TP546 - Internet das Coisas e Redes Veiculares

Instituto Nacional de Telecomunicações
Mestrado em Telecomunicações
Igor Gonçalves de Souza - 931

Segurança em Redes IoT

Uma pesquisa sobre formas de ataques e medidas de proteção

1 Introdução

As tecnologias e protocolos das redes baseadas na Internet das Coisas (IoT) têm como objetivo conectar dispositivos inteligentes pela Internet, possibilitando a comunicação e a troca de serviços entre eles. Em aplicações de IoT, como assistência médica e casas inteligentes, a transmissão de dados pessoais é extremamente comum e, portanto, a privacidade e a segurança desses dados emergem como uma das questões mais desafiadoras para desenvolvedores e usuários, sendo a principal preocupação em qualquer aplicativo ou rede IoT [1].

Os dispositivos IoT, muitas vezes, são vulneráveis a ataques mal-intencionados, especialmente porque muitos deles armazenam dados sensíveis de forma inadequada ou insegura. Invasores podem acessar redes IoT em diferentes camadas — tanto na camada física quanto na de rede — explorando brechas como senhas fracas, autenticação deficiente e software desatualizado. Assim, a implementação de medidas de segurança adequadas é crucial para garantir a integridade, a privacidade e a confidencialidade dos dados transmitidos e armazenados por esses dispositivos [2].

Um dos ataques mais comuns é o conhecido ''Man-in-the-Middle'', em que um invasor intercepta a comunicação entre partes confiáveis, permitindo roubar informações críticas, como senhas e números de identificação pessoal, que podem ser utilizadas de forma indevida. Outro ataque, denominado ''Clone ID'', envolve a clonagem da identidade de um nó vítima, o que permite ao invasor redirecionar pacotes de dados, criar múltiplas cópias e adquirir segredos criptográficos e a identidade do nó afetado.

Além dessas ameaças, existem outras preocupações significativas em redes IoT. Por exemplo, a falta de padrões de segurança robustos entre fabricantes pode resultar em dispositivos vulneráveis e não atualizáveis. O gerenciamento inadequado de credenciais e a ausência de autenticação forte contribuem para a exposição dos sistemas a ataques. A fragmentação do ecossistema IoT, com uma variedade de protocolos e dispositivos, também dificulta a criação de soluções de segurança eficazes.

Dada a importância da segurança em redes IoT e as diversas formas pelas quais os dispositivos podem ser alvo de invasões e ter dados roubados, este documento tem como objetivo apresentar e descrever possíveis formas de ataque a uma rede IoT, com ênfase no ataque ''Man-in-the-Middle'', bem como discutir medidas de mitigação e melhores práticas que podem ser adotadas para fortalecer a segurança em ambientes de IoT, protegendo assim tanto os dispositivos quanto os dados dos usuários.

2 Formas de Ataque

Os ataques a redes e dispositivos IoT têm se tornado cada vez mais comuns e diversificados. Eles podem ser categorizados em várias formas, incluindo ataques físicos, que visam diretamente o *hardware* do sistema; ataques de rede, que buscam extrair grandes volumes de dados remotamente; ataques à criptografia, que tentam quebrar chaves de criptografia para acessar informações sensíveis; e ataques de *software*, que exploram vulnerabilidades para instalar *malware* e vírus, comprometendo todo o sistema.

Esta seção aborda alguns detalhes das principais modalidades de ataque, suas características e implicações para a segurança das redes IoT. Cada um desses ataques representa um desafio significativo, exigindo uma abordagem robusta para proteger dispositivos e dados contra potenciais ameaças.

2.1 Botnets

Botnets são computadores comprometidos controlados remotamente por invasores que realizam fraudes e ataques cibernéticos, como roubo de informações privadas, exploração de dados e envio de e-mails de *phishing*. Os botnets são habilitados para transferência de dados automaticamente por meio de uma rede e são difíceis de detectar porque o usuário não tem conhecimento de que o dispositivo está comprometido. Os botnets seguem o modelo de comando e controle, no qual o servidor central controla os *bots* na rede [1].

2.2 Ataque de espionagem

No ataque de espionagem ou *sniffing* o invasor pode interceptar o tráfego da rede e roubar as informações confidenciais que dispositivos IoT transmitem pelas redes corporativas. Isto é possível devido ao link de comunicação não seguro para acessar dados pessoais entre dois dispositivos finais, em que o invasor encontra uma conexão enfraquecida entre um dispositivo IoT e um servidor [1].

2.3 Sequestro de *firmware*

O sequestro de *firmware* faz com que o invasor sequestre o dispositivo e substitua o *firmware* de um dispositivo IoT por um malicioso. Isso é possível quando um dispositivo IoT baixa as atualizações de *firmware* de uma fonte ilegítima e pode permitir que o invasor controle o dispositivo ou use-o para realizar atividades inadequadas [1].

2.4 *Ransomware*

O *ransomware* é um tipo de *malware* que criptografa os dados de um dispositivo IoT e exige um resgate para desbloqueá-los. Como muitos dispositivos IoT são usados em ambientes críticos, como hospitais e fábricas, os ataques de *ransomware* IoT podem ter consequências graves, por exemplo, os invasores podem adulterar um sistema de saúde inteligente e enviar uma notificação ao proprietário para pagar um resgate [1].

2.5 *Man-in-the-Middle*

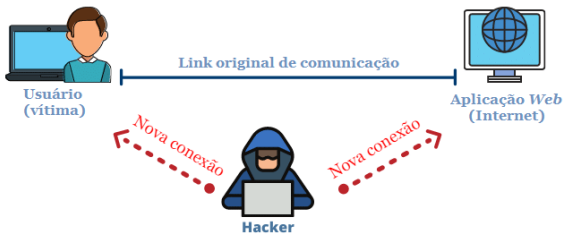
Os ataques *Man-in-the-Middle* ocorrem quando o invasor viola a comunicação entre dois sistemas finais, injetando um nó malicioso entre nós legítimos ou visando os protocolos de comunicação na rede IoT. O invasor pode alterar o tráfego e reconfigurar a topologia da rede, criar identidades falsas e gerar informações maliciosas para comprometer o sistema IoT [3].

Há ainda outras formas de ataque, como escalonamento de privilégios, negação de serviços e ataque de sumidouro. Este último, é o ataque de roteamento mais destrutivo no ambiente IoT. A próxima seção aborda com mais detalhes o ataque *Man-in-the-Middle*.

3 *Man-in-the-Middle*

O ataque *Man-in-the-Middle* (MitM), ilustrado na Figura 1, é um tipo de ataque criptográfico que ocorre em um canal de comunicação, realizado por um invasor malicioso que assume o controle do canal entre duas partes legítimas. Nesse ciberataque, o invasor pode interceptar, ler e modificar o tráfego de comunicação entre as vítimas, de forma invisível para os usuários [3].

Figura 1: Interceptação da comunição por um invasor no ataque MitM.



3.1 Metodologia de Invasão

Um ataque MitM envolve duas etapas principais: interceptação e descriptografia. A interceptação geralmente requer proximidade física ao alvo, enquanto a descriptografia pode ser realizada exclusivamente por *malware*. Em um ataque convencional, o invasor precisa ter acesso a um roteador Wi-Fi inseguro ou mal configurado, frequentemente encontrado em locais públicos e residências. O invasor escaneia o roteador em busca de vulnerabilidades, como senhas padrão ou fracas. Identificada vulnerabilidade, ferramentas entre o computador da vítima e os sites acessados coletam dados [3].

A etapa inicial intercepta a atividade da vítima antes que ela alcance seu destino pretendido. O método mais comum para isso é um ataque passivo, no qual o invasor cria *hotspots* Wi-Fi acessíveis ao público, que não são protegidos por senha. Assim que a vítima se conecta a esse *hotspot*, o invasor ganha visibilidade sobre as trocas de informações.

Uma variação mais recente desse ataque é o *man-in-the-browser*. Nesse caso, o invasor apenas precisa injetar *malware* no computador da vítima, que se instala no navegador sem o seu conhecimento, registrando as informações transmitidas entre a vítima e sites específicos, como instituições financeiras. O *malware* envia os dados programados ao invasor assim que são coletados.

3.2 Sinais e Detecção de Ataque MitM

Ataques *man-in-the-middle* podem ser difíceis de detectar, pois são projetados para acontecer em segundo plano sem o conhecimento do usuário. No entanto, há sinais que pode ser observados.

- **erros de certificado SSL**: mensagem de erro sobre um certificado SSL inválido ou expirado ao tentar acessar um site. O certificado SSL pode redirecionar para um site malicioso que se parece com um site legítimo. O site falso solicita credenciais de login que o invasor utiliza para fazer login no site legítimo;
- **conexão de internet não confiável**: latência muito elevada e desconexões frequentes;
- **site falso**: verificação de diferenças sutis nas características do site, como em fontes, cores ou logotipos, pop-up aleatórios ou solicitações suspeitas.

3.3 Formas de Bloqueio

Bloquear ataques MitM requer uma combinação de técnicas de criptografia e verificação para aplicações, além de ações práticas por parte do usuário, como:

- evitar conexões Wi-Fi que não estejam criptografadas por senha;
- atentar à avisos do navegador que reportam sites como não seguros;
- realizar logout de aplicações seguras quando não estiver em uso;
- não utilizar redes públicas ao realizar transações financeiras sensíveis.

Sistemas antivírus fornecem aos usuários e administradores de sites uma criptografia SSL/TLS de ponta a ponta, como parte de serviços de segurança. Protocolos de comunicação seguros, como TLS e HTTPS, ajudam a mitigar ataques, criptografando e autenticando fortemente os dados transmitidos. Isso impede a interceptação da atividade do site e dificulta a decodificação de informações sensíveis, como *tokens* de autenticação. É considerado uma boa prática que as aplicações utilizem SSL/TLS para proteger cada página, e não apenas as páginas que exigem que os usuários façam login.

Conclusão

A segurança das redes IoT é uma questão crítica que deve ser abordada com urgência, dado o crescimento exponencial desses dispositivos e a quantidade de dados sensíveis que eles manipulam. O ataque *Man-in-the-Middle* exemplifica as vulnerabilidades que podem ser exploradas por invasores para comprometer a privacidade e a integridade das informações dos usuários. A diversidade de protocolos

e a falta de padrões de segurança robustos exacerbam esse problema, tornando os dispositivos IoT alvos fáceis para cibercriminosos.

Para mitigar essas ameaças, é fundamental que desenvolvedores e usuários adotem práticas de segurança eficazes, como a implementação de autenticação forte, o uso de criptografia robusta e a atualização regular de softwares. Além disso, a conscientização sobre as melhores práticas de segurança deve ser promovida para minimizar riscos. Ao adotar uma abordagem proativa em relação à segurança, podemos proteger não apenas os dispositivos, mas também os dados pessoais e a privacidade dos usuários, garantindo um ambiente mais seguro e confiável para a Internet das Coisas.

Referências

[1] N. Sivasankari e S. Kamalakkannan. "Detection and prevention of man-in-the-middle attack in iot network using regression modeling". Em: *Advances in Engineering Software* 169 (2022), p. 103126. ISSN: 0965-9978. DOI: https://doi.org/10.1016/j.advengsoft.2022.103126. URL: https://www.sciencedirect.com/science/article/pii/S0965997822000370.

[2] Asma Jahangeer, Sibghat Ullah Bazai, Saad Aslam, Shah Marjan, Muhammad Anas e Sayed Habibullah Hashemi. "A Review on the Security of IoT Networks: From Network Layer's Perspective". Em: *IEEE Access* 11 (2023), pp. 71073–71087. DOI: 10.1109/ACCESS.2023.3246180.

[3] Avijit Mallik, Abid Ahsan, Mhia Shahadat e Jia-Chi Tsou. "Man-in-the-middle-attack: Understanding in simple words". Em: *International Journal of Data and Network Science* 3 (2019), pp. 77–92. DOI: 10.5267/j.ijdns.2019.1.001.