS [4].

[2] http://www.alliedelec.com
[3] http://www.element14.com/community/community/raspberry-pi
[4] http://www.element14.com/community/community/raspberry-pi

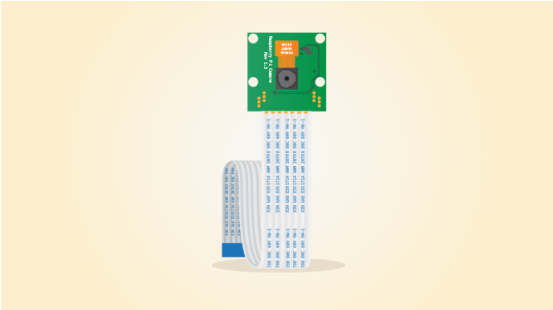

Figura 3.3.: Câmara para Raspberry Pi (Pi)

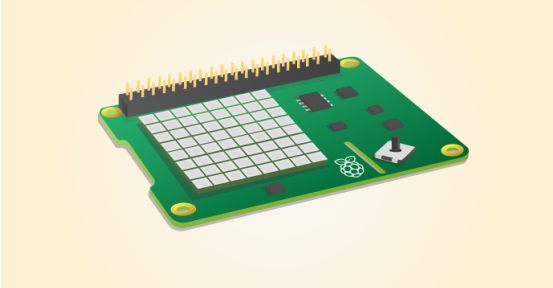

Figura 3.4.: Sense hat para Raspberry Pi (Pi)

Este último acessório é particularmente interessante dado que foi desenvolvido no âmbito do projeto Astro Pi [5]. Este projeto teve início graças à fusão entre o astronauta britânico Tim Peake e a Raspberry Pi com diversas organizações espaciais do Reino Unido para oferecer a oportunidade a estudantes de enviar dois computadores Raspberry Pi e verem as suas aplicações e o seu código em execução no espaço, mais concretamente na estação espacial internacional.

Esta pequena tem uma grelha de LEDs de 8x8, cinco botões, um *joystick* e atua também como sensor com as seguintes possibilidades:

- Giroscópio
- Acelerómetro
- Magnetómetro
- Temperatura
- Pressão barométrica
- Humidade

[5] `https://www.raspberrypi.org/blog/astro-pi/`

Desenvolvimento

Sendo que o objetivo principal do Raspberry Pi é assemelhar-se a um computador normal, este vem equipado com uma interface gráfica e *software* para o desenvolvimento de aplicações nas linguagens mencionadas.

Figura 3.5.: Ambiente gráfico Raspberry Pi (P1)

Um dos ambientes de desenvolvimento oferecidos para *Python* é o IDLE. Este oferece um REPL (*Read-Evaluate-Print-Loop*), ou seja, permite que sejam inseridos comandos em *Python* de forma sequencial e obter *output* dos mesmos. Tal como mostra a figura, estão disponíveis duas versões de *Python*, 2 e 3.

Listing 3.1: Exemplo de REPL em *Python*

```
>>> 1 + 2
3
>>> name = "Joao"
>>> "Hello␣" + name
'Hello␣Joao'
```

3.1.2. BeagleBone Black

O *BeagleBone Black* é uma evolução da *BeagleBone* que, por sua vez é uma evolução do computador de baixo consumo, baixo custo e *open source Beagleboard* desenvolvida pela Texas Instruments. Esta placa foi concebida por uma pequena equipa de engenheiros com o intuito de demonstrar o chip da fabricante (OMAP3530) e como instrumento educacional para demonstração das capacidades do *software* e *hardware open source*. Esta é vendida com uma licença *Creative Commons*.

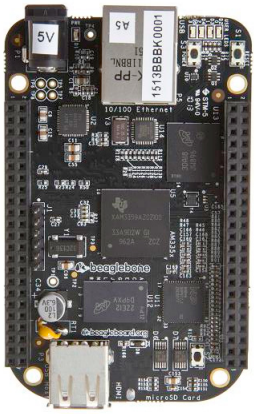

Figura 3.6.: BeagleBone Black (Beagleboard)

Especificações

Este pequeno computador com dimensões de 8.6cmx5.3cm e 39g de peso ostenta os seguintes componentes físicos:

- Processador AM3358/9 1GHz ARM® Cortex-A8;
- Armazenamento de 4Gb 8-bit eMMC on-board;
- Placa gráfica PowerVR SGX530 (200MHz);
- Acelerador de gráficos 3D;
- Memória RAM DDR3 de 512Mb;
- 2 Microcontroladores de 32-bits PRU;
- 2 Porta USB (1x Standard A, 1x mini B);
- 1 Porta Ethernet;
- 1 Porta HDMI;
- Leitor de cartões microSD;
- 2 x 46 pins.

Esta placa vem com o sistema operativo Debian Gnu/Linux™ mas é compatível com outros como Android, Ubuntu e Fedora. Esta vem ainda com a plataforma Node.js e a biblioteca BoneScript (biblioteca desenvolvida para a família de computadores Beagle) instaladas.
Este foi um grande avanço por parte da empresa fabricante dado que, em relação às versões

anteriores, aumentou o relógio do processador de 720MHz para 1GHz, aumentou a RAM de 256Mb para 512Mb, acrescentou a entrada HDMI e a memória flash eMMC de 2Gb. Tudo isto conseguindo reduzir o preço deste pequeno computador.

Como método para permitir a extensão das funcionalidades de I/O existem 92 pins, em que cada um deles pode assumir 8 modos diferentes, incluindo GPIO.

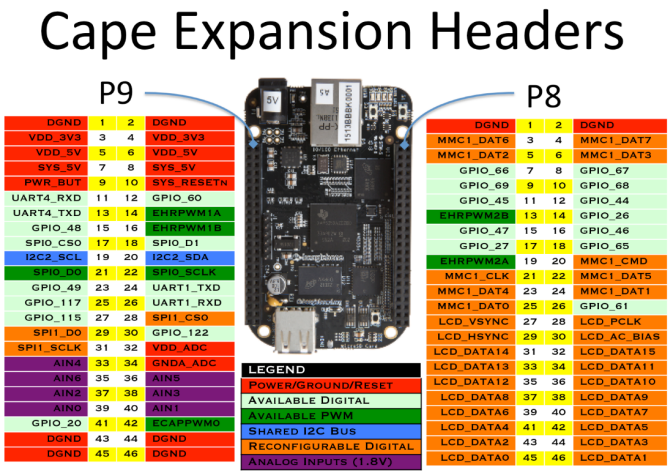

Figura 3.7.: Pins de extensão da BeagleBone Black (Beagleboard)

Capas

As capas para os produtos *BeagleBone* são extensões às características atuais desenvolvidas pela comunidade para a comunidade. Podem ser fabricadas independentemente e depois registadas para que outros utilizadores interessados saibam como as adquirir. Neste momento existem mais de 80 capas para ecrãs (LCD, VGA, HDMI, etc), controlo motor, fontes de energia (baterias, solar, etc), entre outras funcionalidades.

Todas estas capas são desenhadas e desenvolvidas com o intuito de Plug & Go, ou seja, devem ser de montagem rápida e fácil de modo a serem facilmente integradas com a placa de qualquer utilizador.

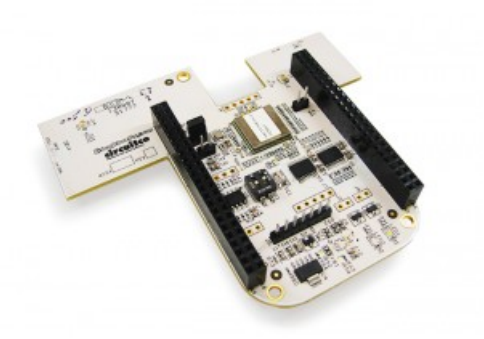

Figura 3.8.: Chip antena (BoardZoo)

Figura 3.9.: Display LCD de 7 polegadas (Wiki)

Desenvolvimento

O BeagleBone Black é vendido com uma distribuição Angstrom com C++, Perl e Python, porém e graças à sua comunidade e o facto de aceitar cartões SD torna a sua personalização muito simples e intuitiva. Podendo mesmo ser iniciado a partir do cartão SD para execução de um outro sistema operativo.

BoneScript

BoneScript é uma biblioteca escrita em Javascript sobre a plataforma Node.js que permite interagir com as funcionalidades físicas mais básicas de cada placa. Possui funções muito semelhantes às do Arduino mas foi otimizada para a família de produtos Beagle. Estas funções permitem aos programadores interagir diretamente com as capacidades físicas da placa. Ao

contrário da programação em microcontroladores em C, o Javascript e o seu interpretador Node.js realizam todas as tarefas de uma forma assíncrona e utilizando *callbacks*. Todo este é o conceito do Node que utiliza a metodologia de event-driven, ou seja, é orientado por eventos e o seu código está em contínua execução em loop até que seja interrompido por algum processo de I/O. No entanto, os desenvolvedores do Node.js, decidiram retirar esta limitação ao fazerem com que a plataforma não bloqueasse na eventualidade de processos I/O. Isto é conseguido através da presunção de que todas as funções retornam imediatamente uma resposta, ou seja, interpretador passa muito rapidamente para a rotina seguinte mas quando a sua verdadeira resposta está disponível esta pode ser acedida através de uma função denominada *callback*. O modelo utilizado pela plataforma foi concebido para aplicações em tempo real, de alta intensidade, leves e eficientes.

Listing 3.2: Exemplo de utilização de LEDs em *BoneScript*

```
var b = require('bonescript');

b.pinMode('USR0', b.OUTPUT);
b.pinMode('USR1', b.OUTPUT);
b.pinMode('USR2', b.OUTPUT);
b.pinMode('USR3', b.OUTPUT);

b.digitalWrite('USR0', b.HIGH);
b.digitalWrite('USR1', b.HIGH);
b.digitalWrite('USR2', b.HIGH);
b.digitalWrite('USR3', b.HIGH);

// Restaura as luzes posicionando os 4 USRs com b.LOW
setTimeout(restore, 2000);
```

Este pequeno excerto de código faz com que todas as LEDs incluídas na placa BeagleBone Black se acendam durante dois segundos. Na primeira linha de código, é possível notar que existe uma variável a ser declarada com a biblioteca em causa. De seguida, é declarado o modo de acesso às quatro luzes USRs como *OUTPUT* e posteriormente são posicionadas em *HIGH* (= estado aceso).

Cloud9

Visto tratar-se de simples desenvolvimento de *scripts* utilizando a linguagem Javascript, não é requerido qualquer tipo de ambiente de desenvolvimento específico. Nem mesmo a instalação do Node.js. No entanto, e para conseguir executar o interpretador Node, deve ser utilizada a

IDE baseada em navegador Cloud9.

Esta poderosa IDE funciona com uma enorme variedade de ambientes (incluído Rails, PHP, Node.js, C++, entre outros) e oferece toda a liberdade ao utilizador que este necessita para rapidamente iniciar um novo projeto com todas as suas configurações. Como ferramenta integrada de desenvolvimento, é possível a programação concorrente entre vários utilizadores mas sempre com o controlo sobre o que é partilhado dentro do projeto. Oferece ainda a incrível capacidade de voltar atrás no tempo com repetições de todo o código editado num determinado intervalo de tempo. Com consola integrada, ferramentas próprias de cada linguagem e um sólido debugger, esta torna-se uma excelente opção de desenvolvimento para quem estiver preparado a utilizar a próxima geração de IDEs.

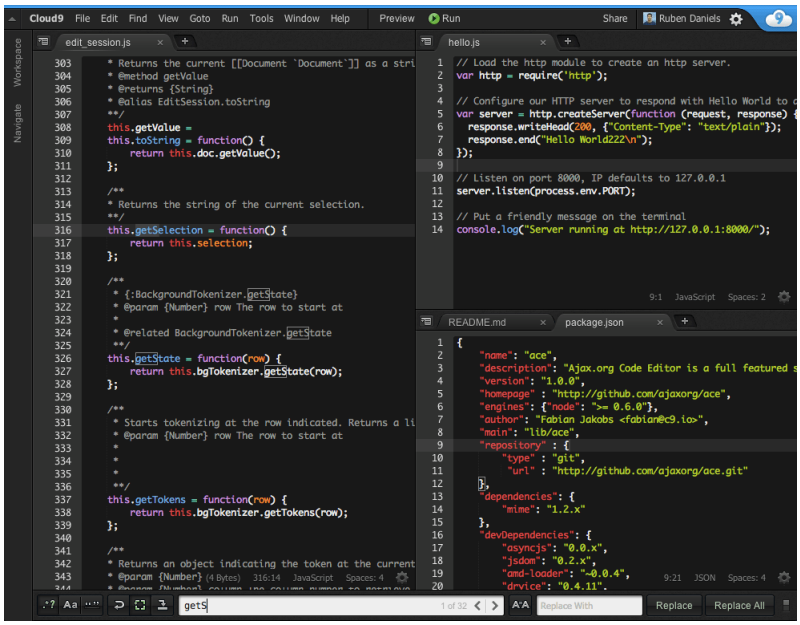

Figura 3.10.: IDE Cloud9 (Google)

Todos os ficheiros gerados podem ser colocados em /var/lib/cloud9/autorun pois existe um daemon de BoneScript (bonescript-autorun.service) que permite analisar todo o conteúdo da pasta e executar os seus ficheiros no arranque do computador.

Para aceder à consola do computador remotamente, existem duas possibilidades: ligação por USB ao computador ou através do cabo de corrente elétrica e de um cabo de rede. Assim que o dispositivo estiver conectado e ligado, é possível aceder através de um cliente SSH (ex.: Putty) com o IP estático do aparelho 192.168.7.2. No caso do acesso à IDE Cloud9, o acesso é efetuado através do mesmo endereço mas dirigido à porta 3000.

3.1.3. Conclusão

O BeagleBone original começou com um processador de um telemóvel e o Raspberry Pi com um chip multimédia. Mesmo com a evolução do Raspberry Pi neste último modelo, o Pi 2 ainda parece orientar muito o seu desenvolvimento para ambientes multimédia e para a utilização de ambientes gráficos. O BeagleBone e o BeagleBone Black (os Beagle), no entanto, começaram com um chip de controlo e de comunicações, o TI Sitara AM335x. Estes pontos de começo e as respetivas evoluções de cada um dos computadores, levaram a que estes dois sejam utilizados em ambientes com propósitos distintos. Em que, os Beagle, são mais utilizados para projetos de pequenos equipamentos interligados e os Raspberry em ambientes gráficos e multimédia.

Os Beagle possuem melhores capacidades de I/O com um ADC [6] de 7 canais a 200kHz e 12-bit, 8 PWMs [7], 4 UARTs [8], *hardware* codificador de quadratura e muito mais. Estes também têm um melhor controlo em tempo real com duas unidades de programação em tempo real (PRUs) RISC [9] de 32-bit e 200MHz. Além disso, as suas extensivas capacidades de I/O já permitiram a criação de mais de 100 capas para adicionar as mais diversas funcionalidades a cada Beagle. Por fim, de frisar que este *hardware* é completamente open-source o que vai de encontro com os objetivos desta tese.

Dadas estas conclusões, optou-se, portanto, pela utilização de um BeagleBone, mais concretamente, o BeagleBoneBlack para o *hardware* a ser utilização na construção da fechadura eletrónica.

3.2. Canal de comunicação

Na secção que se segue é apresentado o estudo feito sobre o canal de comunicação. Este é um aspecto bastante importante dado que os requisitos não funcionais definidos para a solução dependem gravemente dele. Deve ser um canal compatível tanto com os dispositivos móveis que controlam a fechadura como com a fechadura em si (i.e. o *hardware* definido anteriormente), deve ser seguro e bastante rápido para efetuar comunicações. Tal como foi apresentado no capítulo anterior, algumas fechaduras sofriam de atrasos na resposta ao mecanismo de bloqueio/desbloqueio. Este facto tanto pode advir do canal de comunicação como do processo criptográfico por trás desta ação. Para o caso em estudo, serão analisadas três hipóteses para transmissão de dados entre os dispositivos: **Wi-Fi**, **NFC** e **Bluetooth**.

[6] Analog-to-digital converter
[7] Pulse-width modulation
[8] Universal Asynchronous Receiver/Transmitter
[9] Um computador baseado num processador ou processador desenhado para realizar um determinado número de operações extremamente rápido

3.2.1. Wi-Fi

O Wi-Fi (ou WiFi) é uma tecnologia de redes locais sem fios que permite dispositivos eletrónicos ligarem-se entre si, geralmente a operar sobre a banda 2.4GHz UHF (*Ultra high frequency*) e 5GHz SHF (*Super high frequency*). As primeiras redes começaram a surgir como ligação das ilhas Havaianas em 1971. Estas utilizavam pacotes UHF através do sistema ALOHAnet desenvolvido pela universidade do Havai. Posteriormente começaram a ser desenvolvidos os primeiros protocolos para este tipo de comunicações mas não foi antes de 1999 que se formou a *Wi-Fi Alliance*. Uma associação sem fins lucrativos que reúne um vasto leque de empresas tecnológicas com o objetivo de oferecer a melhor experiência possível aos utilizadores da tecnologia de redes sem fios. Além disso, esta associação também promove a inovação e melhoramento deste tipo de tecnologias, assim como liderar, desenvolver e adotar padrões aceites pela indústria. Por fim, esta associação é responsável pela marca Wi-Fi^{TM} entre muitas outras. Nos dias de hoje, praticamente todos os dispositivos eletrónicos são capazes de possuir uma ligação Wi-Fi, desde televisões e automóveis às impressoras e frigoríficos e claro, fechaduras eletrónicas.

Características gerais

Rádio frequência

Segundo as normas 802.11b e 802.11g, os dispositivos que comunicam através de Wi-Fi operam sobre a banda 2.4GHz ISM (*Industrial, Scientific and medical*). Além disso, existem ainda a distribuição das comunicações pelos canais disponíveis que varia de acordo com o país. No Japão existem 14 canais disponíveis, enquanto que na Austrália e Europa estão disponíveis apenas 13 e por fim nos Estados Unidos e resto do mundo, apenas 11 canais podem ser utilizados para as comunicações. O sinal Wi-Fi ocupa 5 canais na banda 2.4GHz. Quaisquer dois canais que se encontrem separados por cinco canais (ex.: 2 e 7) não se sobrepõem. Por fim, na norma 802.11a, existe ainda a utilização da banda 5GHz o que, para a maioria do mundo, oferece 23 canais não sobrepostos.

Endereçamento

De modo a conseguir trocar pacotes de dados entre dispositivos através de Wi-Fi, e quase implicitamente, através da Internet, o *Internet protocol* (IP) é utilizado. Este protocolo serve como o protocolo principal de comunicações de todo um conjunto de protocolos necessários para interagir com estas tecnologias. Este protocolo tem como principal objetivos entregar pacotes de dados de uma origem a um destino. A primeira grande versão deste protocolo, e a dominante na atualidade, é a versão 4 conhecida como IPv4.

Esta versão utiliza endereços de 32 bits, o que limita o número total de endereços a 4 294 967 296(2^{32}) e são representados por quatro octetos. Dos endereços disponíveis, existem três classes de endereços que são reservados para utilização em redes privadas e são ignorados por *routers* públicos.

Classe	Intervalo de endereços	Endereços disponíveis
Classe A	10.0.0.0 – 10.255.255.255	16 777 216
Classe B	172.16.0.0 – 172.31.255.255	1 048 576
Classe C	192.168.0.0 – 192.168.255.255	65 536

Tabela 3.1.: Classes de endereços privados IPv4

A limitação de endereços apresentada pela versão 4, levou ao desenvolvimento da mais recente versão, o IPv6. A motivação para o desenvolvimento desta versão surge da "necessidade", já apresentada no primeiro capítulo desta tese, de interligar todos os objetos e seres vivos do mundo numa única rede sem fios, a Internet. A versão 6 do *Internet protocol* apresenta vantagens significativas em relação ao seu sucessor. O endereçamento possui 128 bits com a possibilidade de se expandir. Existem três tipos de endereços IPv6:

- Endereços *unicast* - este tipo de endereços funciona como um identificador para uma única interface que pode pertencer a vários nós da rede;
- Endereços *multicast* - este tipo de endereços atua como identificador de um grupo de interfaces que pode pertencer a diversos nós. Um pacote de dados dirigido a esse endereço, é entregue às múltiplas interfaces a ele associadas;
- Endereços *anycast* - este tipo de endereços funciona como os *multicast*, no entanto, um pacote de dados enviado para um endereço deste tipo é entregue a qualquer uma das interfaces a ele associadas.

Os endereços IPv6 são representados por oito grupos de quartetos hexadecimais separados por dois pontos (:), ex.: 2001:cdba:0000:0000:0000:0000:3257:9652. Uma característica deste tipo de endereços é que qualquer grupo de quatro zeros pode ser reduzido a um único zero ou mesmo omitido do endereço, sendo que continua a atuar como o endereço original. Logo, todos os endereços seguintes são válidos:

- 2001:cdba:0000:0000:0000:0000:3257:9652
- 2001:cdba:0:0:0:0:3257:9652
- 2001:cdba::3257:9652

Segurança

O grande problema de redes sem fios é o seu simplificado acesso às mesmas comparado com as tradicionais redes com fios, como a *Ethernet*. Em redes com fios, um intruso necessita de obter acesso físico às instalações que pretende atacar ou penetrar uma *firewall* externa. No caso das redes sem fios, o intruso basta estar ao alcance da rede Wi-Fi.

Riscos de segurança de dados

O mais comum padrão de encriptação de redes sem fios, *Wired Equivalent Privacy* (WEP), mostrou-se facilmente contornado e, por isso, um grave risco de segurança para quem dele depende. Para isso, surgiu a encriptação *Wi-Fi Protected Access* (WPA e WPA2) que começou a estar disponíveis em meados de 2003 e revelou resolver problema em causa, desde que utilizado com uma forte frase-chave. Como não é só a segurança que evolui mas também os métodos de a quebrar, foi sugerida uma abordagem diferente denominada WPA-OTP ou WPA3. Essencialmente, esta modificação armazena um *one-time pad* [10] em todos os dispositivos conectados e é atualizada frequentemente utilizando uma forte criptografia com os dados a serem enviados ou recebidos. Apesar desta técnica ser tecnologicamente muito boa, pois seria impossível de quebrar com a tecnologia disponível atualmente, não é viável pois este tipo de método requiriria um armazenamento na ordem dos *gigabytes*, o que seria demasiado caro para os consumidores.

3.2.2. NFC

O NFC (*Near Field Communication*) é um conjunto de protocolos que permite a dispositivos eletrónicos estabelecerem comunicações rádio ao se tocarem ou aproximarem-se a uma distância de 10 ou menos centímetros. Possui uma largura de banda de 424 bits/segundo. Esta tecnologia nasceu a partir do RFID (*Radio Frequency Identification*), cujo primeiro registo remota a uma patente registada por Charles Walton em 1983 mas só em 1997 é que foram realizados os primeiros desenvolvimentos para NFC. Os padrões NFC são definidos pelo Fórum NFC [11], um consórcio global criado em 2004 e composto por múltiplas empresas internacionais como: Qualcomm, LG, Nokia, Google, Microsoft, Paypal, Visa, Mastercard, Toshiba, entre muitas outras. Esta tecnologia pode ter as mais diversas utilidades e funcionar como documento de identidade ou ser usado para realizar um pagamento.

Características gerais

Modos

Cada dispositivo NFC pode funcionar em três modos principais:

- Modo leitura/escrita - quando este modo se encontra ativo, um dispositivo NFC pode ler e escrever em etiquetas ou autocolantes NFC. Por exemplo, é possível ler os dados de contacto de uma pessoa através de uma etiqueta ou autocolante NFC;
- Modo P2P (*Peer-2-peer*) - quando este modo se encontra ativo em dois dispositivos NFC, permite que os mesmos troquem dados entre si. Por exemplo, é possível enviar informações sobre *links* Bluetooth (ver secção sobre Bluetooth) e automaticamente estabelecer uma ligação entre dois dispositivos sem o normal processo de emparelhamento;

[10] Técnica criptográfica que, quando bem utilizada, não é possível ser quebrada.
[11] `http://nfc-forum.org/`

- Modo emulação de cartão - ativando este modo num dispositivo NFC, permite que um outro dispositivo NFC o consiga ler como um outro qualquer *smart card*. Por exemplo, é possível fazer com que o primeiro dispositivo atue como sistema de pagamento sem qualquer necessidade de mudança de infraestruturas.

Como é possível constatar, esta multiplicidade de modos dos dispositivos NFC faz com que a sua utilização em casos de uso reais seja imensa o que motiva a que mais e mais empresas continuem os desenvolvimentos para equipar os seus dispositivos com esta tecnologia. Não só as empresas que produzem os dispositivos mas também as empresas que se encarregam do desenvolvimento do padrão em si.

Rádio frequência

Os dispositivos NFC operam sobre a mesma banda que HF RFID (*High frequency RFID*), nos 13,56MHz, e funciona mesmo como uma extensão dos padrões definidos pelo HF RFID, sendo que partilham algumas semelhanças físicas. O NFC respeita os *standards* definidos pelo ISO 14443.

Identificadores

Ao contrário das restantes tecnologias sem fios abordadas neste documento, o NFC não necessita de qualquer tipo de especificação em relação ao endereçamento dos dispositivos. Isto porque, além de funcionar a distâncias muito curtas e os dispositivos não estarem simplesmente disponíveis para comunicações, é baseado em RFID o que pressupõe a leitura de um identificador próprio em cada dispositivo. Cada dispositivo e principalmente para etiqueta NFC possuem então em identificador único programado e registado pelo fabricante. No caso das etiquetas NFC do tipo 1 e 2, e como descrito pelo Fórum NFC, possuem um identificador único (*UID*) de 7 *bytes*. Isto oferece a possibilidade de existência de 2^{56} identificadores diferentes. Para as etiquetas baseadas em *Mifare Classic da NXP*, que não estão incluídas na especificação do Fórum NFC mas muitos dispositivos conseguem ler, existem 4 *bytes* disponíveis para a programação do identificador único. O que significa que podem existir até 4.3 biliões de dispositivos únicos deste género.

Arquitetura

Ao utilizar padrões existentes e reconhecidos como ISO/IEC 18092 e ISO/IEC 14443-2, 3, 4, assim como JIS X6319-4, o Fórum NFC conseguiu chegar a uma especificação da tecnologias que permitiu criar uma arquitetura homogénea, suportando os três modos possíveis do NFC.

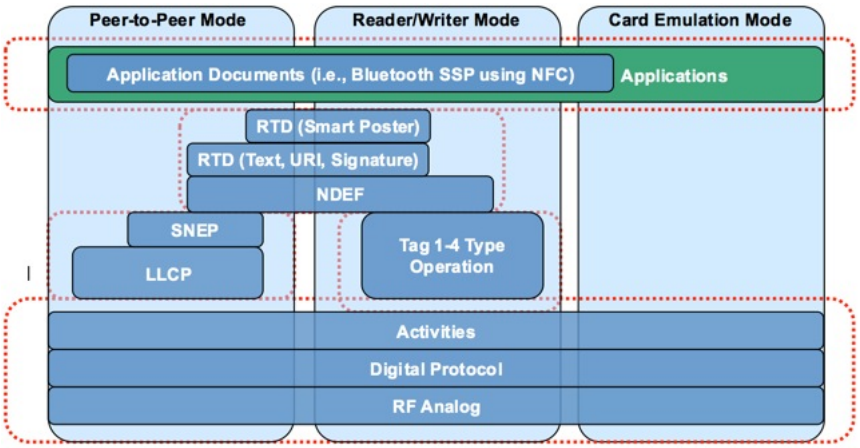

Figura 3.11.: Arquitetura NFC (Forum)

Logical Link Control Protocol (LLCP)

Esta especificação define um protocolo da camada 2 do modelo OSI que suporta comunicações *peer-to-peer* entre dois dispositivos NFC, o que é essencial para as comunicações bidirecionais. Esta especificação define dois tipos de serviço: sem conexão e orientado a conexão. Estes tipos de serviços encontram-se divididos em três classes: serviço sem conexão, serviço orientado a conexão e serviço sem e orientado a conexão. Os serviços do tipo sem conexão oferecem o mínimo de configurações sem confiança nenhuma ou controlo de fluxo, enquanto que os orientados a conexão oferecem confiança na entrega, controlo de fluxo e uma camada de serviço *multiplexing* baseado em sessões.

Digital Protocol

Esta especificação define um protocolo que harmoniza as tecnologias integradas e especifica opções de implementação, assim como limitação da interpretação dos padrões. Essencialmente, torna-se numa forma de mostrar ao programadores como lidar com o NFC de modo a garantir uma interoperabilidade global entre os mais diversos dispositivos NFC.

Activity Technical

Esta especificação define como é que a especificação *Digital Protocol* pode ser utilizada para estabelecer uma comunicação entre um dispositivo NFC e outro dispositivo ou uma etiqueta NFC. Esta descreve blocos, chamados Atividades, para configurar um protocolo de comunicação. Estas atividades podem ser utilizadas como estão definidas ou serem modificadas para utilização em diferentes casos de uso de definição de um protocolo de comunicação. As atividades podem ser combinadas em Perfis. Cada perfil envolve um conjunto de configurações adaptado a cada caso de uso.

Simple NDEF Exchange Protocol (SNEP)

Esta especificação permite a uma aplicação num dispositivo NFC realizar uma troca de mensagens em formato NDEF (*NFC Data Exchange Format*) com outro dispositivo NFC, quando estes se encontram a operar sobre o modo *peer-to-peer*. Este protocolo faz uso

do LLCP para um nível de transporte orientado à conexão e deste modo garantir uma troca de dados confiável.

Analog

Esta especificação aborda as características analógicas das rádio frequências de dispositivos NFC. O propósito desta especificação é caracterizar e especificar os sinais observáveis por parte de dispositivos NFC sem realizar qualquer tipo de especificação em relação à antena do mesmo. Isto inclui requisitos de potência, transmissão, receção e formas de sinal. Esta especificação deve ser utilizada pelos fabricantes quando pretende implementar a tecnologia NFC em qualquer dispositivo novo.

Control Interface

A especificação *NFC Control Interface* (NCI) define um padrão entre um dispositivo NFC, um controlador NFC e o principal processador do dispositivo. O NCI torna a tarefa dos fabricantes de integrar *chipsets* de diferentes fabricantes muito fácil e define um nível comum de funcionalidade e interoperabilidade entre os componentes de dispositivos NFC.

Segurança

Quando o propósito da tecnologia NFC se começou a orientar para âmbitos de pagamento, muitos consumidores ficaram, naturalmente, preocupados com diversas fraquezas que a tecnologia pudesse trazer. No entanto, existem múltiplas formas de combater as mais comuns formas de ataque.

Espionagem

Espionagem, no mundo das redes sem fio, acontece quando um atacante interceta uma ligação sem fios e consegue aceder a qualquer informação que a vítima e o legítimo destinatário estejam a trocar. Não é necessário que o atacante obtenha acesso a todos os pacotes de dados transmitidos de modo a conseguir ter acesso a informação privada. De qualquer forma, o NFC tenta prevenir este tipo de ataques com dois métodos. O primeiro, é o alcance da tecnologia em si, dado que o utilizador para realizar algum tipo de troca de dados necessita de estar a uma distância bastante curta do destinatário, não existe espaço para que um atacante se sinta o confortável para realizar um ataque furtivo. Segundo, está a encriptação utilizada pelo NFC, assim que um canal de comunicação seguro é estabelecido, todas as informações são encriptadas e apenas podem ser lidas por um dispositivo autorizado.

Corrupção e manipulação de dados

Corrupção e manipulação de dados ocorre quando um atacante interceta informações de terceiros e as manipula de modo a obter algum tipo de vantagem ou lucro com a ação. Este tipo de ataques pode ser prevenido utilizando também canais de comunicação seguros.

Estes dois exemplos são apenas os mais básicos no que toca a possíveis ataques a dispositivos NFC e nenhum deles é 100% fiável. Por exemplo, em relação à curta distância de comunicações entre dispositivos NFC, um atacante poderia colocar uma etiqueta NFC dissi-

mulada num PoS (*Point-of-sale*) e roubar as informações de todas as pessoas que utilizassem aquele serviço. A partir deste momento, além de informações privadas do utilizador como cartões de crédito e números de telefone, existe ainda a possibilidade de manipulação, através de NFC, do dispositivo em si. Esta manipulação pode abranger ações como *download* de *malware*, envio de SMSs, realização de chamadas, entre muitas outras coisas.

3.2.3. Bluetooth

O nome Bluetooth provém da homenagem ao rei da Dinamarca e Noruega Harald Blåtand (em inglês, Harold Bluetooth) que ficou conhecido pela unificação das tribos norueguesas, suecas e dinamarquesas. Da mesma forma, o protocolo pretende unir diferentes tecnologias, sistemas e dispositivos.

O Bluetooth é uma tecnologia sem fios padrão para a troca de dados em curtas distâncias e construir áreas de redes pessoais. O Bluetooth como especificação industrial é levado a cabo pela Bluetooth SIG (*Special Interest Group*). Esta é uma organização sem fins lucrativos fundada em 1998 pela Ericsson, IBM, Toshiba, Nokia e Intel e cujo principal objetivo é supervisionar o desenvolvimento das normas da especificação Bluetooth. Esta é também responsável pela posse da Bluetooth™. As principais tarefas desta organização são a publicação das especificações Bluetooth, administração do programa de qualificação, proteção da marca Bluetooth™ e evangelizar a tecnologia sem fios. Esta organização não fabrica, desenvolve ou vende qualquer tipo de equipamentos Bluetooth. A Bluetooth SIG tem vindo a trabalhar para melhorar cada vez mais a tecnologia com publicações frequentes de especificações sendo que a mais recente se encontra na versão 4.1, publicada a 3 de Dezembro de 2013.

Características gerais

Classes

O Bluetooth é uma tecnologia sem fios, geralmente de curta distância, com intenção de substituir cabos que conectam diversos dispositivos eletrónicos. Apesar do alcance para a maior parte dos dispositivos atingir os 10 metros, o Bluetooth é subdividido em três classes:

Classe	Energia	Alcance
Classe 1	100 mW (20 dBm)	100 metros
Classe 2	2,5 mW (4 dBm)	10 metros
Classe 3	1 mW (0 dBm)	1 metro

Tabela 3.2.: Classes de dispositivos Bluetooth

Sendo que a classe 1 é utilizada em situações industriais e a classe 2 é encontrada na maior parte dos dispositivos móveis.

Rádio frequência

O Bluetooth opera sobre a banda ISM entre as frequências 2,402GHz e 2,480GHz, o que significa que pode variar entre 79 diferentes canais de comunicações com 1MHz de espaçamento entre cada um deles. Este utiliza a técnica de *spread-spectrum frequency hopping* [12] (espectro de difusão em frequência variável). Esta técnica de transmissão de sinais rádio tem a particularidade da mudança rápida de transmissor entre os diferentes canais disponíveis através de uma sequência pseudo aleatória conhecida para ambos o emissor e o recetor. Isto deve-se principalmente para a possibilidade de interferência com outros dispositivos como telefones sem fios e micro-ondas que funcionam na mesma frequência da banda ISM. Durante operações normais, a troca de canais pode atingir as 1600 vezes/segundo, enquanto em procedimentos especiais como pesquisa e conexão de dispositivos, pode ir até às 3200 vezes/segundo.

Endereçamento

Cada unidade Bluetooth possui um endereço Bluetooth único de 48 bits (*BD_ADDR*). Este endereço é composto por várias subdivisões de octetos.

Atribuído pelo fabricante						**Identificação do fabricante**					
LAP						*UAP*		*NAP*			
0000	0001	0000	0010	0110	0000	0001	1000	1110	0101	0011	0101

Tabela 3.3.: Estrutura de endereço Bluetooth

Dado que este endereço é definido pelo fabricante do equipamento, este encontra-se dividido em duas partes de 24 bits cada uma. A primeira é constituída pela LAP (*Lower Address Part*) e é definido internamente pelo fabricante. Estes primeiros 3 bytes do endereço são transmitidos em cada pacote de dados como cabeçalho da transmissão. A segunda é constituída pela UAP (*Upper Address Part*) e pela NAP (*Non-significant Address Part*) que ocupa os dois finais octetos. A UAP é atribuída pela IEEE e é o byte intermédio entre a LAP e a NAP o que pode derivar do pacotes de dados a ser transmitido. Por fim, a NAP é também atribuída pela IEEE e pode ser consultada publicamente1. Esta última é atribuída ao fabricante e serve como identificação do mesmo, para cada fabricante podem estar atribuídas dezenas de porções de NAP. Por exemplo, para a Xerox está atribuídos do 00-00-00 até ao 00-00-99 (mas também o 00-00-AA e o 9C-93-4E) enquanto com uma pesquisa na base de dados da IEEE foi possível obter 250 resultados só para a Motorola. O endereçamento Bluetooth é muito importante na segurança da tecnologia pois com um endereço Bluetooth é possível 'farejar' sinais Bluetooth próximos e caso seja detetado qual o dispositivo *Non-significant Address Part* (secção seguinte, 2.3) é possível levar a cabo um ataque. Importante referir que a técnica de *frequency hopping* é definida pelo endereço MAC e relógio do dispositivo *Non-significant Address Part.* Um possível ataque poderá consistir fazer-se passar por um dipositivo Bluetooth que não o real e em dizer ao dispositivo *Non-significant Address Part* que a *link key* foi esquecida obrigando assim a um

[12] Técnica inventada por Hedy Lamarr (1914-2000).

novo emparelhamento e redefinição da respetiva *link key*.

Como os endereços Bluetooth possuem a característica da unicidade, existem valores LAP que se encontram reservados para processos de pesquisa e uso futuro. Estes valores não devem ser usados independentemente do UAP e NAP.

LAP (número hexadecimal)	**Reservado para**
0x9E8BB00	Pesquisa dedicada
0x9e8b01 – 0x9e8b32	Uso futuro
0x9e8b	Pesquisa geral
0x9e8b34 – 0x9e8b3f	Uso futuro

Tabela 3.4.: Valores de LAP reservados e seu uso

No contexto da técnica de *frequency hopping* mencionado anteriormente, são usados os 28 bits menos significativos de endereçamento juntamente com o relógio nativo para se conseguir efetuar o mapeamento da técnica.

Topologias

Os dispositivos Bluetooth comunicam entre si utilizando o protocolo *Master-Slave*. Isto significa que por cada ligação Bluetooth existe um *master* e um *slave*, sendo que o *master* é aquele responsável pelo início da comunicação e pelo envio de pedidos, enquanto que o *slave* apenas se limita a receber, reconhecer, tratar e enviar a resposta. Um *slave* nunca inicia uma comunicação. De cada vez que uma ligação é formada entre dispositivos Bluetooth (*link*), é criada uma PAN denominada *piconet*. Uma *piconet* consiste em dois ou mais dispositivos que ocupam o mesmo canal físico, isto é, encontram-se sincronizados num relógio comum e sequência de *hopping*. Em especificações anteriores o limite de dispositivos ligados por *piconet* é de 8 (sendo que 1 deles é o *master* e os outros 7 os *slaves*), enquanto que em especificações mais recentes o número ascende a 15. Estes *piconets* podem ser formados em áreas sobrepostas até um máximo de 10 sendo que a estas sobreposições se dá o nome de *scatternet*.

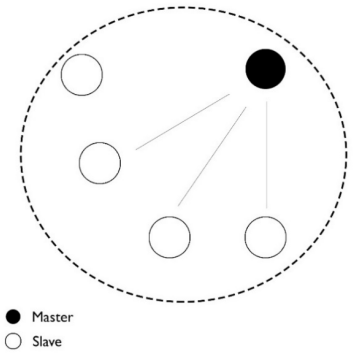

Figura 3.12.: Exemplo de *piconet*

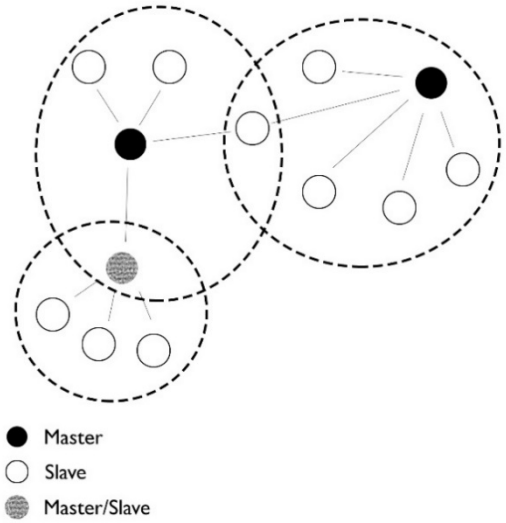

Figura 3.13.: Exemplo de *scatternet*

Existem situações em que, tal como demonstrado na segunda imagem, nas redes sobrepostas aquele que é *master* numa rede pode ser *slave* noutra.

Arquitetura

O sistema base da arquitetura Bluetooth encontra-se divido em quatro camadas e pelos seus protocolos associados assim definido na especificação Bluetooth. Existe ainda o *service discovery protocol* (SDP) que é responsável pelo processo de pesquisa de dispositivos Bluetooth, ou seja, que este processo seja o mais transparente e simples possível através da representação da gama de UUIDs num formato mais curto e o *generic access profile* (GAP) que permite definir um nível básico de funcionalidade para todos os dispositivos Bluetooth independentemente do nível de funcionalidade que suportam, ou seja, permite definir procedimentos de pesquisa, conexão entre dispositivos, procedimentos de segurança e convenções de nomes utilizadas.

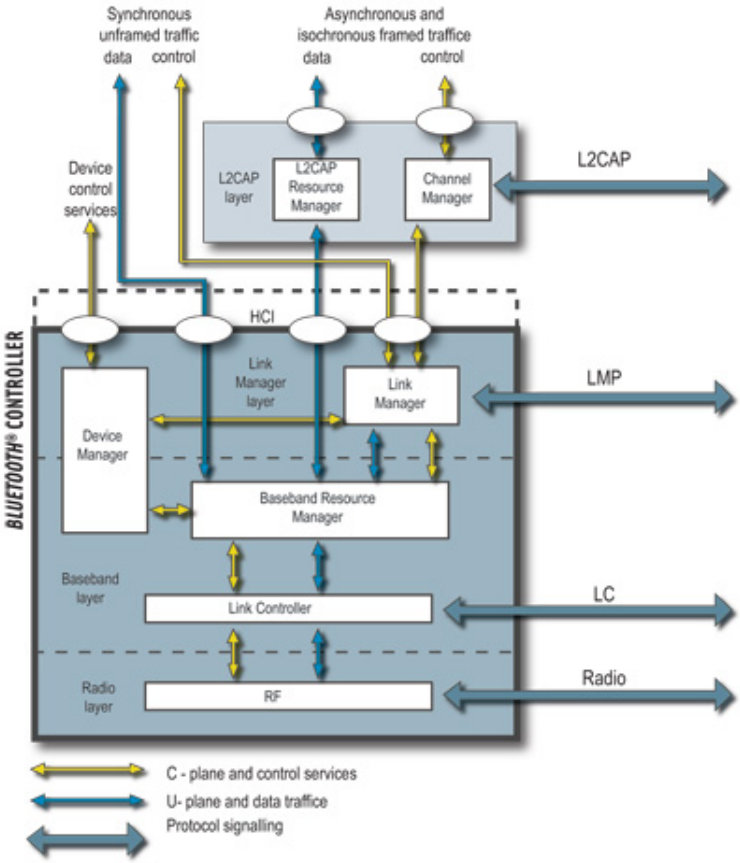

Figura 3.14.: Arquitetura Bluetooth (Developer)

Bluetooth controller

As três camadas mais baixas são geralmente agrupadas num subgrupo denominado *Bluetooth controller*. Este tipo de implementação é comum de modo a encapsular a camada física e fornecer a possibilidade de utilização de uma interface para a comunicação com o restante sistema Bluetooth. Para que exista coerência na definição desta interface, a especificação Bluetooth define a estrutura e formato das mensagens a serem trocadas através desta interface. Apesar de ser algo opcional, o desenho da arquitetura está preparado para a sua existência e características.

Logical Link Control and Adaptation (L2CAP)

Este protocolo suporta *multiplexing* [13] e é responsável pela segmentação de pacotes entre as camadas mais altas da *stack* Bluetooth e transporte da informação da qualidade de serviço. O L2CAP fornece canais lógicos que fazem o mapeamento dos *links* lógicos L2CAP. Este permite ainda a aplicações e protocolos de níveis mais elevados enviar e receber pacotes de dados de

[13] Processo em que múltiplos sinais analógicos ou informação digital são combinados num só de modo a reduzir custos de transmissão.

camadas superiores até 64 *kilobytes* de comprimento. O conceito geral do L2CAP está na utilização de canais, cada um dos *endpoints* de um canal L2CAP está identificado pelo identificador de canal (CID). Este pode ainda operar sobre um dos seguintes três modos de acordo com a escolha de uma camada superior.
O L2CAP funciona à base de pacotes de comunicações mas sempre com o conceito de canais, ou seja, cada cada representa um fluxo de dados entre entidades L2CAP em dispositivos remotos. Toda a sinalização de comandos é enviada para o canal com o CID 0x0001. Esta sinalização está disponível assim que o transporte lógico ACL esteja pronto e o tráfego L2CAP esteja disponível num *link* lógico do L2CAP.

Channel manager

O *channel manager* é responsável pela criação, gestão e destruição dos canais L2CAP para o transporte de protocolos de serviço e informação da aplicação. Este utiliza o protocolo L2CAP para realizar o mapeamento dos canais no dispositivo remoto de modo a que estes se liguem aos seus *endpoints* respetivos.

L2CAP resource manager

Este bloco é responsável pela gestão do ordenamento de submissões de unidades de protocolo (PDUs) para a baseband e pela monitorização da programação entre canais de modo a assegurar que os compromissos de QoS são cumpridos.

Device manager

O *device manager* é o grande responsável por todo o comportamento geral do dispositivo Bluetooth que não diga respeito ao transporte de informação, como a pesquisa de dispositivos próximos, a conexão a outros dispositivos e a definição de tornar o dispositivo visível e conectável para outros.

Link manager

Esta é a camada que é responsável pela criação, gestão e destruição de *links* lógicos entre dispositivos Bluetooth. Isto inclui a definição de funções de segurança com autenticação e encriptação, através da geração, troca e validação das chaves criptográficas e controlo de negociação do tamanho dos pacotes.

Baseband resource manager

A *baseband* é o bloco que se responsabiliza por toda a comunicação dirigida ao rádio. Dada a utilização da técnica de *frequency hopping* para a transmissão de dados, esta faz com que exista sincronização entre relógios nas frequências definidas e sincroniza a transmissão.

Link controller

O *link controller* é responsável pela codificação e descodificação de pacotes Bluetooth da informação e parâmetros relacionados o canal físico, transporte lógico e *link* lógico.

Segurança

Terminologias

- Ameaça de divulgação – quando informação de um sistema é divulgada para terceiros indesejados;
- Falha de integridade – quando a informação a ser transmitida é corrompida por uma terceira entidade, modificando-a;
- Negação de serviço – quando recursos ou informação são bloqueados por um atacante malicioso. Falha de disponibilidade;
- Autenticação – processo que determina a identidade de um utilizador;
- Autorização – processo de verificação de direitos de acesso a determinados recursos por parte do utilizador. Conceito de 'confiável'.

Modos de segurança

Tal como todas as tecnologias sem fios, também o Bluetooth se encontra suscetível a espionagem e interceção de comunicações. Para isso este oferece diversos modos de segurança incorporados com o protocolo cuja definição recai sobre o fabricante do equipamento. Estes modos de segurança servem essencialmente para determinar a que altura do processo de conexão se devem iniciar os procedimentos de segurança.

Modo de segurança 1 (não seguro): Quando um dispositivo se encontra no modo de segurança 1, não inicia qualquer tipo de procedimento de segurança. O único nível de segurança implementado é o método de data hopping e a curta distância de comunicação. Um bom exemplo de dispositivos que normalmente implementam este modo de segurança são auscultadores sem fios. Dado que não existe nenhum requisito de segurança para o emparelhamento dos mesmos.

Modo de segurança 2 (segurança ao nível do serviço): Neste segundo modo, não é executado nenhum método de segurança enquanto não for iniciado um pedido de estabelecimento de canal por parte de outro dispositivo ou do próprio dispositivo em causa. Quando um dispositivo se encontra neste modo deve classificar os requisitos de segurança de acordo com os seguintes padrões mínimos, cuja informação é armazenada na base de dados do serviço do gestor de segurança.

Requisito de autorização – este padrão requer sempre autenticação para verificar a verdadeira identidade do dispositivo e só inicia uma ligação automaticamente se este estiver indiciado como confiável (esta informação está armazenada na base de dados Bluetooth do dispositivo).

Requisito de autenticação – Antes de existir alguma ligação, o dispositivo remoto deve estar autenticado.
Requisito de encriptação – o link deve ser atualizado para modo de encriptação antes de aceder ao serviço.
Caso não exista qualquer registo na base de dados, são utilizados os seguintes valores por defeito:

Ligação recebida – autorização e autenticação necessárias.
Ligação enviada – autenticação necessária.

Modo de segurança 3 (segurança ao nível do link): Quando um dispositivo se encontra neste nível de segurança, deve iniciar os procedimentos necessários para uma ligação segura antes mesmo de um canal ter sido estabelecido.

Níveis de segurança

Este nível de segurança de dispositivo determina a que serviços este tem autorização para aceder
Dispositivo confiável – dispositivo previamente autenticado e assinalado como confiável na base de dados, a chave de ligação (link) entre os dispositivos é armazenada.
Dispositivo não confiável – dispositivo previamente autenticado mas não assinalado como confiável na base de dados, a chave de ligação (link) entre os dispositivos é armazenada na mesma.
Dispositivo desconhecido – não existe qualquer tipo de informação sobre o dispositivo na base de dados, dispositivo não confiável.

Autenticação

O processo de autenticação em Bluetooth passar por saber 'quem' está do outro lado da comunicação a tentar estabelecer um canal. Isto pode ser conseguido através de uma link key previamente guardada ou através do emparelhamento. Este último consiste num esquema de desafio-resposta como é demonstrado na seguinte figura:

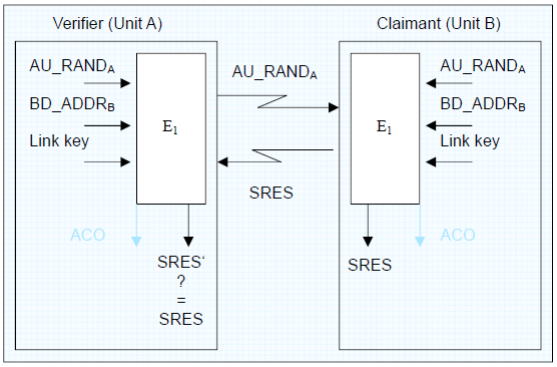

Figura 3.15.: Esquema desafio-resposta Bluetooth (OF COMPUTER SCIENCE, 2003)

Existem quatro entidades principais durante este processo:

- **PIN** – número até 128bits que pode ser fixo (menos seguro) ou acordado entre dispositivos e inserido em ambos igualmente;
- **BD_ADDR** – o endereço Bluetooth de ambos os dispositivos, fator único que os identifica;
- **Chave privada de encriptação** – chave de tamanho variável (8-128bits) que é recalculada com a transmissão de cada link key;
- **RAND** – também chamado de nonce, trata-se de um número de 128bits atualizado frequentemente e gerado de forma aleatória pelo dispositivo.

Processo de comunicação

Para iniciar um processo de comunicação entre dois dispositivos, são necessárias cinco condições de modo a garantir a segurança na autenticação e integridade de comunicações.

Geração de uma chave inicial – este passo só ocorre pela primeira vez que dois dispositivos comunicam entre si. Esta chave pode ser gerada através dos dados anteriormente mencionados e utilizando a função

$$F(PIN, sizeof(PIN), RAND, BD_ADDR) \tag{3.1}$$

, onde PIN é o número definido pelos utilizadores, RAND é o número aleatório gerado pelo dispositivo e BD_ADDR é a constante que identifica unicamente o dispositivo. Esta chave inicial irá servir como chave temporária de comunicação enquanto os dispositivos não decidirem que tipo de link key irão utilizar para futuras comunicações.

Autenticação – como descrito anteriormente, este processo pode ser conduzido de duas maneiras: mútuo ou não mútuo. Caso seja, mútuo ambos os dispositivos atuam como verificadores e este processo é levado a cabo duas vezes em que cada uma delas o papel verificador permuta. Sendo que a seguinte função é executada em ambos os dispositivos

$$E1(d, BD_ADDR, linkkey) \tag{3.2}$$

, onde d é o desafio proposto pelo dispositivo A, BD_ADDR é o endereço Bluetooth do dispositivo B e link key é chave atual gerada anteriormente. O processo é repetido invertendo os papéis de A e B.

Geração da *link key* – a chave unitária não muda, esta foi definida quando o dispositivo foi instalado.

Troca da *link key* – Após a chave unitária ter sido guardada no outro dispositivo, a chave inicial é descartada completamente.

Geração da chave criptográfica – Neste passo final, ambos os dispositivos concordam numa chave a utilizar e no seu tamanho, podendo variar entre 1-16 bytes.

Notas gerais sobre segurança

Autenticação de dispositivo é diferente de autenticação de utilizador. O Bluetooth autentica o primeiro e isto pode ser considerado um problema de segurança. Existe também o conceito de segurança específica do dispositivo e do serviço, em que a primeira deve ser implementada por todos os serviços do dispositivo em causa.
Por fim, a dependência em chaves, endereços fixos e PINs fixos, pode também conduzir a um problema grave de segurança.

Vulnerabilidades conhecidas

- **Blue Bug** - este tipo de vulnerabilidade existente nos telemóveis permite que um atacante consiga descarregar toda a lista de contactos, lista de chamadas ou até mesmo mensagens enviadas e recebidas. Esta vulnerabilidade demora apenas dois segundos a tomar efeito e o dispositivo do atacante não deve estar a mais do que 10-15 metros da vítima para este surtir efeito. Dado que o ataque toma partido da execução comandos sem que o dono se aperceba ou dê autorização, este pode mesmo iniciar chamadas telefónicas, enviar mensagens, ligar-se à Internet entre outras ações;
- **Long Distance Snarf** - esta experiência tomou lugar na Califórnia em Agosto de 2004 em que cinco pessoas estavam envolvidas. Na experiência estava a ser utilizada uma an-

tena unidirecional que apontava para um local elevado e um telemóvel Nokia. Passadas algumas tentativas, o telemóvel conseguiu detetar a vítima como se estivesse a realizar um ataque Blue Bug próximo dela. Isto veio a revelar que é possível executar comunicações Bluetooth com dispositivos que se encontram 170 vezes mais longe do que o definido pela especificação Bluetooth para a classe 2 (10 metros);

- **Bluetooone** - este processo consiste em modificar o equipamento Bluetooth para que as ondas radio passem a ser unidirecionais em vez de bidirecionais, o que aumenta a capacidade de alcance do equipamento. Esta modificação poderia ser utilizada em conjunto com um long distance snarf;

- **Blueprinting** - é o processo de obter todas as informações possíveis sobre os equipamentos Bluetooth ao alcance do atacante. Ao obter este tipo de informações e estatísticas, podem depois ser exploradas vulnerabilidades conhecidas para determinados equipamentos de certos fabricantes;

- **Blooover** - é uma ferramenta que pode ser executada em dispositivos móveis (ao invés dos típicos portáteis utilizados em ataques) para obter todo o tipo de informações sobre equipamentos Bluetooth;

- **BL Audit** - fornece ferramentas que permite pesquisar e descobrir canais abertos nos dois principais protocolos da stack Bluetooth: L2CAP e RFCOMM;

- **Bluesmack** - é um tipo de ataque que suprime imediatamente outros dispositivos Bluetooth através de um ping;

- **Blue Snarf** - este tipo de ataque consiste na ligação ao OBEX Push Profile (OPP) que é um tipo de perfil que não requer autenticação. Uma vez ligado, o atacante pode extrair informação de contactos e calendários;

- **Car Whisperer** - este tipo de ataque tira partido de um script que é executado sem cessar até que encontra um equipamento Bluetooth do tipo kit mãos livres presente nos automóveis e automaticamente se liga ao mesmo. A partir deste momento, e através de outros scripts, é possível obter o PIN que é usado para o emparelhamento de novos dispositivos e deste modo obter acesso total ao equipamento áudio do automóvel. Isto inclui intercetar e efetuar comunicações através do equipamento;

- **Blue Jacking** - este trata-se apenas de um tipo de ataque evasivo e não altera nenhuma informação presente no equipamento, trata apenas de enviar (sem ser solicitado) cartões-de-visita ou mensagens para a vítima.

3.2.4. Conclusão

Na seguinte tabela estão detalhadas algumas das características essenciais que foram consideradas para a escolha do canal principal de comunicações entre os dispositivos móveis e o dispositivo de acesso.

Fator	Bluetooth	Wi-Fi	NFC
Alcance	1 - 100 metros	32 - 95 metros (com norma 802.11b/g)	10 centímetros
Disponibilidade	Suportado em larga escala nos dispositivos móveis	Altamente utilizado na maior parte dos dispositivos atuais	Parcialmente suportado por dispositivos móveis
Facilidade de implementação	Fácil de configurar e estabelecer ligações e efetuar comunicações entre dispositivos	Maior nível de complexidade e configuração tanto a nível de hardware como de software	Fácil de configurar e mais fácil de efetuar comunicações
Hardware	Módulo bluetooth	Módulo Wi-Fi, router e/ou access point	Módulo NFC
Segurança	Nível de segurança básico	Abordagem mais complexa e robusta	Segurança básica mas confiável devido ao seu alcance
Taxa de transmissão	2.1 Mbps	600 Mbps	0.4 Mbps
Autoridades de especificações	Bluetooth SIG	IEEE, WECA	ISO/IEC
Standard de comunicação	IEEE 802.15.1	IEEE 802.11	ISO 13157 etc.

Tabela 3.5.: Comparação de tecnologias sem fios

Analisando o NFC como canal de comunicação foi possível concluir que esta não seria a opção mais indicada por duas principais razões: falta de suporte por parte dos *smartphones* a nível global e alcance. Quanto ao alcance, este pode ser visto como um fator a favor e como um fator contra. Sendo que esta tecnologia foi concebida com o intuito de "*Tap & Pay*", o curto alcance pode ser algo difícil de colmatar ao tentar implementar funções como abertura de porta automática. No entanto, seria bastante positivo o facto do curto alcance não permitir ataques *Man-in-the-Middle* [14].

Ora quando o Wi-Fi foi considerado, o primeiro pensamento recaiu sobre a segurança. Dado ser uma tecnologia altamente adotada mundialmente, é também das mais exploradas a nível de segurança informática e existem relatórios que provam o quanto se pode tornar perigoso transmitir dados sensíveis desprotegidos através deste canal. Também foi tido em conta que existem diversas soluções a serem implementadas neste momento e que a proteção contra qualquer tipo de ataque involuirá no futuro próximo, no entanto foi excluída temporariamente como opção pois existe a possibilidade de expansão futura de modo a adotar esta tecnologia.

[14] `https://www.owasp.org/index.php/Man-in-the-middle_attack`

Por fim, foi então decidido utilizar o Bluetooth como meio de comunicação mas também este apresenta as suas limitações. No caso de existir uma distância considerável entre o dispositivo móvel e o controlador na porta, não há qualquer possibilidade de comunicação entre os dois (algo que o Wi-Fi poderia colmatar) o que pode tornar a solução pouco prática. No entanto, foi uma decisão tomada em prol da segurança. Ora, tal como o NFC este também beneficia do curto o alcance e do facto de ser possível limitar as comunicações com dispositivos apenas num determinado raio de distância.

3.3. Sumário

Neste capítulo foi possível estudar e analisar as diferentes tecnologias e *hardware* ponderados para o projeto desta tese. Para o *hardware* foram consideradas duas possibilidades, o Raspberry Pi e o BeagleBone Black, sendo que a escolha recaiu sobre a última hipótese. Como canal de comunicação, foram analisadas as especificações e capacidades de três tecnologias distintas, o Wi-Fi, o NFC e o Bluetooth. Apesar da decisão se ter debruçado sobre Bluetooth, este projeto não descarta a utilização e integração das restantes tecnologias abordadas numa possível versão futura do projeto como meio de expansão de capacidades ou melhoramento de características. Após esta análise é então possível responder à questão relativa ao *hardware*, apresentada no capítulo inicial desta tese:

SQ-3: "Qual o *hardware* necessário para uma fechadura eletrónica?"

Considerando o componente principal de *hardware* para o projeto e o canal de comunicação, são necessários os seguintes componentes:

- BeagleBone Black
- Módulo Bluetooth
- *Breadboard*
- Fios para *breadboard*
- Resistências

O BeagleBone Black pode ser adquirido através de um dos muitos parceiros da fundação BeagleBoard que se encontram presentes em diversos continentes. Quanto ao módulo Bluetooth, este deveria ser da categoria *Bluetooth Low Energy* ou *Bluetooth Smart*, de acordo com as especificações apresentadas na solução proposta no seguinte capítulo, e deverá ter uma interface USB para se ligar ao BeagleBone Black. Os restantes componentes são apenas alguns dos materiais necessários para o desenvolvimento da solução a nível eletrónico. Dado o *hardware* apresentado, podemos também tirar algumas conclusões sobre o *software*, no entanto a quinta

e última pergunta de pesquisa apenas será respondida no capítulo seguinte, onde poderão ser dados mais detalhes não só sobre ferramentas de desenvolvimento mas também sobre bibliotecas entre outros recursos utilizados para melhorar ou facilitar o desenvolvimento.

SQ-2.1.1: "Quais os preferenciais?"

Tendo em conta a resposta da SQ-2.1 e das justificações já aqui apresentadas, o único canal de comunicação escolhido para o projeto é o Bluetooth.

Capítulo

4 Proposta de solução

De seguida, será apresentada uma detalhada descrição de todos os componentes da solução proposta nesta tese. Será iniciada por uma breve descrição do funcionamento da mesma e a primeira secção abordará a temática da segurança, onde será explicado como seria implementado um protocolo de autenticação. Nas duas secções seguintes, é explicado com recurso a exemplos de código fonte como funcionariam a aplicação móvel e o mecanismo de fechadura em relação às comunicações Bluetooth e à encriptação das mensagens.

4.1. Descrição da solução

Tal como mencionado anteriormente, esta solução assenta sobre duas componentes principais: uma aplicação móvel e um dispositivo de acesso. A aplicação móvel serve como meio de controlo, verificação do estado e bloqueio/desbloqueio do dispositivo. Serve também como meio de distribuição e revogação de chaves eletrónicas que, servirão posteriormente como meio de autenticação para terceiros possuírem as mesmas habilidades que o dono em relação à fechadura. Será também dada a possibilidade do dono da fechadura verificar um detalhado registo de entradas e saídas através da aplicação. A segunda componente, a fechadura, serve como mecanismo de controlo de entradas e saídas, logo terá que realizar a verificação de autorização dos utilizadores, registar novas chaves eletrónicas e manter um registo dos utilizadores que utilizarem a fechadura.

4.1.1. Testes

Os testes de *software* servem para providenciar informações sobre a qualidade do produto que está a ser desenvolvido. Estes testes são importantes para avaliar o desempenho da solução, se o *software* responde bem a qualquer *input* do utilizador, se fornece o *output* esperado, se pode (ou deve) ser utilizado em múltiplos ambientes e se, no geral, atinge os objetivos pretendidos.

Para o projeto atual, o que se pretende evidenciar é a proposta para uma possível solução do problema apresentado. Apesar de ter sido construído um protótipo parcial, foi considerado que a aplicação de testes unitários ou outros, seria mais benéfica num desenvolvimento posterior face ao desenvolvimento do protótipo.

4.2. Segurança

Todos os dispositivos Bluetooth estão suscetíveis a ataques e apesar da especificação Bluetooth apresentar soluções de autenticação e encriptação, estas podem mostrar-se insuficientes no que toca a segurança do lar. Além disso, para especificações de Bluetooth anteriores a 2.1 a encriptação é algo opcional e pode ser desligada a qualquer altura. No entanto, a encriptação em Bluetooth não é suficientemente segura podendo ser descoberta a chave de encriptação em menos de 1 dia usando ataques XOR (Academy).

Nota: Para efeitos académicos, foi estudada e explorada a possibilidade de implementação de um sistema de troca de chaves. Num ambiente real esta situação deveria ser evitada e utilizado um protocolo de autenticação criado por especialistas e testado contra ataques reais.

4.2.1. Simetria vs. Assimetria

Em segurança existem dois conceitos de simetria e assimetria no que toca a chaves criptográficas e distribuição das mesmas assim como algoritmos. Em **algoritmos simétricos** existe uma chave comum, ou chave secreta, que ambas as partes têm conhecimento e utilizam para encriptar as mensagens enviadas. Neste caso, os algoritmos são computacionalmente mais rápidos do que os assimétricos mas o tamanho da chave é crítico para o sucesso do processo (normalmente entre 160 a 512 bits). Onde assenta o grande risco de segurança nesta solução? Na distribuição da chave comum e no canal utilizado para o efeito. Dado que irá ser o único segredo mantido entre as partes envolvidas, a descoberta do mesmo poderá colocar em causa toda a encriptação e futuras mensagens. Em **algoritmos assimétricos** são usadas duas chaves (pública e privada) para a encriptação e desencriptação de mensagens. Cada sujeito da comunicação possui uma chave pública e uma chave privada que são inversamente funcionais uma da outra, ou seja, quando uma é utilizada para encriptar uma mensagem a outra é utilizada para a desencriptação da mesma. Sendo que a chave privada nunca é divulgada por nenhuma das partes, apenas a chave pública é divulgada. Este método retira todo o risco na transmissão das chaves entre entidades.

Tipicamente num sistema de chaves simétricas (Young), estas são:

- Aleatoriamente geradas com k-bit;
- Simples de gerar;
- Não têm propriedades especiais.

Num sistema de chaves assimétricas, estás são:

- Têm uma estrutura especial (ex.: números primos enormes);
- Bastante difíceis de gerar.

Apesar destas características ambos os tipos de chaves não são comparáveis quando se pode afirmar que a segurança fornecida por uma chave simétrica de 128-bit pode ser equivalente a uma chave assimétrica de 3000-bit.

Conforme mencionado nos casos de uso, um utilizador pode adicionar/registar novas fechaduras à sua aplicação móvel sondando a sua rede Bluetooth e inserindo o código físico da fechadura. Este código é aleatório e único e é o que permite estabelecer uma ligação entre o dispositivo e a fechadura. Esta ligação permite que ambos efetuem a troca de chaves criptográficas simétricas através do método *Diffie-Hellman* (Rouse, 2007). A escolha de chaves simétricas em vez de chaves assimétricas é justificada pelo facto do processamento ser efetuado em dispositivos que podem não ter uma grande capacidade de processamento. Apesar da decisão sobre um dispositivo como o *BeagleBone Black* que, em comparação com os seus semelhantes possui maior poder de computação, foi decido implementar a utilização de chaves simétricas. A grande desvantagem das chaves simétricas recai sobre o método de partilha das chaves entre as entidades, desvantagem esta que é colmatada através do método *Diffie-Hellman* para partilha das mesmas em meios inseguros. Segue-se a explicação sobre como implementar a geração e troca destas.

4.2.2. Criptografia com curvas elípticas

A criptografia com curvas elípticas é uma abordagem a chaves públicas baseada na estrutura das curvas elípticas algébricas sobre campos finitos. Esta abordagem foi sugerida em 1985 por Neal Koblitz e Victor Saul Miller (Namin, 2005). Comparado com outras abordagens esta oferece o mesmo nível de segurança utilizando chaves de menor dimensão. Tem também a particularidade de possuir um processamento mais rápido e uma poupança significativa de memória, energia e largura de banda.

Criptografia com curvas elípticas é um dos mais poderosos meios criptográficos utilizados hoje em dia mas de todos o menos entendido. Um crescente número de entidades está a introduzir a sua utilização extensiva para utilizar desde ligações HTTPS a como a informação é transmitida entre utilizadores e os *data centers*. Antes de mais, é importante definir que nos sistemas criptográficos existe um algoritmo que processa a informação facilmente numa direção mas o seu processo inverso é extremamente difícil. Aos algoritmos que possuem esta característica, chamamos de funções *trapdoor*. Encontrar uma boa função *trapdoor* é essencial para qualquer sistema criptográfico, quanto mais difícil for de processar a informação inversamente, melhor será a segurança do mesmo.

Foi então que, em 1985, surgiu o algoritmo criptográfico baseado no ramo esotérico da matemática chamado curvas elípticas. Uma curva elíptica é um conjunto de pontos que satisfaz uma equação matemática do tipo curva cúbica e cujas soluções se encontram confinadas a um determinado espaço (Sullivan, 2013). Topologicamente, estas assemelham-se a um torus. A equação matemática mencionada será algo como:

$$y^2 = x^3 + ax + b \tag{4.1}$$

O que esta solução poderia gerar seria algo como:

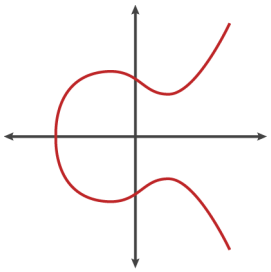

Figura 4.1.: Representação de uma curva elíptica (Sullivan, 2013)

Existem outras representações possíveis para as curvas mas esta é a que melhor representa a função em causa. No entanto, esta não se trata apenas de uma simples figura mas possui propriedades verdadeiramente interessantes. Uma delas é a simetria horizontal, qualquer ponto pode ser refletido no eixo X e permanecer na mesma curva. Uma outra propriedade é que qualquer linha não vertical irá intercetar a curva no máximo em três pontos. Tomando esta última propriedade, temos então o seguinte: ao obter dois pontos pertencentes à curva e traçando uma linha não vertical entre eles, é possível obter um terceiro ponto. A partir deste, é possível traçar uma outra linha (vertical) que estende até ao eixo negativo de Y caso o ponto esteja no positivo e vice-versa. Ao executar este processo múltiplas vezes e gerando novos pontos a partir do mais recente criado, é extremamente difícil para alguém que saiba o ponto final determinar o ponto original e todas as linhas intermédias geradas. Ou seja, este é um exemplo de uma boa função *trapdoor*. A este processo dá-se o nome de *dotted*.

Este é um bom exemplo mas não representa exatamente como as curvas elípticas se parecem quando usadas para criptografia. Neste caso, é necessário limitar os valores dos pontos na curva até um máximo. Quando é atingido um valor superior a esse máximo é necessário dividir esse valor pelo máximo definido e retirar o resto. Caso este limite máximo seja um número primo, a curva elíptica é chamada de curva prima e tem excelentes propriedades criptográficas.

Com esta nova representação de curvas elípticas é possível representar mensagens como pontos na curva. Um sistema criptográfico de curvas elípticas pode ser definido pela escolha de um valor máximo como um número primo, uma equação de curva elíptica e um ponto qualquer da curva definido como público. Ao definir um número privado (*priv*), é possível aplicar

o processo "dotted" apresentado anteriormente e aplica-lo ao ponto *priv* vezes. A computação deste número privado através do ponto público é chamado de função logarítmica discreta da curva elíptica e é esta a função *trapdoor* procurada para este sistema. O problema da função logarítmica discreta da curva elíptica é algo que os matemáticos estão a tentar resolver há cerca de três décadas e parece que não irá existir nenhum tipo de avanço nos anos que se seguem. O poder computacional está rapidamente a aumentar mas o aumento de processo de chaves criptográficas maiores também está a crescer.

4.2.3. Diffie-Hellman

O método de troca de chaves criptográficas *Diffie-Hellman* foi criado em 1976 por Whitfield Diffie e Martin Hellman. Este método foi criado com o intuito de troca de chaves sobre um canal inseguro e assumindo que nenhumas das partes possuía conhecimento prévio sobre a outra. Ora esta abordagem oferece o melhor dos algoritmos simétricos e assimétricos explicados anteriormente, pois utiliza o conceito de chaves públicas durante o seu processo mas com o objetivo de trocar uma chave que irá ser utilizada como chave simétrica. Chave esta que depois poderá ser utilizada para a encriptação das comunicações. A seguinte ilustração descreve o funcionamento do método utilizando cores em vez de números muito grandes.

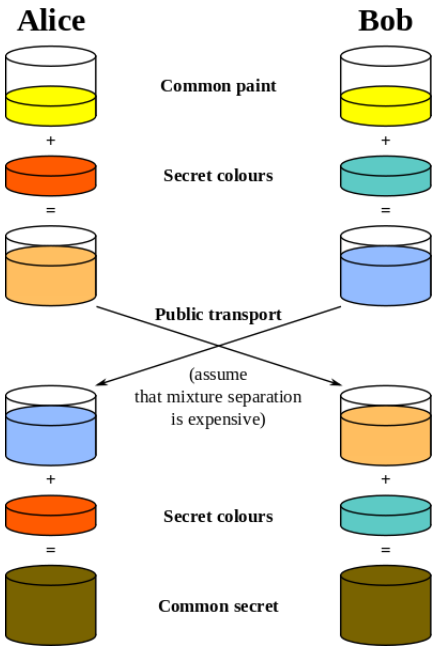

Figura 4.2.: Ilustração do método *Diffie-Hellman* (Wikipedia)

A explicação criptográfica da ilustração anterior pode ser explicada pelos seguintes passos, considerando que todos os números apresentados seriam de elevada dimensão num caso real:

1. A entidade **Alice** e **Bob** concordam em utilizar um número primo **p** e uma base **g**;

2. **Alice** escolhe então um número inteiro secreto **a** e envia a **Bob**:

$$X = g^a \ mod \ p \tag{4.2}$$

3. **Bob** escolhe então um inteiro **b** e envia a **Alice**:

$$Y = g^b \ mod \ p \tag{4.3}$$

4. **Alice** calcula:

$$s = Y^a \ mod \ p \tag{4.4}$$

5. E **Bob** calcula

$$s = Y^b \ mod \ p \tag{4.5}$$

6. Ambos partilham agora o mesmo segredo **s** sem que este tenha sido transmitido num canal inseguro.

Isto é particularmente interessante pois, apesar de terem sido trocados valores públicos é praticamente impossível calcular o segredo a partir destes. Isto é possível graças a uma propriedade de modulação exponencial, especificamente:

$$(g^a \ mod \ p)^b \ mod \ p = g^a b \ mod \ p \tag{4.6}$$

$$(g^b \ mod \ p)^a \ mod \ p = g^b a \ mod \ p \tag{4.7}$$

É aqui que é possível atingir *perfect forward secrecy*, esta é uma propriedade de um sistema de chaves públicas que é atingida quando consegue gerar chaves públicas aleatórias por sessão apenas para a troca de chaves e não utiliza qualquer tipo de algoritmo determinístico para o alcançar. Isto significa que o compromisso de uma mensagem não invalida as outras e que não existe nenhum valor secreto que ponha também em causa todas as outras mensagens. Enquanto o problema do logaritmo discreto é usado tradicionalmente, o processo geral pode ser alterado com criptografia de curvas elípticas.

4.2.4. Troca de chaves Diffie-Hellman usando curvas elípticas

A criptografia utilizando curvas elípticas é um cripto sistema emergente em ambientes sem fios e para dispositivos móveis na medida que em comparação com, por exemplo, o RSA [1]

[1] Algoritmo de criptografia cujo nome é definido pelos seus três inventores: Ronald **R**ivest, Adi **S**hamir e Leonard **A**dleman

consegue oferecer o mesmo nível de segurança com custos computacionais bastante inferiores. Aplicando os dois conceitos introduzidos anteriormente é possível chegar à solução da troca de chaves *Diffie-Hellman* utilizando curvas elípticas. Inicialmente está definido um domínio de parâmetros para números primos adequado a curvas elípticas:

- E – função da curva elíptica;
- F – campo finito sobre a qual a função é criada;
- n – ordem da função da curva elíptica (valor inteiro máximo apresentado na secção 4.4.2);
- G – ponto inicial da curva, ou ponto gerador.

Relembra-se que todos os números aqui declarados são de elevada dimensão. Cada entidade define um número aleatório (privado)

$$d \in [1, n-1] \tag{4.8}$$

e um número público

$$Q = dG \tag{4.9}$$

Sendo então o par público-privado da entidade **A**

$$(d_A, Q_A) \tag{4.10}$$

e o par público-privado da entidade **B**

$$(d_B, Q_B) \tag{4.11}$$

Cada entidade calcula os seus respetivos pontos K com as coordenadas

$$(x_k, y_k) \tag{4.12}$$

em que a de **A** é obtida por

$$K_A = (X_A, Y_A) = (d_A * Q_B) \tag{4.13}$$

e a de **B** por

$$K_B = (X_B, Y_B) = (d_B * Q_A) \tag{4.14}$$

Sendo que:

$$d_A * Q_B = d_A d_B G = d_B d_A G = d_B * Q_A \tag{4.15}$$

, logo

$$K_A = K_B \tag{4.16}$$

Ambos possuem agora o segredo partilhado (coordenada x do ponto) sem que este tenha sido transmitido pelo canal de comunicação.

Variações

Em certos casos, este segredo obtido pode ainda ser um passo intermédio para a obtenção da chave secreta final devido à possibilidade de cálculo da função de derivação da chave [2]. As chaves públicas utilizadas podem ser estáticas ou efémeras. Chaves efémeras são chaves que variam no tempo e não são necessariamente autenticadas.

As curvas elípticas estão em crescente popularidade desde há muitos anos, alguns dos seus usos são: a proteção das comunicações internas do governo dos Estados Unidos da América, o anonimato do projeto Tor [3], prova de autenticidade na moeda criptográfica Bitcoin, assinaturas digitais no serviço de mensagens da Apple iMessage, encriptação de informação de DNS com DNSCurve e é o método preferido para autenticação segura em *websites* sobre o protocolo SSL/TLS. Caso um utilizador esteja a utilizar uma versão recente dos *browsers* Google Chrome ou Mozilla Firefox, este estará a utilizar criptografia com curvas elípticas.

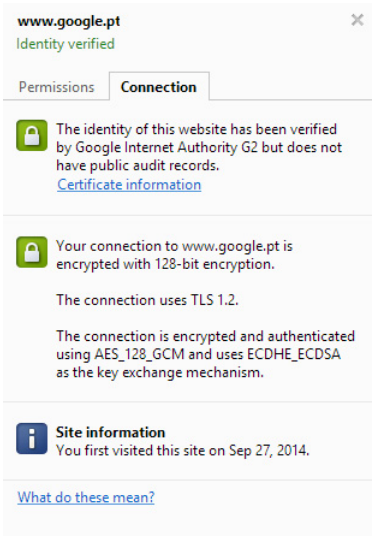

Figura 4.3.: Apresentação da conexão efetuada ao *website* da Google

Websites que usam RSA usam-no porque o seu certificado SSL é ligado a um par de chaves RSA. *Browsers* modernos também suportam certificados baseados em curvas elípticas. Se o certificado SSL de um *website* é um certificado de curva elíptica, esta parte da página declararia ECDHE_ECDSA. A prova da identidade do servidor seria feito usando ECDSA, a curva elíptica Digital Signature Algorithm. Aqui está uma curva elíptica criptográfica para ECDHE (esta é a

[2] Utilizado em criptografia, *key derivation function* (KDF), deriva uma ou mais chaves secretas através de uma função pseudo aleatória.

[3] `https://www.torproject.org/`

mesma curva usada pelo Google.com):

máximo: 115792089210356248762697446949407573530086143415290314195533631308867097853951, curva:

$$y^2 = x^3 + ax + b \tag{4.17}$$

a = 115792089210356248762697446949407573530086143415290314195533631308867097853948

b = 410583q637251521421293261297800472684091144410159937255548352563140394674012911

A desvantagem

Quando se fala sobre curvas elípticas nem tudo são vantagens. Existem uma razão para o facto de esta ainda não ter sido completamente aceite pela indústria. Um ponto que alarma algumas mentes é a *Dual Elliptic Curve Deterministic Random Bit Generator* (Dual_EC_DRBG). Este é um gerador de números aleatórios padronizados pelo NIST e promovido pela NSA. Dual_EC_DRBG gera números aleatórios ou pseudo aleatórios usando a matemática das curvas elípticas. O algoritmo em si envolve a recolha de pontos numa curva e a realização repetida da operação de curva elíptica "dotted". Após a sua publicação, foi relatado que ele poderia ter sido projetado com um *backdoor* [4], o que significa que a sequência de números retornados pode ser totalmente previsto por alguém com o número privado certo. Sendo ou não este gerador de números aleatórios escrito com um *backdoor* ou não muda a força da tecnologia em si, mas levanta questões sobre o processo de normalização de curvas elípticas. Também é parte da razão que as pessoas deviam dedicar mais tempo a garantir que o sistema utiliza verdadeiramente números aleatório.

Alguns dos criptógrafos mais céticos do mundo agora têm uma desconfiança geral pela NIST e as normas que já foram apoiadas pela NSA. Quase todas as curvas elípticas amplamente implementadas se enquadram nesta categoria. Não há ataques conhecidos sobre estas curvas especiais, escolhidas pela sua aritmética eficiente, mas existem curvas com más características e alguns acham que é melhor prevenir do que remediar. Houve progressos no desenvolvimento de curvas com aritmética eficiente fora do NIST, incluindo curva de 25519 criado por Daniel Bernstein (DJB) e curvas mais recentemente calculadas por Paulo Baretto e colaboradores. Mas a ampla adoção dessas curvas é de vários anos de distância. Até que essas curvas não-tradicionais são implementados pelos *browsers*, não será capaz de ser usado para garantir o transporte de criptografia na Web. Outra incerteza sobre a criptografia das curvas elípticas

[4] Método para contornar autenticação casual e garantir acesso a um determinado sistema

está relacionada com patentes. Existem mais de 130 patentes que cobrem usos específicos de curvas elípticas de propriedade da BlackBerry (através da aquisição da Certicom de 2009). Muitas dessas patentes foram licenciadas para uso por organizações privadas e até mesmo a NSA. Isso tem dado alguns programadores algo em que pensar antes de realizarem qualquer tipo de ação.

A assinatura digital ECDSA tem uma desvantagem em relação ao RSA na medida em que requer uma boa fonte de entropia. Sem aleatoriedade adequada, a chave privada pode ser revelada. Uma falha no gerador de números aleatórios no Android permite a *hackers* encontrar a chave privada ECDSA usada para proteger as carteiras Bitcoin de várias pessoas na implementação início de 2013. O ECDSA da Sony PlayStation tinha uma vulnerabilidade similar. Uma boa fonte de números aleatórios é necessária na máquina fazendo as assinaturas. Dual_EC_DRBG não é recomendado.

4.2.5. Encriptação

Um algoritmo de encriptação define um tipo de transformação de dados que não é facilmente reversível para utilizadores não autorizados. A escolha sobre o algoritmo a utilizar pode definir o sucesso ou insucesso da segurança de uma aplicação. Existem diversos algoritmos de encriptação disponíveis e estes são apresentados sucintamente de seguida:

- DES – o antiquado algoritmo já não deve ser utilizado devido à sua fraca chave de encriptação, o seu sucessor 3DES (triplo DES) ainda é considerado seguro mas não a melhor opção;
- RSA – é um algoritmo de chaves públicas que utiliza tamanhos de chaves entre 2048 e 4096 bits e é baseado em exponenciação modular;
- AES – surge como substituto do DES e atualmente o padrão do NIST. Vem com as versões de 128, 192 e 256 bits.

Para o projeto em causa, foi considerado o algoritmo de encriptação AES (*Advanced Encryption Standard*). Este algoritmo é baseado no princípio de substituição e permutação, ou seja, uma série de operações matemáticas utilizadas em blocos de cifras do algoritmo. Estes blocos possuem um tamanho fixo de 128 bits. Ao contrário do DES, que utiliza a rede *Feistel* [5], este é uma variação de *Rijndael* que é a nova geração de blocos de cifra simétricos. Esta utiliza, de acordo com o tamanho da chave escolhida, um determinado número de repetições de transformação de dados:

- 10 Ciclos de repetição para chaves de 128 bits;

[5] Estrutura simétrica de construção de blocos de cifra.

- 12 Ciclos de repetição para chaves de 192 bits;
- 14 Ciclos de repetição para chaves de 256 bits;

Cada ciclo consiste num conjunto de quatro passos semelhantes mas diferentes a serem aplicados na informação a encriptar que no final irá o texto cifrado (*cyphertext*). Existe um outro conjunto de passos a aplicar quando se pretende transformar texto cifrado de volta ao original.

Encriptação autenticada

Ao utilizar o algoritmo AES, existem diversos modos que este pode implementar para reforçar a segurança ou adicionar novas funcionalidades. Existe um conjunto muito variado mas os mais comuns são apresentados de seguida. Todos eles suportam Associated Data (AD) o que significa que suportam a utilização de um cabeçalho não encriptado na mensagem opcional. Além disso, todos eles necessitam de uma chave única e de um vetor de inicialização (nonce [6]).

[6] Número arbitrário utilizado apenas uma única vez (daí o nome) numa comunicação criptográfica para prevenir ataques *replay*.

	GCM (Galois Counter Mode)	OCB (Offset Codebook Mode)	EAX	CCM
Velocidade de encriptação/desencriptação	Rápido	Muito rápido	Lento	Lento
Dificuldade de implementação	Difícil	Fácil	Fácil	Fácil
Implementações existentes	Sim	Não	Sim	Sim
On-line [a]	Sim	Sim	Sim	Não
Patenteado	Não	Sim	Não	Não

Tabela 4.1.: Comparação de modos de encriptação autenticada

[a] Modos *on-line* significa que não é necessário saber, previamente, o tamanho da mensagem antes de começar a encriptar ou desencriptar.

Tendo em conta os resultados apresentados, a escolha ideal seria OCD devido à sua facilidade de implementação e capacidade de processamento, no entanto não existem implementações disponíveis (gratuitas pelo menos) devido ao facto de esta ser patenteada. Logo a escolha recaiu sobre o modo GCM. Este modo tornou-se bastante popular e existem boas implementações do mesmo disponíveis. Além disso, é um modo que oferece além da confidencialidade (encriptação), integridade e autenticidade. É também conhecido pela sua capacidade de processamento.

Resumindo, para implementar a encriptação das comunicações neste projeto será utilizado o algoritmo AES com uma chave de 256 bits em modo GCM (AES_256_GCM).

4.3. Aplicação móvel

Dando continuidade a um dos principais objetivos do projeto de trabalhar com tecnologias *open-source*, foi decidido desenvolver uma aplicação móvel para a plataforma Android. Tendo em conta as respostas às questões de pesquisa 2 e 3, sobre os requisitos funcionais e não funcionais, foi realizado um estudo mais atento e feitas algumas alterações dando origem às seguintes listagens:

Objetivos funcionais

- Autenticação do utilizador;
- Bloqueio/desbloqueio da fechadura através de um dispositivo móvel;
- Registo de bloqueios/desbloqueios;
- Transmissão de chaves eletrónicas;
- Transmissão do domínio (*ownership*) de uma fechadura para outro dispositivo;
- Alertas sobre o estado da fechadura para o utilizador (bateria, temperatura do computador, etc.).

A autenticação do utilizador foi acrescentada como mais um fator de segurança na aplicação em caso de perda do dispositivo. Dado que o canal de comunicação será Bluetooth, não existirá qualquer forma de revogação de dispositivos à distância, logo é imperativo que o telemóvel se encontre o mais protegido possível. Esta autenticação irá ser baseado na introdução de um código numérico de quatro ou mais dígitos. Este tipo de sistema já é conhecido para os utilizadores no caso do processo de autorização em cartões SIM e em certezas aplicações móvel de *cloud storage* como Dropbox [7] e Mega [8]. Quanto à transmissão de domínio, chegou-se à conclusão que seria importante para uma pessoa que viva com mais pessoas para no caso empresarial com múltiplos funcionários e hierarquias, que exista uma transmissão de domínio em que todas as chaves do dono anterior são eliminadas e criadas novas para o novo dono. Por fim, existe a necessidade de manter os utilizadores da fechadura informados sobre o estado da mesma. Este objetivo deve-se essencialmente à preocupação com os níveis de bateria do dispositivo.

Objetivos não funcionais

- Segurança
  - Excluir a possibilidade de backups por parte de aplicações de terceiros ou do sistema operativo;
  - Integração de um teclado virtual para introdução do PIN na autorização do utilizador;
  - Ignorar/bloquear todas as tentativas de comunicações superiores a um determinado raio da fechadura (ex.: 4 metros);
- Baixos consumos de bateria por parte da aplicação;
- Rápido processamento no bloqueio/desbloqueio da fechadura.

Em relação aos requisitos não funcionais, foi simplesmente expandido o da segurança tendo em conta algumas variáveis de teor técnico. A primeira surge como prevenção de roubo de dados por parte de aplicações de terceiros (i.e. aplicação de cópia de segurança de dados) às informações contidas no dispositivo móvel. A segunda, para evitar que aplicações de terceiros, com capacidades de acesso ao *input* do teclado consigam ler quais os códigos utilizados para o acesso à aplicação. Por fim, a terceira surge como tentativa conjunta, da aplicação móvel e do dispositivo da fechadura, de diminuir o risco de segurança das comunicações Bluetooth.

[7] `https://dropbox.com/`
[8] `https://mega.nz/`

4.3.1. Design

Para facilitar o desenho da aplicação programaticamente, foram desenvolvidos esboços dos três principais ecrãs da aplicação móvel. Além da segurança, o segundo objetivo mais importante da aplicação móvel era o da simplicidade, logo foi tentado atingir um design global "limpo" e visualmente agradável mas que ao mesmo tempo se mostrasse como uma aplicação robusta e segura.

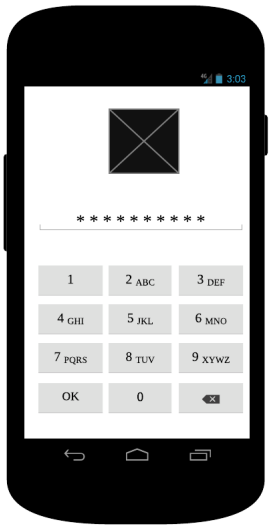

Figura 4.4.: Ecrã 1 (Introdução do PIN)

Figura 4.5.: Ecrã 2 (Vista de fechaduras)

Ao observar o ecrã 1, é possível ver o ecrã de autorização do utilizador. Este ecrã é composto por uma caixa de texto e 12 botões que formam o teclado numérico virtual que permitirá ao utilizador inserir o seu PIN de segurança.

Após autorização, o utilizador é conduzido para o segundo ecrã. Aqui é possível visualizar rapidamente todas as fechaduras a que este smartphone está associado. Uma fechadura associada pode ser uma que ele possui ou outra fechadura que um utilizador tenha partilhado com ele. Caso seja uma fechadura partilhada, aparecerá um icon demonstrativo da lado direito da linha alinhado com o nome da mesma.

Figura 4.6.: Ecrã 3 (Vista de detalhe de fechadura)

Por fim, ao selecionar uma das fechaduras associados ao aparelho, sucede-se o ecrã número 3. No topo, pode ser visto um ícone de uma fechadura ou aloquete representativo do estado da fechadura (aberta ou fechada) juntamente com a descrição textual por baixo. Imediatamente em baixo, está uma listagem de definições que permitem ao utilizador configurar parâmetros como: abertura automática da porta por aproximação e respetiva hora para o evento, nome da fechadura, entre outros. No final do ecrã, são mostrados (caso o utilizador atual seja o dono da fechadura) os outros utilizadores com a qual a fechadura está a ser partilhada naquele momento. A qualquer momento estes podem revogar estas permissões clicando no ícone alojado na extremidade direita de cada outro utilizador.

4.3.2. Desenvolvimento

A maior parte do desenvolvimento da aplicação foi baseado na gestão de ligações Bluetooth e transmissão de dados, assim como na segurança da mesma. A plataforma Android fornece um excelente suporte sobre a *stack* Bluetooth através das APIs Bluetooth para Android. Este conjunto de APIs permite às aplicações ligarem-se a outros dispositivos Bluetooth. Com a utilização destas APIs Bluetooth, é possível:

- Procurar por dispositivos Bluetooth
- Interrogar o adaptador Bluetooth sobre dispositivos já emparelhados
- Estabelecer canais RFCOMM
- Estabelecer ligações com outros dispositivos

- Transferir dados entre dispositivos
- Gerir múltiplas ligações

Desde a versão de Android 4.3 (API 18) que foi introduzido suporte para a mais recente versão da tecnologia Bluetooth de baixo consumo (*Blueooth Low Energy - BLE*). Eis alguns conceitos básicos sobre BLE:

- *Generic Attribute Profile* (GATT) - Este perfil é um especificação geral para enviar e receber pequenos dados entre dispositivos Bluetooth ligados entre si. Um perfil é uma especificação sobre como um dispositivo se deve comportar em determinadas situações. Apesar de todas as ligações atuais se basearem neste perfil, a Bluetooth SIG tem mais perfis definidos que podem ser implementados
- *Attribute Protocol* (ATT) - o GATT é desenvolvido em cima deste protocolo e também pode ser referido como GATT/ATT. O ATT foi otimizado para "correr" em dispositivos BLE e para isso consome o mínimo de *bytes* possíveis. Cada atributo neste protocolo está identificado, de forma uniforme, com um identificador único universal (UUID) de 128 *bits* para identificar as informações. Os atributos transportados pelo ATT são formados por características e serviços
- Característica - uma característica contém um único valor e 0-n descritores que descrevem o valor da característica
- Descritor - os descritores podem ser definidos como atributos que definem os valores das características. Podem, por exemplo, especificar uma descrição facilmente lida por um humano, um conjunto de valores ou uma unidade de medida
- Serviço - um serviço é um conjunto de características

Bluetooth

De modo a efetuar a uma ligações entre dois dispositivos Bluetooth (criar um *link*) é necessário efetuar primeiro uma pesquisa sobre equipamentos disponíveis e visíveis no raio de alcance. Para realizar uma pesquisa de dispositivos Bluetooth, é possível utilizar o seguinte método:

Listing 4.1: Exemplo de pesquisa Bluetooth

```
public class DeviceScanActivity extends ListActivity {
  private BluetoothAdapter mBluetoothAdapter;
  private boolean mScanning;
  private Handler mHandler;
```

```
    // Stops scanning after 10 seconds.
  private static final long SCAN_PERIOD = 10000;

  private void scanLeDevice(final boolean enable) {
    if (enable) {
            // Stops scanning after a pre-defined scan period.
      mHandler.postDelayed(new Runnable() {
        @Override
        public void run() {
          mScanning = false;
          mBluetoothAdapter.stopLeScan(mLeScanCallback);
        }
      }, SCAN_PERIOD);

      mScanning = true;
      mBluetoothAdapter.startLeScan(mLeScanCallback);
    } else {
      mScanning = false;
      mBluetoothAdapter.stopLeScan(mLeScanCallback);
    }
  }
}
```

Fatores a ter em conta quando e pesquisa dispositivos Bluetooth:

- Assim que o dispositivo pretendido aparece, parar de imediato a pesquisa
- Nunca executar pesquisas num *loop*
- Um dispositivo pretendido pode já ter uma ligação, logo deve-se verificar as ligações atuais antes de efetuar uma pesquisa
- Definir um tempo limite de pesquisa

Tudo isto são fatores importantes, principalmente quando se trata de dispositivos com BLE. Para estabelecer uma ligação com o servidor GATT do dispositivo, basta executar o seguinte método:

Listing 4.2: Conexão a outro dispositivo Bluetooth

```
mBluetoothGatt = device.connectGatt(this, false, mGattCallback);
```

Após a ligação estar estabelecida, é devolvida uma instância do *BluetoothGatt* que irá permitir realizar um conjunto de ações do cliente. No exemplo a seguir, temos um serviço

que permite estabelecer ligações, mostrar dados e serviços e características GATT através do dispositivo.

Listing 4.3: Exemplo de serviço Bluetooth

```
public class BluetoothLeService extends Service {
  private final static String TAG =
  BluetoothLeService.class.getSimpleName();

  private final BluetoothGattCallback mGattCallback =
  new BluetoothGattCallback() {
    @Override
    public void onConnectionStateChange(
      BluetoothGatt gatt,
      int status,
      int newState
    ) {
      // Handle connection state change
    }

    @Override
    // New services discovered
    public void onServicesDiscovered(
      BluetoothGatt gatt,
      int status
    ) {
      // Handle service discovery
    }

    @Override
    // Result of a characteristic read operation
    public void onCharacteristicRead(
      BluetoothGatt gatt,
      BluetoothGattCharacteristic characteristic,
      int status
    ) {
      // Handle characteristic read
    }
  };
}
```

Segurança

De acordo com a secção de segurança do capítulo corrente, era esperado implementar um sistema de troca de chaves Diffie-Hellman utilizando curvas elípticas e encriptar todas as mensagens com o algoritmo AES em modo GCM. Para trazer este tipo de capacidades para os dispositivos Android, é utilizada a coleção de bibliotecas Java denominada **Bouncy Castle**. A Bouncy Castle é um conjunto de APIs mantidas por uma instituição de caridade Australiana, a *Legion of the Bouncy Castle, Inc.* No entanto, a Bouncy Castle só começou a suportar curvas elípticas a partir da versão 4.0 do sistema operativo (possivelmente para poupar espaço). Para solucionar isto, é possível incluir a coleções de APIs Bouncy Castle manualmente mas daí advinham alguns problemas no conflito de nomenclaturas de classes. Para solucionar esses problemas, foi utilizada a versão cujo nome do pacote foi modificado e que se denomina por **Spongy Castle**. Ao incluir os ficheiros Java, esta biblioteca pode ser incluída importando a coleção de APIs:

```
import org.spongycastle.jce.provider.BouncyCastleProvider;
```

E, de seguida, adicionado um novo fornecedor através da classe central de segurança de Android:

```
Security.addProvider(new BouncyCastleProvider());
```

A partir deste ponto é possível criar um novo par de chaves através da metodologia de curvas elípticas:

Listing 4.4: Geração de chaves pública e privada usando curvas elípticas

```
private void generateNewECDHKey() {
  ECGenParameterSpec ecParamSpec = new ECGenParameterSpec(
    "secp256k1"
  );
  KeyPairGenerator kpg = KeyPairGenerator.getInstance(
    "ECDH",
    "SC"
  );
  kpg.initialize(ecParamSpec);

  KeyPair deviceKeyPair = kpg.generateKeyPair();

  String pubStr = Crypto.base64Encode(
    deviceKeyPair.getPublic().getEncoded()
  );
  String privStr = Crypto.base64Encode(
    deviceKeyPair.getPrivate().getEncoded()
```

```
    );
}
```

Após a chaves serem geradas, a chave pública deve ser enviada para a outra entidade e a partir deste momento ambas podem começar a trocar mensagens encriptadas. Para tal, foi utilizada a classe *Cipher* de Android que permite a encriptação de mensagens conforme os requisitos deste projeto.

Listing 4.5: Encriptação/desencriptação de mensagens

```
public SecurityHelper() {
  c = Cipher.getInstance("AES/GCM/PKCS5Padding");
}

public String encrypt(SecretKey secret, String cleartext) {
  byte[] iv = generateIv();
  String ivHex = HexEncoder.toHex(iv);
  IvParameterSpec ivspec = new IvParameterSpec(iv);

  encryptionCipher.init(c.ENCRYPT_MODE, secret, ivspec);
  byte[] encryptedText = encryptionCipher.doFinal(
    cleartext.getBytes("UTF-8")
  );
  String encryptedHex = HexEncoder.toHex(encryptedText);

  return ivHex + encryptedHex;
}

public String decrypt(SecretKey secret, String encrypted) {
  String ivHex = encrypted.substring(0, IV_LENGTH * 2);
  String encryptedHex = encrypted.substring(IV_LENGTH * 2);
  IvParameterSpec ivspec = new IvParameterSpec(
    HexEncoder.toByte(ivHex)
  );
  c.init(c.DECRYPT_MODE, secret, ivspec);
  byte[] decryptedText = c.doFinal(
    HexEncoder.toByte(encryptedHex)
  );
  String decrypted = new String(decryptedText, "UTF-8");

  return decrypted;
```

}

Neste pequeno excerto de código é possível verificar como encriptar e desencriptar mensagens provenientes da fechadura eletrónica. Ambas as funções começam pela iniciação e geração dos parâmetros necessários para realizar as operações pretendidas, como a geração de um vetor de inicialização (*generateIv()*). Após existir um vetor de inicialização (VI), a cifra é iniciada com o modo correspondente, a chave privada gerada anteriormente e o VI. Após estes passos, basta aplicar uma última função (*doFinal()*) para finalizar a transformação de múltiplas partes e assim retornar os bytes da mensagem em questão.

4.4. Mecanismo da fechadura

Dado o âmbito do projeto atual, o dispositivo de acesso desenvolvido utilizando o BealgeBone Black, não tem qualquer integração com uma fechadura eletrónica, pelo que este estudo focou-se na parte "inteligente" da solução. Este dispositivo tem portanto, as mais básicas das funcionalidades, receber e enviar dados relativos ao acesso à fechadura, enviar dados sobre o estado desta e controlar os acessos por parte dos utilizadores.

Objetivos funcionais

- Verificar autorização de chaves eletrónicas
- Realizar operações de bloqueio e desbloqueio da fechadura (não abordado)
- Registo de acesso
- Transmissão de informações para o dono da fechadura

Sempre que existir uma transmissão de chaves eletrónicas, este processo deve ficar registado na fechadura para que esta possa aceder às chaves disponíveis e deste modo conseguir autorizar ou não a entrada de um qualquer sujeito. Este processo implica a proximidade física de todos os intervenientes no processo, dada a limitação de alcance do canal de comunicação. Esta é vista como uma clara desvantagem para o consumidor mas é uma forte característica de segurança que previne, a um elevado nível, os ataques de interceção de comunicações. Em relação à transmissão de informações, será realizada uma verificação diária (ou de outra frequência conforme as necessidades de cada parâmetro) sobre o estado da fechadura (memória interna, temperatura do computador, bateria, etc.) e após esta verificação, da próxima vez que o dono da fechadura se aproximar desta, recebe imediatamente um alerta sobre as informações recolhidas, assim como um atualizado registo de entradas e saídas.

Em relação aos objetivos não funcionais, estes passam por objetivos semelhantes dos já mencionados para a aplicação móvel ou por completa-los de alguma maneira.

4.4.1. Ligações Bluetooth

Para conseguir interagir com a *stack* Bluetooth no BeagleBone Black, foi primeiro necessário ativar o serviço. Para tal, foi acedido ao ficheiro de configurações `/var/lib/connman/settings` e adicionada as linhas:

```
[Bluetooth]
Enable=true
```

De seguida, é necessário autorizar o serviço de sistema Bluetooth. Isto irá permitir que o BeagleBone Black possa ser emparelhado com outros dispositivos e realizar outras operações relacionadas com Bluetooth

```
systemctl enable bluetooth.service
```

Não ocorrendo nenhum erro depois deste processo, é necessário iniciar o serviço com seguinte comando:

```
systemctl start bluetooth.service
```

Neste momento, o serviço Bluetooth encontra-se ativo e em funcionamento. A partir deste ponto, é possível manipular ligações e realizar outro tipo de operações utilizando a camada HCI (*Host Controller Interface*) da arquitetura Bluetooth. Esta camada fornece uma interface para o *baseband controller*, para o *link manager* e aos parâmetros de configurações. Deste modo, existe uma forma unificada de acesso às capacidades *baseband* do Bluetooth.

Tal como mencionado anteriormente, todo o desenvolvimento feito no BeagleBone Black é realizado através de um navegador acedendo à placa remotamente e todo o controlo é realizado através de um qualquer cliente SSH, como por exemplo **PuTTY**. Ao aceder através deste cliente e nos autenticarmos, temos acesso a um terminal para o sistema operativo Linux ou podemos realizar múltiplas tarefas. Uma delas, é a utilização da ferramenta `hcitool` para aceder à camada HCI da *stack* Bluetooth para Linux, o **BlueZ**. Esta ferramenta serve para configurar ligações Bluetooth. Os comandos mais utilizados para as configurações necessárias e presentes num ficheiro de configurações iniciais eram:

- `hciconfig -a hci0` - sendo "hci0" a interface a que queremos aceder, este comando permite obter um estado completo sobre esta;
- `hciconfig hci0 reset` - este comando restaura todas as definições padrão;
- `hciconfig hci0 name <NOME A ATRIBUIR>` - este comando permite definir o nome pela qual o BeagleBone Black aparece nas pesquisas de outros dispositivos.

Sendo que nas situações estudadas o BeagleBone Black irá ser o *slave* da ligação, este apenas terá que ser emparelhado uma primeira vez com o dispositivo móvel em questão e escutar por comunicações. Para efeitos de segurança, o BeagleBone Black encontra-se num modo de *no scan*, ou seja, não está visível para outros dispositivos Bluetooth por perto que

tentem pesquisar por novos equipamentos para emparelhar. Deste modo, foi idealizado um sistema que permita, ou pressionar um botão no BeagleBone Black, este mude o modo do Bluetooth do mesmo e volte a restaurar o seu estado passados uns segundos. O esquema seria idealizado como a seguinte figura ilustra:

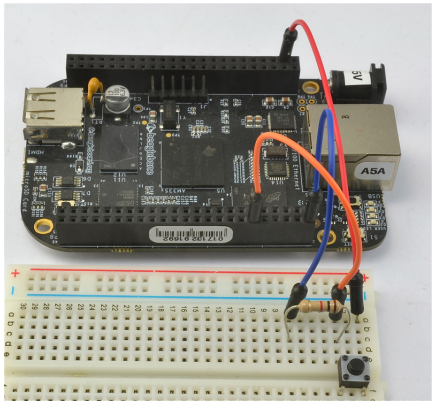

Figura 4.7.: Esquema de ligação de botão ao BeagleBone Black (Monk, 2013)

Este esquema deve ser montado de com o computador desligado de modo a garantir que todos os pins GPIO estão no seu estado de *input*. Após estar concluída a montagem, o seguinte código irá ser executado sempre que existir um pressionar do botão:

Listing 4.6: Ativação da disponibilidade de pesquisa *page* e *inquiry*

```
var exec = require('child_process').exec;
var b = require('bonescript');
var TIMEOUT = 30000;

b.pinMode("P8_12", b.OUTPUT);

setInterval(buttonPushListener, 100);

function buttonPushListener() {
  var state = GPIO.input("P8_12");

  if (state == 1) {
    piScan();
  }
}

function piScan() {
  exec('hciconfig hci0 piscan', function(
```

```
    error,
    stdout,
    stderr
  ) {
    setTimeout(noScan, TIMEOUT);
  });
}

function noScan() {
  exec('hciconfig hci0 noscan', function(
    error,
    stdout,
    stderr
  ) {
    b.pinMode("P8_12", b.OUTPUT);
  });
}
```

O que este código faz é "escutar" pela mudança de estado do GPIO PIN8_12 e, caso houvesse uma mudança no mesmo, executar o comando `hciconfig hci0 piscan` que habilita imediatamente as pesquisas do tipo *scan* e *inquiry*. A pesquisa *inquiry* é a que permite a um dispositivo Bluetooth ser encontrado por outros, enquanto que a *page* é a que permite conexões com outros dispositivos. Passados trinta segundos, é executada a função de *callback* que volta a repor a "invisibilidade" do dispositivo executando o comando `hciconfig hci0 noscan` e voltando a colocar o estado do GPIO ao seu estado original `b.pinMode("P8_12", b.OUTPUT)`.

4.4.2. Transmissão de dados Bluetooth

Tal como mencionado, a fechadura irá ter a necessidade de envio de dados ocasionalmente. Após existir uma ligação segura entre o BeagleBone Black e o dispositivo móvel, estes podem trocar informações a qualquer altura. A transmissão de dados utilizando *bonescript* é bastante simples e pode ser conseguido da seguinte maneira:

Listing 4.7: Envio de mensagens Bluetooth

```
var bt_serial_port = require('bluetooth-serial-port');
var bt_serial = new (bt_serial_port).BluetoothSerialPort();
var msg = new Buffer('Hello Android');

bt_serial.connect('00:10:60:AA:36:F8', 23);
bt_serial.write(msg, function(err, bytesWritten) {
```

```
  // Handle response
});
```

O que este pequeno excerto de código demonstra é como iniciar uma ligação Bluetooth com o dispositivo pretendido através da *BluetoothSerialPort*. No caso apresentado, é efetuada uma ligação ao endereço `00:10:60:AA:36:F8` através do canal `23`. Depois é criado um *buffer* contendo a mensagem que pretendida e utilizando a função `write`, esta é enviada para o dispositivo em questão.

4.4.3. Receção de dados Bluetooth

Tal como a necessidade de envio de dados, também existe a necessidade de receção de dados. Para isso, a aplicação deve estar constantemente a "escutar" por tentativas de envio de dados por parte de terceiros.

Listing 4.8: Receção de mensagens Bluetooth

```
var bt_serial_port = require('bluetooth-serial-port');
var bt_serial = new (bt_serial_port).BluetoothSerialPort();

bt_serial.on('data', function(data) {
  console.log('data received: ' + data);
});
```

O que este pequeno excerto de código demonstra é um simples *listener* que fica em espera até que sejam enviados dados para a fechadura e tem como *callback* uma função para tratar dos dados de acordo.

4.4.4. Segurança

De acordo com a secção de segurança do capítulo corrente, era esperado implementar um sistema de troca de chaves Diffie-Hellman utilizando curvas elípticas e encriptar todas as mensagens com o algoritmo AES em modo GCM. O Node.js presente no BeagleBone Black vem com um módulo instalado chamado `crypto` que possui um leque de operações criptográficas de modo a facilitar a sua utilização. Utilizando esse módulo, é possível criar as chaves públicas e privadas.

Listing 4.9: Geração de chaves ECDH

```
var crypto = require('crypto');
var ECDH = crypto.createECDH('secp256k1');
var pubKey = ECDH.generateKeys('base64');
```

Neste pequeno excerto de código é possível verificar como são criadas as chaves pública e privada da fechadura. Depois de requerida a biblioteca necessária, é criada uma instância da

classe ECDH utilizando a curva `secp256k1`. Estas curvas são *arrays* de objetos com valores predefinidos que representam os parâmetros de criação de curvas elípticas. No caso da curva escolhida, os valores são os seguintes:

Listing 4.10: Parâmetros da curva elíptica

```
"secp256k1": {
  "p": "fffffffffffffffffffffffffffffffe
␣␣␣␣ffffffffffffffffffffffffefffffc2f",
  "a": "00",
  "b": "07",
  "n": "fffffffffffffffffffffffffffffffe
␣␣␣␣baaedce6af48a03bbfd25e8cd0364141",
  "h": "01",
  "Gx": "79be667ef9dcbbac55a06295ce870b
␣␣␣␣07029bfcdb2dce28d959f2815b16f81798",
  "Gy": "483ada7726a3c4655da4fbfc0e1108
␣␣␣␣a8fd17b448a68554199c47d08ffb10d4b8"
}
```

A criação de chaves deve ser um passo a ser tomado durante o processo de configuração e após isso, as chaves devem ser armazenadas encriptadas no dispositivo. Após a criação da instância da classe ECDH, é possível verificar qual o segredo partilhado, com a função `ECDH.computeSecret(chave_publica[, input_encoding][, output_encoding])`, sendo que os parâmetros necessários são: a chave pública da outra entidade e o tipo de *encoding* de entrada e saída. A partir do momento em que temos as chaves pública e privada, assim como a chave pública da outra parte, é possível iniciar o processo de encriptação e desencriptação de mensagens através de um canal inseguro. Como a biblioteca de funções `crypto` não oferece o modo GCM para encriptação em AES, foi utilizada outra biblioteca para o efeito.

Listing 4.11: Encriptação/desencriptação de mensagens

```
var aes_gcm = require('node-aes-gcm');
var encryptedMsg = aes_gcm.encrypt(key, iv, data, aad);
var decryptedMsg = aes_gcm.decrypt(key, iv, data, aad, auth_tag);
```

Sendo que os parâmetros das funções são os que se seguem:

- *key* - Chave AES utilizada para a encriptação;
- *iv* - Vetor de inicialização;
- *plaintext* - texto a ser encriptado;

- *aad* - objeto que representa *additional authenticated data*, não está encriptado mas serve como autenticação para *authentication tag*;
- *authentication tag* - objeto que contém informação que verifica a autenticidade e correção de dados encriptados e da *aad*.

Juntando todo o código apresentado nesta secção, é possível efetuar todas as comunicações com segurança sobre um canal inseguro.

4.5. Sumário

Neste capítulo foi possível encontrar descrições técnicas detalhadas sobre a solução apresentada para esta tese. Foram demonstrados os pontos essenciais de cada componente da solução e ficou conhecida qual a plataforma em que a aplicação móvel iria ser desenvolvida, o Android. Além disso, foi apresentado um estudo sobre uma possível implementação de um esquema de segurança idealizado para esta solução. No final, ficaram a ser conhecidas todas as componentes da solução proposta e como implementar as mais básicas funcionalidades desta. A partir deste ponto, é possível responder à quinta e última questão de pesquisa apresentada na introdução deste documento.

SQ-4: "Qual o software necessário para uma fechadura eletrónica?"

Tendo em conta as tecnologias utilizadas, são aqui listadas todas as ferramentas necessárias para o desenvolvimento da fechadura eletrónica e todas as bibliotecas necessárias para cada componente.

- Aplicação móvel
  - *Software*: Android Studio [9]
  - Bibliotecas:
    - *Spongy Castle* [10]
- Mecanismo da fechadura
  - *Software*:
    - *Browser*
    - Cloud9
    - PuTTY
  - Bibliotecas
    - *bonescript* [11]

[9] `https://developer.android.com/sdk/index.html`
[10] `https://rtyley.github.io/spongycastle/`
[11] `http://beagleboard.org/Support/BoneScript`

* *crypto* [12]
* *node-aes-gcm* [13]

Todo o *software* aqui listado é, de alguma forma, gratuito e pode ser utilizado livremente. Em relação às bibliotecas apresentadas, cada uma delas deve ser utilizada segunda a licença que possui.

[12] `https://www.npmjs.com/package/crypto`
[13] `https://www.npmjs.com/package/node-aes-gcm`

Capítulo

5 Análise e conclusões

Neste capítulo será apresentada uma validação do trabalho desenvolvido e demonstrados os resultados desse mesmo trabalho. Serão revistas todas as perguntas de pesquisa apresentadas neste documento e respondida a questão principal que esta tese se propôs a responder. Por fim, serão também realizadas comparações com as fechaduras analisadas no segundo capítulo face aos parâmetros mais pertinentes do mesmo, de modo a conseguir obter algum grau de comparação entre soluções empresariais e com algum grau de maturidade e uma solução "caseira", construída com componentes exclusivamente *open-source*.

5.1. Comparações e análise

De modo a conseguir responder à pergunta de pesquisa principal, serão aqui abordados alguns dos tópicos de comparação entre fechaduras utilizados no segundo capítulo para determinar se a solução apresentada é, efetivamente, viável de construir e se é capacitada das mesmas habilidades que as outras.

5.1.1. Visão global

A solução apresentada neste documento não será certamente um substituto para as soluções existentes atuais, não devido ao grau de maturidade dos produtos existentes mas também em relação a toda uma infraestrutura por trás destes. Esta fechadura declara-se sim, como uma solução completamente *open-source* e baseada em componentes não proprietários. A documentação aqui apresentada poderá servir para quem quiser prosseguir o trabalho deste tópico para quem quiser implementar a sua própria solução caseira.

Desde há alguns meses atrás que esta solução, no que toca ao preço, seria a mais vantajosa de todas aqui apresentadas, no entanto, e com a evolução dos produto existentes, ficou muito difícil de competir com o preço apresentado pela **Lockitron** ($99). Continuando

esta uma solução mais barata, o que é apresentado por um preço semelhante é difícil de comparar em termos de tecnologia disponível. Apesar de tudo isto, e como falamos de projetos *open-source*, qualquer pessoa interessada e com conhecimentos técnicos para tal poderá copiar o projeto BeagleBone disponível na plataforma upverter (`https://upverter.com/Beagle/afdfe0be7c0bcec5/BeagleBoneBlack/`).

5.1.2. "Chaves" e gestão de acessos

Em relação às chaves e gestão dos acessos, a solução aqui apresentada funciona como a maior parte das fechaduras existentes, através das *eKeys*. Tal como nas soluções existentes, também a estas chaves é possível associar um tempo limite de utilização, bem como utilizações recorrentes. Uma adição em relação ao acesso restrito das outras soluções que foi idealizado para esta, e graças ao registo de utilizações da fechadura, foi associar a cada chave um número de utilizações máximo. Este novo tipo de restrição pode ser útil quando se pretende oferecer acesso a um local apenas uma vez mas não é possível identificar a hora exata de chegada do convidado. Em relação a níveis de acesso, esta solução assemelha-se à **August**, oferecendo dois níveis de acesso:

- Dono
  - Modificar configurações da fechadura
  - Gerir convidados
  - Transferência de domínio (transferir o seu papel de dono para outra pessoal)
  - Bloquear/desbloquear fechaduras
- Convidado
  - Bloquear/desbloquear fechaduras

Quanto à transmissão de chaves em si, esta solução é, de alguma maneira, limitada. Dado o canal de comunicação ser única e exclusivamente Bluetooth, não existem comunicações a largas distâncias o que significa que as chaves eletrónicas não podem ser enviadas. O que acontece neste caso, é que existe um processo de registo de um dispositivo móvel quando se pretende fornecer acesso a terceiros. Num primeiro passo, mal a fechadura é instalada, o dono da fechadura inicia o processo de registo pressionando o botão descrito no capítulo anterior. A partir deste momento, a fechadura encontra-se disponível para receber ligações e o dispositivo móvel fica registado como "dono" através do endereço Bluetooth. No caso do registo de terceiros, a pessoa em causa deve estar fisicamente próxima da fechadura, bem como o dono, e pressionando o botão descrito no capítulo da solução, a pessoa poderá "registar-se" como "visitante". A qualquer momento o dono poderá revogar estes acesso sem que a pessoa

em causa esteja fisicamente por perto. Todos os processo de registo passam pela troca de chaves descrita no capítulo anterior como forma de autenticação.

Esta é, sem dúvida, uma forma algo "primitiva" de realizar esta operação mas é um método que apesar das dificuldades se torna bastante seguro e com um grau de ataques bastante baixo. Em comparação com as restantes fechaduras, esta perde então em comodidade mas fica à frente no que toca a segurança.

5.1.3. Mecanismo de bloqueio/desbloqueio

O mecanismo de bloqueio/desbloqueio da solução desta tese é bastante simples. Apesar de não ter existido qualquer integração com uma fechadura eletrónica, foi estudada a possibilidade de futura integração com uma. A maneira como as fechaduras eletrónicas funcionam é diferente das fechaduras normais. Dentro das fechaduras eletrónicas existe um componente chamado *deadbolt*, que é o que mantém a porta trancada. Para este componente se manter fechado, existe um outro componente eletromagnético ligado. Quando é passada corrente pelo componente eletromagnético, este permite que a porta se abra. O que seria pretendido com a integração com a fechadura eletrónica seria um controlo do BeagleBone Black em relação à corrente que passava para a fechadura em si. Deste modo, seria possível enviar comandos que ditariam o estado da fechadura.

Ao contrário das soluções atuais, não foi idealizado nenhum método de abertura automático pois, tal como referido, este tipo de "atalhos" vem com demasiadas falhas de segurança associadas. O que seria possivelmente interessante, era o estudo e análise da tecnologia (infelizmente proprietária) utilizada pela **Unikey** em relação às aberturas automáticas. De maneira a conseguir detetar se a pessoa que está a tentar abrir a porta se encontra do lado seguro ou inseguro.

5.1.4. Comunicação

Tal como já mencionado, a solução apresentada encontra-se dotada apenas de comunicações Bluetooth, fazendo uso da nova tecnologia BLE. Enquanto que as outras fechaduras se encontram equipadas de outras tecnologias de comunicações, a solução aqui apresentada foi idealizada para um funcionamento básico mas funcional. A inclusão exclusiva de Wi-Fi esteve sempre de parte devido às limitações da tecnologia e das possíveis falhas de segurança. Quando um dispositivo se encontrava ligado apenas por Wi-Fi existem muitos fatores que podem correr mal, como: falha de Internet, comunicações lentas, falhas de energia, entre outras. No entanto, não existe qualquer impedimento de, no futuro, estudar a possibilidade de incluir outras tecnologias de comunicação de forma a melhorar esta solução. Não só de Wi-Fi e NFC mas também pensar em algo como a **Danalock** e estudar a possibilidade de incluir a tecnologia Z-Wave.

5.1.5. Segurança

Em relação ao tópico de segurança é bastante difícil fazer comparações dada a pouca especificidade e detalhe sobre a segurança das outras fechaduras. Tal como mencionado na secção de segurança da descrição da solução, foi idealizado um protocolo de autenticação específico para este caso de uso e este só poderia ser posto à prova em ambientes reais e com a validação dos devidos especialistas. No entanto, para o âmbito deste projeto, acredita-se que a solução apresentada é robusta e segura o suficiente. Sendo que, para um ambiente de utilização real, seria interessante explorar outros ângulos em relação à segurança lógica da solução.

5.1.6. Bateria e falhas de energia

Em relação à bateria, podemos encontrar a solução nas capas descritas no capítulo 3 para o BeagleBone Black. Existem algumas soluções no mercado atual mas apresenta-se aqui uma hipótese de uma capa de bateria:

Figura 5.1.: Capa de bateria para o BeagleBone Black (Wiki)

Esta capa fornece uma solução de bateria portátil para os dispositivos BeagleBone Black com uma fonte de alimentação de 5V, utilizando 4 células de bateria de lítio AA. Além disso, esta capa vem equipada com um interruptor de alimentação e um indicador LED. Em relação ao desenvolvimento de *software*, o sinal LBO de bateria fraca pode ser mapeado para GPIO1_16 e assim acedido através de *bonescript*. Além de existir a possibilidade de expansão de bateria, esta solução já oferece algo muito semelhante ao encontrado nas fechaduras atuais. Sendo que, a qualquer momento, toda a fechadura pode funcionar à base de energia proveniente de uma tomada elétrica com um carregador de 5V.

5.2. Validação de resultados

Ao longo deste documento foram apresentadas diversas provas literárias que demonstram como as perguntas de pesquisa foram respondidas mas também existem perguntas que apenas foi possível responder pela experimentação e testes. De seguida, é apresentado um resumo da metodologia de trabalho utilizada passando pela avaliação da solução e por fim, é dada a resposta à questão principal.

5.2.1. *Design Science Research*

Apesar de existir um modelo geral de processamento de *Design Science Research*, foram definidos muitos outros modelos por outros autores. O modelo apresentado por Peffers segue um conjunto de passos que permite gerar diversos *outputs*. *Outputs* esses que contribuem para o fluxo de conhecimento e sucessivos passos de todo o modelo.

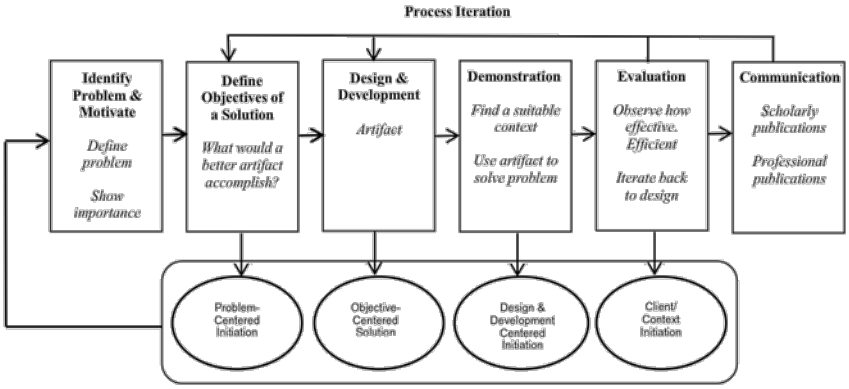

Figura 5.2.: Modelo de processamento de *Design Science Research* (Vaishnavi/Kuechler, 2004)

O primeiro passo é a identificação do problema. Algo interessante que possa ser descoberto ou algo que possa ser melhorado de alguma maneira. Esta contribuição deve gerar conhecimento para os especialistas da área de trabalho e deve conter alguma relevância para a comunidade da área em questão. De seguida, são definidos os objetivos da solução. O que é pretendido com o projeto? O que vai ser melhorado com a sua conclusão? Estas são as respostas que devem ser dadas nos objetivos do projeto. Por fim, existe todo o processo de desenvolvimento. Este desenvolvimento, tal como mencionado na introdução desta tese, deve gerar um artefacto. Este artefacto é o que irá ser demonstrar o trabalho desenvolvido, logo, é necessário que demonstre todas as suas capacidades. Posteriormente, são executadas as iterações de demonstração e avaliação. Nestas duas fases, é esperado que o artefacto seja utilizado num contexto adequado e sejam aplicadas medições de modo a observar o grau de eficiência e eficácia do mesmo. Por fim, existe a comunicação das descobertas, ou seja, a escrita e publicação dos achados de todo o modelo de processamento da metodologia.

5.2.2. Questões de pesquisa

Nesta secção irá ser feita uma recapitulação das questões de pesquisa, e respetivas respostas, de modo a perceber o estado final do projeto. As questões 1, 2 e 2.1 foram respondidas depois de analisar seis fechaduras eletrónicas distintas no segundo capítulo. As questões 3 e 2.1.1 foram respondidas no terceiro capítulo, depois de pesquisar, analisar e avaliar as tecnologias para duas componentes do projeto em causa. Por fim, a questão 4, foi respondida posteriormente ao desenvolvimento da solução de modo a conseguir fazer um levantamento

de todos os componentes de *software* necessários para uma solução com as características aqui apresentadas.

SQ-1: "Quais os requisitos funcionais de uma fechadura eletrónica?"

- Bloqueio/desbloqueio da fechadura através de um dispositivo móvel
- Registo de bloqueios/desbloqueios
- Transmissão de chaves eletrónicas

SQ-2: "Quais os requisitos não funcionais de uma fechadura eletrónica?"

- Segurança
- Baixos consumos de bateria por parte da aplicação
- Rápido processamento no bloqueio/desbloqueio da fechadura

SQ-2.1: "Quantos canais de comunicação devem estar disponíveis?"

Apenas um.

SQ-2.1.1: "Quais os preferenciais?"

Bluetooth.

SQ-3: "Qual o *hardware* necessário para uma fechadura eletrónica?"

- BeagleBone Black
- Módulo Bluetooth
- *Breadboard*
- Fios para *breadboard*
- Resistências

SQ-4: "Qual o software necessário para uma fechadura eletrónica?"

- Aplicação móvel
  - *Software*: Android Studio
  - Bibliotecas:

        * *Spongy Castle*

- Mecanismo da fechadura
  - *Software*:
    * *Browser*
    * Cloud9
    * PuTTY
  - Bibliotecas
    * *bonescript*
    * *crypto*
    * *node-aes-gcm*

5.2.3. Avaliação da solução

De acordo com a metodologia estudada, existem diversas abordagens para a avaliação do artefacto gerado. Cada avaliação segue o seu próprio modelo de regras e estruturação de modo a conseguir melhores resultados.

Segundo Bjorn Niehaves e Daniel Pfeiffer, a qualidade e assim a avaliação de modelos conceptuais é de alta relevância económica. Esta qualidade tem um grande impacto noutros artefactos das tecnologias de informação (TI). Sistemas de *software* são baseados em explícitas especificações de requisitos que vêm na forma de modelos conceptuais. No momento da sua contribuição para o campo da avaliação de modelos conceptuais, a sua preocupação baseava-se em se existia ou não um abordagem holística para determinar a qualidade de modelos conceptuais. Estes estruturaram a sua contribuição baseada em três questões de pesquisa:

- **Q1** - Quais os elementos de uma abordagem holística na avaliação de artefactos de TI?
- **Q2** - Já existe uma abordagem holística para determinar a qualidade de um modelos conceptual?
- **Q3** - Como é que o estruturalismo consegue contribuir para uma abordagem holística na avaliação de modelos conceptuais?

A *framework* de avaliação proposta expande-se para duas dimensões "artefacto" e "avaliação". A dimensão de artefacto cobre quatro tipos de artefacto, já mencionados no primeiro capítulo, um modelo, um método, uma construção e uma instanciação de algo. Enquanto que a avaliação cobre a estrutura do artefacto e os critérios e abordagens de avaliação. A principal contribuição dos autores surge numa abordagem para avaliar modelos de informação utilizando estruturalismo.

Em 2003, Peter Fettke e Peter Loos, desenvolveram uma *framework* multiperspetiva para a avaliação de modelos de referência. Também eles se focaram no tipo modelo de artefacto e motivaram o seu desenvolvimento devido ao esforço de modelação demorado e propenso a erros. Apesar do significado evidente de um modelo de referência e alta qualidade para a dedução de modelos individuais, os autores constituíram uma falta de abordagens adequadas para a avaliação de modelos de referência nos sistemas de informação e disciplinas semelhantes. Quanto à dimensão do método de pesquisa, estes diferenciam entre o analítico e o empírico. Fettke e Loos, explicam brevemente todas as 15 perspetivas, bem como as suas vantagens e desvantagens. Os autores não afirmam a conclusão do estudo da sua *framework* mas antes desafiam outros investigadores a tomarem a sua *framework* como base para trabalho futuro.

A abordagem proposta por Ulrich Frank, como as anteriores, foca-se na avaliação de modelos conceptuais e, em particular, na avaliação de modelos de referência. Também Frank deplora a falta de metodologias apropriadas de avaliação nos sistemas de informação e sugere uma estrutura referência baseada em quatro perspetivas fundamentais: económica, desenvolvimento, engenheira e epistemológica. Todas elas são essenciais à avaliação holística de um modelo de qualidade de referência.

Keng Siau e Matti Rossi conduzem uma extensiva análise ao tópico de metodologias de avaliação para métodos de modelação e, por isso, só se focam num artefacto de *Design Science Research*. Ao contrário de alguns dos anteriores autores, estes citam um conjunto enorme de outros métodos desenvolvidos por investigadores. A *framework* que estes acabam por desenvolver serve como sistematização de uma coleção de metodologias e obtém duas dimensões ontológicas e epistemológicas, facilitando assim a classificação dos métodos em termos de filosofia subjacente à ciência.

Por fim, Anne Cleven, Phillip Gubler e Kai M. Hüner desenham uma proposta de avaliação por variáveis e valores de modo a avaliar artefactos de DSR. As variáveis apresentadas pelos autores são em parte provenientes de sistemas de informação e em parte de outros campos de estudo como administração empresarial e sociologia que ambos têm um longo passado de avaliação. As variáveis definidas pelos autores, bem como os possíveis valores, são os que se seguem:

Após a explicação de alguns exemplos de metodologias de avaliação de artefactos, foi optado por seguir este modelo e a solução apresentada nesta tese poderá ser então avaliada segundo as variáveis definidas pelos autores na seguinte configuração:

- **Abordagem**: quantitativa - considera-se que a solução é de carácter quantitativo dado que as características da mesma podem ser avaliadas de modo numérico como consumo de bateria, velocidade de processamento, nível de segurança, etc.;
- **Foco do artefacto**: técnico - a solução é de foro técnico, pois foca-se no desenvolvimento de um método de desenvolvimento de um produto, na qual se abordam algoritmos de autenticação entre outros;

Variável	**Valor**				
Abordagem	Qualitativa			Quantitativa	
Foco do artefacto	Técnico		Organizacional		Estratégico
Tipo	Construção	Método	Modelo	Instanciação	Teoria
Epistemologia	Positivismo			Interpretativismo	
Função	Conhecimento	Controlo	Desenvolvimento		Legitimização
Método	Pesquisa	Caso de estudo	Experiência de campo		Provas formais
	Experiência controlada		Protótipo		Inquérito
Objeto	Artefacto		Construção de artefacto		
Ontologia	Realismo		Nominalismo		
Perspetiva	Económica	Desenvolvimento	Engenheira		Epistemológicas
Posição	Externa		Interna		
Ponto de referência	Artefacto contra falha		Artefacto contra mundo real		Falha de pesquisa contra mundo real
Tempo	Ex ante		Ex post		

Tabela 5.1.: Variáveis e valores para a avaliação de artefactos DSR

- **Tipo**: método - tal como referido no ponto anterior, esta solução é um artefacto do tipo método devido a sua representação em forma de algoritmos e procedimentos para um dado problema;
- **Epistemologia**: positivista - qualquer que seja o sujeito de avaliação em causa, os resultados de avaliação do artefacto devem gerar sempre os mesmo resultados;
- **Função**: desenvolvimento - os processos de aprendizagem associados à função de desenvolvimento são baseados nas introspeções das funções de controlo e conhecimento;
- **Método**: protótipo - considera-se que a avaliação baseada num protótipo facilita o processo de determinar se uma solução é adequada a um determinado problema, através da sua implementação genérica;
- **Objeto**: artefacto - o artefacto DSR pode ser, por si, alvo de avaliação;
- **Ontologia**: realismo - considerando a parte filosófica da ciência sobre o que considerar como "o que existe" ou "o como existe", o realismo dá uma perspetiva de que o mundo existe independentemente da perceção humana;
- **Perspetiva**: engenheira - dado que a solução se foca em metodologias, linguagens de programação e descrição de componentes, esta deve ser avaliada com uma perspetiva engenheira;
- **Posição**: externa - a avaliação é feita por pessoas externas ao artefacto DSR
- **Ponto de referência**: artefacto contra o mundo - neste caso, o cabimento do artefacto é avaliado de acordo com padrão do mundo real e comparado contra os parâmetros definidos pelo mesmo;

- **Tempo**: ex post - toda a avaliação é realizada após a implementação.

5.2.4. Questão principal

Por fim, e depois de toda a análise conduzida, procede-se à resposta da questão principal proposta no início deste documento.

"Seria possível e viável construir um sistema de fechadura eletrónica usando componentes *open-source*?"

A resposta a esta pergunta poderá depender de bastantes fatores mas de acordo com a configuração apresentada na secção anterior, estima-se que seja possível construir um sistema de fechadura eletrónica usando componentes *open-source*. Os primeiros resultados do inacabado protótipo desenvolvido, demonstraram bons resultados e tudo indica que após mais algum tempo de desenvolvimento seja possível fabricar uma solução com as características apresentadas.

5.3. Conclusão

Nesta secção final são apresentadas as deliberações finais sobre o projeto. É feita uma avaliação aos objetivos definidos no início do mesmo, assim como feita uma análise ao possível desenvolvimento futuro. Para finalizar, é feito um remate final sobre o projeto e a tecnologia abordada durante toda a tese.

5.3.1. Objetivos

Concluindo o atual trabalho, foi possível verificar o cumprimento dos objetivos estabelecidos no primeiro capítulo deste documento. Imediatamente no segundo capítulo foi apresentado um detalhado estudo sobre as fechaduras eletrónicas inteligentes mais relevantes no mercado da atualidade. Desse estudo, foi possível verificar as principais características de cada uma das fechaduras e qual o seu percurso empresarial ao longo do tempo. Além disso, foram identificadas as forças e fraquezas mais pertinentes das mencionadas fechaduras. Tudo isto, não só contribuiu para um melhor desenvolvimento do trabalho atual mas serve como primeiro aspeto dos objetivos na medida em que, qualquer pessoa interessada no assunto das fechaduras eletrónicas poderá consultar esta tese como fonte de informação. No seguimento da tese, foram apresentados estudos e provas que projetam o desenvolvimento de uma solução baseada em tecnologias *open-source*. Esta solução não só serve para futuros investigadores prosseguirem trabalho na área e explorarem os vários ângulos da solução mas também para realçar a importância do *hardware* e *software open-source* na realidade atual e nas possibilidades que contribuições externas podem trazer para todo o tipo de projetos.

5.3.2. Desenvolvimentos futuros

Tal como mencionado no capítulo anterior, o inacabado protótipo construído demonstrou fortes possibilidades de se tornar um elemento relevante no mercado das fechaduras eletrónicas inteligentes. Como trabalho futuro, seria interessante finalizar o protótipo atual e conduzir os primeiros testes com uma fechadura eletrónica real.

Após resultados positivos, prosseguir-se-ia à análise e desenvolvimento do aumento dos canais de comunicação de modo a facilitar determinadas operações. Além disso, a expansão para múltiplas plataformas seria uma adição bastante positiva na medida que, além de oferecer a solução a um nicho de pessoas mais alargado, também traria mais *feedback* e experiências de utilizadores que poderiam ser utilizadas para outro tipo de desenvolvimento futuros da solução.

5.3.3. Conclusão final

Após a conclusão do projeto atual, e com os objetivos cumpridos, pode-se afirmar que a adição de um melhor e mais pormenorizado planeamento traria sérios benefícios ao protótipo. Benefícios esses que, possivelmente, permitiriam a implementação das melhorias anteriormente mencionadas, o que traria um aumento de valor enorme para o projeto. Desde a análise das outras fechaduras até ao desenvolvimento da própria solução, e apesar da generalização dos casos, sempre se considerou o caso de uso doméstico para portas. No entanto, e com mais algum estudo envolvido, poderia ser possível expandir a metodologia atual para outros componentes como automóveis, cacifos, malas, etc. As capacidades e falta de limites das aplicações *open-source* poderiam trazer esse tipo de projetos para a realidade.

Por fim, foi também possível concluir que a tecnologia está a avançar num ritmo acelerado mas que ainda é necessária uma maior evolução para que as pessoas possam atribuir um maior grau de confiança nela. Os *smartphones* já estão a substituir cartões de crédito, interruptores de luz, comandos de televisão e comandos de automóveis. Em breve, irão substituir por completo as chaves.

5.4. Sumário

Neste capítulo foi possível realizar uma medição dos resultados e conduzir uma análise sobre o que é a solução final face às fechaduras apresentadas no segundo capítulo. Dessa análise, foi possível concluir que, apesar das limitações, a solução atual teria as mesmas funcionalidades que uma fechadura eletrónica inteligente "normal". Face a estas comparações e análises, bem como a uma breve explicação sobre a metodologia utilizada *Design Science Research*, concluiu-se que um projeto de desenvolvimento de um produto/protótipo com um simples caso de estudo, pode ser considerado um trabalho científico. Após a abordagem sobre o método de avaliação, foi respondida a questão principal desta tese.

Por fim, foram também apresentadas as conclusões finais da tese fazendo uma breve recapitulação sobre os objetivos definidos e abordando possíveis desenvolvimentos futuros.

Bibliografia

Symmetric vs. Public key Cryptography. ⟨URL: http://www.programmerinterview.com/index.php/general-miscellaneous/symmetric-vs-public-key-cryptography/⟩

Advanced Encryption Standard (AES). National Institute of Standards and Technology, 2001 – Technical report

International Conference on Machine Learning and Computing (Org.) – *Improvement Bluetooth Authentication and pairing protocol using Encrypted Key Exchange and Station-to-Station – MAC Protocols*. 2009

Academy, Khan – *XOR bitwise operation*. ⟨URL: https://www.khanacademy.org/computing/computer-science/cryptography/ciphers/a/xor-bitwise-operation⟩

Agency, National Security – *Bluetooth Security*. 2007

Amedee, Collin – *Easy Bluetooth Enabled Door Lock With Arduino + Android*. ⟨URL: http://www.instructables.com/id/Easy-Bluetooth-Enabled-Door-Lock-With-Arduino-An/⟩

Anson, Scott – *Bluetooth Security*. University of Washington, 2001 – Technical report

August – *August press*. ⟨URL: http://www.august.com/press.html⟩

Beagleboard – *BeagleBone Black*. ⟨URL: http://beagleboard.org/BLACK⟩

—— *BeagleBone Hardware*. ⟨URL: http://beagleboard.org/Support/bone101/#hardware⟩

BoardZoo – *BeagleBone Chip Antenna*. ⟨URL: http://boardzoo.com/index.php/catalog/product/view/id/146/category/8#.Vh2MZ3UVikp⟩

Bodell, Paul – *Communications: Bluetooth vs. NFC.* ⟨URL: http://www.securityinfowatch.com/article/11034554/smartphone-access-control⟩

Chakraborty, Goutam et al. – *Analysis Of The Bluetooth Device Discovery Protocol.* Springer Science 2008

Chang, Alexandra – *Your Door Is About to Get Clever: 5 Smart Locks Compared.* ⟨URL: http://www.wired.com/2013/06/smart-locks/⟩

Chang, Richard; Shmatikov, Vitaly – *Formal Analysis of Authentication in Bluetooth Device Pairing.* The University of Texas at Austin, 2007 – Technical report

Chen, Perry; Strickler, Yancey; Adler, Charles – *Kickstarter Is Not a Store.* ⟨URL: https://www.kickstarter.com/blog/kickstarter-is-not-a-store⟩

Chevassut, Olivier – *Authenticated group Diffie-Hellman key exchange: theory and practice.* University of California, 2002 – Technical report

Cleven, Anne; Gubler, Philipp; Hüner, Kai M. – *Design Alternatives For The Evaluation Of Design Science Research Artifacts.* University of St. Gallen, Institute of Information Management, 2015 – Technical report

Computer Science, Department of – *Bluetooth: Authentication - Authorisation - Encryption.* 2003

Cooper, Justin – *BeagleBone Black: Installing Operating Systems.* 2014

Crist, Ry – *How secure is the deadbolt in the Kwikset Kevo smart lock?* ⟨URL: http://www.cnet.com/news/how-secure-is-the-deadbolt-in-the-kwikset-kevo-smart-lock/⟩

Czagan, Dawid – *Symmetric and Asymmetric Encryption.* ⟨URL: http://resources.infosecinstitute.com/symmetric-asymmetric-encryption/⟩

Danalock – *Danalock press.* ⟨URL: https://danalock.com/?page_id=39⟩

Developer, Bluetooth – *Bluetooth Architecture.* ⟨URL: https://developer.bluetooth.org/TechnologyOverview/Pages/Core.aspx⟩

Developers, Android – *Bluetooth Low Energy.* ⟨URL: http://developer.android.com/guide/topics/connectivity/bluetooth-le.html⟩

Dworkin, Morris – *Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC.* National Institute of Standards and Technology, 2007 – Technical report

EagerBeagler – *Bluetooth PAN Network on the Beagle.* ⟨URL: https://eagerbeagler.wordpress.com/⟩

Element14 – *Raspberry Pi 2 GPIO Header.* ⟨URL: http://www.element14.com/community/docs/DOC-73950/l/raspberry-pi-2-model-b-gpio-40-pin-block-pinout⟩

Fettke, Peter; Loos, Peter – *Multiperspective Evaluation of Reference Models – Towards a Framework.* Springer Berlin Heidelberg 2003

Filho, Flavio de Castro Alves – *Compilando o Android para a BeagleBone Black.* ⟨URL: http://www.embarcados.com.br/compilando-o-android-para-beaglebone-black/⟩

Fleishman, Glenn – *Inside Bluetooth 2.0.* ⟨URL: http://www.macworld.com/article/1042714/bluetooth2.html⟩

Forum, NFC – *NFC Forum Specification Architecture.* ⟨URL: http://nfc-forum.org/our-work/specifications-and-application-documents/specifications/⟩

Franklin, Curt; Layton, Julia – *How Bluetooth Works.* ⟨URL: http://electronics.howstuffworks.com/bluetooth.htm⟩

Gerdessen, Anton – *Framework Comparison Method.* Diploma Thesis University of Amsterdam, 2007

Goji – *Goji press.* ⟨URL: http://gojiaccess.com/pages/press.html⟩

Gonsalves, Antone – *Smartphones Could Evolve Into Password Killers.* ⟨URL: http://www.csoonline.com/article/2133826/mobile-security/smartphones-could-evolve-into-password-killers.html⟩

Google – *Cloud9 IDE.* ⟨URL: https://sites.google.com/site/texteditors/Home/files/Cloud9IDE.png⟩

Green, Matthew – *A Few Thoughts on Cryptographic Engineering.* ⟨URL: http://blog.cryptographyengineering.com/2012/05/how-to-choose-authenticated-encryption.html⟩

Haven – *Haven.* ⟨URL: http://www.havenlock.com/⟩

Hut, The Pi – *Raspberry Pi 2 - Model B.* ⟨URL: http://thepihut.com/products/raspberry-pi-2-model-b⟩

Java2s – *Diffie-Hellman Key Agreement : Diffie Hellman « Security « Java Tutorial.* ⟨URL: http://www.java2s.com/Tutorial/Java/0490__Security/DiffieHellmanKeyAgreement.htm⟩

LARIVIERE, Paul; HALL, Stephen – *Making Smart Locks Smarter (aka. Hacking The August Smart Lock).* ⟨URL: http://blog.maintenancewindow.ca/post/2015/03/29/Making-Smart-Locks-Smarter-(aka.-Hacking-the-August-Smart-Lock)⟩

LEVI, Albert et al. – *Relay Attacks on Bluetooth Authentication and Solutions.* Springer-Verlag 2004

LIU, Alan; LEE, Leon – *Host Controler Interface.* University Of Taiwan, 2001 – Technical report

LOCKITRON – *Lockitron press and media.* ⟨URL: https://lockitron.com/media⟩

LUMME, Juha – *BeagleBone Home Automation.* Packt Publishing, 2013

MAHMUD, Syed Masud – *Bluetooth Technology.* Wayne State University, 2005 – Technical report

MATTHEW – *Asymmetric vs Symmetric Encryption.* ⟨URL: http://security.stackexchange.com/questions/7219/asymmetric-vs-symmetric-encryption⟩

MATTHIAS – *Data encryption on Android, AES-GCM or plain AES?* ⟨URL: http://stackoverflow.com/questions/13420065/data-encryption-on-android-aes-gcm-or-plain-aes⟩

MEI, Jiexiang Marvyn; SALIM, Agus – *Access Control using Bluetooth.* Diploma Thesis The University Of New South Wales, 2003

MENON, Am Hanish – *Short and simple commandline Bluetooth in any new Linux distros.* ⟨URL: https://hanishkvc.wordpress.com/2007/05/16/short-and-simple-commandline-bluetooth-in-any-new-linux-distros/⟩

METTALA, Riku – *Bluetooth Protocol Architecture.* Bluetooth Special Interest Group, 1999 – Technical report

MONK, Simon – *Connecting a Push Button to BeagleBone Black.* ⟨URL: https://learn.adafruit.com/connecting-a-push-button-to-beaglebone-black/overview⟩

NAMIN, Ashkan Hosseinzadeh – *Elliptic Curve Cryptography.* University of Windsor, 2005 – Technical report

PI, Raspberry – *Raspberry Camera Module.* ⟨URL: https://www.raspberrypi.org/products/camera-module/⟩

—— *Raspberry Pi - How To Use - Python.* ⟨URL: https://www.raspberrypi.org/documentation/usage/python/README.md⟩

—— *Raspberry Sense Hat.* ⟨URL: https://www.raspberrypi.org/products/sense-hat/⟩

PORTNOI, Marcos – *Criptografia Com Curvas Elípticas*. Universidade Salvador, 2005 – Technical report

PRETTY, Bill – *Building a Home Security System with BeagleBone*. Packt Publishing, 2013

ROBERTSON, Cameron – *The Story Of Lockitron: Crowdfunding Without Kickstarter*. ⟨URL: `http://techcrunch.com/2012/10/07/the-story-of-lockitron-crowdfunding-without-kickstarter/`⟩

ROUSE, Margaret – *Diffie-hellman Key Exchange (exponential Key Exchange) Definition*. ⟨URL: `http://searchsecurity.techtarget.com/definition/Diffie-Hellman-key-exchange`⟩

SANDHU, Ravi S. et al. – *Role-Based Access Control Models*. IEEE Computer 1996

SETHI, Amit; MANZOOR, Omair; SETHI, Tarun – *User Authentication on Mobile Devices*. Cigital 2012

SIAU, Keng; ROSSI, Matti – *Evaluation Techniques For Systems Analysis And Design Modelling Methods – A Review And Comparative Analysis*. Information Systems Journal 2007

SINGH, Nishant Kumar – *Bluetooth Interfacing On Beagle Bone Black*. 2014

SMARTLOCKREVIEWS – *The Smartphone Enabled Door Lock vs. the Traditional Key*. ⟨URL: `http://www.smartlockreviews.com/the-smartphone-enabled-door-lock-vs-the-traditional-key-2/`⟩

SULLIVAN, Nick – *A (relatively Easy To Understand) Primer On Elliptic Curve Cryptography*. ⟨URL: `http://arstechnica.com/security/2013/10/a-relatively-easy-to-understand-primer-on-elliptic-curve-cryptography/`⟩

TOPTENREVIEWS – *Smart Locks Review*. ⟨URL: `http://smart-locks-review.toptenreviews.com/`⟩

TOWNE, Schuyler – *The Current State of Smart Locks*. ⟨URL: `http://schuylertowne.com/blog/smart-locks`⟩

ULRICH, Frank – *Evaluation of Reference Models*. University of Duisburg-Essen, 2007 – Technical report

UNIFORMS, First Class – *Key fob*. ⟨URL: `http://www.fcuniforms.com/products/RFID_Key_Fob_Tag_Grey-866-60.html`⟩

UNIKEY – *Unikey press*. ⟨URL: `http://www.unikey.com/press-room/`⟩

VAISHNAVI, Vijay; KUECHLER, Bill – *Design Science Research in Information Systems*. 2004

WIGMORE, Ivy – *Internet of Things (IoT)*. ⟨URL: http://whatis.techtarget.com/definition/Internet-of-Things⟩

WIKI, Embedded Linux – *BeagleBone Battery*. ⟨URL: http://elinux.org/CircuitCo:BeagleBone_Battery⟩

—— *BeagleBone LCD7*. ⟨URL: http://elinux.org/CircuitCo:BeagleBone_LCD7⟩

WIKIPEDIA – *Diffie-Hellman key exchange*. ⟨URL: https://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman_key_exchange⟩

YEUNG, Calvin – *Symmetric vs. Asymmetric Encryption: Which Way is Better?* ⟨URL: http://blog.atmel.com/2013/03/11/symmetric-vs-asymmetric-encryption-which-way-is-better/⟩

YOUNG, Bill – *Foundations of Computer Security*.

ZEPHYR-LABS – *Bluetooth LE on BeagleBone Black with TI SensorTag*. ⟨URL: http://www.zephyr-labs.com/?p=87⟩

Apêndice

A Casos de uso

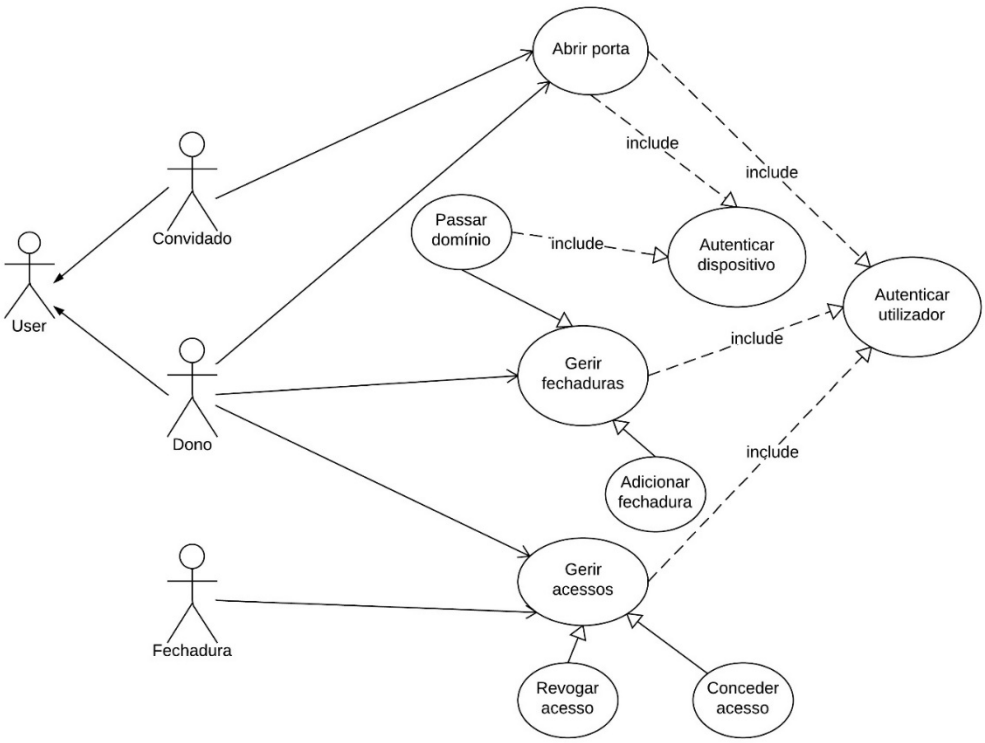

Figura A.1.: Casos de uso

A.1. Caso de uso: abrir porta

A.1.1. Formato casual

O utilizador seleciona a ação de abrir a fechadura ou, caso esteja a opção de abertura automática selecionada, este aproxima-se da porta e ativa o mecanismo de abertura. Caso esteja devidamente autenticado, a porta é aberta.

A.1.2. Formato completo

Ator principal

Utilizador.

Partes interessadas e seus interesses

Dono e convidado. Ativar o mecanismo da fechadura que permita a abertura da porta.

Pré condições

Utilizador tem acesso ao seu smartphone com a aplicação instalada e este tem acesso à fechadura em questão.

Pós condições

Utilizador foi autenticado e autorizado e foi-lhe concedido acesso à fechadura.

Fluxo principal de sucesso

1. Utilizador introduz o PIN de segurança na aplicação;
2. Utilizador seleciona a fechadura a abrir da sua lista;
3. O dispositivo é autenticado;
4. A fechadura concede acesso.

Fluxos alternativos

1. Utilizador tem a abertura de porta automática selecionada nas preferências (não é necessário PIN);
2. Verificação da validade da hora;
3. O dispositivo é autenticado;
4. A fechadura concede acesso.

Exceções

1. Utilizador não autorizado. Exceção de autorização;
2. Hora de entrada automática inválida. Exceção de autorização;
3. Dispositivo não autorizado. Exceção de autorização.

Pressupostos

Fechadura inteligente instalada e configurada nas portas em questão.

A.2. Caso de uso: passar domínio

A.2.1. Formato casual

Dono seleciona a fechadura que pretende passar o domínio e o utilizador para quem quer passa-lo.

A.2.2. Formato completo

Ator principal

Dono.

Partes interessadas e seus interesses

Dono. Passar o domínio de uma fechadura para outro utilizador que não é dono da mesma.

Pré condições

Utilizador tem acesso ao seu smartphone com a aplicação instalada e este tem acesso à fechadura em questão.

Pós condições

Domínio da fechadura foi concedido ao utilizador.

Fluxo principal de sucesso

1. Dono introduz o PIN de segurança na aplicação;
2. Seleciona a fechadura da sua lista;
3. Dispositivo é autenticado;

4. Seleciona o utilizador;

5. Concede acesso ao utilizador.

Exceções

1. Utilizador não autorizado. Exceção de autorização;

2. Dispositivo não autorizado. Exceção de autorização.

Pressupostos

Fechadura inteligente instalada e configurada nas portas em questão.

A.3. Caso de uso: adicionar fechadura

A.3.1. Formato casual

Dono sonda fechaduras nas proximidades, seleciona a fechadura a adicionar e introduz o código físico da fechadura. A fechadura é adicionada ao smartphone do dono e o seu dispositivo é adicionado à lista de dispositivos da fechadura.

A.3.2. Formato completo

Ator principal

Dono.

Partes interessadas e seus interesses

Dono. Registar nova fechadura.

Pré condições

Dono tem acesso ao seu smartphone com a aplicação instalada, assim como a proximidade física da porta.

Pós condições

A fechadura é adicionada ao dispositivo do dono e vice-versa.

Fluxo principal de sucesso

1. Dono introduz o PIN de segurança na aplicação;
2. Sonda fechaduras nas proximidades;
3. Seleciona a fechadura a registar;
4. Introduz o código da fechadura;
5. A fechadura concede acesso.

Exceções

1. Utilizador não autorizado. Exceção de autorização;
2. Dispositivo não autorizado. Exceção de autorização.

Pressupostos

Fechadura inteligente instalada e configurada nas portas em questão.

A.4. Caso de uso: revogar acesso

A.4.1. Formato casual

O dono seleciona a fechadura que pretende e o utilizador cujo acesso será revogado.

A.4.2. Formato completo

Ator principal

Dono e fechadura.

Partes interessadas e seus interesses

Dono e fechadura. Revogar acesso a convidados.

Pré condições

Dono tem acesso ao seu smartphone com a aplicação instalada e este tem acesso à fechadura em questão, assim como a proximidade física da porta.

Pós condições

Autorização do utilizador para a fechadura em questão foi revogada.

Fluxo principal de sucesso

1. Dono introduz o PIN de segurança na aplicação;
2. Seleciona a fechadura da sua lista;
3. Seleciona o utilizador pretendido;
4. Autorização é revogada.

Fluxos alternativos

1. Utilizador tem acesso temporário à fechadura;
2. Verificação da validade da data e hora por parte da fechadura;
3. Autorização é revogada.

Exceções

1. Utilizador não autorizado. Exceção de autorização;
2. Dispositivo não autorizado. Exceção de autorização.

Pressupostos

Fechadura inteligente instalada e configurada nas portas em questão.

Questões em aberto

Não ser necessária a proximidade física da fechadura e os acessos serem sincronizados da próxima vez que a fechadura estiver ao alcance do dispositivo.

A.5. Caso de uso: conceder acesso

A.5.1. Formato casual

O dono seleciona a fechadura que pretende e o utilizador a quem pretende conceder acesso.

A.5.2. Formato completo

Ator principal

Dono e fechadura.

Partes interessadas e seus interesses

Dono e fechadura. Revogar acesso a convidados.

Pré condições

Dono tem acesso ao seu smartphone com a aplicação instalada e este tem acesso à fechadura em questão, assim como a proximidade física da porta e do utilizador.

Pós condições

Autorização do utilizador para a fechadura em questão foi concedida.

Fluxo principal de sucesso

1. Dono introduz o PIN de segurança na aplicação;
2. Seleciona a fechadura da sua lista;
3. Seleciona o utilizador pretendido;
4. Autorização é concedida.

Exceções

1. Utilizador não autorizado. Exceção de autorização;
2. Dispositivo não autorizado. Exceção de autorização.

Pressupostos

Fechadura inteligente instalada e configurada nas portas em questão.

Questões em aberto

Não ser necessária a proximidade física da fechadura e os acessos serem sincronizados da próxima vez que a fechadura estiver ao alcance do dispositivo.