Mestrado em Engenharia Informática
Estágio
Relatório Final

Segurança e Privacidade na Massificação da Internet dos Objetos

Gonçalo Nuno Freitas Valério
gvalerio@student.dei.uc.pt

Orientadores:
Mestre Jorge Santos
Professor Doutor João Vilela

Data: 1 de Setembro de 2015

FCTUC DEPARTAMENTO
DE ENGENHARIA INFORMÁTICA
FACULDADE DE CIÊNCIAS E TECNOLOGIA
UNIVERSIDADE DE COIMBRA

Mestrado em Engenharia Informática
Estágio
Relatório Final

Segurança e Privacidade na Massificação da Internet dos Objetos

Gonçalo Nuno Freitas Valério
gvalerio@student.dei.uc.pt

Júri:
Professor Doutor Jorge Granjal
Professor Doutor Jorge Henriques
Professor Doutor João Vilela

Data: 1 de Setembro de 2015

FCTUC DEPARTAMENTO
DE ENGENHARIA INFORMÁTICA
FACULDADE DE CIÊNCIAS E TECNOLOGIA
UNIVERSIDADE DE COIMBRA

UNIVERSIDADE DE COIMBRA

Resumo

Faculdade de Ciências e Tecnologia
Departamento de Engenharia Informática

Mestrado em Engenharia Informática

Segurança e Privacidade na Massificação da Internet dos Objetos

por Gonçalo Valério

O termo "Internet of Things" (em português, Internet dos objetos) refere-se à ideia de uma rede global que interliga um vasto conjunto de equipamentos, que vai muito para além dos tradicionais computadores pessoais e servidores, à Internet. Este é um conceito que veio para ficar e está na base da recente onda de dispositivos que têm chegado ao mercado de consumo, muitos dos quais já se infiltraram no nosso quotidiano. Desde os *smartmeters*, utilizados para realizar uma boa gestão energética das residências, aos *wearables* que nos acompanham no dia a dia e que permitem monitorizar, por exemplo, os nossos sinais vitais. Todos eles têm um aspeto em comum, o facto de direta ou indiretamente comunicarem com uma rede global.

Nesta nova realidade, uma pergunta pertinente que se coloca é o quanto podemos confiar nestes dispositivos. Dada a sua ubiquidade e dependendo da sua utilidade, um defeito explorado por uma entidade exterior ou o desleixo no tratamento da informação recolhida, podem por em causa a privacidade e a segurança dos seus utilizadores.

Este trabalho analisa alguns dos aspetos de segurança de um grupo de produtos deste tipo que estão no mercado e as garantias que oferecem perante a possibilidade de serem o alvo de um agente malicioso com intenção de colocar em cause a segurança e privacidade dos utilizadores.

A partir dos testes realizados a uma pequena amostra de equipamentos, foram descobertos alguns problemas de segurança, para os quais são descritas possíveis estratégias de mitigação. Tendo por base os problemas encontrados, é ainda proposto um mecanismo de configuração, com ênfase na segurança, para dispositivos que necessitam de acesso a uma rede Wi-Fi local, processo este que é iniciado pelo utilizador.

UNIVERSITY OF COIMBRA

Abstract

Faculty of Science and Technology
Informatics Engineering Department

Masters in Informatics Engineering

Security and Privacy in the massification of the Internet of Things

by Gonçalo Valério

The term "Internet of Things"refers to the idea of a global network that interconnects a vast group of equipments, that goes far beyond from the traditional personal computers and servers, to the Internet. This concept is here to stay and is the basis of the recent wave of devices that recently reached the market and many of them are already part of our daily lives. From the smartmeters, used to improve the energy management of residences, to the wearables that follow us through the day and that, for example, monitor our health. All of them have an aspect in common, the fact that directly or indirectly they communicate with a global network.

In this new reality, an important question that must be asked is how much do we trust these devices. Given their ubiquity and depending on their utility, a simple defect that could be exploited by an external entity or some negligence in the treatment of the collected information, can affect the privacy and security of its users.

This work analyses some security aspects of a group of these devices that already are in the market and the guarantees they offer in the eventuality of being targeted by an attacker trying to violate the security and privacy of the device's users.

From the tests made to this small sample of the devices, some security issues were found and mitigation strategies provided for them. Also, a setup mechanism with focus on security is proposed to devices that need Wi-Fi access to the local network, where the process the executed by the user.

Agradecimentos

Gostaria de agradecer em primeiro lugar aos meus orientadores, Professor Doutor João Vilela e ao Mestre Jorge Santos, por todo o apoio e sugestões dadas durante a realização do trabalho. Da mesma forma, quero deixar claro o meu agradecimento a toda a equipa da *Whitesmith*, pela confiança depositada em mim e pelas condições de trabalho acolhedoras que proporcionaram durante a execução do meu estágio.

Aos meus colegas de estágio, quero também deixar umas palavras de apreço, pelo companheirismo e entre-ajuda que existiu desde o primeiro dia.

Por fim, mas não menos importante, gostaria de agradecer a toda a minha família pela força e pelo suporte que me foram dados desde o inicio da minha vida académica, com um especial destaque para o meu pai, mãe e irmã que estiveram sempre ao meu lado.

Índice

Resumo iii

Abstract v

Agradecimentos vii

Lista de Figuras xiii

Lista de Tabelas xv

Lista de acrónimos xvii

1 Introdução 1
- 1.1 Motivação . . . 2
- 1.2 Objetivos . . . 2
- 1.3 Entidade acolhedora . . . 3
- 1.4 Planeamento e cronograma . . . 3
- 1.5 Estrutura do documento . . . 5

2 Estado da arte 7
- 2.1 Internet dos objetos . . . 7
  - 2.1.1 Abordagens no desenvolvimento da IoT . . . 10
  - 2.1.2 Tecnologias especificas para a IoT . . . 11
- 2.2 Segurança na Internet dos objetos . . . 12
  - 2.2.1 Privacidade . . . 15
- 2.3 Problemas de segurança comuns . . . 16
- 2.4 Testes de penetração . . . 17
  - 2.4.1 Metodologias . . . 19
- 2.5 Análise de tráfego . . . 21
- 2.6 Ferramentas . . . 22
  - 2.6.1 Wireshark . . . 22
  - 2.6.2 Aircrack-ng . . . 23
  - 2.6.3 Metasploit . . . 23
  - 2.6.4 ZAP . . . 24
  - 2.6.5 Nmap . . . 24
  - 2.6.6 Nogotofail . . . 25

2.6.7 OpenVAS . . . 25
2.6.8 Ettercap . . . 26
2.7 Mecanismos de configuração . . . 26
2.8 Infraestrutura de chaves públicas e ciclo de vida dos equipamentos . . . 28

3 Metodologia **29**
3.1 Foco do estudo . . . 29
3.1.1 Superfícies de ataque . . . 29
3.1.2 Modelo . . . 30
3.2 Dispositivos . . . 30
3.2.1 LifX . . . 31
3.2.2 Cloogy . . . 32
3.2.3 ChromeCast . . . 33
3.2.4 Qold . . . 33
3.2.5 Energyhive . . . 34
3.2.6 Withings Smart Body Analyzer . . . 34
3.2.7 Fitbit Flex . . . 35
3.2.8 Superfície de ataque por dispositivo . . . 36
3.3 Política de divulgação . . . 36

4 Resultados **39**
4.1 Execução dos testes . . . 39
4.2 Resultados . . . 40
4.3 Discussão dos problemas encontrados . . . 41
4.4 Estratégias de mitigação . . . 42

5 Mecanismo de configuração **45**
5.1 Requisitos . . . 46
5.1.1 Requisitos funcionais . . . 46
5.1.2 Requisitos não-funcionais . . . 46
5.2 Modelação de ameaças . . . 47
5.2.1 Objetivos de segurança . . . 48
5.2.2 Visão geral da aplicação . . . 48
5.2.3 Decomposição da aplicação . . . 49
5.2.4 Ameaças identificadas . . . 49
5.3 Desafios . . . 50
5.4 Especificação . . . 51
5.5 Descrição do prototipo . . . 54
5.6 Validação . . . 56

6 Conclusão **59**
6.1 Trabalho futuro . . . 60

Bibliografia **61**

Anexos **64**

A Dados recolhidos sobre o funcionamento dos alvos **65**

B Ataques conhecidos **71**

C Guia de boas práticas **73**

D Planeamento inicial **83**

Lista de Figuras

1.1 Execução do trabalho ao longo do segundo semestre 5

3.1 Lâmpada que será alvo dos testes. 31
3.2 Equipamentos que constituem o Cloogy. 32
3.3 Chromecast 33
3.4 Qold Hub 33
3.5 Hub do Energyhive 34
3.6 Balança da Whithings 35
3.7 Pulseira da Fitbit 35

5.1 Processo iterativo de modelação de ameaças 48
5.2 Visão do sistema no inicio da configuração 49
5.3 Interações entre os diferentes elementos. 53

Lista de Tabelas

3.1 Critérios usados na escolha dos dispositivos 31
3.2 Áreas a testar por dispositivo 36

5.1 Requisitos funcionais 47
5.2 Requisitos não funcionais 47
5.3 Configurações do equipamento 52

D.1 Planeamento inicial 83

Lista de acrónimos

AES Advanced Encryption Standard.

API Aplication Programming Interface.

CLI Command-line Interface.

CoAP Constrained Application Protocol.

CoRE Constrained Restful Environments.

DDoS Distributed Denial of Service.

DTLS Datagram Transport Layer Security.

ECC Elliptic Curve Cryptography.

EPoSS European Technology Platform on Smart Systems Integration.

GPL GNU General Public License.

GPRS General Packet Radio Service.

GUI Grafical User Interface.

HDMI High-Definition Multimedia Interface.

HTTP Hypertext Transfer Protocol.

HTTPS HTTP Secure.

IETF Internet Engineering Task Force.

IoT Internet of Things.

IPSec Internet Protocol Security.

LED Light-Emitting Diode.

M2M Machine to Machine.

MITM Man-in-the-Middle.

NIST National Institute of Standards and Technology.

OSSTMM Open Source Security Testing Methodology Manual.

OWASP Open Web Application Security Project.

PFS Perfect Forward Secrecy.

PIN Personal Identification Number.

PKC Public Key Cryptography.

PSK Pre-shared Key.

PTES Penetration Testing Execution Standard.

RBAC Role-based Access Control.

REST Representational State Transfer.

RFID Radio Frequency Identification.

SaaS Software as a Service.

SDK Software Development Kit.

SHA Secure Hash Algorithm.

SNMP Simple Network Management Protocol.

SSL Secure Socket Layer.

STAR Security Test Audit Report.

TCP Transmission Control Protocol.

TLS Transport Layer Security.

UDP User Datagram Protocol.

UMTS Universal Mobile Telecomunications System.

USB Universal Serial Bus.

WEP Wired Equivalent Privacy.

WPA Wi-Fi Protected Access.

WSN Wireless Sensor Network.

XSS Cross-site Scripting.

Capítulo 1

Introdução

Este trabalho realizado no âmbito da disciplina de Dissertação/Estágio do Mestrado em Engenharia Informática da Universidade de Coimbra, aborda a temática da segurança e da privacidade neste novo conceito denominado de Internet dos objetos. Esta nova noção compreende uma expansão da Internet e das tecnologias que dela fazem parte, a um alargado número de outros dispositivos. Estes não só estão acessíveis para comunicar com os humanos como também comunicam entre si e com o ambiente que os rodeia.

Coloca-se então um conjunto de perguntas relacionado com a segurança dos dados e dos equipamentos. Este trabalho responde a algumas delas através de uma quantidade de testes de penetração e da análise do tráfego, a dispositivos disponíveis hoje no mercado, de modo a retirar conclusões sobre como têm sido abordadas estas questões pelos fabricantes.

Após efetuada a análise, foi elaborado um conjunto de recomendações sobre o que pode ser feito para melhorar a segurança oferecida por estes equipamentos.

Dados os resultados obtidos é ainda proposto um mecanismo para realizar a configuração dos dispositivos de forma segura caso estes que reúnam um determinado conjunto de características.

As recomendações e o mecanismo resultantes da elaboração deste trabalho servirão então de base para a implementação de mecanismos de segurança nos produtos da *Whitesmith*, a entidade acolhedora deste trabalho.

1.1 Motivação

Nos últimos anos o mundo tem assistido a uma tendência crescente para adaptar e ligar vários objetos e utensílios do nosso dia a dia à Internet, com o objetivo de os tornar mais interativos, fáceis de usar e inteligentes. Pretende-se libertar o utilizador de várias tarefas incómodas ou fornecer algum tipo de informação e controlo sobre aspetos que anteriormente se encontravam inacessíveis. Acompanhando esta tendência e com a evolução dos sistemas embebidos, têm vindo a surgir também novos objetos e dispositivos ligados à rede que nos fornecem funcionalidades e informações anteriormente inexistentes.

O aspeto a ter em conta neste novo mundo é que estes equipamentos estão presentes em muitos dos aspetos do nosso quotidiano e geralmente estão ligados à rede global. Apesar de no passado este tipo de serviços e produtos já se encontrarem disponíveis em algumas áreas, indústrias e mercados de nicho, só agora é que se começa a assistir à sua massificação e democratização no mercado de consumo.

Outra vertente relacionada com a Internet dos objetos, é que estes dispositivos geralmente podem ser integrados com vários serviços já existentes, mesmo que não pertençam ao mesmo fabricante. Por vezes estes serviços até recomendam aos seus clientes a aquisição de equipamentos de terceiros.

Esta nova realidade vem acompanhada de novos problemas e desafios, dentro dos quais se encontram as garantias de segurança e a privacidade do consumidor. Fatores estes que são protegidos por várias leis e que se explorados podem trazer graves consequências para o utilizador.

Assim torna-se essencial analisar e verificar o nível de proteção que estes equipamentos fornecem aos consumidores nestas duas componentes, assim como propor alternativas e melhorias para estes sistemas, pois assegurar a segurança e a privacidade do utilizador é do interesse de todos os intervenientes.

1.2 Objetivos

Com a realização do presente trabalho pretende-se atingir os seguintes objetivos:

- Verificar até que ponto estes produtos disponíveis no mercado apresentam falhas de segurança;

- Verificar se tem havido a preocupação por parte dos fabricantes em manter os equipamentos protegidos contra as mais recentes ameaças conhecidas;
- Inferir se a privacidade do consumidor não está em risco, podendo estar a ser recolhidos mais dados do que aqueles estritamente necessários;
- Com base nos dados recolhidos, realizar uma análise aos problemas encontrados e fornecer um conjunto de recomendações gerais que possam ser seguidas na conceção de novos equipamentos deste género;
- Propor e especificar mecanismos para lidar com problemas semelhantes aos identificados anteriormente, que forneçam determinadas garantias de segurança.

1.3 Entidade acolhedora

O estudo foi realizado na sede da empresa *Whitesmith* e contou com a sua colaboração em muitos aspetos, tais como o fornecimento de um espaço dedicado ao trabalho e de todos os equipamentos utilizados na sua execução.

A *Whitesmith* é uma empresa fundada em 2012, sediada no Instituto Pedro Nunes em Coimbra, que se dedica maioritariamente à prestação de serviços na área do desenvolvimento de software e em parte à construção dos seus próprios produtos, todos eles relacionados com a Internet dos objetos.

Como exemplos temos os casos do *Unplugg* e do *Qold* que tiveram um papel importante na motivação da empresa em apoiar o presente trabalho. O primeiro é uma plataforma que funciona como Software as a Service (SaaS) e que interage com dados de vários dispositivos relacionados com a gestão energética do lar. Já o segundo é um novo equipamento que se encontra numa fase avançada de desenvolvimento que tem como objetivo a monitorização e controlo de características como a temperatura em equipamentos de refrigeração.

1.4 Planeamento e cronograma

De forma a compreender o presente trabalho é importante analisar o percurso efetuado durante o período no qual decorreu o estágio. Este passou por diversas fazes, nas quais foram realizados vários ajustes aos planos traçados de modo a maximizar a pertinência e qualidade do resultado final. Inicialmente, no mês de Setembro foi estabelecido que o trabalho se regesse pelos conteúdos já existentes na proposta de estágio, que previa a

definição dos vários equipamentos que iriam ser integrados no estudo, o aprofundar dos conhecimentos necessários à realização do trabalho e o planeamento das várias etapas a realizar no segundo semestre. Para este último ponto a opção inicial foi o seguinte cenário:

- Realização da preparação do ambiente de testes, durante a segunda metade do mês de Fevereiro.
- Execução da análise aos vários equipamentos de acordo com a metodologia definida, durante os meses de Março, Abril e Maio.
- Preparação de um documento com boas práticas na abordagem aos problemas encontrados.
- Realização do relatório final detalhando o trabalho efetuado.

No anexo D, pode ser consultado o diagrama de gantt construido para este planeamento inicial.

Após o mês de fevereiro, e de acordo com as recomendações feitas ao trabalho na apresentação intermédia, foram realizados vários ajustes ao plano de modo a tornar a contribuição do estágio mais sólida, que contemplaram melhorias nas componentes já planeadas e a adição de novas etapas. De uma forma mais resumida as principais alterações ao plano foram as seguintes:

- Redução ao número de dispositivos em teste, de forma a focar naqueles que poderiam trazer mais valor à entidade acolhedora;
- Reformulação de alguns dos objetivos do estágios;
- Removida a componente de automatização de testes;
- Adicionada uma nova fase ao trabalho, dado o seu âmbito e as necessidades da entidade acolhedora.

Na figura 1.1 encontra-se representado o diagrama de *Gantt* que contem a representação temporal do trabalho efetivamente realizado durante no segundo semestre, tendo em conta as alterações e adaptações necessárias face aos contratempos que ocorreram e que se encontram descritos no capítulo 4.

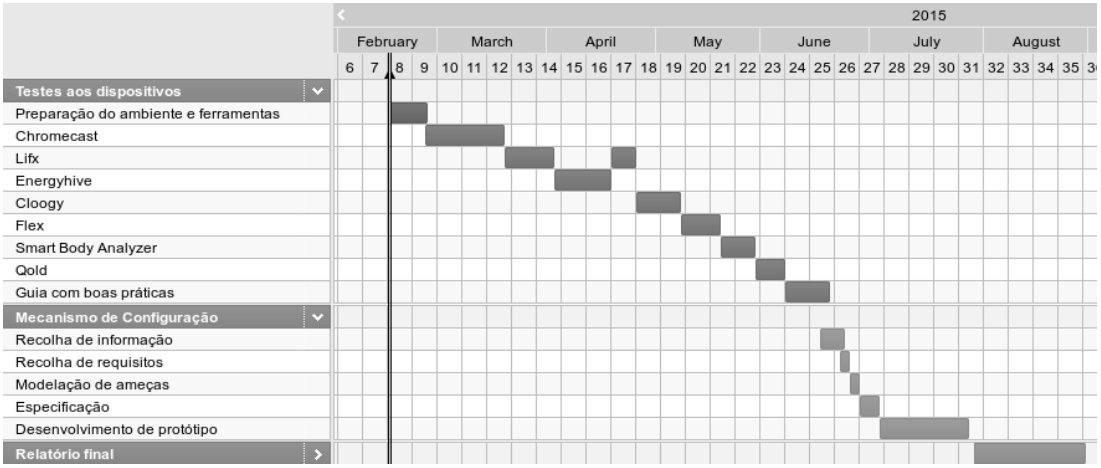


FIGURA 1.1: Execução do trabalho ao longo do segundo semestre

1.5 Estrutura do documento

Este relatório encontra-se estruturado através de 6 capítulos, onde se fundamenta, descreve e justifica todo o trabalho realizado.

No capítulo 2, é feita uma breve introdução à Internet dos objetos, onde se aborda a visão, as potencialidades, tecnologias desenvolvidas para este novo "conceito" e propostas para a arquitetura de novos sistemas baseados na Internet of Things (IoT). São depois discutidos alguns dos desafios e soluções que se colocam para que se possa garantir a segurança e a privacidade neste ambiente.

Neste capítulo, são ainda abordados os testes de penetração, uma forma de testar e descobrir falhas de segurança em sistemas informáticos, que é utilizada na realização do presente trabalho. É feita também uma revisão dos aspetos que em 2014 mais afetaram a segurança em equipamentos relacionados com a IoT.

No terceiro capítulo, é descrito o modo como foi realizado o trabalho, os equipamentos incluídos no estudo, que aspetos foram testados e o modo de divulgação dos resultados.

No quarto capítulo, são apresentados os resultados obtidos, detalhados para cada um dos equipamentos, discutidos os aspetos de maior risco e o que pode ser feito para mitigar estes problemas.

No quinto capítulo, é proposto um mecanismo que garante ao utilizador a configuração de determinados dispositivos de forma segura. Neste capitulo é realizada a recolha dos requisitos, a modelação das ameaças, descrita a especificação e validação da solução.

No último capítulo, é feita uma reflexão sobre todo o trabalho realizado e os passos necessários para num futuro próximo dar continuidade a tudo o que foi desenvolvido.

Capítulo 2

Estado da arte

2.1 Internet dos objetos

O termo "Internet of Things"(IoT) foi referenciado pela primeira vez em 1999 num contexto da área da gestão, por Kevin Asthon [1].

Na ultima década esta definição tem vindo a sofrer algumas adaptações e neste momento engloba tudo o que é dispositivo ligado de certa forma à rede global, desde que tenha a capacidade de interagir com o mundo que o rodeia. As aplicações deste novo conjunto de equipamentos interligados englobam as mais variadas áreas que vão desde a saúde aos transportes, passando pela indústria e pela automação do lar [1].

Recentemente, vários autores tentaram definir de uma forma precisa o conceito, mas até ao momento não existe um consenso alargado, onde cada um deles aborda a questão de acordo com a visão que tem para o futuro.

O grupo de trabalho na tecnologia Radio Frequency Identification (RFID) do European Technology Platform on Smart Systems Integration (EPoSS) [2] define a IoT como:

> "Uma rede global de objetos interligados, unicamente acessíveis através de protocolos de comunicação *standard*."

Por outro lado o CERP-IOT, uma rede de investigação na Europa, usa a seguinte definição [3] :

> "Objectos" são participantes em processos sociais, de negócio e de informação onde lhes é dada a possibilidade de interagir e comunicar entre eles e o ambiente que os rodeia através da troca de dados recolhidos desse ambiente, enquanto reagem autonomamente a eventos do mundo real de forma a o poder influenciar através a execução de processos que criam ações e serviços com ou sem intervenção humana.

Autores como Gubbi et al. [1] por sua vez, definem a *Internet of Things* da seguinte forma:

> A interligação de sensores e atuadores que têm a capacidade de partilhar a informação por múltiplas plataformas através de uma *framework* unificada, criando uma visão que permite a criação de aplicações inovadoras. Isto é obtido através de recolha permanente, análise de dados e representação da informação com a computação na nuvem como tecnologia unificadora.

Miorandi et al. [4] opta por uma definição mais simples:

> Plataforma global que permite máquinas e objetos inteligentes comunicar, dialogar, computar e coordenar

Apesar das suas diferenças é possível observar alguns aspetos em comum, que nos dão uma ideia do fim a que se pretende chegar.

A evolução da Internet para uma rede cada vez mais composta por objetos interligados, que não só recolhem informação sobre o meio ambiente como também agem sobre o mesmo, combinado com a utilização dos standards existentes tem permitido criar e desenvolver novos serviços em várias áreas que vão desde a mera transferência de informação, à análise de dados e construção de novas aplicações que até há bem pouco tempo pertenciam à área da ficção. Utilizando tecnologias de comunicação existentes como o *Bluetooth*, RFID, Wi-Fi ou rede telefónica, juntamente com sensores e atuadores, a IoT deixou de ser um conceito de um futuro distante mas algo já presente no nosso dia a dia [1].

O número de "coisas" que trocam informação entre elas e que estão ligadas à Internet será muito maior que o número de pessoas, tornando os humanos numa minoria, no que toca à geração e receção de tráfego [5].

De uma forma geral, o termo IoT é amplamente utilizado para nos referirmos a [4]:

- Uma rede global de objetos inteligentes interligados por meio de tecnologias relacionadas com a Internet;
- Uma coleção de tecnologias necessárias para realizar essa visão, tais como RFID, sensores, dispositivos de comunicação Machine to Machine (M2M), etc;
- A construção de aplicações e serviços que tirem partido destas tecnologias de modo a gerar novas oportunidades de negócio e de mercado.

Miorandi et al. [4] fundamenta que os três pilares fundamentais para um dispositivo ser considerado parte da IoT são: ser identificável, comunicar e interagir. Deste modo, as relações entre objetos podem ser especificadas no mundo digital mesmo que não exista interligação no mundo real, a comunicação é feita através de redes sem fios comuns ou ad-hoc e os objetos interagem com o meio que os rodeia quer seja através de sensores ou de atuadores, no caso de estarem presentes.

Para que possamos então usufruir de uma IoT de qualidade, os seguintes componentes/-características de sistema necessitam de estar presentes [4]:

- Heterogeneidade de dispositivos;
- Escalabilidade;
- Troca de dados através de tecnologias sem fios;
- Gestão de energia otimizada;
- Capacidades de localização e monitorização;
- Capacidade de auto-organização;
- Interoperabilidade e gestão de dados;
- Mecanismos de segurança e privacidade embutidos.

Para que tudo isto seja possível, no mundo da Internet dos objetos as ligações sem fios serão o meio predominante na transmissão e receção de informação. Nos dias que correm e tendo por base a tecnologia atual podemos já contar com dispositivos que usam RFID,

ZigBee, Universal Mobile Telecomunications System (UMTS), General Packet Radio Service (GPRS), WiFi, WiMax, etc [5].

Assegurar a segurança é um ponto crítico, pois o sistema geralmente está ligado a atuadores, tornando-se a proteção dos sistemas um aspeto muito importante [1]. Exemplo disso são os novos produtos desenvolvidos para ajudar e melhorar a qualidade de vida de pessoas com limitações físicas, pois como são mais vulneráveis, falhas de segurança poderão colocar a sua integridade física em risco [6].

2.1.1 Abordagens no desenvolvimento da IoT

A visão da IoT pode ser vista como centrada na Internet ou centrada nos *objetos*. Na arquitetura centrada na Internet, as aplicações e serviços são o centro das atenções enquanto que os "objectos" funcionam apenas como terminais com o objetivo de disponibilizar dados. Na visão centrada nos "objectos" estes são tratados como o principal componente. Todo o sistema está focado na comunicação entre os seus intervenientes [1, 7]. De acordo com Gubbi et al., para usufruir de todo o potencial da computação da nuvem e da informação recolhida por todos os objetos, uma *framework* centralizada na "nuvem" parece a mais viável.

Apesar dos objetos "inteligentes" poderem correr alguns serviços ou programas leves é muito pouco provável que venham a executar tarefas dispendiosas ou operar grandes quantidades de dados ao mesmo tempo. Desta forma um aspeto fundamental da IoT é a interligação à atual infraestrutura da Internet de modo a poder fornecer os dados e um determinado raio de ação aos serviços web baseados na "nuvem", que por sua vez têm ao seu dispor uma enorme capacidade de processamento e armazenamento. Permitindo deste modo trazer um melhor controlo e mais benefícios para o utilizador final [4].

O paradigma de computação na nuvem garante estes recursos em grandes *datacenters*, permitindo recolher e tratar todos os dados provenientes dos sensores, transformá-los em informação útil e se necessário desencadear uma resposta através dos atuadores [1].

Estas duas visões abordam utilizações distintas para as quais diferentes dispositivos são desenvolvidos. Neste estudo estão em análise equipamentos que se encaixam em cada uma delas. De uma forma geral quer as características de um objeto estejam mais perto de uma visão ou de outra, este irá acabar por se enquadrar no amplo conceito que é a Internet dos objetos.

2.1.2 Tecnologias especificas para a IoT

Na última década as Wireless Sensor Network (WSN) têm sido utilizadas com sucesso nos mais variados ambientes. Estas redes são bastante heterogéneas pois foram implementadas com recurso a diferentes tecnologias [8], entre as quais:

- **ZigBee**, um conjunto de protocolos, composto por várias camadas, que vão desde a camada física à de aplicação. O desenvolvimento desta tecnologia é baseado em perfis, que servem para especificar características e políticas de modo a validar a interoperabilidade entre dispositivos.
- **Z-Wave**, um protocolo desenvolvido pela ZenSys para automação residencial e pequenos espaço comerciais. O principal objetivo é a transmissão de mensagens de uma unidade de controlo para um ou mais nós da rede.
- **INSTEON**, um protocolo com uma topologia *mesh*, caracterizada por cada nó poder servir de intermediário no encaminhamento do tráfego, permitindo assim que a comunicação entre dois nós que estejam fora do alcance um do outro, possa ser realizada através de saltos entre outros nós.

No entanto, hoje em dia o objetivo é que os dispositivos estejam acessíveis através de protocolos baseados em IP, de forma a poderem comunicar através da Internet. Num futuro próximo quando a utilização do IPv6 se tornar mais generalizada será possível atribuir um endereço a cada um destes equipamentos, embora que para este tipo de equipamentos é necessário encontrar uma alternativa mais leve [8].

Para resolver este assunto encontra-se a ser desenvolvida uma versão mais leve do protocolo IPv6, o 6LoWPAN. Este protocolo é pensado para dispositivos embebidos que necessitam de comunicar com a Internet.

No 6LoWPAN os dispositivos são ligados a Internet através de um "router" que faz a ligação, compressão e descoberta dos objetos[8].

Devido ao facto do protocolo Hypertext Transfer Protocol (HTTP) ser hoje amplamente utilizado na Internet e de forma a facilitar a integração de sistemas, é importante que os novos dispositivos sejam capazes de comunicar com serviços na Internet através deste protocolo. Mas o HTTP não foi pensado para esta nova realidade, os seus cabeçalhos são frequentemente de grandes dimensões e têm de ser fragmentados quando este é usado com o 6LoWPAN. Juntando o facto de não utilizar o protocolo User Datagram Protocol (UDP), faz com que seja preciso encontrar uma alternativa. O grupo de trabalho Constrained Restful Environments (CoRE) da Internet Engineering Task Force (IETF),

encontra-se a trabalhar numa alternativa chamada Constrained Application Protocol (CoAP), um protocolo compatível com o HTTP, mas pensado para dispositivos embebidos com muitas limitações, sendo capaz de ser usado sobre o UDP [6, 8].

No entanto podemos observar que por uma questão de compatibilidade e facilidade de instalação muitos destes objetos que chegam ao mercado de consumo comunicam através de tecnologias convencionais, tais como *BlueTooth* e *Wi-Fi*.

2.2 Segurança na Internet dos objetos

A segurança será uma das maiores preocupações assim que estas redes começarem a ganhar dimensão. Os sistemas poderão ser atacados de imensas formas, de modo a impedir o correto funcionamento da rede, a injetar dados incorretos, ou ganhar acesso a informação confidencial [1].

Estas preocupações com a segurança no que toca à IoT são mais que pertinentes, nunca é demais reforçar a ideia de que num cenário de adoção global da Internet dos objetos, grande parte dos objetos do nosso dia a dia tornar-se-ão riscos para a segurança quer da informação quer da população. Sendo um dado adquirido que a IoT poderá distribuir estes riscos muito mais amplamente do que a Internet o fez até ao momento [7].

Como em muitos casos estes "objectos" são quase invisíveis para o utilizador comum, vêm potenciar mecanismos de vigilância que poderão estar presentes na maior parte do nosso quotidiano. Desta forma, assegurar que existem mecanismos de segurança implementados e garantias que os dados recolhidos não violam a privacidade dos utilizadores ou alvos, é importantíssimo [7]. Tal como na Internet que todos conhecemos, uma primeira linha de defesa é sem dúvida o recurso à criptografia.

A segurança é um componente crítico para que se possa começar a assistir a uma adoção em massa da Internet dos objetos e das suas aplicações. Sem garantias de confidencialidade, autenticidade e privacidade, muitos dos interessados neste novo paradigma poderão não ter reunidas as condições necessárias para iniciar o processo de mudança [4].

Se tivermos em conta uma utilização generalizada e aberta de todo o ecossistema da IoT, encontraremos certamente situações em que uma entidade possui e opera os dispositivos, outra entidade armazena e processa os dados e outras entidades usam a informação gerada para diferentes fins. Neste contexto notamos logo que existem vários aspetos, em diferentes momentos, em que a segurança tem de ser garantida [4].

Outro aspeto que dificulta ainda mais o trabalho a efetuar neste tema, é o ambiente inóspito em que a IoT e os dispositivos que a constituem têm que atuar. Torna-a extremamente vulnerável, devido a vários fatores tais como o facto de estarem fisicamente mais expostos, a maior parte da comunicação ser feita sem fios e por terem fracos recursos de armazenamento e de processamento. Nestas condições a implementação de mecanismos de segurança mais complexos torna-se bastante difícil [7].

Vários autores já propuseram arquiteturas de segurança pensadas para a IoT, que têm em mente possíveis problemas de segurança nas várias camadas de rede. São propostas também algumas técnicas, algoritmos e tecnologias na comunicação entre dispositivos, na proteção dos dados dos sensores e mesmo nos mecanismos de encriptação usados. Mas devido ao facto de ainda não existir um consenso sobre uma estrutura de segurança apropriada para a IoT, leva a crer que hajam muitas deficiências nesta área, principalmente nos dispositivos que já se encontram no mercado [9].

Sem dúvida que a melhor forma de abordar o problema está em "atacar" as questões relacionadas com a segurança desde o momento em que se conceptualiza um novo produto/equipamento. Esta é a uma das recomendações da União Europeia, que é tida em conta num *whitepaper* realizado pelo *NCC Group* [10]. Neste documento é especificado um guia para o desenvolvimento de dispositivos para a IoT com a segurança em mente, mesmo que compromissos e decisões difíceis tenham de ser feitas opondo a segurança à usabilidade.

A decisão de atacar um sistema geralmente é feita com um ou vários objetivos em mente, onde se incluem a extração de alguma informação, o ganho de controlo sobre o sistema, a modificação de informação que esteja armazenada ou mesmo fazer com que o sistema não funcione da forma esperada [11].

Desta forma os principais desafios que se colocam neste novo ambiente de forma a que um sistema possa ser considerado seguro são a Confidencialidade, Integridade, Disponibilidade, Privacidade, Autenticação e Autorização. Qualquer ataque que seja efetuado à rede ou aos equipamentos terá sempre de comprometer um dos aspetos acima mencionados.

Estes aspetos dependem de uma boa infraestrutura para gestão de chaves, de forma fornecer os elementos necessários aos algoritmos criptográficos [12]. De uma forma mais detalhada vejamos a razão porque têm de ser garantidos:

A Confidencialidade dos dados no contexto da Internet significa que apenas pessoas ou objetos autorizados podem aceder e modificar ao seu conteúdo. Na IoT o contexto torna-se um pouco mais complexo, pois até ao momento apenas os humanos

entravam na equação e agora temos de ter em conta os outros objetos [4]. O uso de Transport Layer Security (TLS) e o seu equivalente Datagram Transport Layer Security (DTLS) permite tornar os dados confidenciais enquanto se encontram em trânsito, e são usados juntamente com Transmission Control Protocol (TCP) e UDP respetivamente [12]. Permitindo desta forma abranger dispositivos mais e menos capazes e com diferentes restrições energéticas.

A Integridade dos dados é a garantia que os mesmos não são modificados entre a origem e o destino sem que essa alteração seja detetável. O desafio de garantir esta componente é já um tópico comum na área da segurança das comunicações. No contexto da IoT não deixa de ser relevante assegurar que um atacante não consegue modificar os dados que estão a ser transmitidos ou armazenados sem que o sistema detete a alteração [7]. O uso de TLS para além da confidencialidade também resolve este problema.

A Disponibilidade é descrita como a capacidade do dispositivo, independentemente das circunstâncias, estar acessível e garantir os serviços que são da sua responsabilidade. Esta é outra componente muito importante a ter em conta na IoT, pois um tipo de ataque muito comum na Internet é o Distributed Denial of Service (DDoS), que visa impedir que o serviço esteja disponível para executar as suas tarefas. Dado o largo espectro das aplicações da IoT e a fraca capacidade dos equipamentos, as consequências de não ser garantido este aspeto podem ser graves e difíceis de recuperar [9].

A Autenticação e a autorização são aspetos essenciais de forma a fornecer a garantia que quem produz ou acede aos dados é quem diz ser e que tem permissão para o fazer. O uso de TLS já fornece uma base para a autenticação e para a autorização. Uma boa política para a IoT seria a implementação de um sistema de Role-based Access Control (RBAC), em que as permissões não são dadas aos utilizadores mas sim aos papéis para os quais foram destacados. No entanto, são necessárias algumas modificações pois em certos casos estamos a falar de fluxos de dados em tempo real e não a dados estáticos [4].

Todos estes aspetos já são abordados há muito tempo no caso da Internet, no entanto a adaptação à IoT de algumas das tecnologias utilizadas, como por exemplo o TLS, nem sempre é possível. Tornando-se assim essencial estudar novas formas de resolver estes problemas.

Já a privacidade é um tema que com a IoT ganha uma nova dimensão, não só a nível técnico como em muitos outros aspetos [13–15].

2.2.1 Privacidade

A noção de privacidade pressupõe a ocultação de informação pessoal assim como a capacidade de controlar o que acontece com essa informação. O direito à privacidade é considerado como um direito básico e inalienável do ser humano ou é mesmo tratado como uma posse pessoal [14].

A utilização de dispositivos relacionados com a IoT ou mesmo o uso de etiquetas RFID, pode levar a que determinadas informações pessoais sejam partilhadas/armazenadas sem o conhecimento do utilizador.

Algumas entidades públicas já se encontram cientes de alguns dos riscos da IoT, como por exemplo a União Europeia, que emitiu algumas recomendações sobre a implementação de alguns mecanismos relacionados com a privacidade nos dispositivos relacionados com a IoT. Está provado que preocupações sobre a proteção da privacidade dos utilizadores são uma grande barreira à adoção e difusão de tecnologias relacionadas com a IoT [7].

Um problema comum na abordagem às questões de segurança e privacidade está relacionado com o facto de que as preocupações com estes aspetos não são idênticas em todas as regiões e culturas do mundo, o que torna a aplicação de algumas medidas e princípios difíceis quando a implementação é feita a um nível global [14].

O grau de privacidade dado pelo sistema é definido pelas regras pelas quais os dados podem ser acedidos. A capacidade de manter um elevado grau de privacidade na IoT é fundamental porque esta tem a capacidade de ser muito mais invasiva na vida das pessoas do que se possa imaginar. Neste aspeto a IoT ao contrário da Internet convencional coloca problemas não só ao nível da privacidade das pessoas que a usam mas também de outros que não esteja a usufruir de qualquer produto ou serviço relacionado com a IoT [4, 7, 16].

Miorandi et al. [4] propõe a existência de 3 desafios fundamentais que se colocam à IoT relacionados com a privacidade:

- Definição de um modelo geral de privacidade na IoT;
- Desenvolvimento de técnicas que imponham o cumprimento das normas de privacidade e que sejam capazes de lidar um sistema de grande escala e bastante heterogéneo;
- Desenvolver soluções que permitam um equilíbrio entre as necessidades de privacidade de algumas soluções e as necessidades de localização e *tracking* de outras.

De uma forma geral, é importante que o utilizador tenha conhecimento da informação que está a ser agregada, que tenha dado permissão para a sua recolha e que apenas esse conjunto especifico do dados seja recolhido.

2.3 Problemas de segurança comuns

Durante estes últimos anos assistiu-se à chegada de um vasto número de equipamentos relacionados com a Internet dos objetos ao mercado de consumo. Muitos, apesar de não utilizarem exclusivamente tecnologias e protocolos pensados para a IoT, estão ligados direta ou indiretamente à Internet.

Dada esta nova realidade e devido ao facto de estes dispositivos se estarem a infiltrar cada vez mais em diferentes aspetos do quotidiano da população, a segurança destes equipamentos tem vindo a ser alvo de várias análises e estudos.

A Open Web Application Security Project (OWASP), uma organização sem fins lucrativos cujo objetivo está focado na melhoria da segurança a nível do software, compilou uma lista de problemas de segurança críticos que se encontram presentes em muitos dispositivos com ligação à rede global relacionados com a IoT.

Denominada de *OWASP Internet of Things Top 10*, este projeto para além de enumerar e descrever os problemas, exemplifica de uma forma simplificada possíveis ataques e como podem ser resolvidas as falhas.

Na versão de 2014, os seguintes aspetos foram considerados os mais problemáticos:

Interface web insegura A existência de interfaces web para aceder à administração dos dispositivos, que não necessitem de credenciais (ou as padrão sejam fracas) é um aspeto comum. Assim como interfaces com falhas na validação de *inputs* que exponham os utilizadores a possíveis ataques por Cross-site Scripting (XSS).

Fracos mecanismos de autenticação e autorização A utilização de *passwords* fracas na verificação dos utilizadores, os fracos mecanismos de controlo de acessos e mecanismos de recuperação de palavras-passe deficitários, são problemas que são fáceis de explorar e ainda são comuns.

Serviços de rede inseguros A utilização de software para a interação com a rede (na suas diferentes camadas) não atualizado (ou desnecessário) e com falhas conhecidas pode deixar o dispositivo à mercê de ataques que exploram *buffer overflows* ou mesmo de DDoS.

Ausência de encriptação na transmissão Em muitas ocasiões os dispositivos ao comunicar entre si, com serviços na rede local ou mesmo através da Internet transmitem os dados sem recorrer a qualquer tipo de encriptação, permitindo a um atacante visualizar e modificar todo o seu conteúdo.

Privacidade Os problemas com privacidade surgem sobretudo na ausência do uso de encriptação quer no dispositivo quer nas comunicações do mesmo. Outra questão é a recolha e partilha de informações desnecessárias ao funcionamento do dispositivo ou sobre as quais o utilizador não deu permissão para o fazer.

Interface na *Cloud* insegura A falta de encriptação e de mecanismos de segurança, na comunicação e nas interfaces dos serviços na Internet, com os quais o dispositivo interage são problemas que podem ter muito impacto, pois muitos destes equipamentos podem ser controlados ou acedidos remotamente.

Interface com dispositivos móveis insegura Da mesma forma que a interface com a *Cloud*, a interação com as aplicações móveis ou mesmo as próprias aplicações podem ser comprometidas.

Configuração insuficiente A ausência de controlos que permitam ao utilizador configurar os parâmetros de segurança do dispositivo, impedem o utilizador de personalizar e aumentar o nível de segurança presente por predefinição.

Atualizações de software inseguras Novas versões do software/firmware utilizado no equipamento transmitidas sem encriptação e sem uma verificação da fonte, podem comprometer o dispositivo sem deixar quaisquer rastos de um ataque.

Fraca segurança física do equipamento Dada a grande exposição deste tipo de equipamentos, a existência de interfaces Universal Serial Bus (USB) e a facilidade de desmontar e voltar a montar o dispositivo sem deixar sinais que a sua integridade física foi violada, é um problema grave.

Como é possível observar na lista acima, existem muitas falhas consideradas básicas nos dias de hoje que necessitam de ser corrigidas, apesar de algumas serem mais difíceis de explorar que outras, dependendo das circunstâncias.

2.4 Testes de penetração

Na sua essência, os testes de penetração consistem na análise de um determinado aspeto de um sistema, na expectativa de encontrar alguma vulnerabilidade. São uma forma de simular os métodos que um atacante poderá usar para ultrapassar os controlos

e configurações de segurança de um determinado sistema e por em causa quer o seu funcionamento quer a sua informação [17–19].

Se os benefícios de comprometer um sistema forem grandes, é muito provável que os possíveis atacantes tenham mais recursos disponíveis que uma equipa que realize testes de penetração. Uma forma de equilibrar a balança é fornecer mais informação à equipa que se encontra a realizar os testes de forma a que possam ter um acesso a todos os aspetos que um atacante possa descobrir [17].

Existem algumas vantagens em conhecer o funcionamento do sistema e já ter à partida alguma informação interna na altura de planear o teste. Por outro lado poderá influenciar de certa forma os testes não verificando a resposta do sistema a certo tipo de ataques. Este tipo de abordagem é também conhecida *Whitebox* ou mesmo *Crystalbox* dependendo da profundidade e qualidade da informação que a pessoa que vai testar tem em sua posse, é usado em situações em que o tempo é limitado ou a fase de procura e rastreio de todo o sistema se encontra fora do âmbito do trabalho.

Em muitos casos, os testes de penetração são feitos a partir do ponto de vista de um atacante, também conhecido como uma abordagem *Blackbox*, o que implica desconhecer à priori o funcionamento interno do sistema. Esta abordagem é muito mais dispendiosa ao nível dos recursos e do tempo utilizados, pois precisa ainda de reunir informação sobre o sistema e geralmente é utilizada com o objetivo não de reunir um vasto número de vulnerabilidades mas sim encontrar a forma mais fácil de penetrar num sistema sem ser detetado [18–20].

Existem no mercado algumas ferramentas que permitem automatizar o processo de encontrar vulnerabilidades comuns, evitando um trabalho manual e repetitivo, fornecendo já alguns dados interessantes. Estes programas não garantem uma cobertura total das vulnerabilidades e podem apresentar um número variável de falsos positivos, mas são já um bom ponto de partida [18, 20].

Os testes de penetração têm sido uma área muito controversa ao longo do tempo [18], mas na ultima década têm vindo a ser adotados por muitas empresa, quer pelos benefícios quer por serem uma componente importante de muitos *standards*, certificações e regulações que estas necessitam para fazer negócio como por exemplo o *PCI Data Security Standard* [21].

Este tipo de atividade geralmente obtém melhores resultados se for realizado de uma forma estruturada, com um plano bem definido, desta forma o âmbito e a abrangência do teste podem ser geridas de forma correta. No entanto a execução dos testes de penetração nem sempre segue um caminho único e a descoberta de vulnerabilidades pode levar à descoberta de outras e outros vetores de ataque o que pode levar à criação de novos

testes no momento. Desta forma, é importante que exista alguma flexibilidade, mas nunca abandonar um certo nível de disciplina e documentar todo o progresso efetuado [18].

2.4.1 Metodologias

Existem hoje em dias várias propostas de alto nível que pretendem documentar e guiar a forma como estes testes são efetuados, através de um conjunto de etapas pelas quais o trabalho deverá passar. Entre elas temos o Penetration Testing Execution Standard (PTES), o Open Source Security Testing Methodology Manual (OSSTMM), *OWASP Testing Guide* (OWASP TG) e o National Institute of Standards and Technology (NIST) SP 800-115.

Para o presente trabalho pretende-se que as várias fases do processo sejam explicitas e isoladas, que o material seja facilmente adaptável a diferentes circunstancias e que seja abrangente ou seja que não se limite a cobrir um grupo restrito de aspetos independentemente da sua importância.

Abaixo seguem-se algumas características de cada um dos documentos supracitados:

PTES Este standard iniciou-se em 2009, com o propósito de descrever uma metodologia e processo exclusivamente dedicada aos testes de penetração. Pensado para servir como guia, tanto para clientes como para consultores, sobre o modo como os testes deverão ser executados. Para além das várias fases que compõem o processo, é dada ainda muita atenção aos aspetos técnicos necessários para a conclusão do mesmo. As várias etapas são descritas individualmente, aprofundando em cada uma delas os detalhas importantes em ter em conta e como deverá ser conduzido o processo, e vão desde a negociação com o cliente até à elaboração do relatório final.

OSSTMM Já na sua terceira versão e com a quarta em desenvolvimento, este standard descreve de uma forma mais teórica e exaustiva como deverão ser conduzidos os vários aspetos de um teste de segurança. São explicados os vários termos, as razões pelas quais devem ser feitas a análises de segurança, que componentes devem ser tidos em conta e as formulas utilizadas para calcular o nível de segurança de cada um deles. O final os resultados obtidos deverão ser transformados num relatório (Security Test Audit Report (STAR)), para o qual é fornecido um modelo.

OWASP TG Este documento desenvolvido pela OWASP, descreve vários aspetos sob a forma de *checklist* que deverão ser testados e como deverão ser realizados esses testes durante e depois do desenvolvimento do produto. Não descreve um processo

com várias etapas e encontra-se mais focado em questões técnicas, não garantindo neste momento todos os critérios estabelecidos. Não é exclusivamente dedicado aos testes de penetração e está muito focado em aplicações e serviços web, não sendo deste modo o mais apropriado para avaliação de segurança em dispositivos da Internet dos objetos.

SP 800-115 Publicado pelo NIST, este conjunto de recomendações, focado na verificação da segurança da informação, que apesar de abordar muitos aspetos pertinentes, faz questão de informar na sua introdução que não é o seu objetivo abordar de uma forma extensiva e aprofundada a realização de testes de segurança. Tenta então desta forma abordar por alto um conjunto de boas práticas e metodologias, focando nos seus pontos fortes e limitações de modo a poder apresentar algumas recomendações.

Dados os critérios estabelecidos, tanto o PTES como o OSSTMM poderão ser usados. No entanto, para a realização deste trabalho optou-se pelo PTES dada a forma simples que usa para descrever uma *framework* genérica de mais alto nível, assim como pela descrição de aspetos técnicos, que são muito úteis. Das propostas descritas é a única pensada exclusivamente para testes de penetração, o que facilitará o planeamento e execução de todo o trabalho a realizar.

O PTES compreende então um processo pelo qual deverão passar os testes de penetração que contém 7 etapas. Estas são executadas sequencialmente e têm as seguintes características:

Abordagem Inicial Nesta etapa, é feita a primeira abordagem ao problema, onde são definidos os objetivos, a abrangência, o contexto e as datas nas quais ocorrerão os testes. São também definidas as regras que irão reger o trabalho.

Recolha de Informações Este capitulo descreve a pesquisa que deverá ser feita sobre o alvo e que tipo de informação deverá ser recolhida, que posteriormente servirão de base para os testes de penetração a ser realizados.

Definição das Ameaças Nesta etapa e com base nas informações previamente recolhidas, são definidos que componentes e processos se encontram expostos e que deverão ser alvo do trabalho. Compreende ainda a seleção das ferramentas mais adequadas para cada caso.

Análise de vulnerabilidades Nesta fase, dada toda a informação existente, é iniciado então o processo de procura e validação de vulnerabilidades. São utilizadas formas ativas e passivas de procura, recorrendo-se muitas vezes à automatização.

Exploração Depois de conhecidas as vulnerabilidades, o objetivo passa então por tentar através das mesmas ultrapassar os mecanismos de segurança e conseguir o acesso a recursos que de outra forma estariam fora do alcance de um atacante.

Pós-Exploração O objetivo desta etapa é então avaliar o valor dos recursos que foram comprometidos e tentar manter o controlo sobre os mesmos.

Elaboração do relatório A última fase contempla então a produção de um relatório, que contém todos os resultados do trabalho, informação detalhada sobre as falhas descobertas e sugestões para a correção das mesmas.

2.5 Análise de tráfego

Para além dos testes de penetração, a análise de tráfego pode fornecer informações importantes sobre vários aspetos do funcionamento de um determinado equipamento. No caso das comunicações não se encontrarem bem protegidas existe a probabilidade de se poder aceder ao conteúdo das mesmas bem como levar à descoberta de novos vetores de ataque.

A análise de tráfego é um conceito que pode ser descrito como conjunto de processos e técnicas que intercetam uma dada comunicação de modo a analisar e compreender os seus conteúdos, quer direta quer indiretamente, deduzindo certas informações dos padrões identificados no tráfego.

Na redes informáticas e na Internet estes dados são recolhidos de forma passiva, muitas vezes utilizando ferramentas denominadas de *packet sniffers*. Estas ferramentas recolhem e guardam todo o tráfego que passa numa determinada interface de rede, de modo a que estes dados possam ser analisados posteriormente [22].

Em determinadas situações, onde o atacante não tem acesso ao meio por onde circula o tráfego, é possível através de ataques já conhecidos redirecionar o tráfego de modo a ficar acessível ao atacante para que este possa efetuar a sua captura.

Após capturados os dados, no caso estarem protegidos, a entidade que se encontra a realizar a captura poderá utilizar os chamados meta-dados (parâmetros e informações acessórias) para inferir determinadas características acerca da comunicação. O reconhecimento de padrões e um conjunto de outros ataques como *timming attacks*, *Packet Counting Attacks* e outros, poderão ser utilizados para aprofundar o conhecimento sobre o conteúdo da comunicação [23].

Neste trabalho, estas técnicas são usadas apenas de uma forma mais superficial, de modo a detetar possíveis problemas que sejam mais óbvios.

2.6 Ferramentas

Neste capitulo é feita uma breve descrição das ferramentas usadas para executar a análise aos dispositivos selecionados de modo a descobrir ou explorar vulnerabilidades na segurança dos equipamentos e serviços que os acompanham.

Na lista apenas são abordados os programas usados para as finalidades específicas do trabalho, sendo deixados de fora muitos outros utilitários (não relacionados com análise de segurança) utilizados para executar tarefas auxiliares.

Cada um dos programas especificados abaixo é focado numa área específica, mesmo que algumas das funcionalidades se possam sobrepor. Assim será possível abranger diferentes aspetos tais como a recolha de informação da rede, procura de vulnerabilidades nos serviços de rede e das aplicações, recolha do tráfego da rede, análise das implementações criptográficas, etc.

Os critérios usados para a escolha de cada uma das ferramentas variam de acordo com a área à qual se aplicam, pois dependem de diferentes características e têm diferentes condições para a sua aquisição. Desta forma para cada uma das opções são mencionadas também as alternativas e as razões que tiveram mais peso na decisão.

2.6.1 Wireshark

O Wireshark é um sistema de análise de pacotes de rede muito utilizado atualmente e que se encontra disponível num grande número de plataformas. Permite recolher o tráfego captado pela interface de rede, quer este tenha como destino a própria máquina ou não.

Para além de recolher o tráfego é também capaz de o analisar e realizar um variado conjunto de operações que tornam a tarefa de retirar informação pertinente dos dados recolhidos mais fácil. Entre as principais características deste programa, as seguintes são importantes para os trabalhos relacionados com segurança:

- Fácil inspeção de centenas de protocolos utilizados nas várias camadas de rede.
- Captura do tráfego para posterior análise *offline*.
- Capacidade de desencriptar protocolos como Internet Protocol Security (IPSec), Kerberos, Secure Socket Layer (SSL)/TLS, Simple Network Management Protocol (SNMP)v3, Wired Equivalent Privacy (WEP) e Wi-Fi Protected Access (WPA)/WPA2.

- Todos os dados recolhidos podem ser exportados em vários formatos de modo a poderem ser analisados utilizando outras ferramentas.
- Capacidade de estender as funcionalidades através de *plugins*.

Atualmente esta ferramenta é disponibilizada com a licença GNU General Public License (GPL) v2. Uma possível alternativa à utilização do Wireshark é o tcp-dump, mas esta última foi preterida devido ao facto do autor já ter uma maior experiência com o Wireshark e da existência da interface gráfica.

Site oficial: https://wireshark.org/

2.6.2 Aircrack-ng

O Aircrack-ng é um conjunto de ferramentas feitas com o objetivo de atacar redes sem fios que utilizam a tecnologia Wi-Fi(802.11), que são disponibilizadas com a licença GPL.

Entre as ferramentas disponibilizadas encontramos algumas muito pertinentes para o presente trabalho que permitem realizar as seguintes operações:

- Injetar pacotes na rede.
- Colocar placas de rede em modo *monitor*.
- Descobrir as chaves utilizadas em redes WEP e WPA.
- Capacidade de se fazer passar por um *access point*.

Site oficial: http://www.aircrack-ng.org/

2.6.3 Metasploit

Disponibilizada em 2004 e desenvolvida inicialmente em *Perl*, o Metasploit é uma *framework* para o desenvolvimento e execução de testes de penetração. É hoje em dia um dos softwares mais utilizados para efetuar testes de penetração e de segurança nos mais variados sistemas.

Atualmente escrito em Ruby, a componente base desta ferramenta é disponibilizada com uma licença BSD e algumas versões com funcionalidades extra usam licenças proprietárias.

Algumas das funcionalidades e características que tornam a ferramenta essencial para este estudo são:

- Grande base de dados de vulnerabilidades e falhas que podem ser exploradas
- Facilidade em desenvolver e automatizar os processos/ataques.
- Inclui vários componentes que permitem explorar as falhas encontradas.

A escolha pela utilização desta ferramenta em prol de alguns dos seus concorrentes tais como *Core Impact* e *Canvas*, mesmo sendo alguns mais poderosos, prende-se com o facto de existir uma grande comunidade que utiliza o Metasploit, com a documentação existente e com o facto a utilização dessas ferramentas terem preços muito para além dos recursos disponibilizados para o presente trabalho.

Site oficial: http://www.metasploit.com/

2.6.4 ZAP

Esta ferramenta, desenvolvida com o apoio da OWASP, é direcionada para o teste de aplicações web. Foi utilizada durante o estudo, pois um dos componentes alvo dos testes são as interfaces web existentes nos dispositivos. As funcionalidades desta ferramenta vão desde o mapeamento da "superfície de ataque" de uma aplicação ou web-site, à deteção de vulnerabilidades comuns nesta plataforma.

Existem algumas alternativas com licenças comerciais e de fonte aberta, entre as quais podemos encontrar o *Burp Suite*, o *w3af* e o *IronWASP*. O ZAP foi escolhido devido à sua performance no *The Web Application Vulnerability Scanners Benchmark de 2014* onde obtém resultados entre os melhores em muitos dos aspetos. O w3af foi assim preterido pelos seus resultados, o *IronWASP* por não estar disponível de forma nativa para Linux e o *Burp suite* porque para se poder tirar o máximo partido desta ferramenta ser necessário adquirir uma licença.

Site oficial: https://www.owasp.org/index.php/ZAP

2.6.5 Nmap

O Nmap é uma ferramenta de auditoria de rede muito flexível e poderosa, disponibilizada sob a licença GPL em 1997. Originalmente estava disponível apenas em sistemas baseados em Linux mas atualmente está disponível em múltiplas plataformas. Permite

fazer o mapeamento de uma rede e recolher informações sobre os dispositivos que dele fazem parte. Entre as funcionalidades e informações que fornece abaixo encontram-se algumas que são pertinentes para este trabalho:

- Descoberta de dispositivos na rede;
- Procura dos portos abertos nos dispositivos;
- Deteção dos serviços que usem determinados portos;
- Deteção do sistema operativo.

Existem diversas ferramentas alternativas ao Nmap, mas a escolha deste software deve-se ao facto de ser quase um standard na auditoria de rede, estar muito bem documentado e a comunidade de utilizadores ser extensa, facilitando assim a obtenção de algum suporte.

Site oficial: http://nmap.org/

2.6.6 Nogotofail

Esta ferramenta desenvolvida pela Google e disponibilizada com a licença Apache 2.0, tem como objetivo ajudar programadores a encontrar e corrigir problemas nas ligações SSL/TLS nas suas aplicações e dispositivos.

A escolha do uso deste ferramenta para este trabalho é baseada no uso das seguintes funcionalidades:

- Testar falhas com a verificação de certificados
- Encontrar componentes que estejam a ser transmitidos sem o recurso a encriptação
- Encontrar problemas nas bibliotecas utilizadas para implementar o uso de SSL/TLS.

Site oficial: https://github.com/google/nogotofail

2.6.7 OpenVAS

O OpenVAS é uma ferramenta que teve a sua origem num *fork* de outro projeto (Nessus) que em 2005 se transformou em software proprietário. A principal funcionalidade deste projeto é a capacidade de rastrear os elementos da rede por vulnerabilidades conhecidas de uma forma automatizada. A sua base de dados é extensa e atualizada muito frequentemente com as falhas e problemas mais recentes.

O software oferece ainda uma componente de gestão onde pode ser feita a alteração das configurações, o tratamento dos resultados obtidos e o agendamento de novos rastreios.

A escolha deste software em alternativa à ferramenta mais popular atualmente no mercado o Nessus ou até do Nexpose, desenvolvida pela mesma empresa que o Metasploit, deve-se ao fator preço para uma versão não limitada destas últimas.

Site oficial: http://www.openvas.org/

2.6.8 Ettercap

O Ettercap é uma ferramenta dedicada especialmente para ataques Man-in-the-Middle (MITM) em redes locais. Fornece um conjunto de funcionalidades que permitem intercetar, capturar e interagir em "tempo-real" com o tráfego.

Esta ferramenta é disponibilizada através de uma licença GPL e pode ser utilizada através das suas diferentes interfaces (Command-line Interface (CLI) e Grafical User Interface (GUI)).

A sua utilização neste trabalho deve-se às suas capacidades de aplicar filtros personalizados de forma a efetuar manipulações no conteúdo das comunicações de uma forma transparente e fácil.

Site oficial: https://ettercap.github.io/ettercap/

2.7 Mecanismos de configuração

Uma das características comuns a muitos dos equipamentos da IoT destinados ao uso doméstico, é o facto de necessitarem de uma forma segura de se poderem ligar à Internet. Em alguns dos objetos este processo é feito através de uma ligação com fios, noutros é usada uma ligação sem fios configurada no próprio dispositivo, mas uma situação muito comum é o equipamento não ter qualquer interface com o utilizador e ser configurado através de outro equipamento.

Uma grande parte dos equipamentos utiliza o seu próprio mecanismo proprietário, que permite ao utilizador efetuar a configuração de forma fácil, por exemplo através do *smartphone*, mas que nem sempre garante a segurança deste processo.

Recentemente vários autores têm abordado este problema [24] e várias empresas têm patenteado soluções nesta áreas [25, 26]. No entanto estas soluções ou não abordam o tema da segurança ou não se adaptam a todas as situações.

Dado que, na segunda etapa do trabalho o problema da configuração inicial é abordado, neste capítulo são analisados vários métodos muito utilizados nesta situação e os seus principais "defeitos".

Wi-fi Protected Setup Esta tecnologia desenvolvida em 2007, é um standard para a configuração de dispositivos de forma segura sem que seja necessário o utilizador comunicar os dados da rede ao dispositivo. Tem por base a existência de um Personal Identification Number (PIN) que deve ser comunicado ao dispositivo ou a ativação do sistema fisicamente no *access point*. Ao longo do tempo este sistema apresentou-se vulnerável ataques de *bruteforce* e no caso de se ativar o sistema fisicamente, a segurança será ignorada por 2 minutos [27, 28].

Access Point Utilizado por muitos produtos, este método pressupõe que o próprio dispositivo inicia em modo *access point*, ao qual o utilizador se pode ligar. Através de uma aplicação ou interface web, são então enviadas as credenciais da rede ao equipamento. No entanto só por si, não fornece garantias de segurança. Obrigando a que estas questões sejam tratadas na camada de aplicação (sendo muitas vezes ignoradas) [27].

Ligação Bluetooth Em muitos dispositivos é optada pela tecnologia *bluetooth*. Neste cenário é criada uma ligação direta ao dispositivo para realizar a configuração. Uma vez que o dispositivo pode não ter interface, os mecanismos de *pairing* muitas vezes são desativados, delegando assim a autenticação e segurança para a camada de aplicação, tal como no cenário anterior.

Blink Up Desenvolvido pela *Electric Imp*, este método permite transferir as credenciais da rede à qual o objeto se deve ligar, através do piscar da luminosidade do ecrã do telemóvel. Esta informação é captada por um sensor ótico existente no dispositivo. No entanto este método requer que seja necessário acesso físico ao dispositivo e a sua especificação não se encontra publicada [29].

SmartConfig Esta tecnologia desenvolvida pela *Texas Instruments* visa configurar os dispositivo sem realizar qualquer ligação ao mesmo. Ao ser ligado o equipamento ativa o modo promiscuo da interface de rede, ficando à escuda de mensagens transmitidas pelo agente que se encontra a realizar a configuração e que já se encontra na rede. A partir de características destas mensagens é possível obter os dados necessários para efetuar a ligação (que podem ser encriptadas com uma chave pré-partilhada). No entanto esta tecnologia apenas se encontra disponível para equipamentos que usam um *chip*, da gama CC3000, desta empresa [27, 30].

2.8 Infraestrutura de chaves públicas e ciclo de vida dos equipamentos

Para satisfazer os vários requisitos de segurança que as implementações relacionadas com a IoT devem contemplar, é necessário por parte do fabricante ponderar toda uma infraestrutura que fornece o suporte para todas as suas operações.

Dada a natureza e as condicionantes da IoT e dos seus dispositivos, a aplicação de algoritmos criptográficos e protocolos não é fácil de implementar. Para além do mais funcionalidades como configuração, gestão, controlo e atualização por parte fabricante tornam a tarefa ainda mais complica, requerendo medidas de autenticação e autorização apropriadas [31].

Entre as soluções existentes para este problema, encontramos o uso de chaves pré-partilhadas(Pre-shared Key (PSK)) e o recurso a criptografia de chave-publica (Public Key Cryptography (PKC)) [32]. Soluções com diferentes características, vantagens e desvantagens, que foram por exemplo incluídas no standard do CoAP [31].

A criptografia de chave pública apesar da desvantagem de ser demasiado pesada, foi demonstrado que mesmo utilizando hardware com características muito limitadas (processador de 4–8 MHz, 4–16 kB de RAM, 48–256 kB de *flash*) esta acaba por ser uma opção viável para dispositivos atuando apenas como "cliente" [33]. A utilização de PKC acaba por ser recomendada [34], por tornar mais acessíveis todas as outras funções que são necessárias à gestão destes equipamentos em escalas maiores.

Desta forma na generalidade dos casos é assumido que as chaves necessárias é autenticação dos dispositivos com o servidor e vice-versa são instaladas no equipamento durante o fabrico. Estas chaves podem estar no formato base (*raw public key*) ou incluídas num certificado. Apesar de ser preferível o segundo formato, dados todos os standards e ferramentas já disponíveis para lidar com o mesmo que transitam da Internet "convencional", nem sempre pode ser adequado a todos os casos, daí a necessidade de incluir o formato base na especificação de protocolos *standard*, como por exemplo o CoAP [34].

Capítulo 3

Metodologia

3.1 Foco do estudo

Um aspeto fulcral na preparação de uma análise de segurança a qualquer tipo de sistema, é a definição dos componentes que serão alvo dos testes, assim como a descrição do modo como estes serão conduzidos.

Só deste modo é possível planear com algum grau de exatidão o trabalho e o seu grau de profundidade. Para este trabalho foram definidos 2 elementos que forneceram a base para o restante planeamento, que são as superfícies alvo de ataque nos dispositivos e o conhecimento inicial sobre o funcionamento dos equipamentos.

3.1.1 Superfícies de ataque

Para a realização do presente trabalho foi estabelecido um grupo restrito de "superfícies" para serem alvo dos testes, todas elas relacionadas com os problemas mais comuns detetados em 2014 pela OWASP. Dado que o funcionamento e o modo de utilização dos vários dispositivos não são homogéneos e os testes são realizados em diferentes circunstâncias, alguns dos pontos não se puderam aplicar a todos os equipamentos. Desta forma os parâmetros abordados no trabalho são os seguintes:

1. Interface web;
2. Mecanismos de autenticação e autorização;
3. Serviços de rede;
4. Transmissão de dados;

5. Dados recolhidos sobre o utilizador;
6. Interface com dispositivos móveis;
7. Liberdade de configuração;
8. Atualizações de software.

Não foram alvo deste trabalho os temas como a segurança física dos objetos ou a segurança dos serviços na Internet com os quais os dispositivos interagem.

3.1.2 Modelo

Dado que não existe qualquer tipo de acesso a informação interna sobre o funcionamento dos dispositivos, sendo toda a informação recolhida através da sua utilização ou através da Internet, o modelo usado é denominado de *Blackbox*.

Com este conhecimento inicial muito limitado, o trabalho é feito de um ponto de vista muito próximo ao de um atacante, tendo como principal desvantagem o facto de ser necessário em primeiro lugar realizar um maior trabalho de reconhecimento e descoberta antes poder efetuar os testes propriamente ditos.

3.2 Dispositivos

Em seguida são descritos os vários dispositivos usados durante a realização de todo o trabalho. A escolha dos equipamentos foi feita com base nos seguintes critérios:

Disponibilidade - a capacidade do autor para adquirir ou ter o equipamento disponível durante a fase em que foram realizados os testes.

Pertinência para a atividade da empresa - Foi dada alguma atenção a equipamentos que sejam relevantes para a área de atuação da empresa responsável pelo estágio.

Popularidade - A utilização dos dispositivos a nível global. Para este critério, dados os equipamentos disponibilizados, foram escolhidos aqueles que reuniam um maior número de downloads das suas aplicações na loja de aplicações da Google.

Os critérios acima listados encontram-se pela ordem de importância que foi atribuída a cada um. A seguinte tabela mostra como é que cada um contribuiu para a escolha dos equipamentos:

Tabela 3.1: Critérios usados na escolha dos dispositivos

Produto / Área	Disponibilidade	Pertinência	Popularidade
Lifx	✓		✓
Cloogy	✓	✓	
ChromeCast	✓		✓
Qold	✓	✓	
Energy Hive	✓	✓	
Smart Body Analyzer	✓		✓
Fitbit Flex	✓		✓

✓- Característica que diferenciou o equipamento de outros dispositivos que não se encontram presentes no estudo.

Estes dispositivos foram escolhidos com o objetivo de ter uma amostra o mais variada possível, de forma a poder representar uma fatia razoável dos vários tipos de dispositivos que nestes últimos anos têm surgido no mercado de consumo e que podem ser enquadrados no âmbito da Internet dos objetos.

Um fator importante na escolha dos equipamentos foi a disponibilidade dos mesmos para aquisição e o material já existente na empresa.

3.2.1 LifX

Figura 3.1: Lâmpada que será alvo dos testes.

Este dispositivo é uma lâmpada Light-Emitting Diode (LED) com a capacidade de ser controlada remotamente através de um *smartphone*, capaz de produzir diversas cores e que através de uma aplicação é capaz de reproduzir diversos efeitos e comportamentos pré-programados, como por exemplo acender gradualmente.

A LifX expõe ainda uma Aplication Programming Interface (API) para os dispositivos móveis que estejam dentro da rede local, estando o seu código disponível no Github[1] e

[1]Perfil da empresa: https://github.com/lifx

site da empresa responsável. A documentação oficial sobre o funcionamento da mesma no momento da análise era escassa.

O projeto para a criação desta lâmpada foi um dos que mais financiamento conseguiu através do processo de *Crowdfunding* sendo um equipamento muito vendido nos dias de hoje. A sua escolha na participação neste trabalho justifica-se por representar este segmento das lâmpadas "inteligentes" que se está a tornar comum nos dias que correm.

3.2.2 Cloogy

FIGURA 3.2: Equipamentos que constituem o Cloogy.

O Cloogy é uma solução de gestão energética residencial desenvolvida pela ISA, uma empresa portuguesa sediada em Coimbra. Na sua forma mais simples é composto por um *clamp*, um transmissor, um hub e uma *power plug*.

O *clamp* é um dispositivo que quando colocado sobre um condutor elétrico permite medir as propriedades da corrente que passa pelo mesmo. A funcionalidade do transmissor passa então por enviar os dados recolhidos através do *clamp* para o *hub*, que por sua vez está ligado à Internet e transfere a informação para que possa ser armazenada. A *power plug* é uma tomada inteligente que permite monitorizar os consumos de um único equipamento ou tomada.

Esta solução mede os consumos energéticos da residência em questão e depois comunica com os servidores da empresa de forma a que toda a informação possa ser tratada e disponibilizada ao utilizador através das aplicações móveis e web.

Com as *power plugs* ainda é possível controlar a utilização de um dado equipamento de modo a controlar o seus consumos e desligá-lo se necessário.

A escolha deste dispositivo para integrar o leque de equipamentos em teste, deve-se ao facto do mesmo estar entre os equipamentos suportados pela plataforma *Unplugg* desenvolvida pela empresa responsável pelo estágio onde este trabalho é efetuado, representando o segmento de gestão energética relacionado com a IoT.

3.2.3 ChromeCast

FIGURA 3.3: Chromecast

Desenvolvido pela Google, este equipamento permite fazer *stream* para uma televisão, com suporte para High-Definition Multimedia Interface (HDMI), de elementos multimédia a partir de outros dispositivos tais como *smartphones*, *tablets* ou computadores pessoais.

Desta forma é possível passar para o grande ecrã o mais variado tipo de conteúdos, quer estejam num dispositivo da rede local quer estejam disponíveis na Internet.

A escolha deste equipamento para participar neste trabalho resulta da crescente popularidade e notoriedade que tem vindo a obter e pelo facto de múltiplos concorrentes estarem a surgir no mercado utilizando o mesmo modo de funcionamento.

3.2.4 Qold

FIGURA 3.4: Qold Hub

O Qold é um pequeno sensor desenvolvido com o objetivo de monitorizar e controlar a temperatura ao longo do dia dos equipamentos de refrigeração presentes em estabelecimentos comerciais, de modo a que as normas de controlo de qualidade dos alimentos sejam cumpridas. Libertando assim os funcionários desta tarefa recorrente ao longo do dia e propícia ao esquecimento.

Os dados são comunicados com uma entidade central que os armazena e trata, para que possam ser consultados através da Internet. No caso de ocorrência de algum desvio ou anomalia permite ainda avisar os responsáveis para que se possa corrigir a situação atempadamente.

O Qold foi incluindo no estudo, pois é desenvolvido pela empresa responsável pelo trabalho/estágio, que tem todo o interesse em assegurar a segurança do sistema.

3.2.5 Energyhive

FIGURA 3.5: Hub do Energyhive

Tal como o Cloogy, este produto destina-se à gestão e monitorização energética do lar. É composto por um *hub* que recebe as medições energéticas, obtidas através de um *clamp* e de um transmissor compatíveis, e comunica a informação para os servidores da empresa de modo armazenar as leituras realizadas.

Para além dos dados poderem ser consultados através da aplicação web disponibilizada pela empresa, está ainda disponível uma API de forma a que os dados possam ser utilizados por outras aplicações.

A escolha deste dispositivo para integrar este estudo advém do facto do equipamento estar disponível na empresa responsável por este trabalho. Estando o dispositivo a ser estudado para uma possível integração com a plataforma Unplugg.

3.2.6 Withings Smart Body Analyzer

Este dispositivo é uma balança inteligente que calcula também o índice de massa corporal. Tem a capacidade de distinguir sem necessidade de configuração o perfil de até 8 pessoas e de comunicar os dados para uma plataforma online.

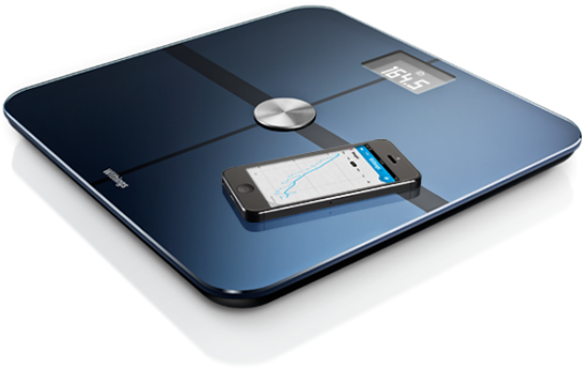


FIGURA 3.6: Balança da Whithings

Os dados nesta plataforma podem ser acedidos através da Internet, das aplicações ou através de outros serviços que têm algum tipo de integração com o sistema.

Estas balanças fornecem ainda ao fabricante informação sobre a sua localização geográfica para poderem receber informação sobre variações gravitacionais e compensar os resultados obtidos.

Foram escolhidas para participar no estudo pois recolhem e enviam para armazenamento na Internet dados fisiológicos dos seus utilizadores. Informação esta que está sujeita a regulamentação muito rigorosa em alguns países.

3.2.7 Fitbit Flex

FIGURA 3.7: Pulseira da Fitbit

O Flex é uma pulseira que monitoriza um conjunto de dados sobre a atividade física do seu utilizador, tais como o número de passos dados, a distância percorrida, as calorias gastas e a qualidade do sono.

Para além da monitorização a pulseira ainda contém outras funcionalidades tais como despertador inteligente regulado pelos ciclos do sono e alertas quando determinados objetivos são atingidos.

Este dispositivo comunica então por *bluetooth* os dados para o telemóvel ou computador pessoal do utilizador quando se aproxima dos mesmos, que podem então depois ser sincronizados com serviços para este efeito na Internet.

Foi escolhido para participar no estudo pois encontra-se disponível para testes na empresa e representa um segmento de dispositivos relacionados com a Internet dos objetos que tem sido alvo de algum interesse recentemente (os *wearables*).

3.2.8 Superfície de ataque por dispositivo

Dada a grande diferença que existe no funcionamento de alguns dos dispositivos, nem sempre todas as superfícies de ataque puderam ser testadas. Um exemplo disso são dispositivos que não têm interação com dispositivos móveis ou interface de administração.

A tabela abaixo mostra o que foi testado em cada um deles:

Tabela 3.2: Áreas a testar por dispositivo

Produto / Área	*Interface Web*	*Autenticação*	*Serviços de rede*	*Transmissão de D.*	*Privacidade*	*I. com Smartphones*	*Configuração*	*Actualizações*
Lifx	x	✓	✓	✓	✓	✓	x	✓
Cloogy	x	-	✓	✓	✓	x	-	-
ChromeCast	x	✓	✓	✓	✓	✓	x	✓
Qold	x	✓	✓	✓	✓	x	x	✓
Energy Hive	x	-	✓	✓	✓	x	-	-
Smart Body Analyzer	x	✓	✓	✓	✓	✓	x	-
Fitbit Flex	x	✓	x	✓	✓	✓	✓	-

✓- Aplica-se ao equipamento / x - Não se aplica ao equipamento / "-" - Não foi possível efetuar a análise.

3.3 Política de divulgação

A divulgação dos resultados obtidos com este trabalho é muito importante, mas a forma como deve ser feita deve seguir um conjunto de passos bem definidos. A forma de

divulgar uma vulnerabilidade num determinado programa ou sistema pode seguir uma das 3 seguintes estratégias:

Divulgação Total Quando esta política é adotada, os resultados são publicados imediatamente. Os defensores desta estratégia, defendem que é a forma mais rápida dos responsáveis agirem de modo a que uma solução seja encontrada.

Divulgação Coordenada Aqui é definido um conjunto de regras, algumas das quais passam por informar os responsáveis pelo sistema e definir um prazo para a sua correção e divulgação.

Ausência de Divulgação A ideia principal desta política, está em corrigir (ou não corrigir) mas não divulgar a existência da falha.

Existe algum debate sobre as vantagens e desvantagens das diferentes políticas, no entanto neste trabalho será seguida uma estratégia de divulgação coordenada, que terá as seguintes etapas:

- A vulnerabilidade com toda a sua informação será comunicada ao fabricante através do email especificado pelo mesmo para questões de segurança.
- Será mantido um canal de comunicação de forma a poder esclarecer quaisquer duvidas do "fabricante".
- Depois de garantida que a informação foi recebida, será dado um limite de 30 dias para a correção do problema ou 45 dias desde o momento do primeiro contacto, caso não exista uma resposta por parte de entidade responsável. Informação esta que será fornecida no primeiro contacto assim como a intenção de divulgar a informação no final do processo.
- Este prazo pode ser estendido por um período limitado de tempo, atendendo a um pedido explicito do fabricante.
- Terminado o prazo, será preparado um documento com as informações técnicas da vulnerabilidade para que possa ser divulgado na Internet. Este documento não terá qualquer programa ou código-fonte que possa ser utilizado para explorar a vulnerabilidade encontrada.

Desta forma pretende-se preservar ao máximo os interesses dos utilizadores e dos fabricantes dos dispositivos que serão sujeitos aos testes.

Capítulo 4

Resultados

O estudo e a vertente prática do presente relatório foram realizados durante o segundo semestre entre os meses de Fevereiro e Junho. Consistiu em efetuar um conjunto de testes utilizando as ferramentas previamente descritas de modo a testar a implementação e a segurança dos dispositivos selecionados.

Neste capítulo é abordada a forma como decorreram os trabalhos, são descritos os problemas encontrados e o caminho que levou à sua descoberta.

No final do capítulo é feito um pequeno resumo dos problemas mais graves, acompanhado das respetivas propostas de solução que poderão ser adotadas pelos fabricantes dado o contexto do seu dispositivo.

4.1 Execução dos testes

A execução dos testes foi feita de forma sequencial em cada um dos dispositivos, onde só se iniciou o trabalho no equipamento seguinte após terem sido finalizados os testes no anterior. Esta estratégia foi escolhida dado que a grande maioria dos equipamentos não estiveram disponíveis durante todo o período no qual decorreram os trabalhos e de forma a maximizar o foco em encontrar problemas no dispositivo em teste num determinado momento.

Deste modo, para os 3 meses durante os quais decorreu o período de testes, foram inicialmente agendados 9 dias para serem dedicados cada um dos equipamentos, planeamento este que nem sempre foi possível cumprir.

De uma forma geral, para cada um dos equipamentos o processo passou pelas seguintes etapas baseadas no PTES:

1. Recolha de informação;
2. Configuração do equipamento;
3. Modelação das ameaças;
4. Análises de vulnerabilidades;
5. Exploração das vulnerabilidades;
6. Documentação dos resultados.

Os documentos resultantes, dedicados a cada um dos dispositivos, que foram enviados aos fabricantes, podem ser consultados nos anexos confidenciais do presente relatório.

A escolha de testar os dispositivos sequencialmente fez com que o impacto de determinados atrasos que ocorreram durante o estudo fosse maior. Estes atrasos foram causados por diversos fatores tanto internos como externos e que podem ser resumidos nos seguintes pontos:

- Problemas com *hardware* necessário para efetuar os testes;
- Dada a suspeita de um determinado problema, nem sempre foi possível completar a verificação dentro do prazo inicialmente estabelecido para o respetivo dispositivo;
- Problemas com os dispositivos que necessitaram de intervenção do fabricante.

Desta forma ao longo do período em que foram efetuados os testes foi necessário realizar algumas adaptações ao planeamento para poder concluir tudo dentro do prazo estabelecido.

4.2 Resultados

A documentação dos resultados específicos para cada um dos dispositivos e a descrição forma como foi conduzido o trabalho em cada um deles, foi movida para os anexos confidenciais do presente trabalho. Esta decisão deve-se ao facto de ainda não ter sido obtida resposta por parte de alguns fabricantes e por algumas das respostas obtidas terem explicitamente pedido um tempo extra para poderem analisar os conteúdos dos documentos enviados (Apesar ainda se encontrarem dentro do período contemplado pela política de divulgação).

Deste modo, no anexo confidencial A poderá ser encontrada a descrição do trabalho efetuado e dos resultados obtidos em cada um dos dispositivos, enquanto que no anexo confidencial B encontram-se respetivos relatórios.

4.3 Discussão dos problemas encontrados

De uma forma mais geral e resumida, os problemas de segurança mais preocupantes, quer devido a falhas ou mero desinteresse, que foram encontrados na execução deste trabalho são:

- Ausência de qualquer tipo de encriptação nas comunicações com a Internet;
- Falta de proteção das credenciais da rede durante a configuração do dispositivo;
- Mecanismo de recuperação de password inseguro;
- Utilização do mecanismo de atualização de software para comprometer os restantes dispositivos;
- Autenticação insuficiente.

Da lista exposta acima é possível concluir que a maior parte destes problemas são relativamente fáceis de detetar e também de resolver. Para a maioria das falhas, existe muita informação disponível detalhando possíveis soluções e implementações que garantem a segurança do respetivo processo.

Começando pelo primeiro, a ausência de encriptação nas comunicações com a Internet, expõe os utilizadores a atacantes que estejam intercetar as ligações de modo a recolher os dados do utilizador ou mesmo a ataques de MITM onde o conteúdo que se encontra a ser transmitido é adulterado. Dado que é demasiado fácil explorar este problema a tendência na Internet nos últimos anos tem sido expor os serviços web apenas através de ligações encriptadas.

Os segundo problema tem muitas semelhanças com o primeiro, mas está relacionado com a comunicação entre o computador/telemóvel do utilizador e o dispositivo. Neste cenário alguns fabricantes assumem que o ambiente no qual o dispositivo está a ser configurado com acesso à rede é seguro, descartando assim atacantes com proximidade física do dispositivo. Neste contexto as credenciais da rede são enviadas de forma insegura, quer através de *bluetooth* ou Wi-Fi, podendo um atacante as intercetar para ganhar acesso à rede local. Dado que nos dias que correm uma grande parte da população vive em apartamentos nas grandes cidades, este cenário torna-se muito provável.

Com base no facto de que os protocolos relacionados com o email não são totalmente seguros, confiar absolutamente nesta tecnologia para transmitir passwords de acesso à conta do utilizador não é uma boa prática. Este problema verificou-se num website que dá suporte a um dos dispositivos testados onde a nova password é enviada para o email

do utilizador e com a qual o utilizador pode passar a realizar a autenticação. O grande problema neste método é que o código secreto é transmitido em claro e o web-site não requer que seja alterada após a primeira utilização.

O quarto problema está relacionado com o mecanismo de atualizações de software que estão presentes na maior partes destes dispositivos. Apesar de existirem casos em que o utilizador necessita de fazer o download de programas de fontes inseguras para poder realizar a atualização, o caso mais graves surgiu da utilização deste tipo de sistemas para "infectar" outras máquinas. Este problema surge porque o sistema montado continha uma falha onde as chaves que davam acesso aos dispositivos para descarregar o novo software também tinham permissão para alterar o conteúdo do repositório. Deste modo um atacante poderia tentar executar código nos restantes dispositivos instalados pela empresa.

Por fim, outro aspeto que se notou em alguns destes dispositivos, foi a falta de autenticação em algumas situações em que seria pertinente um mecanismo mais apertado. Em determinados dispositivos é possível trocar a conta à qual o mesmo pertence por meios oficiais sem que o dono seja notificado ou dê a sua permissão. Como para efetuar a sincronização dos dados não é necessário qualquer tipo de autenticação os dados são sincronizados para a nova conta.

4.4 Estratégias de mitigação

Para os problemas identificados na secção anterior, existem um conjunto de boas práticas que podem e devem ser seguidas, as quais evitam que os utilizadores destes dispositivos sejam expostos a possíveis atacantes e garantem que os seus dados se encontram seguros nestas situações.

Para estes problemas as recomendações passam por:

- Encriptar as comunicações realizadas pelos equipamentos
- Garantir que todos os intervenientes estão devidamente autenticados antes de realizar qualquer operação.
- Implementar um sistema de permissões onde os dispositivos apenas estão autorizados a efetuar um conjunto limitado de operações no servidor.
- Ao implementar um mecanismo de recuperação de passwords, certificar-se que o utilizador escolhe uma nova password após efetuada a verificação, que deverá ser realizada através de um *token* temporário.

- Garantir que o dispositivo é configurado de forma segura.

De um modo geral estas recomendações podem parecer superficiais, no entanto diminuem em muito o risco ao qual é exposto o utilizador quando utiliza o equipamento, pois elevam barreiras que são precisas ultrapassar, tornando difícil a tarefa até para atacantes com mais recursos, tanto técnicos como financeiros.

Começando pelo primeiro item, o recurso a encriptação usando TLS ou DTLS com configurações e tamanhos de chaves superiores a 2048 bits deverá ser equacionado. É certo que nem sempre é possível implementar esta solução, no entanto no mínimo deverá estar presente uma solução em que é usada encriptação simétrica na presença de uma chave partilhada previamente.

Garantir de todos os intervenientes estão autenticados e que o nível de acesso que lhes é concedido é adequado, é vital. Para novos equipamentos e serviços, a utilização de uma infraestrutura de chaves públicas é recomendável, no entanto poderá já não ser exequível para dispositivos já no mercado. Alternativas adequadas ao contexto deverão ser ponderadas de modo a garantir estes dois pontos. As permissões deverão ser alvo de uma análise cuidadosa de modo a certificar que cada interveniente só tem acesso à informação e funcionalidades absolutamente necessárias para desempenhar o seu papel.

Muitas vezes tornado alvo por parte de atacantes está o sistema de recuperação das credenciais necessárias para aceder a uma determinada conta. Ao implementar este sistema, uma password nunca deverá ser transmitida através de canais inseguros. A recomendação é que um *token* com um prazo de validade reduzido seja transmitido e que este seja usado pelo utilizador para poder introduzir uma nova password. Para sistemas mais críticos a utilização de autenticação através 2 fatores deverá ser equacionada.

Relativamente à configuração do acesso sem fios à Internet do dispositivo, é preciso garantir que os primeiros 3 pontos se encontram resolvidos. Só desta forma o utilizadores poderá identificar os seus dispositivos, o dispositivo poderá confirmar que está a comunicar com o proprietário e transmitir as credenciais da rede de forma segura. No capitulo seguinte é apresentada uma possível solução para estes problema.

Para um conjunto de recomendações mais detalhadas e objetivas o anexo C deverá ser consultado. Neste estão resumidas boas práticas e parâmetros de configuração que poderão ser utilizados, assim como referências importantes para documentos que ajudam ao desenvolvimento de equipamentos para a IoT tendo por base a segurança dos mesmos.

Capítulo 5

Mecanismo de configuração

Como foi observado durante a execução do estudo descrito no capitulo anterior, os dispositivos que necessitam de acesso à Internet através da rede Wi-Fi local, passam por um processo de configuração que é efetuado pelo utilizador.

Em todos estes casos, o modo de configuração apresentou algum problema com a segurança do processo. Apesar de certos aspetos serem tratados corretamente, as falhas são suficientes para comprometer de certa forma a segurança da operação ou a permitir que se tire partido da mesma.

Este problema relacionado com as instalações dos equipamentos da IoT e a sua segurança tem sido destacado por especialistas, tanto que grandes empresas com interesses no ramo têm abordado recentemente este tema com algumas soluções [25, 26].

Alguns autores [31], apesar de apoiarem o uso de standards defendem que nem todas as componentes, como a instalação, gestão de chaves, autorização, privacidade entre outros, necessitam obrigatoriamente de ser incluídas deixando estas questões para os fabricantes, pois devem ser abordadas de acordo com o domínio em questão.

Nesta segunda parte do trabalho é proposto um mecanismo de configuração para o *Qold*, o dispositivo em desenvolvimento na empresa onde todo este trabalho foi realizado e que ainda não tem esta componente implementada, com base no que foi possível aprender do estudo dos restantes equipamentos.

Ao longo do restante capítulo, serão descritas todas as suas componentes e todos os passos dados para chegar à solução apresentada.

5.1 Requisitos

Para a implementação deste mecanismo foi recolhida junto dos responsáveis pelo desenvolvimento do dispositivo, um conjunto de funcionalidades e características que o mesmo deverá conter.

Estas características são determinantes nas decisões técnicas tomadas na conceção do mecanismo e traduzem decisões importantes de usabilidade e interoperabilidade que terão um forte impacto na opinião dos utilizadores sobre o produto no geral.

Neste contexto foram assim impostas algumas restrições e limitações, que a solução deverá respeitar e que se encontram descritas nos seguintes pontos:

- Para maximizar a compatibilidade, a solução deverá ser baseada em tecnologias *Bluetooth* ou Wi-Fi;
- No caso de ser utilizado *Bluetooth* a solução deverá ser compatível com equipamentos mais antigos;
- A solução deverá funcionar com o hardware que já é utilizado pelo hub do *Qold*;
- A utilização de algoritmos criptográficos deverá estar limitada a standards abertos.

5.1.1 Requisitos funcionais

Na tabela 5.1, encontram-se expostos os requisitos funcionais da aplicação e de todo o sistema (quer seja para *smartphone* ou para computador pessoal). Estes têm uma grande influência no modo como o dispositivo poderá ser configurado. Os requisitos encontram-se ordenados pela seu grau de importância para o produto final. Esta métrica poderá conter um dos seguintes 3 valores: Elevada, Média ou Baixa.

5.1.2 Requisitos não-funcionais

Para além dos requisitos funcionais, a implementação da solução teve em consideração os atributos de qualidade descritos na tabela 5.2. Que resumidamente salientam a importância de todo o processo ser seguro, mas tendo em conta que todas essas questões devem ser abstraídas do utilizador.

Tabela 5.1: Requisitos funcionais

Código	Designação	Importância	Descrição
F01	Transmissão das credenciais da rede	Elevada	O utilizador deverá conseguir transmitir para o dispositivo todos os dados necessários à configuração do acesso à rede local .
F02	Escolha do dispositivo	Elevada	Deverão ser listados os dispositivos locais, para que o utilizador escolha qual pretende configurar
F03	Feedback dos dados enviados	Elevada	Caso o dispositivo não consiga utilizar com sucesso os dados inseridos o utilizador deverá ser notificado.
F04	Associação do dispositivo à conta	Média	O utilizador deverá associar o dispositivo à sua conta no serviço web durante a configuração.
F05	Criação de conta	Baixa	A configuração só poderá ser efetuada após o utilizador possuir uma conta no serviço web.
F06	Transmissão de configurações opcionais	Baixa	O utilizador deverá poder transmitir mais configurações opcionais juntamente com os dados essenciais.

Tabela 5.2: Requisitos não funcionais

Código	Designação	Importância	Descrição
NF01	Facilidade de utilização	Elevada	O mecanismo deverá ser fácil de utilizar e compreender, independentemente da experiência do utilizador. Este não deverá levar mais do que 5 minutos para concluir a operação.
NF02	Segurança	Elevada	O sistema final deverá garantir de que a informação é transmitida de forma segura entre utilizador e o dispositivo. O mecanismo deverá estar imune aos problema encontrados em outros dispositivos do estudo.

5.2 Modelação de ameaças

Dadas as características do produto atual e das condições nas quais se espera que exista a utilização do mecanismo, foi realizado uma análise às ameaças a que os dispositivos e os clientes poderão estar expostos. Para tornar a análise clara e completa foi utilizado a metodologia denominada *Microsoft Threat Modeling Process* [35].

Com base neste exercício, feito para identificar e compreender que tipo de ameaças podem os intervenientes estar sujeitos, são então definidos os desafios que deverão ser resolvidos para obter um sistema seguro.

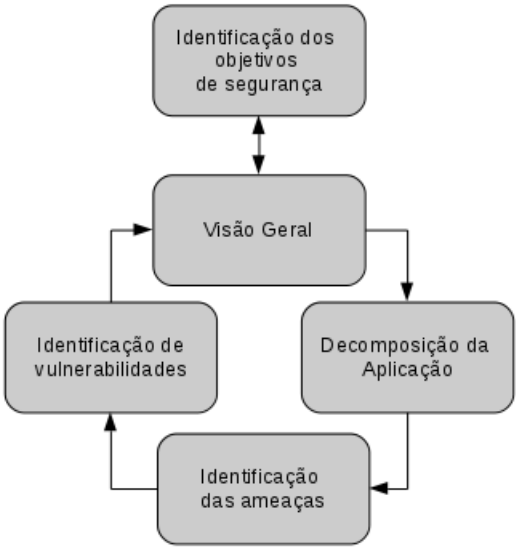


FIGURA 5.1: Processo iterativo de modelação de ameaças

5.2.1 Objetivos de segurança

Ao desenvolver esta solução pretende-se então garantir que os seguintes pontos relacionados com a confidencialidade e integridade dos dados, e com a autenticação dos intervenientes:

- Garantir que o dispositivo e o utilizador são corretamente autenticados;
- Garantir que existe autorização para a comunicação entre os dois elementos;
- A informação trocada, que pode conter credenciais e configurações, está encriptada e protegida contra adulteração.

Ao analisar as consequências do não cumprimentos destes objetivos, verifica-se que o risco financeiro direto é baixo, no entanto os risco de danos na reputação (quer dos clientes quer da empresa) é elevado.

5.2.2 Visão geral da aplicação

Durante a etapa de configuração do equipamento, existe a intervenção de 3 elementos do sistema, o utilizador (aplicação), o servidor e o dispositivo. No diagrama seguinte estão representados estes elementos assim como as suas ligações e resultado que se espera obter.

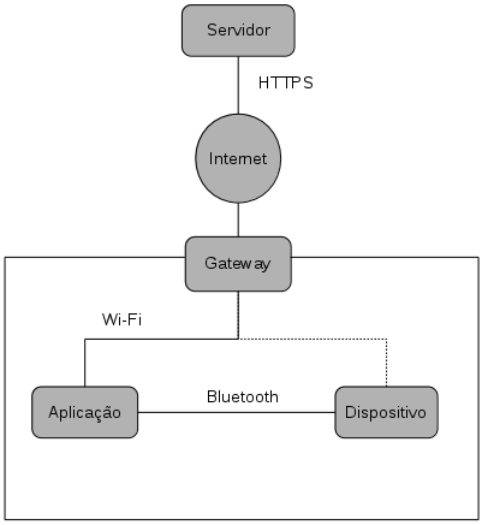


FIGURA 5.2: Visão do sistema no inicio da configuração

5.2.3 Decomposição da aplicação

De modo a entender que componentes do sistema terão um maior impacto na segurança durante o processo de configuração, definiram-se as fronteiras onde dentro das quais existe a confiança de que os *inputs* são seguros e de onde se pode esperar que os *outputs* sejam corretos. Dentro destas fronteiras estão o software desenvolvido para cada umas das componentes e as bibliotecas nas quais estes se baseiam. Quaisquer dados originados fora destas fronteiras, devem ser tratados com especial atenção.

Relativamente aos pontos de entrada e saída de dados, o dispositivo apenas contempla uma hipótese, ou seja a ligação Bluetooth. O módulo do servidor, contém 2 possíveis pontos de entrada e saída, o primeiro trata-se da API Representational State Transfer (REST) que comunica com as aplicações e uma ligação a um sistema de gestão de base de dados. Já a aplicação necessita de se preocupar com as ligações HTTP Secure (HTTPS) com o servidor, com a ligação Bluetooth ao dispositivo e com o *input* fornecido pelo utilizador em diversos passos.

Com a exceção do servidor, tanto a aplicação como o dispositivo durante o funcionamento do processo de configuração apenas lidam com os dados em memória, não armazenando qualquer informação em disco.

5.2.4 Ameaças identificadas

Com base nos dados expostos nas secções anteriores, é possível observar que existem um conjunto elementos que poderão ser alvo de interesse por parte de um atacante. Pela

análise do sistema chega-se à conclusão que os seguintes vetores de ataque serão os mais prováveis:

- O atacante poderá observar os dados que estão a ser transmitidos (divulgação de informação).
- O atacante poderá realizar a configuração do dispositivo em vez do utilizador (falsificação de identidade).
- O atacante poderá fazer-se passar por um dispositivo genuíno (falsificação de identidade).
- O atacante poderá querer injetar dados inválidos (adulteração de dados e negação de serviço).
- O atacante poderá impedir o correto funcionamento do dispositivo (negação de serviço).

A pessoa por detrás de um ataque poderá estar incluída num dos seguintes grupos: consumidores, competidores ou reguladores da área onde se insere o negócio do utilizador. Onde as suas motivações poderão passar por diversão, reputação, lesar a competição ou mesmo o ativismo.

5.3 Desafios

Após identificados os componentes e atores que poderão representar as maiores ameaças ao sistemas e aos seus utilizadores, é possível enumerar os desafios que uma implementação de um mecanismo de configuração que se pretende seguro deverá endereçar. A proposta que é feita neste trabalho tenta assegurar os seguintes pontos:

1. Garantir que o equipamento só comunica com o seu proprietário;
2. Garantir ao proprietário que está a comunicar com o dispositivo correto;
3. Proteger todos os dados que são transmitidos durante a configuração;
4. Proteger todas as comunicações seguintes entre o equipamento e os seus servidores;
5. Garantir um atacante não consegue causar ataques de DDoS ao dispositivo durante a configuração.

5.4 Especificação

Nesta secção é apresentada a especificação do mecanismo de configuração proposto. Antes de avançar com todos os detalhes é importante referir as premissas que terá por base.

Deste modo, com esta proposta assume-se que:

- A segurança do serviço na Internet é assegurada por outros mecanismos e que não foi comprometida;
- O dispositivo não foi comprometido e que as suas chaves estão bem guardadas;
- O sistema operativo onde é executada a aplicação isola corretamente o espaço de memória dedicado à mesma.

Conhecidos estes elementos base, para o utilizador a configuração do dispositivo é vista como um processo de 7 passos, que lhe são expostos da forma mais clara e intuitiva possível. Estes podem ser descritos resumidamente como:

1. Montar o dispositivo no local apropriado;
2. Descarregar a aplicação do dispositivo, a partir da loja oficial para o sistema operativo em causa;
3. Criar uma conta no serviço web ou autenticar-se com uma já existente, usando a aplicação;
4. Selecionar a identificação do dispositivo que pretende configurar, ou adicionar uma nova a partir do identificador impresso no interior da caixa do dispositivo;
5. Carregar no botão existente no equipamento, para iniciar o modo de configuração;
6. Escolher o dispositivo Bluetooth na aplicação, para realizar a ligação ("pairing");
7. Introduzir o nome e password da rede à qual os dispositivo se deverá ligar.

Do ponto de vista do equipamento, de modo a garantir a segurança do processo ou evitar possíveis vulnerabilidades que o possam comprometer, é importante que as características/configurações explicadas na tabela 5.3, sejam implementadas.

Com estes aspetos estabelecidos, podemos então descrever os mecanismo/processo que será utilizado para realizar a configuração. Um aspeto que é relevante referir, é que

Tabela 5.3: Configurações do equipamento

Propriedade	Razão
Todos os portos UDP e TCP fechados	Como que não são necessários para o funcionamento do equipamento devem estar fechados. Todo o tráfego será *outbound*, ou seja terá se ser iniciado pelo dispositivo.
Bluetooth ligado apenas por um período de tempo limitado	Para iniciar esta interface deve ser necessário acesso físico ao equipamento e apenas se deverá manter ligada por um curto espaço de tempo.
Uma única ligação *Bluetooth* de cada vez	Dado que apenas 1 utilizador pode configurar o dispositivo não é necessário aceitar mais ligações.

este sistema esta dependente uma infraestrutura de chaves publicas implementada pelo fabricante. Esta pode ser baseada em chaves "normais" ou com base em certificados, sendo esta segunda hipótese preferível em relação à primeira por se poderem usufruir das vantagens dos formatos standard.

Deste modo todos os intervenientes nas comunicações serão identificados pela sua chave publica. O papel do servidor como entidade central, será verificar a identidade dos elementos presentes em cada operação de configuração. Por sua vez cada dispositivo, durante o processo de fabrico será provido de um par chaves e da chave do servidor.

No processo de configuração a aplicação do utilizador gerará um par de chaves que serão apenas válidos por um curto espaço de tempo, que serão comunicados ao servidor e servirão para autenticar o utilizador perante o dispositivo.

Todo o processo pode ser observado no diagrama de sequência presente na figura 5.3, a partir da etapa 3. Neste processo como foi exposto na figura 5.2 é esperado que a ligação ao servidor por parte do utilizador seja exclusivamente efetuada usando HTTPS.

Nos parágrafos seguintes iremos representar o servidor por s, a aplicação por a, o dispositivo por d, uma *hash* do conteúdo x por $h(x)$, a chave publica do elemento y por pk_y, uma assinatura do conteúdo x por parte do elemento y por $Sig_y(x)$, o texto x encriptado pela chave pública do elemento y por $Enc_y(x)$ e o elemento x encriptado pela chave simétrica y como $Sym_y(x)$. Todo o conteúdo anterior da mensagem será representado por α.

Como é possível observar na imagem, o processo é composto por 8 etapas essenciais. Estes passos requerem um conjunto de informações e ações que podem ser detalhados da seguinte forma:

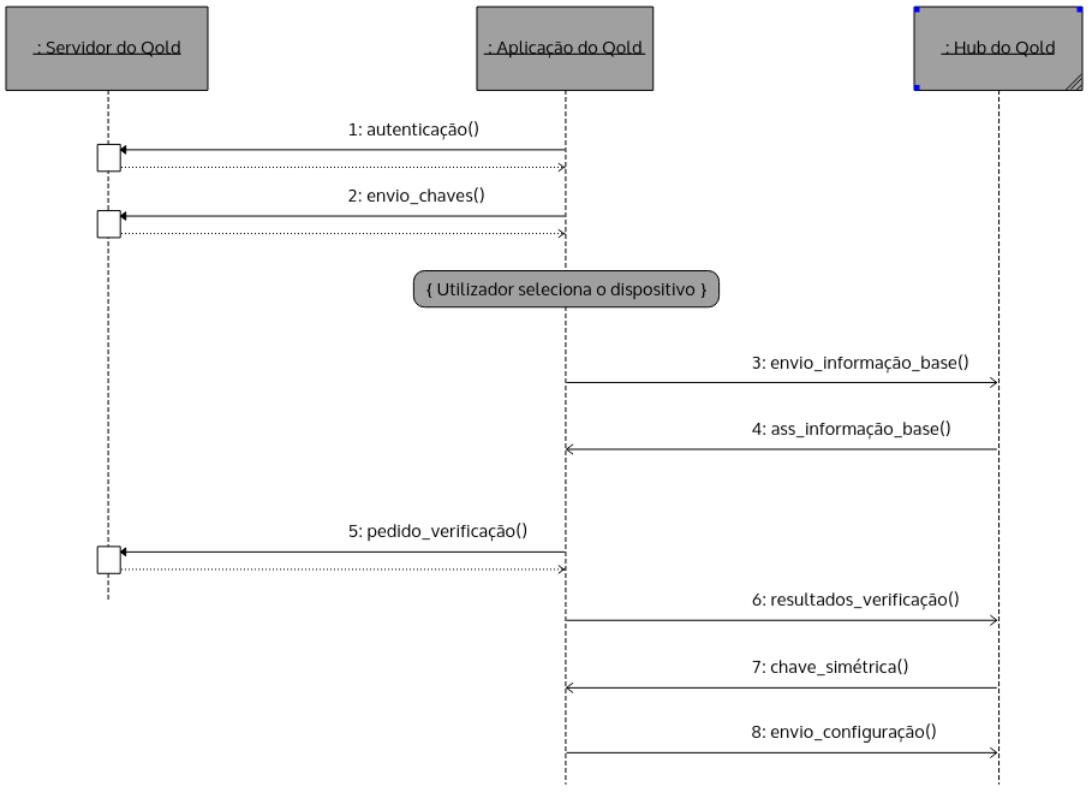


FIGURA 5.3: Interações entre os diferentes elementos.

Autenticação Neste passo o utilizador fornece as credenciais da sua conta e após verificação das mesmas a aplicação fornece um *token* (chave de sessão) que será utilizado para futuras interações com o servidor.

Envio de Chaves Antes de continuar com este processo a aplicação terá de gerar um par de chaves para serem utilizados na configuração. A chave pública será então enviada ao servidor que lhe atribui um prazo de validade suficiente para completar o restante processo.

Envio de Informação base Ao iniciar a ligação ao equipamento, a aplicação deverá fornecer ao dispositivo 3 *hashes* (*token*, identificação do dispositivo e nome de utilizador) juntamente com a sua chave pública.
Exemplo: $h(token) : h(Id) : h(username) : pk_a$

Assinatura da informação base Neste passo, o dispositivo devolve à aplicação a informação recebida acompanhada da sua chave pública, conteúdo este que é assinado pelo dispositivo. Antes do envio o dispositivo deve ainda verificar que o *hash* do ID enviado corresponde com o seu.
Exemplo: $h(token) : h(Id) : h(username) : pk_a : pk_d : Sig_d(\alpha)$

Pedido de Verificação Após receber os dados assinados, a aplicação reenvia para o servidor, que irá proceder à verificação e validação de ambas as partes. Deverá começar por verificar que a assinatura corresponde ao dispositivo em questão, de que o *hash* do *token* assinado corresponde ao utilizador em questão e de que as chaves publicas trocadas são de facto validas para as identidades. Se todos os parâmetros corresponderem o servidor deverá devolver as chaves acompanhadas das respetiva assinatura.
Exemplo: $pk_a : pk_d : Sig_s(\alpha)$

Resultados da verificação A aplicação deverá reencaminhar a resposta obtida pelo servidor para o dispositivo. Se a resposta for válida, a aplicação tem a confirmação que está comunicar com o dispositivo correto.
Exemplo: $pk_a : pk_d : Sig_s(\alpha)$

Chave Simétrica Após receber a confirmação do servidor e validar a sua assinatura, o dispositivo gera uma password aleatória que será usada na encriptação simétrica na transmissão das mensagens seguintes. É então assinada a mensagem, encriptada com a chave pública da aplicação e transmitida.
Exemplo: $Enc_a(password : timestamp : Sig_d(\alpha))$

Envio de Configuração Após recebida e verificada a password temporária, os dados de configuração submetidos pelo utilizador, podem ser encriptados e enviados para o dispositivo em segurança.
Exemplo: $Sym_{password}(config : timestamp)$

No fim deste processo, a aplicação deverá descartar as chaves geradas pois não terão mais nenhuma utilidade.

5.5 Descrição do prototipo

Com base no sistema que foi detalhado na secção anterior foi desenvolvido um prototipo composto por 3 componentes independentes que comunicam de acordo com a especificação.

Desta forma, para a componente do servidor foi implementada uma API REST que executa a gestão de chaves dos dispositivos e das aplicações dos utilizadores, assim como implementa os mecanismos de autenticação e o *endpoint* de verificação definidos na especificação. Este serviço web foi desenvolvido utilizando a *framework* "Django" e a biblioteca "Django Rest Framework". As implementações das rotinas relacionadas com a criptografia ficaram a cargo do biblioteca "PyCrypto".

Para a componente que interage com o utilizador foi desenvolvida uma aplicação *Android* simples que implementa todas as funcionalidades necessárias. Esta aplicação nativa recorre a apenas duas bibliotecas externas, uma para realizar as comunicações HTTP de forma assíncrona (*android-async-http*) e outra para utilizar implementações de funções criptográficas não suportadas de origem pelo Software Development Kit (SDK) do sistema operativo (*Spongy Castle*).

O terceiro componente diz respeito ao software que corre no dispositivo e que deverá ser executado sempre que o botão de configuração for pressionado. Este foi testado num dispositivo executando o sistema operativo *Raspbian* e o seguinte hardware:

- Raspberry Pi 1 Model A
- Wireless USB 11N Nano Adaptor 802.11N
- 2.4GHz Wireless NRF24L01 Transceiver Module
- Kingston Technology 8 GB microSDHC Class 10 Flash Card with SD card adapter
- Nano USB to Bluetooth Dongle V2.0

Para implementar todas as funcionalidades desejadas foi utilizada a linguagem de programação *Python* juntamente com as bibliotecas "PyBluez" e "Pycrypto", para comunicar por *Bluetooth* e implementar as rotinas criptográficas respetivamente.

Para a implementação da especificação foi ainda necessário tomar algumas opções relativamente aos algoritmos e tecnologias usadas. Para este prototipo optou-se pela utilização das seguintes características:

Criptografia de chave pública Usou-se RSA com chaves de 2048 bits.

Criptografia Simétrica Foi utilizado Advanced Encryption Standard (AES) com chaves de 256 bits.

Funções de *hash* Foi escolhida o Secure Hash Algorithm (SHA)-256.

A escolha destes algoritmos um pouco mais pesados deve-se à capacidade de processamento relativamente grande (na escala da IoT) de todos os equipamentos utilizados no *Qold*. Estes algoritmos e parâmetros deverão ser pensados e ponderados caso a caso de acordo com a situação e características dos equipamentos.

Num futuro próximo espera-se poder vir a disponibilizar o código fonte de uma versão mais sólida segundo uma licença que permita a utilização deste mecanismo por parte de outras entidades e dispositivos.

5.6 Validação

Nesta secção é feita uma análise às características do mecanismo de autenticação proposto, onde se tenta explica de que forma este resolve os desafios de segurança colocados na secção de modelação das ameaças.

Começando pela decisão de apenas ser possível iniciar o processo após ativado um botão no dispositivo, em vez de iniciar automaticamente sempre que a ligação não for válida, impede que um possível atacante possa explorar este sistema sem acesso físico ao dispositivo. Diminuindo assim a janela de oportunidade disponível para lançar algum ataque.

Entre os ataques aos quais estes dispositivos poderão estar mais expostos encontram-se a observação do tráfego, ataques de MITM ativo, ataques de repetição, falsificação de identidade e ataques de DDoS. Situações estas que se encontram contempladas e que são resolvidas da seguinte forma:

Falsificação de Identidade Através do uso de uma terceira entidade (servidor), que tem conhecimento prévio das chaves dos restantes intervenientes é possível provar a identidade de ambos. Isto é verificado tanto pela aplicação como pelo dispositivo através da assinatura das chaves publicas por parte do servidor.

Observação do tráfego Na utilização deste mecanismo são trocados em claro *hashes* e chaves públicas, informação que não tem utilidade para o atacante. A restante informação é sempre transferida devidamente encriptada impedindo assim a sua observação.

MITM ativo Como foi descrito nas medidas que impedem que um agente malicioso se faça passar por um genuíno, a validação ativa da identidade de ambas as partes, impede este tipo de ataques, pois após verificada a chaves, todo o tráfego é encriptado com as chaves do verdadeiro destinatário.

Ataques de repetição O facto de durante todo o processo ser mantido estado por parte dos intervenientes dificulta a execução de um ataque de repetição, no entanto não impede. Mas devido ao facto de a chave gerada pela aplicação ter um prazo muito curto (alguns minutos), se o suposto atacante conseguir iniciar e executar o processo, repetindo o conteúdo que foi capturado, este só será aceite pelo dispositivo dentro da janela em que a chave é válida, inviabilizando assim a utilidade deste tipo de ataque.

DDoS Dado que o dispositivo só deverá aceitar 1 ligação durante o processo de configuração limita a capacidade de um atacante de efetuar este tipo de ataques. No

entanto através da alteração dos conteúdos da comunicação através de um ataque MITM, de modo a simular interferência poderá ainda ser possível.

Desta forma, o mecanismo é capaz de garantir a segurança das comunicações dada a utilização de algoritmos que sejam considerados seguros para as diferentes componentes desde a PKC (ex. RSA ou Elliptic Curve Cryptography (ECC)), encriptação simétrica (ex. AES) e *hashing* (ex. SHA2), utilizando tamanhos adequados para as chaves.

No entanto, este mecanismo tal como está descrito ainda não garante a propriedade denominada por Perfect Forward Secrecy (PFS). Esta propriedade na prática implica que não seja possível obter as chaves de sessões anteriores a partir de uma chave privada comprometida. Apesar de as chaves privadas utilizadas na encriptação serem apagadas mal termine o processo, algumas alterações ainda serão necessárias para cumprir este requisito.

Capítulo 6

Conclusão

O trabalho efetuado permitiu conhecer as características de um novo conceito de equipamentos, as suas tecnologias específicas e de como todas as componentes do sistema interagem. Para poder efetuar um estudo sobre a sua segurança, um grande nível de compreensão sobre o seu funcionamento é essencial, de forma perceber os vetores de ataque a que este tipo de dispositivos estão expostos e ter a capacidade de detetar falhas no funcionamento das suas interfaces.

Posto isto, um facto que é importante salientar é que na maioria dos dispositivos testados as tecnologias utilizadas não são recentes e são utilizadas noutras áreas, sendo a maior "ìnovação" o novo contexto e ambientes onde é feita a sua aplicação.

Deste modo a necessidade de familiarização com as técnicas, metodologias e ferramentas utilizadas na área da segurança informática foi um aspeto fulcral abordado na primeira etapa do trabalho.

Durante a execução dos testes nos dispositivos selecionados observou-se que grande parte dos problemas encontrados são se devem a vulnerabilidades no software, mas sim a um processo de design que não deu o devido valor a aspetos relacionados com a segurança e a implementações que não seguem práticas já estabelecidas em outras áreas da Internet.

A resolução destes problemas, na maioria dos casos, é clara e exequível sem ser necessário um grande esforço por parte dos fabricantes. No entanto um aspeto importante que se observou na realização do trabalho, foi a inexistência de um processo padrão de configuração inicial que desse algumas garantias de segurança, apesar dos cenários serem muito semelhantes.

Foi então efetuada uma proposta, que fornece algumas garantias de segurança essenciais para esta etapa importante no funcionamento dos vários equipamentos, na expectativa poder deste modo fornecer uma base na qual muitos destes dispositivos se possam basear.

Em jeito de conclusão, é possível observar que ainda há muito a fazer nesta área, onde ultimamente se tem notado uma atenção acrescida por parte da comunidade. No entanto a maior componente deste trabalho estará na consciencialização para importância da segurança nestes dispositivos, que se espera virem a ter uma grande adoção por parte da população.

6.1 Trabalho futuro

Os problemas detetados, são uma pequena fração de todo o universo que poderá ser encontrado nas centenas de dispositivos que estão a invadir o mercado. Desta forma, é importantíssimo continuar a encontrar-los de modo a educar para esta problemática, pois à medida que os fabricantes e utilizadores ganham consciência para estes problemas e que se atribua uma maior importância a esta componente, será possível reduzir a exposição de todos.

Outro componente que foi abordado neste trabalho e que continuará a requerer mais atenção, pois ainda existe espaço para melhorias, é o mecanismo de configuração que foi proposto. A adaptação da especificação para colmatar problemas que se venham a descobrir e a construção de componentes de software mais sólidos que possam a vir ser usados em ambientes de produção, são definitivamente os próximos passos que necessitam de ser dados.

Bibliografia

[1] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of things (IoT): A vision, architectural elements, and future directions," *Future Generation Computer Systems*, vol. 29, pp. 1645–1660, Sept. 2013.

[2] A. Bassi and G. Horn, "Internet of things in 2020: A roadmap for the future," *European Commission: Information Society and Media*, 2008.

[3] P. G. Harald Sundmaeker, "Vision and challenges for realising the internet of things," tech. rep., European Commission, Information society and media, 2010.

[4] D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, "Internet of things: Vision, applications and research challenges," *Ad Hoc Networks*, vol. 10, pp. 1497–1516, Sept. 2012.

[5] L. Tan and N. Wang, "Future internet: The internet of things," in *2010 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE)*, vol. 5, (Chengdu, China), pp. V5–376–V5–380, Aug. 2010.

[6] M. C. Domingo, "An overview of the internet of things for people with disabilities," *Journal of Network and Computer Applications*, vol. 35, pp. 584–596, Mar. 2012.

[7] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," *Computer Networks*, vol. 54, pp. 2787–2805, Oct. 2010.

[8] L. Mainetti, L. Patrono, and A. Vilei, "Evolution of wireless sensor networks towards the internet of things: A survey," in *2011 19th International Conference on Software, Telecommunications and Computer Networks (SoftCOM)*, pp. 1–6, Sept. 2011.

[9] H. Suo, J. Wan, C. Zou, and J. Liu, "Security in the internet of things: A review," in *2012 International Conference on Computer Science and Electronics Engineering (ICCSEE)*, vol. 3, pp. 648–651, Mar. 2012.

[10] O. Whitehouse, "Security of things: An implementers' guide to cyber-security for internet of things devices and beyond." https://www.nccgroup.com/en/learning-and-research-centre/white-papers/security-of-things-an-implementers-guide-to-cyber-security-for-internet-of-things-devices-and-beyond/ (Acedido em Janeiro 2015).

[11] A. Ukil, J. Sen, and S. Koilakonda, "Embedded security for internet of things," in *2011 2nd National Conference on Emerging Trends and Applications in Computer Science (NCETACS)*, pp. 1–6, Mar. 2011.

[12] T. Heer, O. Garcia-Morchon, R. Hummen, S. L. Keoh, S. S. Kumar, and K. Wehrle, "Security challenges in the IP-based internet of things," *Wireless Personal Communications*, vol. 61, pp. 527–542, Dec. 2011.

[13] R. H. Weber, "Accountability in the internet of things," *Computer Law & Security Review*, vol. 27, pp. 133–138, Apr. 2011.

[14] R. H. Weber, "Internet of things – new security and privacy challenges," *Computer Law & Security Review*, vol. 26, pp. 23–30, Jan. 2010.

[15] R. H. Weber, "Internet of things – need for a new legal environment?," *Computer Law & Security Review*, vol. 25, pp. 522–527, Nov. 2009.

[16] A. Perrig, J. Stankovic, and D. Wagner, "Security in wireless sensor networks," *Commun. ACM*, vol. 47, pp. 53–57, June 2004.

[17] M. Bishop, "About penetration testing," *IEEE Security Privacy*, vol. 5, pp. 84–87, Nov. 2007.

[18] G. Hardy, "The relevance of penetration testing to corporate network security," *Information Security Technical Report*, vol. 2, no. 3, pp. 80–86, 1997.

[19] D. Kennedy, J. O'Gorman, D. Kearns, and M. Aharoni, *Metasploit: The Penetration Tester's Guide*. San Francisco: No Starch Press, 1 edition ed., July 2011.

[20] N. Antunes and M. Vieira, "Comparing the effectiveness of penetration testing and static code analysis on the detection of SQL injection vulnerabilities in web services," in *15th IEEE Pacific Rim International Symposium on Dependable Computing, 2009. PRDC '09*, pp. 301–306, Nov. 2009.

[21] PCI Security Standards Council, *Payment Card Industry (PCI), Data Security Standard (DSS) and Payment Application Data Security Standard (PA-DSS)*, 2014. https://www.pcisecuritystandards.org.

[22] M. Qadeer, M. Zahid, A. Iqbal, and M. Siddiqui, "Network Traffic Analysis and Intrusion Detection Using Packet Sniffer," in *Second International Conference on Communication Software and Networks, 2010. ICCSN '10*, pp. 313–317, Feb. 2010.

[23] J.-F. Raymond, "Traffic Analysis: Protocols, Attacks, Design Issues, and Open Problems," in *Designing Privacy Enhancing Technologies* (H. Federrath, ed.), no. 2009 in Lecture Notes in Computer Science, pp. 10–29, Springer Berlin Heidelberg, 2001.

[24] M. Villari, A. Celesti, M. Fazio, and A. Puliafito, "A secure self-identification mechanism for enabling iot devices to join cloud computing," in *Internet of Things. IoT Infrastructures*, pp. 306–311, Springer, 2014.

[25] R. Kim and V. Pathuri, "Setup of multiple iot devices," June 9 2015. US Patent 9,054,961.

[26] A. Baum, I. ZARMI, G. REITER, and A. AYUN, "Auto-provisioning for internet-of-things devices," Aug. 6 2015. US Patent App. 14/611,397.

[27] G. Reiter, "A primer to wi-fi provisioning for iot applications." http://www.ti.com/lit/wp/swry011/swry011.pdf.

[28] J. Xu, "Simple & secure wi-fi configuration for internet of things," 2013.

[29] "Blinkup." https://electricimp.com/platform/blinkup/ (Acedido em Junho de 2015).

[30] "Cc3000 smart config." http://processors.wiki.ti.com/index.php/CC3000_Smart_Config (Acedido em Junho de 2015).

[31] S. L. Keoh, S. S. Kumar, and H. Tschofenig, "Securing the internet of things: A standardization perspective," *Internet of Things Journal, IEEE*, vol. 1, no. 3, pp. 265–275, 2014.

[32] J. Liu, Y. Xiao, and C. P. Chen, "Authentication and access control in the internet of things," *2013 IEEE 33rd International Conference on Distributed Computing Systems Workshops*, vol. 0, pp. 588–592, 2012.

[33] R. Roman, C. Alcaraz, J. Lopez, and N. Sklavos, "Key management systems for sensor networks in the context of the internet of things," *Computers & Electrical Engineering*, vol. 37, no. 2, pp. 147 – 159, 2011. Modern Trends in Applied Security: Architectures, Implementations and Applications.

[34] "Security guidance for early adopters of the internet of things (iot)." https://cloudsecurityalliance.org/media/news/csa-launches-new-security-guidance-for-early-adopters-of-the-iot/ (Acedido em Junho de 2015).

[35] J. Meier, A. Mackman, and B. Wastell, “Threat modeling web applications.” https://msdn.microsoft.com/library/ms978516.aspx (Acedido em Junho de 2015).

Anexo A

Dados recolhidos sobre o funcionamento dos alvos

Neste anexo encontram-se reunidos todos os dados obtidos durante primeira fase de recolha de informação sobre os dispositivos que serão alvo dos testes neste trabalho.

A informação que se segue foi agregada a partir de fontes disponíveis publicamente na Internet, quer sejam documentos oficiais do fabricante quer dados recolhidos de fontes não oficiais como blogues e artigos de utilizadores que documentam aspetos não disponibilizados pelo fabricante.

Não tem o intuito de ser detalhar extensivamente o funcionamento do equipamento pois não resulta de uma análise realizada durante o estudo ao equipamento em si. Alguma informação poderá já estar atualizada, mas continua a ter um certo valor de forma a compreender as decisões tomadas pelas equipas de desenvolvimento.

LifX

O processo para configurar uma nova lâmpada na rede local passa pelos seguintes passos:

1. Ao ligar a lifx cria um rede *ad-hoc*.
2. O utilizador através da aplicação móvel liga-se a essa rede.
3. Através desta rede é possível passar à lâmpada a informação necessária para que esta se possa ligar à rede local.
4. Ao terminal o processo a *Lifx* liga-se à rede e passará a estar acessível receber instruções restantes dispositivos.

É possível definir uma lâmpada como *master* de forma a controlar um conjunto de lâmpadas que desempenharão funções de *slave*. Esta comunicação é feita por 6LowPAN.

O serviço "LifX Cloud" permitirá controlar as lâmpadas, mas neste momento a única funcionalidade está relacionada com a integração com o Nest.

Decisões técnicas

O modulo Wi-Fi da lâmpada funciona com *routers* de suportem 802.11 b/g/n.

Como a introdução de novo equipamento na rede local pode ser vista como um novo vetor de ataque, a *Lifx* utiliza os mecanismos de segurança existentes como o WPA 2. No caso da comunicação inicial entre lâmpadas, de forma a que uma nova lâmpada possa entrar na rede, existe um processo para que se possa comprovar que a nova pertence ao mesmo dono e evitar que lâmpadas externas à rede se juntem à mesma. O processo segue os seguintes passos:

- No equipamento com as funções de *master* é definida uma cor e quantas vezes a nova lâmpada deverá piscar.
- A lâmpada *slave* ao descobrir uma nova *master* irá piscar um determinado numero de vezes uma cor.
- No caso de não coincidir, esta deverá continuar a pesquisa por uma nova *master*.

`http://lifxtech.blogspot.pt/`

Informação do blog oficial

No blog da empresa é possível encontrar alguma informação sobre os detalhes da implementação de determinadas funcionalidades. Desta forma, sabe-se que o serviço *cloud* disponibilizado expõe uma API JSON, que recebe os dados das aplicações e por sua fez comunica com o equipamento onde quer que ele esteja.

Dentro da rede optaram por usar um protocolo mais leve para comunicar com as lâmpadas. Esta decisão levou a escolha dos "Protocol Buffers", desenvolvido pela Google, por tornar a comunicação mais rápida e consumindo menos tráfego.

`http://blog.lifx.co/2013/03/04/developers-developers-developers/`

`https://github.com/google/protobuf/`

Protocolo

Não foi encontrado nenhum documento oficial que descreva as características do protocolo para comunicar com o equipamento.

A única referência existente é um documento de um utilizador que intercetou as comunicações entre a aplicação e a lâmpada e descreveu tudo o que encontrou:

```
https://github.com/magicmonkey/lifxjs/blob/master/Protocol.md
```

A exploração do código-fonte das bibliotecas disponibilizadas, pode ajudar a compreender alguma falha no documento acima citado.

```
https://github.com/lifx
```

Cloogy

A informação disponível sobre o funcionamento deste dispositivo é muito escassa. Depois de uma pesquisa exaustiva na Internet sobre o funcionamento do Cloogy a única informação útil encontrada está presente na seguinte apresentação:

```
http://www.slideshare.net/isasensing2011/cloogy-at-european-utility-week-2013
```

A mesma não é uma apresentação técnica, mas é possível retirar a seguinte informação:

- O *hub* comunica com diferentes tipos de dispositivos.
- A comunicação com o transmissor é através do protocolo "Zigbee".
- Liga-se ao *router* através de uma ligação com fios, de modo a poder comunicar com a Internet.
- Comunicação esta que presumivelmente será através do protocolo HTTP.
- Existe a possibilidade de o *hub* poder suportar outros protocolos.

ChromeCast

O processo para configurar um chromecast é muito semelhante ao usado na Lifx e passa pelo seguintes passos:

1. Ao ligar o chromecast cria um rede *ad-hoc*.

2. O utilizador através da aplicação móvel ou extensão liga-se a essa rede.
3. Através desta rede é possível configurar a informação necessária para que o equipamento se possa ligar à rede local.
4. Ao terminar o processo o chromecast liga-se à rede e passará a estar acessível para receber instruções dos restantes dispositivos.

Anteriormente o protocolo DIAL era utilizado para descobrir dispositivos na rede, o processo foi alterado e agora é usado o mDNS.

As atualizações para este sistema são feitas automaticamente sem o utilizador ser notificado.

Aplicações

O chromecast disponibiliza um SDK para que programadores possam desenvolver aplicações para o dispositivo. Este SDK está disponível para múltiplas plataformas.

Estas podem correr num dispositivo móvel ou computador (aplicações de envio) ou ser executadas pelo chromecast (aplicações de receção).

```
https://developers.google.com/cast/
```

```
https://code.google.com/p/chromecast-mirrored-source/
```

```
https://plus.google.com/communities/115742157569103585450
```

Implementações anteriores

O modo de funcionamento e protocolos descritos nos artigos abaixo já não são usados por estes dispositivos nas versões mais recentes. No entanto esta informação pode ser muito útil durante os testes.

```
https://plus.google.com/u/0/+LeonNicholls/posts/b3wCmToPehK
```

```
http://geeknizer.com/how-chromecast-works-chromecast-protocol-explained/
```

Qold

O Qold é o dispositivo que ainda não chegou oficialmente ao mercado e encontra-se neste momento em fase de testes, daí a informação disponível publicamente ser escassa.

No entanto a partir da informação que foi possível recolher, o qold é composto por dois tipos de dispositivos, os sensores que recolhem os dados e um *hub* que comunica com os sensores por "radio frequência" de modo a recolher e enviar a informação para a Internet.

Este comunica com uma API REST, onde realiza a autenticação através de OAuth, para enviar os dados para armazenamento na *Cloud*. O serviço utilizado para armazenar os dados chama-se *Aqora* e recebe os dados em forma de series temporais.

O utilizador pode consultar os dados através de um cliente web ou através de uma API.

EnergyHive

Apesar de saber como se instala e como funciona, não foi possível encontrar qualquer informação útil sobre as tecnologias utilizadas, decisões técnicas e protocolos de comunicação utilizados por este dispositivo. Situação que vai obrigar a uma pesquisa mais aprofundada na presença do equipamento.

Whithings Smart Body Analyzer

Este equipamento tem suporte para ligações utilizando as tecnologias *Bluetooth low energy* e Wi-FI, a primeira serve para comunicar com dispositivos moveis Android ou IOS de modo a poder configurar a ligação à Internet da balança que será feita através da segunda.

Não foi possível encontrar documentação oficial detalhada sobre o funcionamento do dispositivo, mas existe algum material feito por terceiros que descreve as comunicações feita pela balança. No endereço que se segue é possível compreender os detalhes da API na Internet e dos detalhes que são transmitidos:

```
http://blog.chris007.de/?p=459
```

Relativamente à configuração do equipamento existem na Internet alguns artigos que a descrevem. Apesar de já se encontrarem desatualizados podem fornecer informação útil acerca das decisões técnicas tomadas pela equipa ao longo o tempo:

```
http://www.dcrainmaker.com/2010/05/withings-wifi-scale-in-depth-review.html
```

```
http://www.prolixium.com/mynews?id=915
```

Fitbit Flex

O dispositivo liga-se a dispositivos moveis e a computadores através de *Bluetooth Low Energy*, para estes últimos fornece um recetor que se liga por USB e que permite comunicar com o Flex.

Várias componentes do protocolo usado entre o computador e o recetor encontram-se descritas no seguinte artigo:

```
https://docs.google.com/file/d/0BwJmJQV9_KRcSE0ySGxkbG1PbVE/edit
```

Implementações de código-fonte aberto dos protocolos usados pelas aplicações oficiais podem ser usadas para obter mais detalhes sobre o seu funcionamento. Abaixo encontram-se duas delas:

```
https://bitbucket.org/benallard/galileo
```

```
https://github.com/openyou/libfitbit
```

Uma descrição detalhada do funcionamento deste dispositivo é feita no trabalho realizado por alunos do *Massachusetts Institute of Technology* (MIT) que se encontra abaixo:

```
https://courses.csail.mit.edu/6.857/2014/files/
17-cyrbritt-webbhorn-specter-dmiao-hacking-fitbit.pdf
```

Anexo B

Ataques conhecidos

Ataque conhecidos aos dispositivos

Neste anexo encontram-se listados alguns dos ataques específicos para equipamentos presentes neste trabalho, que se encontram publicados na Internet. Pretende-se através dos mesmos compreender onde falharam as defesas e se estes abrem portas para outro tipo de ataques.

Será ainda verificado se os dispositivos se encontram vulneráveis aos ataques aqui referenciados, apesar dos mesmo já terem sido divulgados, se estes se encontrarem dentro do âmbito do trabalho.

LifX

Este ataque explora uma ausência de encriptação na comunicação entre várias lâmpadas o que permitia obter a password de acesso à rede Wi-Fi.

```
http://www.contextis.co.uk/resources/blog/hacking-internet-connected-light-bulbs/
```

Chromecast

Este primeiro ataque, permite a alguém que não esteja na mesma rede Wi-Fi que o chromecast desconectar o dispositivo e ligá-lo a outra rede. Permite assim ganhar controlo sobre o dispositivo e alterar os conteúdos que se encontram a ser transmitidos:

```
https://www.youtube.com/watch?v=MZUYYgyUyh8
```

Este segundo ataque, que necessita de acesso físico ao dispositivo, explora uma falha na verificação das "imagens" que são carregadas em modo USB, permitindo assim correr software não validado no arranque do equipamento.

```
https://blog.exploitee.rs/2013/chromecast-exploiting-the-newest-device-by-google/
https://www.exploitee.rs/index.php/Google_Chromecast#Bootloader_Exploit_Package
```

Whithings Scale

Em versões anteriores deste dispositivo, a comunicação com a Internet não usava qualquer tipo de encriptação, facilitando assim qualquer tipo de ataque MITM.

```
http://blog.chris007.de/?p=459
```

Fitbit Flex

Não sendo um ataque especifico a este dispositivo, uma equipa conseguiu modificar e injetar a informação enviada pelo dispositivo de forma a obter uma quantidade de "prémios"apenas disponíveis para quem atingisse determinados objetivos. A consistência dos dados não era verificada depois da sua receção.

```
https://securityledger.com/2013/05/
fitbitten-researchers-exploit-health-monitor-to-earn-workout-rewards/
```

```
http://arxiv.org/pdf/1304.5672v1.pdf?goback=.gde_2206357_member_236224214
```

Anexo C

Guia de boas práticas

A guide for securing your IoT device

Gonçalo Valério

August 29, 2015

Date Performed: June 2015
Supervisor: Jorge Santos, Msc

1 Introduction

1.1 Background

This document is the result of a research performed during the internship of the masters degree in Informatics Engineering at Whitesmith [1]. The purpose of the work was initially to study the state of the art of IoT security and other privacy concerns, inspect some popular devices in addition to the in house ones and propose strategies or solutions to improve future releases.
This approach is the reflex of a needed change in the mentality of many manufacturers and the confirmation that the principles and concept of *"security by design"* are in fact important for the success of any IoT offerings.
In addition to the security tests made on some devices a provisioning method was proposed to improve this setup process that was found in many cases insecure. That part of the work is also available publicly at [2].

1.2 Objectives

This document has two main goals, which are to expose the some of the weaknesses found during our research (and their solutions) and to make the bridge to many documents and projects that can help manufacturers improve their offerings.
The research followed mostly a previous work done by OWASP [3] in 2014, that is their "Iot top 10 project" [4], even tough some security concerns were found outside of that scope. These concerns do not only compromise software bugs and the use of outdated and vulnerable implementations, but also were found some security flaws in the design of some processes.
Regarding the second goal, for each security concern we will show what good practices and solutions are described in the existing literature and propose a way to fix them.

2 Why it matters to business

Discussing the business perspective is very important, because much of the decision making in every technology development project is dependent on business. The time frame, the resources, the budget, the features, every one of the previous areas is dependent on the priorities of non technical people focused in maintaining their company floating.
In most cases compromises must be made, but nowadays security shouldn't be in that list. The business impacts of security breaches, data loss, customer privacy violations and damages caused by attacks can lead to serious monetary losses and to the destruction of the company's reputation.
So communicating and making every stakeholder understand the importance of having a *security-by-design mentality* is critical. In this paper we try to cover the possible outcomes in an easy language without lacking in technical aspects and depth, in order to provide both audiences with the information needed to secure certain aspects of the devices and the reason it must be done.

3 What you shouldn't forget to address

3.1 Introduction

During our research, which was done in a relatively small but popular group of devices and included *wearables*, TV Sticks, energy monitors and analysers of several body parameters, we found a diverse number of security problems, that in the vast majority could be easily avoided.
Given that our work was done using the *OWASP Internet of things Top 10 2014* [4] as a reference, the majority of the issues fall into at least one of the categories defined in their "list". However some of them might be a little more complex.
One aspect that you should be aware while reading this document is that it isn't supposed to be the full reference on how to build a secure device and surrounding systems. For that you should check the other referenced materials and consult with a security professional. This document only addresses a subset of all issues that must be kept in mind while building your product.
In the following chapters the most common problems found in the research will be broken down into categories, then discussed separately.

3.2 Transport

Starting with the topic of transport, which means how should the data be transmitted between the device and the cloud, Smartphone or any other device through any channel, which in the majority of the case we should assume as insecure. This is probably the most discussed topic in Internet security in the recent years however some devices still seem to lack any mechanism to safeguard the user's data in this regard.
In our research we found devices that even though they are massively popular, just didn't implement any protection to the shared data. This makes it easy

for any attacker to eavesdrop or do some kind of more complex MITM attack. Other implemented protection mechanisms that are outdated and have been proven insecure.
It is essential that every link between all stakeholders in the system to be encrypted. This encryption should be made using a state of the art standard that as been proven effective [5, 4] given device constrains.
A TLS or DTLS implementation should be used, depending as said on the device constrains. For a generic case, were exists Internet connection, some processing capacity and power is not an issue the mozilla server recommendations [6] should be used. Something like this:

Versions: TLSv1.1, TLSv1.2

RSA key size: 2048

DH Parameter size: 2048

Elliptic curves: secp256r1, secp384r1, secp521r1 (at a minimum)

Certificate signature: SHA-256

DTLS should be used for more constrained devices. Given that all its versions follow the TLS versions described above, the remaining parameters should be matched.
For cases were the use of the above solutions is not possible, check the security specs of the protocol being used or consider using an application layer security protocol.

3.3 Authentication

Following the trend from the previous topic, authentication should not only be addressed when accessing the device but also between all the communications made to and from the device and related services.
It goes several steps further than just saying the user needs stronger password, authentication also means that every stakeholder in the system (servers, devices and users) know and can verify precisely with whom they are "talking" with. For interaction with users this often means passwords but between machines there are several alternatives such as pre-shared keys, raw public keys or certificates [5].
Some devices that were tested had weak authentication mechanisms in some of their actions, making it easy to exploit them in some way. A few examples of the problems found were:

- The server accepted data from a device without checking if it was the right account sending the data.
- The device does not do any kind of identity verification
- Recovery passwords are sent in plain text by email.

So regarding this topic, there are several aspects that a developer/manufacturer should be aware and make sure their device does:

- Use default and widely tested processes for account password recovery in the related web services that communicate with the devices.
- Only accept strong passwords, either on the device or in the related web services/mobile apps.
- Use a string key derivation function to store the passwords (look at scrypt or PBKDF2) [7]
- If possible use a public key infrastructure to assure that all stakeholders verify each others identity.
- Make sure that if any physical action on the device or access to its internal systems is needed, only the manufacturers can perform it.

A good practice would be to use a public key infrastructure so each stakeholder identity would be validated through a certificate [8].

3.4 Provisioning

Another aspect that is very important when developing an IoT solution, is the provisioning method. Not all solutions specially those destined to B2C (Business to Consumer) segment, where is highly probable that the company's engineers will not do the setup for each customer.
This way, for the devices that need wireless connection, a mechanism for the user to easily do the setup and provide access to the network(Internet) generally is developed. This process should ensure 3 main things, that only the owner can run the setup mechanism, the device and the user can authenticate each other and that all the critical information shared between them is well protected.
In our research several devices were in this category and all of them were accompanied with an app that would do the setup either by bluetooth or connection to the device's temporary access point.
All of them failed to secure all 3 aspects mentioned above. Here are the main security issues found:

- Network credentials were transmitted in clear text.
- An attacker could "remotely" initiate the setup process.
- Any person within the reach of the device could connect it to their network.

This issue is very dependent on purposes and constrains of each type of device, but in the case of home and office equipment, this rules should be helpful for developing a more secure mechanism:

- The user should only be able to initiate the setup mechanism with physical access to the device.

- Only allow 1 connection to the device.
- Use standard mechanism to protect the link with the device. For example if the device spawns an access point and a screen, use WPA2 and print the access password on the screen. Otherwise implement the security on the application layer.

With this in mind, we developed a prof of concept setup mechanism, based on some constrains, for a IoT device that would meet all of the 3 aspects. It could be a good starting point is this matter [2].

3.5 Network Services

Since the intent of the Internet of things is to have interconnected devices that interact with the real world, many times this devices need to also accept connections. This is done through exposed network services that are constantly listening for input from other agents in the network. As it is well known, this is one of the major attack vectors for any device, as soon a vulnerability in the software used by these services is found attackers will to exploit any machine that doesn't have been patched.
This is also true for IoT devices, since they typically are updated less frequently than most servers. So the recommendation here (given by almost every security manual out there) is to have the minimum number of services required for the device to work properly actively running. If the device only function is to send information it doesn't need any network service permanently running and listening for connections.
For those services that are essential, frequently check for updated and vulnerabilities so that they an be fixed as soon as possible.

3.6 Firmware Updates

Other aspect that is very important and sometimes is not implemented in a secure matter is the firmware/software update mechanism, this servers not only of major upgrades but also for fixing small bugs and security vulnerabilities. This mechanism should be secure and is recommended to be a base requirement of any new device [9].
During the research we found that the majority of the devices got the this aspect right but yet some fundamental problems still exist as:

- Users downloads a program to his PC to upgrade the device, from a insecure location.
- The mechanism allowed the device to upload, instead of being read-only.

So to have a secure upgrading mechanism it should take care of the following issues:

- The transmission should be encrypted.

- The device should be able to verify (authenticate) the source and the integrity of the code.
- It should be download only.
- The device should automatically check for new updates.

These aspects should be common-sense but is always good to remember as does the OWASP in their recommendations [4].

3.7 Cloud

Even though this aspect was outside of the scope of the study we had some contact with the cloud services that gave support to the devices. Through a normal user utilization it was easy to detect some bad patterns in this services that could throw away most of the security measures implemented in the device level.
If you are exposing a service on the Internet to the user (either through an API or website) you should follow the security best practices of this area. The OWASP website should be good place to start.
Here are some of the critical aspects that were found:

- Cloud services, of a well protected devices, that are only available through HTTP.
- Insecure authentication and mechanisms to recover passwords.

4 Privacy

Privacy is a topic that generally concerns more the users than the manufacturers. In the last decade the trend has been to extract more and more information about the user, from a manufacturer point of view it is great since with more information it is possible to do more and provide *better* services and experiences. However, with the advent of the Internet of things the user's information is expected to be much more available since it is collected automatically and generally without user input.
This fact combined with the overall notion that this devices are, in their vast majority, insecure [10], is everything that is needed to compromise the users privacy more than expected.
Even though this recommendation might go against some business aspects of the product, the development team should try to address it some how. During our tests we've found and confirmed several issues with some devices such as:

- User information is exposed in the network
- Device features allow the user to be tracked by other entities

Given this issues and other concerns manufactures should make sure the development of their device takes the following points into account:

- Inform the user in a clear way about all the data that is being collected
- Do not collect more data than the explicitly needed
- Given the user a change to opt out from the collection of extra data.
- Understand the information that could be indirectly obtained by the collected and aggregated data. Act to minimize the issue.
- Use best practices to protect the data in transit and the one that is stored.

If the above principles are followed and used with a *privacy by design* development process, we are certain that the business goals can be met while protecting the user's privacy.

5 Conclusion

In this small guide we tried to sum in a clear way our main findings when studying how these devices work. The Internet of Things is here to stay and the possibilities are almost limitless, browsing the Internet and reading the newspapers these days will let you with notion of all the excitement in the technology industry about this phenomenon, that while not being new is getting up to speed.
The exposed concerns and suggestions if taken into account, will greatly improve the security and privacy of the users without being restrictive for the manufacturers.
As it as being said in the past [10] the majority of this issues can be described as "low hanging fruit" and can be solved pretty easily, the only requirement being the developers to have a security mindset while designing the whole ecosystem.
The only topic that we have not seen properly addressed, was definitely the provisioning method of the devices. Which given the number of possibilities and usages of this kind of devices, must take into account the local attackers. For this a proof of concept was built to address a common pattern, that is "devices without user interface" that need to connect to a local (and protected) wifi network.
Concluding this guide, we would like to make a call to developers starting new projects to address security from the beginning since it will lead to more secure devices and less troubles along the way. There are many resources and communities trying to get this topic right, with great documentation that could be used [11].

References

[1] "Whitesmith." http://www.whitesmith.co.

[2] "Setup spell - repository." https://bitbucket.org/dethos/setup-spell-device.

[3] "Owasp." https://www.owasp.org.

[4] "Internet of things top 10." https://www.owasp.org/index.php/OWASP_Internet_of_Things_Top_Ten_Project.

[5] "Security guidance for early adopters of the internet of things (iot)." https://cloudsecurityalliance.org/media/news/csa-launches-new-security-guidance-for-early-adopters-of-the-iot/.

[6] "Security/server side tls." https://wiki.mozilla.org/Security/Server_Side_TLS#Modern_compatibility.

[7] "Recommendation for password-based key derivation part 1: Storage applications." http://csrc.nist.gov/publications/nistpubs/800-132/nist-sp800-132.pdf.

[8] "The challenges of iot security and techniques for mitigating risk." http://nquiringminds.com/files/2015/06/NQM-IOT-Security-4.pdf.

[9] O. Whitehouse, "Security of things: An implementers' guide to cyber-security for internet of things devices and beyond." https://www.nccgroup.com/en/learning-and-research-centre/white-papers/security-of-things-an-implementers-guide-to-cyber-security-for-internet-of-things-devices-and-beyond/.

[10] "Internet of things research study." http://www8.hp.com/h20195/V2/GetPDF.aspx/4AA5-4759ENW.pdf.

[11] "Builditsecure.ly." http://builditsecure.ly/.

Anexo D

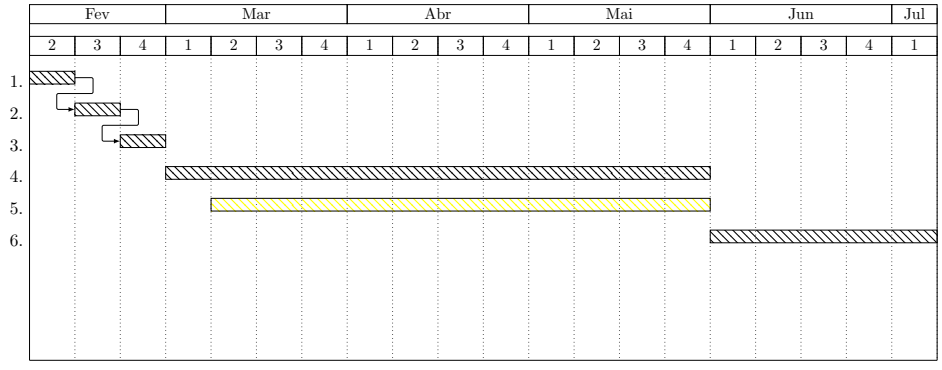
Planeamento inicial

Descrição das várias fases do trabalho que integravam o planeamento inicial do estágio para o segundo semestre:

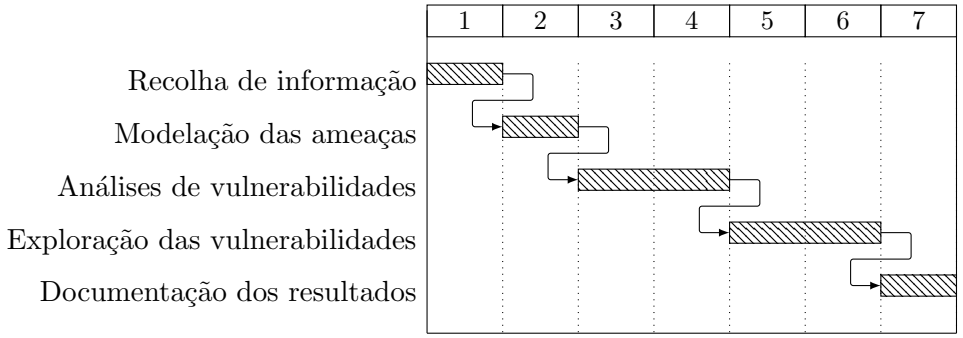
Tabela D.1: Planeamento inicial

Tarefa	Inicio	Fim
1. Definição dos testes	09/02	12/02
2. Configuração e preparação das ferramentas	13/02	17/02
3. Criação de scripts para automatização	18/02	28/02
4. Testes nos dispositivos	01/03	29/05
5. Divulgação dos resultados	10/03	29/05
6. Preparação dos relatório final	30/05	26/06

Abaixo encontra-se a representação das mesmas, de forma mais gráfica, através de um diagrama de Gantt:



A componente relativa aos testes seria dividida em 10 etapas, ou seja uma para cada dispositivo, que seriam executadas a cada 7 dias, como mostra o seguinte diagrama:


1
2
3
4
5
6
7
Recolha de informação
Modelação das ameaças
Análises de vulnerabilidades
Exploração das vulnerabilidades
Documentação dos resultados