Atividades dinâmicas para o ensino de segurança da informação em dispositivos para Internet das Coisas

Larissa Benevides Vieira[1] e André Leon S. Gradvohl[1]

l200805@dac.unicamp.br, gradvohl@ft.unicamp.br

[1]Faculdade de Tecnologia da Universidade Estadual de Campinas – FT/UNICAMP, Limeira-SP

Resumo

A Internet das Coisas tem despertado mais interesse do mercado por causa do seu razoável poder de processamento e possibilidade de integração de diversos dispositivos. Por este motivo, a corrida por lançamentos de novos produtos têm feito a indústria negligenciar as questões de segurança. Por outro lado, a academia não tem conseguido formar recursos humanos suficientes para suprir a demanda de profissionais capazes de lidar adequadamente com as questões de segurança da informação.Considerando esse cenário, este projeto de iniciação tecnológica, elaborou e documentou algumas atividades para tornar mais interessante o ensino de segurança da informação em dispositivos para a Internet das Coisas. A ideia é despertar o interesse dos estudantes na área de segurança da informação para dispositivos IoT.

1. Introdução

Definimos a Internet das Coisas (*Internet of Things* – IoT) como a interconexão via Internet de dispositivos computacionais incorporados em objetos do cotidiano, permitindo que eles enviem e recebam dados (RAWES, 2019).

Com sua capacidade de programação, conexão à Internet e sensoriamento, os dispositivos para IoT produzem dados que são processados e transmitidos pela rede. Esses dados podem ser interceptados, adulterados ou até negados, comprometendo os principais pilares da segurança da informação: confiabilidade, integridade, disponibilidade.

Por este motivo, este projeto de iniciação tecnológica elaborou e documentou algumas atividades práticas para tornar mais interessante o ensino de segurança da informação em dispositivos para a Internet das Coisas. A ideia de documentar essas atividades é despertar o interesse dos estudantes, ao mesmo tempo que os capacita para atuar profissionalmente com as questões de segurança computacional para dispositivos na IoT. É importante ressaltar que este projeto foi encerrado na metade do seu desenvolvimento, em função de intercâmbio acadêmico no exterior.

No entanto, a expectativa deste projeto é que os experimentos práticos possam ser incorporados posteriormente em disciplinas regulares de cursos de graduação na área de Informática

(e. g. Ciência da Computação, Engenharia de Computação, Sistemas de Informação, Tecnologia em Análise e Desenvolvimento de Sistemas) ou em cursos de extensão específicos para complementação da formação profissional nos níveis técnico ou superior.

O restante deste resumo foi organizado da seguinte maneira: a Seção 2 indica os materiais e métodos utilizados neste projeto; a Seção 3 mostra os resultados obtidos; e a Seção 4 apresenta as conclusões do projeto.

2. Materiais e Métodos

No início do projeto, foi realizado um levantamento bibliográfico sobre outros trabalhos similares, bem como a análise dos currículos propostos pela Association for Computing Machinery (ACM), Institute of Electrical and Electronics Engineers (IEEE) e Sociedade Brasileira de Computação (SBC) com vistas à identificar habilidades e competências necessárias para as atividades.

Após o levantamento dos principais conceitos necessários para o ensino de segurança da informação na IoT, o próximo passo foi testar os experimentos práticos para ilustrar esses conceitos.

Para este projeto, foram testadas e implementadas três atividades práticas que correlacionam segurança da informação com dispositivos de IoT. Essas atividades resultaram em experimentos que são descritos na Seção 3 a seguir.

3. Resultados

O primeiro experimento prático envolveu um ataque de negação de serviço a um Arduino conectado a rede, e para isso, utilizou-se a ferramenta hping3 a fim de torna-lo indisponivel.

O segundo experimento abrangeou um ataque a Raspberry Pi utilizando credenciais padrões, a fim de obter acesso privilegiado remotamente. E para este ataque foi utilizado a ferramenta rpi-hunter.

O terceiro experimento prático abrangeu a utililização da ferramenta Bettercap, com o intuito de escanear e interceptar dispositivos Bluetooth.

3.1. Experimento 1 – Ataque de negação de serviço a sistema de IoT.

O ataque *Denial of Service* (DoS), tenta impedir ou restringir o uso normal da rede ou da administração da rede – com ou sem fio –, de modo que a máquina alvo receba solicitações supérfluas com o intuito de sobrecarregá-la e impedir, por exemplo acesso a um *site* ou serviço web (RIBEIRO, 2018). Esse tipo de ataque compromete tanto as redes sem fio, quanto as redes IoT (KALITA; KAR, 2009).

Neste experimento, o objetivo principal foi simular um ataque DoS a uma placa Arduino uno conectada a uma rede local. Para isso foi utilizado uma das mais poderosas ferramentas do Kali linux, o Hping3. Essa ferramenta é capaz de enviar arquivos entre um canal coberto, além de suportar os protocolos TCP, UDP, ICMP (KALI LINUX PENETRATION TESTING TOOLS,

2020b). O Hping3 é considerada uma importante ferramenta para criação de pacotes, além de conter muitos outros recursos úteis (WONDERHOWTO COMPANY, 2013).

Enquanto o ataque estava sendo realizado, consegue-se perceber que o tempo de resposta entre o Arduino e o PC (Kali Alvo) aumenta, ou seja, as funções do Arduino ficam comprometidas. A sobrecarga ocorreu, pois houve um número exorbitante de pacotes enviados rapidamente, comprometendo assim o acesso ao Arduino.

3.2. Experimento 2 – Ataque a Raspberry Pi usando credenciais padrão

Ao configurar um Raspberry Pi, é fácil ignorar a alteração de senha padrão. Como muitos dispositivos de IoT, o sistema operacional Raspbian – padrão do Raspberry Pi – é instalado com uma senha padrão amplamente conhecida, deixando o dispositivo vulnerável ao acesso remoto.

Levando isto em consideração, o propósito deste experimento é demonstrar o quanto dispositivos IoT com senhas padrão podem ser consideradas um risco tanto para o próprio dispositivo, quanto para a rede conectada a ele (GURUNATH et al., 2018).

Utilizando a ferramenta rpi-hunter (BUSESCANFLY, 2018) mostrada na Figura 1, foi possível descobrir, acessar e enviar *payloads* – um código malicioso que executa uma ação destrutiva no sistema alvo, fornecendo acesso privilegiado e permissões (e. g. criar um usuário, iniciar ou migrar um processo e até mesmo apagar arquivos) – para o Raspberry Pi com credenciais padrão conectado à mesma rede local utilizada pelo atacante.

Figura 1: Utilização do *payload whoami*

Utilizou-se também o Nmap, uma importante ferramenta do Kali que é útil na descoberta de portas abertas na rede (KALI LINUX PENETRATION TESTING TOOLS, 2020c).

3.3. Experimento 3 – Interceptação de dispositivo *Bluetooth*

Existem protocolos e tecnologias de comunicação que possuem curto alcance e são comumente usados nas aplicações de IoT. Uma delas é o *Bluetooth* (RIBEIRO, 2018).

Por este motivo, para este experimento, utilizou-se a ferramenta Bettercap (KALI LINUX PENETRATION TESTING TOOLS, 2020a). A mesma é utilizada para escanear e interceptar dispositivos *Bluetooth*. Com esta ferramenta, foi possível obter informações específicas sobre o dispositivo *Bluetooth*, como mostrado na Figura 2, a fim de expor suas vulnerabilidades.

Handles	Service > Characteristics	Properties	Data
0001 -> 0005	Generic Access (1800)		
0003	Device Name (2a00)	READ	iPhone
0005	Appearance (2a01)	READ	Generic Phone
0006 -> 0009	Generic Attribute (1801)		
0008	Service Changed (2a05)	INDICATE	
000a -> 000e	Apple Continuity Service (d0611e78bbb44591a5f8487910ae4366)		
000c	8667556c9a374c9184ed54ee27d90049	WRITE, NOTIFY, X	
000f -> 0013	9fa480e0496745429390d343dc5d04ae		
0011	af0badb15b9943cd917aa77bc549e3cc	WRITE, NOTIFY, X	
0014 -> 0017	Battery Service (180f)		
0016	Battery Level (2a19)	READ, NOTIFY	insufficient authentication
0018 -> 001d	Current Time Service (1805)		
001a	Current Time (2a2b)	READ, NOTIFY	insufficient authentication
001d	Local Time Information (2a0f)	READ	insufficient authentication
001e -> 0022	Device Information (180a)		
0020	Manufacturer Name String (2a29)	READ	Apple Inc.
0022	Model Number String (2a24)	READ	iPhone10,2
0023 -> 002c	Apple Notification Center Service (7905f431b5ce4e99a40f4b1e122d00d0)		
0025	69d1d8f345e149a898219bbdfdaad9d9	WRITE, X	
0028	9fbf120d630142d98c5825e699a21dbd	NOTIFY	
002b	22eac6e924d64bb5be44b36ace7c7bfb	NOTIFY	
002d -> 0038	Apple Media Service (89d3502b0f36433a8ef4c502ad55f8dc)		
002f	9b3c81d857b14a8ab8df0e56f7ca51c2	WRITE, NOTIFY, X	
0033	2f7cabce808d411f9a0cbb92ba96c102	WRITE, NOTIFY, X	
0037	c6b2f38c23ab46d8a6aba3a870bbd5d7	READ, WRITE, X	insufficient authentication

Figura 2: Informações sobre o celular iPhone com o uso da ferramenta Bettercap

4. Conclusões

Neste projeto de iniciação tecnológica, foi proposta a criação de práticas que englobassem a segurança da informação em Internet das Coisas e seu detalhamento, para posterior criação de um material para o ensino.

A ideia é que o material fosse o mais amplo possível em relação as práticas que envolvessem ataques à IoT atuais e distintos . Assim, abordou-se o ataque do tipo Negação de Serviço e demonstrou-se a importância de não manter nos dispositivos credenciais padrão de senha e *login*. Ainda, mostrou-se a importância de não manter o protocolo de comunicação *bluetooth* sempre habilitado.

Portanto, ao longo deste trabalho, verificou-se que há um conjunto de problemas de segurança que não são considerados ao se implementar uma rede de dispositivos para IoT. Além

disso, é notória a falta de um material organizado para o ensino desses conceitos e das medidas para se melhorar a segurança da IoT para estudantes na graduação.

Para finalizar, espera-se que os resultados obtidos possam ser implementados a fim de agregar conhecimento aos estudantes e incentivá-los a explorar a área de segurança da informação relacionada à Internet das Coisas.

Agradecimentos

A primeira autora agradece ao Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq) pelo suporte financeiro para este projeto.

Referências bibliográficas

BUSESCANFLY. **RPI-Hunter**. 2018. Disponível em: <https://github.com/BusesCanFly/rpi-hunter>. Acesso em: 30 set. 2020.

GURUNATH, R.; AGARWAL, M.; NANDI, A.; SAMANTA, D. An Overview: Security Issue in IoT Network. In: ANAIS do International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud). Palladam, India: IEEE, ago. 2018. p. 104–107. ISBN 9781538614426. DOI: 10.1109/I-SMAC.2018.8653728.

KALI LINUX PENETRATION TESTING TOOLS. **Bettercap**. 2020. Disponível em: <https://tools.kali.org/sniffingspoofing/bettercap>. Acesso em: 7 jan. 2020.

_____. **Hping3**. 2020. Disponível em: <https://tools.kali.org/information-gathering/hping3>. Acesso em: 4 jan. 2020.

_____. **Nmap**. 2020. Disponível em: <https://tools.kali.org/information-gathering/nmap>. Acesso em: 4 jan. 2020.

KALITA, H. K.; KAR, A. Wireless sensor network security analysis. **International Journal of Next-Generation Networks**, v. 1, n. 1, p. 1–10, 2009. ISSN 0975-7023.

RAWES, E. **Unsure about just what the Internet of Things is? Here's a breakdown.** 2019. Disponível em: <https://www.digitaltrends.com/home/what-is-the-internet-of-things>. Acesso em: 21 abr. 2019.

RIBEIRO, R. M. O. **Segurança em IoT: Simulação de ataque em uma rede RPL utilizando Contiki**. 2018. f. 70. Trabalho de Conclusão de Curso em Engenharia Eletrônica e de Telecomunicações – Universidade Federal de Uberlândia.

WONDERHOWTO COMPANY. **How to Conduct Active Reconnaissance on Your Target with hping3**. 2013. Disponível em: <https://null-byte.wonderhowto.com/how-to/hack-like-pro-conduct-active-reconnaissance-your-target-with-hping3-0148092/>. Acesso em: 4 jan. 2020.