Internet das Coisas e Redes Veiculares (TP-546)

Samuel Baraldi Mafra

Inatel
Instituto Nacional de Telecomunicações


SEU CELULAR FALOU PARA SEU RELÓGIO INTELIGENTE, QUE FALOU PARA SEU SISTEMA DE AUTOMAÇÃO DE CASA INTELIGENTE QUE ME CONTOU QUE VOCÊ DEVE DESCULPAS À SUA ESPOSA.
DUAS DÚZIAS DE FLORES VERMELHAS ESTÃO POR APENAS R$120.00 POR PRAZO LIMITADO.
TOM FISH BURNE
©marketoonist.com

Segurança em IoT

- Kaspersky detecta mais de 100 milhões de ataques a dispositivos inteligentes no primeiro semestre de 2019;
- Esse número é sete vezes maior que o número encontrado no primeiro semestre de 2018, quando apenas cerca de 12 milhões de ataques foram detectados com origem em 69.000 endereços IP. Aproveitando a fraca segurança dos produtos IoT, os cibercriminosos estão intensificando suas tentativas de criar e monetizar botnets IoT;
- Os pesquisadores conseguiram localizar as regiões que se tornaram fontes de infecção com mais frequência no H1 2019. São a China, com 30% de todos os ataques ocorridos neste país, o Brasil teve 19% e este é seguido pelo Egito (12%).
- No primeiro semestre de 2018, a situação era diferente, com o Brasil liderando com 28%, a China em segundo com 14% e o Japão em seguida com 11%..

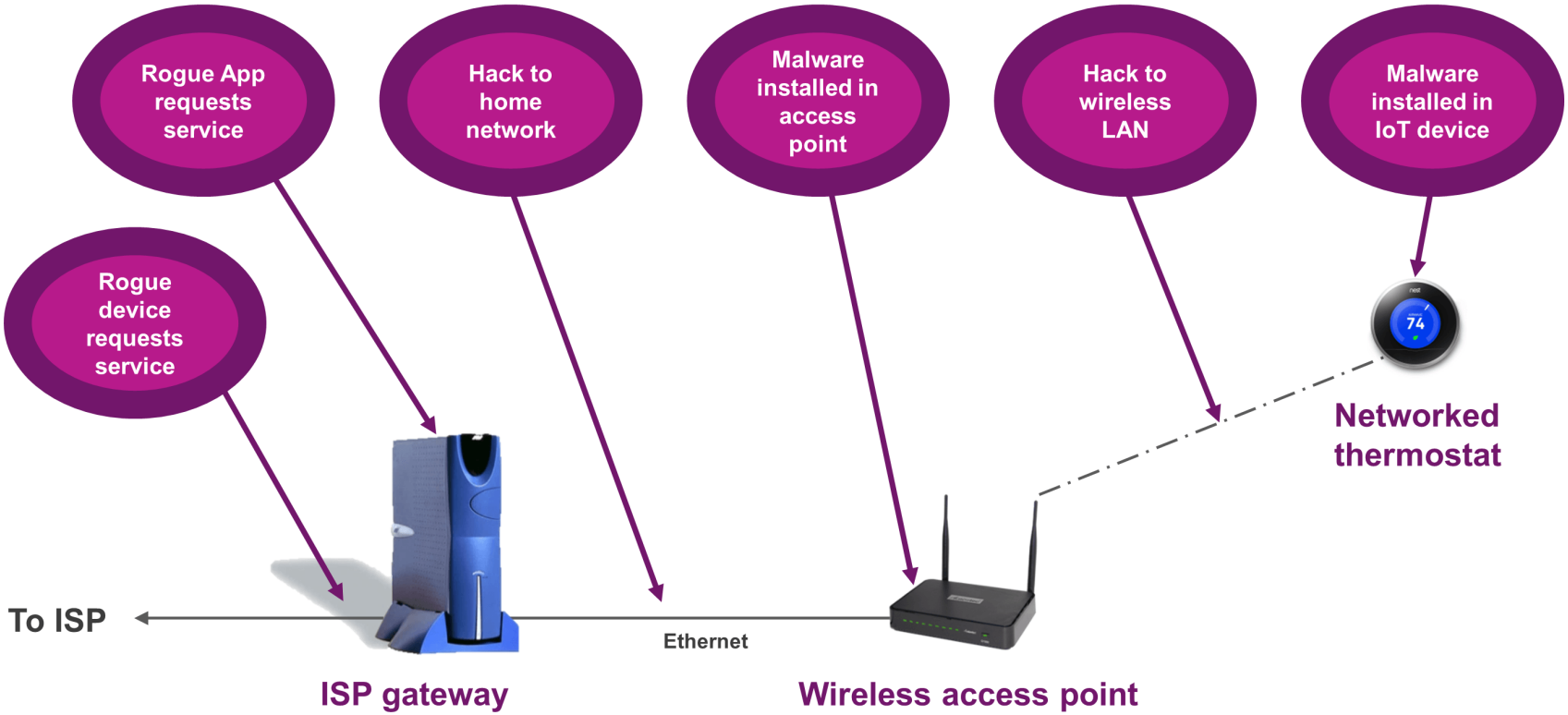
Um pen-drive pode comprometer segurança de uma empresa.

Características dos dispositivos IoT:

- Baixo consumo de energia;
- Baixo poder computacional;
- Baixo custo;
- Desejável plug and play.

Dificuldade para implementar politicas relacionadas a segurança e privacidade

Security attacks



- Dispositivos IoT para crianças são um alvo comum para hackers;
- Dispositivos sempre ouvindo;
- Localização.

Dispositivos para crianças:

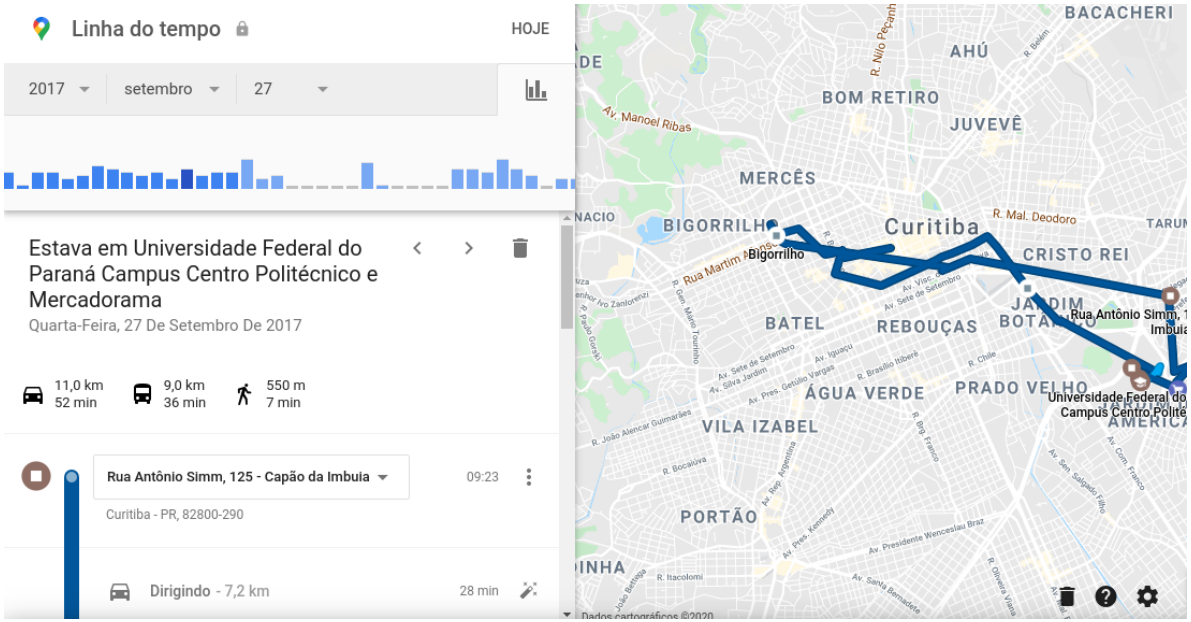
Atackers spoof calls

track current location

Attackers have access to image

Dispositivos sempre escutando:

Localização:



Propriedades desejadas de segurança:

- Confidencialidade: É a propriedade que garante que a informação não seja divulgada ou disponibilizada a qualquer entidade não autorizada.
- Integridade: É a propriedade de salvaguardar a exatidão e integridade dos ativos em um sistema IoT.
- Disponibilidade: refere-se à propriedade que garante que um dispositivo ou sistema IoT seja acessível e utilizável sob demanda por entidades autorizadas.
- Autenticidade: é a garantia de que a transação de informações é da fonte que afirma ser. A autenticidade do dispositivo pode ser verificado por meio de autenticação, que envolve prova de identidade.

- Autorização: uma propriedade que determina se o usuário ou dispositivo tem direitos / privilégios para acessar um recurso ou emitir comandos.
- Responsabilidade: é a propriedade que garante que cada ação pode ser atribuída a um único usuário ou dispositivo.
- Confiabilidade: refere-se à propriedade que garante o comportamento pretendido consistente de um sistema IoT.
- Privacidade: no contexto da IoT, privacidade se refere ao controle do usuário sobre a divulgação de seus dados.

Mecanismos para garantir a segurança:

- Autenticação: é o serviço de segurança que verifica a identidade de um usuário ou dispositivo.
- Controle de acesso: no contexto da IoT, o controle de acesso se refere ao mecanismo de segurança que limita as ações ou operações de um usuário legítimo ou dispositivo em um sistema IoT, bem como definir um limite para programas executados em nome do usuário legítimo.
- Criptografia: é o processo de traduzir ou codificar uma informação em um código secreto de tal forma que apenas entidades autorizadas podem decodifique-o.
- Inicialização segura: Este recurso de segurança permite que um dispositivo verifique cada software usando assinatura digital, incluindo sistema operacional, quando o dispositivo é ligado pela primeira vez ou sempre que ele é reiniciado.

Mecanismos para garantir a segurança:

- Atualizações seguras: certifique-se de que os dispositivos inteligentes autenticam patches de segurança de operadoras usando assinaturas digitais para que patches não podem ser interceptados, extraídos e modificados.
- Backup: É a cópia e o arquivamento de dados valiosos com a finalidade de restaurar o original em caso de perda de dados.
- Detecção de adulteração de dispositivo (DTD);

Internet of Things Security — Ken Munro — TEDxDornbirn

https://youtu.be/pGtnC1jKpMg

Spies and Dolls: The Future of IoT Security — Maire O'Neill — TEDxQueensUniversityBelfast

`https://youtu.be/E0FJ5K16pYE`

Tipos de ataques:

- Ataques Físicos
- Ataques de criptografia
- Botnets
- DoS (negação de serviço)
- Hijacking de firmware
- Man-in-the-Middle
- Ransomware
- Espionagem
- Escalonamento de privilégios
- Ataque de força bruta para descoberta de senha

Ataques Físicos

- Os ataques físicos ocorrem quando os dispositivos IoT podem ser acessados fisicamente por qualquer pessoa.
- Com a maioria dos ataques de cibersegurança ocorrendo de dentro de uma empresa, é essencial que seus dispositivos IoT estejam em uma área protegida, o que muitas vezes não é uma opção.
- Muitos ataques de cibersegurança física começam com o invasor inserindo uma unidade USB para espalhar código malicioso, por isso é mais importante do que nunca adicionar medidas de segurança baseadas em IA para garantir que seus dispositivos e dados estejam protegidos.

Ataques de criptografia

- Quando um dispositivo IoT não é criptografado, o intruso pode observar os dados e capturá-los para uso posterior.
- Além disso, "uma vez que as chaves de criptografia são desbloqueadas, os ciberataques podem instalar seus próprios algoritmos e assumir o controle do seu sistema".
- Por esses motivos, a criptografia é essencial no ambiente de IoT como parte de seus esforços de segurança cibernética.

- Botnets

  Considere o ataque de botnet, Mirai, que transformou dispositivos IoT em rede em bots controlados remotamente, que podem ser usados como parte de um botnet.

- Os botnets têm a capacidade de usar dispositivos inteligentes e conectados para transferir dados corporativos confidenciais e privados, que podem ser vendidos na dark web, ou para desativar um dispositivo.

- Mirai continua sendo um problema hoje, com milhões de dispositivos IoT afetados.

What is Mirai and How do You Protect Yourself Against it?

`https://youtu.be/KKSyB476n9o`

DoS (negação de serviço)

- Um ataque DoS ocorre quando um serviço, como um site da Web, fica indisponível.
- Um grande número de sistemas ataca um alvo por meio des botnet, que solicitam um serviço ao mesmo tempo.
- Embora os invasores, neste caso, normalmente não tenham como objetivo capturar dados, eles estão afetando seriamente os negócios se os serviços ficarem indisponíveis.

- Uma nova vulnerabilidade de alta gravidade que afeta as Philips Hue Smart Light Bulbs que podem ser exploradas pelo ar a mais de 100 metros de distância para entrar em uma rede WiFi direcionada.
- A vulnerabilidade de alta gravidade subjacente, rastreada como CVE-2020-6007, reside na maneira como a Philips implementou o protocolo de comunicação Zigbee em sua lâmpada inteligente.

- O hacker controla a cor ou o brilho da lâmpada para induzir os usuários a pensar que a lâmpada está com defeito.
- A lâmpada aparece como "Inacessível"no aplicativo de controle do usuário, então eles tentarão "reiniciá-la".
- A única maneira de redefinir a lâmpada é excluí-la do aplicativo e, em seguida, instruir a ponte de controle a redescobrir a lâmpada. A ponte descobre a lâmpada comprometida e o usuário a adiciona de volta à rede.

- A lâmpada controlada por hacker com firmware atualizado então usa as vulnerabilidades do protocolo ZigBee para acionar um estouro de buffer, enviando uma grande quantidade de dados para ela. Esses dados também permitem que o hacker instale malware na ponte - que, por sua vez, é conectada à empresa alvo ou à rede doméstica.
- O malware se conecta de volta ao hacker e, usando uma exploração conhecida, pode se infiltrar na rede IP de destino para espalhar ransomware ou spyware.

Hacking Smart Light Bulbs — Latest Research from Check Point
`https://youtu.be/4CWU0DA__bY`

Zigbee War Flying

`https://youtu.be/Ed1OjAuRARU`

- As lâmpadas inteligentes LIFX Mini revelam senhas de Wi-Fi em casa e basicamente não têm segurança.
- As lâmpadas armazenam senhas de acesso Wi-Fi em texto simples, não têm configurações de segurança e codificam uma chave de criptografia privada diretamente no firmware;
- As credenciais são passadas de uma lâmpada em rede para outra em uma rede em malha alimentada por 6LoWPAN.

Hijacking de firmware

- Se você não está acompanhando as atualizações de firmware da IoT, corre o risco de um ataque de segurança cibernética.
- Certifique-se de verificar se suas atualizações são da fonte esperada, caso contrário, um invasor pode sequestrar o dispositivo e baixar software malicioso.
- A maioria dos fabricantes de hardware não assinam firmware embarcado criptograficamente.

Man-in-the-Middle

- Um ataque man-in-the-middle ocorre quando um hacker quebra a comunicação entre dois sistemas separados.
- Ao interceptar secretamente as comunicações entre duas partes, esse tipo de ataque leva o destinatário a pensar que está recebendo uma mensagem legítima. Em outras palavras, o homem do meio começa a se comunicar com ambas as partes, daí o nome. Pode parecer um e-mail do seu banco, solicitando que você faça login para realizar uma tarefa.
- Agora, o site falso dos invasores reúne suas credenciais, para que o invasor possa causar mais danos.

- Em 2015 foi descoberta uma falha de segurança que permitia que hackers tivessem acesso as credenciais do Google do usuário através de uma geladeira inteligente da Samsung. A geladeira tinha uma integração com o calendário do Google;
- O software na geladeira fornecia criptografia SSL (Secure Sockets Layer) para estabelecer um link criptografado, mas na realidade, ele falhou completamente ao validar os certificados SSL.

Ransomware

- Ransomware é um tipo de malware que bloqueia o acesso aos arquivos criptografando-os.
- Em seguida, os invasores vendem a chave de descriptografia para que seus arquivos possam ser acessados novamente.
- Naturalmente, esse tipo de ataque pode atrapalhar os negócios do dia-a-dia e a chave de criptografia geralmente tem um preço alto.

When coffee makers are demanding a ransom, you know IoT is screwed

https://arstechnica.com/information-technology/2020/09/how-a-hacker-turned-a-250-coffee-maker-into-ransom-machine

What a hacked coffee machine looks like.

https://youtu.be/bJrIh94RSiI

https://www.smarter.am/coffee

Espionagem

- Nesse tipo de ataque, um hacker intercepta o tráfego da rede para roubar informações confidenciais por meio de uma conexão enfraquecida entre um dispositivo IoT e um servidor.
- A escuta secreta é normalmente feita ouvindo a comunicação de voz digital ou analógica ou por meio da interceptação de dados detectados.
- Novamente, neste caso, o invasor sai com dados corporativos confidenciais.

Escalonamento de privilégios

- Os hackers procuram bugs e pontos fracos do dispositivo IoT para obter acesso aos recursos que são normalmente protegidos por um aplicativo ou perfil de usuário.
- Nesse tipo de ataque, o hacker busca usar seus privilégios recém-adquiridos para implantar malware ou roubar dados confidenciais.

Ataque de força bruta

- Nesse cenário, os hackers enviam muitas senhas ou frases secretas na esperança de adivinhar a correta, fornecendo a eles acesso aos seus dispositivos IoT.
- Ou usam software para gerar um grande número de suposições consecutivas.
- Agora que o invasor tem acesso ao seu dispositivo, ele pode instalar malware ou roubar dados essenciais aos negócios.

Ataque de força bruta

- Kaji Malware;
- Origem chinesa;
- Linguagem de programação Go;
- Em desenvolvimento;
- Não compromete o dispositivo IoT;
- Ataque de força bruta para realizar ataques DDoS.

Strava

How a Fitness App's Heat Map Uncovers Military Bases — NYT

`https://youtu.be/0IB8p-YpXwA`

WEBINAR recording - IoT Security: the Key Ingredients for Success

https://youtu.be/bcVztl4lJN8

Trabalho

- Fazer uma pesquisa sobre problemas de segurança em redes IoT. Escolher um tipo de problema de segurança. Mostrar como pode ser feito um ataque em específico e quais medidas podem ser utilizadas para sanar o problema.