Estudo sobre a segurança de dispositivos domésticos conectados à Internet das Coisas

Gabriel Esteves Messas[1], Bruno Bogaz Zarpelão[1]

[1]Departamento de Computação – Universidade Estadual de Londrina (UEL)
Caixa Postal 10.011 – CEP 86057-970 – Londrina – PR – Brasil

gabriel_messas@uel.br, brunozarpelao@uel.br

Abstract. *With the growing globalization and popularization of the Internet, the access to devices with this capability has become extremely easy. Increasingly more connected, these devices are now added to the domestic environment, propelled by the concept of the Internet of Things (IoT). Such proximity to the end user brings to the light discussions on the trustworthiness of the equipment in question. This proposal, therefore, aims to thoroughly analyze selected gadgets of this kind in terms of security, user protection, and data privacy. In this sense, the study of possible vulnerabilities can contribute widely to all involved people and organizations.*

Resumo. *Com a crescente globalização e a popularização da Internet, o acesso a dispositivos com tal capacidade se tornou extremamente fácil. Estes, cada vez mais conectados, agora marcam presença no ambiente doméstico, impulsionados pelo conceito da Internet das Coisas (Internet of Things - IoT). Tal proximidade ao usuário final torna relevantes discussões sobre a confiabilidade, em termos de segurança e privacidade, dos equipamentos em questão. Este trabalho, portanto, apresenta uma análise de determinados aparelhos deste tipo, no que tange à segurança, à proteção do usuário, de sua privacidade e de seus dados. Deste modo, o estudo de possíveis vulnerabilidades contribui em âmbito global a todos os grupos envolvidos.*

1. Introdução

O início do século XXI marcou uma sólida aceleração no desenvolvimento de tecnologias eletrônicas, especialmente na área da computação. Esta, agora, inclui dispositivos cada vez mais poderosos e inteligentes, os quais, aliados à crescente abrangência e evolução da Internet, contribuem para tornar a vida humana progressivamente mais fácil [1].

Tais fatos contribuíram fortemente para a democratização do acesso a aparelhos eletrônicos, de maneira que, atualmente, estes se fazem presentes até mesmo no ambiente doméstico [2], impulsionados pelo conceito da Internet das Coisas. Esta proximidade ao usuário final certamente acende um alerta no que tange à real confiabilidade dos equipamentos em questão, haja vista que possuem conexão direta à rede local e, consequentemente, acesso irrestrito às informações intercambiadas [3].

Neste cenário, mesmo que as suspeitas sobre más intenções por parte do próprio dispositivo sejam descartadas, há, ainda assim, a possibilidade de que uma vulnerabilidade seja explorada por um terceiro envolvido. Logo, rotular um dispositivo

como seguro é, ao mesmo tempo, garantir que seu código-fonte não é malicioso por si só e que este não é frágil e/ou abre brechas a ataques externos.

A boa notícia é que há maneiras de colocar tais máquinas à prova a fim de garantir os pontos mencionados [4]. Aquelas se resumem, em sua maioria, a um processo que tem como cerne um objetivo contraintuitivo a priori: invadir o próprio equipamento testado. Desta forma, o resultado se dá pelo sucesso - ou não - do propósito estabelecido, revelando um dispositivo inseguro ou confiável, respectivamente.

Em vista do exposto, o presente projeto tem como intuito primário testar aparelhos selecionados, tais como receptores de IPTV e TV *Boxes* - tomados como exemplo -, realizando rotinas de invasão através da rede [5]. Os resultados, por suas vezes, mostrarão o nível de confiabilidade dos dispositivos, que servirão como representantes da classe de produto à qual estão integrados. Por fim, almeja-se estabelecer um protocolo de verificação que possa ser adotado para avaliação de segurança em dispositivos *IoT*.

2. Fundamentação Teórico-Metodológica e Estado da Arte

2.1 Internet das Coisas

Internet das Coisas, mais conhecida por seu termo em inglês: *Internet of Things* (*IoT*), é um conceito que se refere à interconexão digital de objetos cotidianos com a Internet. É uma extensão da Internet atual que possibilita que objetos do dia-a-dia, contanto que tenham capacidade computacional e de comunicação, se conectem à Internet [6].

Neste cenário, a conexão com a rede mundial de computadores possibilita, primeiramente, interagir remotamente com os objetos e, em segundo lugar, que esses próprios equipamentos sejam usados como provedores de serviços. Essas novas capacidades de aparelhos comuns abrem caminho a inúmeras possibilidades, principalmente no âmbito doméstico.

Segundo a empresa de consultoria Gartner, em 2020, deve haver, no mundo, aproximadamente 26 bilhões de dispositivos com um sistema de conexão à Internet das Coisas. Já a consultoria Abi Research prevê que, no mesmo ano, existirão 30 bilhões de dispositivos sem fio conectados a este segmento da Internet [7]. Estima-se que cada ser humano esteja rodeado por 1 000 a 5 000 desses aparelhos, em média.

O conceito de *smart home* (ou lar inteligente, em português), por exemplo, descreve um lugar equipado com aparelhos eletrônicos ligados a uma rede, Wi-Fi ou Bluetooth, constituído por um sistema integrado que permite controlar múltiplos dispositivos, como sistemas de iluminação e de temperatura, eletrodomésticos ou estações de entretenimento, como receptores de canais via Internet ou gerenciadores de acesso a plataformas de *streaming.*

Todavia, essas características acarretam riscos e implicam grandes desafios técnicos. Tais dispositivos *IoT*, por serem inteligentes e possuírem conexão à rede, possuem um endereço IP, porta de entrada que permite a um agente mal-intencionado se conectar e realizar ataques à segurança e à privacidade dos usuários do equipamento.

Para servir como base, segundo a empresa de segurança virtual Kaspersky Lab, existem pelo menos 7 mil amostras de malwares em dispositivos *IoT*. Além disso, em

setembro de 2016, o site Tecmundo noticiou o maior ataque de negação de serviço já registrado, utilizando dispositivos da Internet das Coisas, roteadores e câmeras de segurança, o que denota a necessidade de tratar o segmento com atenção.

Por serem máquinas pequenas, numerosas e diversas, desenvolver sistemas de defesa torna-se uma tarefa complexa. O fato de possuírem sistemas operacionais super leves e com arquitetura reduzida também não colabora. Logo, garantir que a implementação do dispositivo em si não abre brecha a falhas é crucial.

2.2 Vulnerabilidades e Ameaças Virtuais

Uma vulnerabilidade é definida como uma condição que, quando explorada por um atacante, pode resultar em uma violação de segurança. Exemplos de vulnerabilidades são falhas no projeto, na implementação ou na configuração de programas, serviços ou equipamentos de rede [9].

De acordo com a ISO 27000 [10], conjunto de normas para Sistemas de Gestão de Segurança da Informação elaborada pela ISO (*International Organization for Standardization*), um ataque de exploração de vulnerabilidades ocorre quando um atacante, aproveitando-se de uma fraqueza do sistema, tenta executar ações maliciosas, como invadi-lo, acessar informações confidenciais ou tornar um serviço inacessível.

As vulnerabilidades de segurança podem ser divididas em vários tipos com base em critérios diferentes – como, onde a vulnerabilidade existe, o que a causou ou como ela pode ser usada. Algumas categorias amplas desses tipos de vulnerabilidade incluem:

- Falhas humanas

  O elo mais fraco em muitas arquiteturas de segurança cibernética é o elemento humano. Os erros do usuário podem facilmente expor dados confidenciais, criar pontos de acesso exploráveis para invasores ou interromper sistemas. Os próprios usuários internos às vezes executam arquivos maliciosos que facilitam a intrusão no sistema e a perda de dados e informações, seja por falta de conhecimento, desatenção ou atividades maliciosas de colaboradores.

- Vulnerabilidades de rede

  Problemas com o hardware ou software de uma rede que a expõem a uma possível invasão de terceiros. Os exemplos incluem pontos de acesso Wi-Fi inseguros, *firewalls* mal configurados e falhas de arquitetura.

- Vulnerabilidades de aplicações

  Fraquezas de softwares ou sistema operacional que expõem o dispositivo a riscos de segurança que possam ser utilizadas para ataques, como roubo de dados e sequestro de informações. Um exemplo comum são softwares desatualizados ou mal estruturados.

Uma preocupação atual, por exemplo, é o aumento no número de ataques a dispositivos com Internet das Coisas. Essa tecnologia é uma das bases da transformação

digital e da própria Indústria 4.0, mas traz consigo um risco adicional para a infraestrutura digital das empresas — algo com o qual os peritos em segurança devem saber lidar.

2.3 *Ethical Hacking*

Em âmbito popular, o termo *hacker* é associado ao indivíduo que se dedica a burlar os limites de segurança de dispositivos, sistemas e redes de computadores, cuja intenção é sempre maliciosa [11]. No entanto, esta associação é feita de maneira errônea, uma vez que tal predicado pertence ao termo *cracker* – o verdadeiro vilão mal-intencionado.

Ethical Hacking (do inglês, *hacking* ético), por sua vez, é justamente a alcunha – desta vez, correta – utilizada para se referir ao trabalho desempenhado pelo *hacker* – agente sem intenções maliciosas. É o conceito que representa, de forma legítima, as atividades desempenhadas por aquele que trabalha nesta área, também chamado de *ethical hacker* (*hacker* ético).

Logo, o *hacker* ético é um profissional de tecnologia da informação especializado na área de segurança, cuja função é encontrar vulnerabilidades que um *hacker* malicioso poderia explorar. Para tal, este utiliza, dentre outros métodos, de uma rotina de testes que acabou conhecida como *pentest* (contração oriunda da expressão inglesa *penetration testing*; em português, teste de invasão*).* Além disso, o objetivo primário daquele é gerar um relatório do sistema sob análise, a fim de resolver problemas e implementar melhorias.

Para realizar este serviço, no entanto, o *hacker* deve necessariamente ter permissão para investigar. Caso receba sinal positivo, ele tem ainda outra responsabilidade: respeitar a privacidade e acesso aos arquivos, já que uma série de informações sensíveis podem estar expostas [12]. Portanto, conclui-se que o profissional desta área deve ter conhecimentos iguais ou superiores a um *cracker*, e código de ética invejável.

2.4 *Penetration Testing*

Penetration Testing (ou *pentest*, do inglês, Teste de Penetração) é o procedimento que engloba as atividades que buscam submeter redes, sistemas ou programas a uma série de testes de invasão. Estas são realizadas através de técnicas e ferramentas variadas, testando diversos cenários que possibilitem a identificação de vulnerabilidades de segurança. Em suma, o teste de intrusão simula um ataque malicioso, justamente para que sejam analisadas formas de evitá-lo.

Falhas desconhecidas em *hardwares* ou em *softwares*, junto a deficiências no sistema operacional, são em geral as categorias mais comuns de vulnerabilidades encontradas por testes desta natureza.

O *pentest* – como é popularmente chamado – é comumente contratado por organizações para análise de segurança e pode ser subdividido em diversas categorias, sendo a mais relevante a que o classifica de acordo com o nível de conhecimento do perito sobre o sistema alvo:

- Análise *black-box*

  É o tipo de teste em que o executor (*pentester*) não possui informação técnica alguma sobre a infraestrutura de rede, especificações dos sistemas ou modo de funcionamento dos dispositivos sobre os quais o teste de penetração está sendo realizado.

- Análise *white-box*

  Nesta modalidade, o *pentester* conhece previamente toda a infraestrutura que será analisada, incluindo, dentre outros, o mapeamento de rede, a amplitude dos endereços IP, os *firewalls* e equipamentos de roteamento local existentes, além de informações específicas sobre as máquinas e *softwares* nelas em execução.

Testes do tipo *black-box* simulam um ataque de alguém que esteja familiarizado com o sistema, enquanto um teste *white-box* simula o que pode acontecer após um vazamento de informações, em que o invasor tenha acesso ao código fonte, esquemas de rede e, possivelmente, até mesmo a algumas senhas. Há ainda o *grey-box*, onde o executor possui conhecimento parcial sobre o alvo.

O processo completo deve possuir metodologia bem definida e o protocolo, geralmente, se divide em:

- Fase de planejamento

  Momento anterior ao início do teste em si, onde se define o modelo da análise (interna ou externa, direitos e privilégios habilitados), as metas, os dados de origem e o escopo de trabalho; se desenvolve e adapta a metodologia a ser usada.

- Fase de teste

  Período de execução dos procedimentos técnicos de fato (testes de penetração), que engloba, geralmente, em sequência: a identificação da rede e dos dispositivos alvos; enumeração das ferramentas de intrusão; detecção e exploração de vulnerabilidades nas máquinas, utilização de sistemas comprometidos como um trampolim para novas intrusões; eliminação de falsos positivos.

- Fase de consolidação

  Onde se analisa os resultados obtidos durante as fases anteriores e, principalmente, constrói-se relatórios com os dados coletados, a fim de servirem como recomendações aos responsáveis pelos equipamentos testados para redução de riscos.

Logo, um teste de penetração só é aproveitado ao máximo se houver uma política de segurança bem definida. Por isso, o protocolo e a metodologia do teste

devem ser implementados de maneira assertiva para tornar o teste de penetração mais eficaz.

3. Objetivos

O presente trabalho tem como objetivo estudar o modo de funcionamento de testes de penetração e aplicá-los a dispositivos eletrônicos variados – essencialmente conectados à Internet, primariamente utilizados no ambiente doméstico – a fim de avaliar seus níveis de segurança.

Como resultado de tal, serão redigidos relatórios individuais de cada teste, a servirem como registro da qualidade e proteção dos sistemas sob prova. Aqueles apresentarão detalhes técnicos dos procedimentos realizados, bem como a descrição das respectivas falhas exploradas – quando estas existirem.

Para cada dispositivo analisado, o documento a ser gerado almeja atrair a atenção e incitar os responsáveis a corrigir as brechas de confiabilidade do equipamento. Mais do que isso, entretanto, o relato em questão visa levantar questionamentos sobre a situação de aparelhos semelhantes e estimular a checagem destes mais eficazmente a fim de evitar defeitos.

Por fim, após todas as etapas e informações geradas, será certamente possível estabelecer um protocolo de testagem genérico o suficiente passível de ser aplicado a equipamentos similares aos em evidência. Este tornará os procedimentos mais simples e poderá ser adotado por outros profissionais e pesquisadores para verificação de vulnerabilidades em ambientes conectados.

4. Procedimentos metodológicos/Métodos e técnicas

Inicialmente, será realizado um processo de pesquisa e aquisição de conteúdo – especialmente na forma de livros, majoritariamente sobre testes de penetração e *ethical hacking* [13] –, para prosseguir à revisão bibliográfica. Esta possui como foco primordial a obtenção de experiência, que servirá como base para a fase de realização dos procedimentos técnicos em si.

Em sequência, serão determinados os dispositivos-chave do estudo, a servirem como alvo da análise. Estes serão escolhidos e adquiridos estrategicamente, haja vista que os exemplares devem assumir o posto de “representantes” de suas classes, englobando produtos similares, a fim de expandir a abrangência e validade do presente projeto.

A seguir, o ambiente de operações técnicas será preparado e configurado. Este consistirá basicamente em uma máquina contendo uma instalação do sistema operacional Kali Linux, junto ao seu conjunto completo de ferramentas de *hacking* e exploração. Será também assegurada a configuração da rede, para garantir que os dispositivos estejam acessíveis na rede local.

A partir de então, será iniciada a fase de execução propriamente dita – sequencialmente, para cada dispositivo selecionado. O protocolo a ser seguido é consonante à descrição fornecida acima sobre testes de penetração: planejamento; obtenção de informações sobre o dispositivo; testes de exploração de vulnerabilidades; relatório dos resultados.

Esta etapa utilizará ferramentas e métodos diversos, a serem determinados durante a fase de aquisição de informações sobre o equipamento, de acordo com os dados obtidos. É possível antecipar, entretanto, o provável uso de *exploits* e aplicações pré-existentes de exploração de vulnerabilidades conhecidas nos sistemas operacionais em questão.

Por fim, os resultados serão consolidados na confecção dos relatórios em texto. Estes, individuais a cada dispositivo, descreverão os passos aplicados e os desenlaces gerados.

5. Cronograma de Execução

Atividades:

1. Levantamento e revisão bibliográfica;
2. Escolha dos dispositivos;
3. Preparação do ambiente técnico;
4. Determinação das ferramentas a serem utilizadas;
5. Execução dos procedimentos técnicos;
6. Análise dos resultados;
7. Geração dos relatórios;
8. Redação do TCC;
9. Revisão ortográfica;

Tabela 1. Cronograma de Execução

	Jul	Ago	Set	Out	Nov	Dez	Jan	Fev	Mar	Abr	Mai
Atividade 1	X	X	X								
Atividade 2	X	X	X								
Atividade 3	X	X									
Atividade 4	X	X	X								
Atividade 5	X	X	X	X	X	X					
Atividade 6				X	X	X	X				
Atividade 7						X	X				
Atividade 8						X	X	X	X	X	
Atividade 9											X

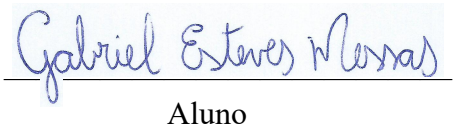
6. Contribuições e/ou Resultados esperados

Este projeto almeja levantar questionamentos no que tange à real segurança e proteção à privacidade do usuário de equipamentos eletrônicos conectados à rede. À medida que estes são postos à prova, espera-se que as situações geradas evidenciem possíveis características desfavoráveis dos aparelhos, as quais servirão como aprendizado ao leitor do trabalho.

Finalmente, com o estabelecimento do protocolo genérico de testagem, ambiciona-se desenvolver uma ferramenta universal de verificação de confiabilidade de dispositivos com conexão à Internet. Objetivos que, por suas vezes, contribuirão tanto para a comunidade científica quanto para a esfera comercial, abrangendo do produtor ao usuário final.

7. Espaço para assinaturas

Londrina, 13 de setembro de 2021.



Aluno

Orientador

Referências

[1] INTERNET. In: WIKIPÉDIA, a enciclopédia livre. Flórida: Wikimedia Foundation, 2021. Disponível em: <https://pt.wikipedia.org/w/index.php?title=Internet&oldid=61763350>. Acesso em: 16 ago. 2021.

[2] Habib, L. (2000) "*Computers and the Family: A Study of Technology in the Domestic Sphere"*. PhD Thesis, London, UK: London School of Economics and Political Sciences (LSE).

[3] Hooijdonk, R. van (2019) "*The hidden dangers of IoT devices*", https://internetofthingsagenda.techtarget.com/blog/IoT-Agenda/The-hidden-dangers-of-IoT-devices. Acesso em: 16 ago. 2021.

[4] Lampe, J (2014) "*How to Test the Security of IoT Smart Devices*", https://resources.infosecinstitute.com/topic/test-security-iot-smart-devices/. Acesso em 19 ago. 2021.

[5] TESTE DE INTRUSÃO. In: WIKIPÉDIA, a enciclopédia livre. Flórida: Wikimedia Foundation, 2020. Disponível em: <https://pt.wikipedia.org/w/index.php?title=Teste_de_intrus%C3%A3o&oldid=57101616>. Acesso em: 19 ago. 2020.

[6] INTERNET DAS COISAS. In: WIKIPÉDIA, a enciclopédia livre. Flórida: Wikimedia Foundation, 2021. Disponível em:

<https://pt.wikipedia.org/w/index.php?title=Internet_das_coisas&oldid=60816330>. Acesso em: 8 set. 2021.

[7] *MORE Than 30 Billion Devices Will Wirelessly Connect to the Internet of Everything in 2020* (2013), https://www.abiresearch.com/press/more-than-30-billion-devices-will-wirelessly-conne/. Acesso em: 8 set. 2021.

[8] VULNERABILIDADE (COMPUTAÇÃO). In: WIKIPÉDIA, a enciclopédia livre. Flórida: Wikimedia Foundation, 2021. Disponível em: <https://pt.wikipedia.org/w/index.php?title=Vulnerabilidade_(computa%C3%A7%C3%A3o)&oldid=61427619>. Acesso em: 25 ago. 2021.

[9] MESQUITA, M. (2020) "O que é a ISO-27001 e o que ela agrega para sua empresa?", https://triplait.com/o-que-e-a-iso-27001/. Acesso em: 26 ago. 2021.

[10] *ETHICAL Hacking* (2021), https://www.portalgsti.com.br/ethical-hacking/sobre/. Acesso em: 26 ago. 2021.

[11] *ETHICAL hacking*: entenda o conceito por trás do hacker do bem (2020), https://blog.unyleya.edu.br/bitbyte/ethical-hacking/. Acesso em: 26 ago. 2021.

[12] Moreno, D. (2015) "Introdução ao Pentest", Novatec Editora Ltda, ISBN: 978-85-7522-618-6.