TRABALHO 03 – INTERNET DAS COISAS E REDES VEICULARES

Trabalho sobre Brechas de Segurança em Aplicações IoT

ALUNOS: Bruno Augusto, Guilherme Kyt Moreira

INTRODUÇÃO

À medida que o número de dispositivos conectados em uma rede cresce, surgem novos desafios para os usuários, principalmente em relação à segurança. Com a rápida evolução das tecnologias móveis, como o recente 5G e o desenvolvimento do 6G, os cenários que envolvem a aplicação de dispositivos IoT *(Internet of Things)* ampliam ainda mais as preocupações com as ameaças de segurança. Entre essas ameaças, um dos ataques mais comuns em redes IoT é o do tipo *Man-in-the-Middle* (MitM)**,** que compromete a privacidade e a integridade das comunicações. Nesta pesquisa, será dado um enfoque de como este tipo de ataque é executado em uma rede IoT, e as medidas de seguranças que podem mitigar esta ameaça.

O QUE É O ATAQUE MITM - MAN-IN-THE-MIDDLE?

Um ataque desse tipo ocorre quando um invasor intercepta e altera os dados trocados entre dois dispositivos, sem que os envolvidos percebam. Em redes IoT, isso é especialmente perigoso, pois envolve a transmissão de informações sensíveis, como dados pessoais, informações de sensores e comandos de controle de sistemas. Durante o ataque *Man-in-the-Middle* (MitM), o invasor pode não só interceptar e analisar os dados transmitidos, mas também modificá-los, enviando informações incorretas ou maliciosas ao receptor, comprometendo a integridade e segurança do sistema.

Nos carros modernos, conhecidos como veículos inteligentes, que dependem de sensores e sistemas de comunicação para funcionalidades como GPS, assistência de direção e monitoramento remoto, o impacto de um ataque MitM pode ser grave. Um *hacker* pode interceptar a comunicação entre o automóvel e um servidor remoto ou entre os diversos componentes internos do veículo, manipulando dados críticos, como a localização GPS ou comandos de controle veicular. Isso pode levar o veículo a seguir uma rota incorreta ou, em casos mais extremos, causar falhas no sistema de direção, gerando acidentes que podem ser fatais para o condutor e os passageiros.

Recentemente dois pesquisadores de segurança, Talal Haj Bakry e Tommy Mysk, demonstraram como realizaram um ataque de *phishing Man-in-the-Middle* (MiTM) para comprometer contas de Tesla, desbloquear carros e ligá-los. O ataque afeta a versão mais

recente do app da Tesla (4.30.6) e o software do carro (11.1 2024.2.7). Eles criaram uma rede Wi-Fi falsa chamada "Tesla Guest" em uma estação de carregamento, imitando redes comuns em centros de serviço Tesla. Usando um dispositivo Flipper Zero, que também poderia ser substituído por um Raspberry Pi ou outro dispositivo com *hotspot* Wi-Fi, eles induziram os donos de Tesla a se conectarem à rede falsa. Ao se conectarem, as vítimas foram direcionadas a uma página de login falsa da Tesla, onde inseriram suas credenciais.

Essas informações foram capturadas em tempo real pelos atacantes. Com essas credenciais, os invasores também coletaram a senha temporária (OTP) para burlar a autenticação de dois fatores e acessar o aplicativo Tesla.

Com acesso à conta, os invasores puderam adicionar uma nova "chave de telefone", sem necessidade de desbloquear o carro ou estar próximo dele, e sem que o dono recebesse notificações sobre isso. Com essa nova chave, o atacante poderia desbloquear e dirigir o carro como se fosse o proprietário.

O ataque foi demonstrado em um Tesla Model 3, e a recomendação dos pesquisadores é que a Tesla adicione uma camada extra de segurança, exigindo o cartão físico do Tesla para adicionar novas chaves de telefone.

MEDIDAS PARA MITIGAÇÃO DE ATAQUES MITM EM REDES IOT

Para proteger redes IoT contra-ataques do tipo *Man-in-the-Middle* (MitM), é fundamental adotar várias medidas de segurança. Algumas estratégias eficazes incluem: *criptografia* de dados, *autenticação* com *certificados digitais*, monitoramento de anomalias na rede, segmentação da rede, segurança em roteadores e atualização de *firmwares*. Abaixo, estão explicadas essas medidas de forma mais detalhada:

- **Criptografia de Dados**: Implementar protocolos de *criptografia* de ponta a ponta, como o *TLS (Transport Layer Security)*, é uma das melhores defesas. Essa abordagem garante que, mesmo que os dados sejam interceptados, eles não possam ser decifrados e compreendidos pelo invasor. Isso é especialmente importante nas redes IoT, onde muitos dados sensíveis estão em jogo.
- **Autenticação e Certificados Digitais**: A utilização de *certificados digitais* e chaves públicas/privadas é crucial para a *autenticação* entre dispositivos. Com a *PKI (Public Key Infrastructure)*, é possível garantir que os dispositivos sejam autenticados corretamente antes de se comunicarem, evitando que invasores se disfarcem como dispositivos legítimos.

- **Monitoramento de Anomalias na Rede**: Sistemas de monitoramento de rede que contam com recursos de *detecção de intrusões (IDS)* desempenham um papel vital na identificação de tentativas de ataques MitM. Esses sistemas analisam padrões de tráfego e conseguem detectar comportamentos incomuns, como volumes anormais de retransmissões de pacotes, facilitando a identificação de intrusões em tempo real.
- **Segmentação da Rede**: A segmentação da rede é uma estratégia eficaz que envolve dividir a infraestrutura em diferentes zonas isoladas. Isso não apenas reduz a superfície de ataque, mas também dificulta a vida dos invasores, que terão mais dificuldade para acessar partes críticas da rede IoT.
- **Medidas de Segurança em Roteadores**: Os ataques MitM frequentemente dependem de técnicas de envenenamento de ARP ou DNS. Para combater isso, é recomendável implementar contramedidas como *DHCP Snooping* e *Dynamic ARP Inspection (DAI)* em switches e roteadores. Além disso, o uso de *DNSSEC (Domain Name System Security Extensions)* pode ajudar a prevenir redirecionamentos de tráfego DNS malicioso.
- **Atualização de Firmwares**: Por último, manter os dispositivos IoT com o *firmware* atualizado é essencial. Isso ajuda a mitigar vulnerabilidades conhecidas que podem ser exploradas em ataques MitM. Os fabricantes frequentemente lançam *patches* de segurança, e é importante aplicar essas atualizações assim que estiverem disponíveis.

Quando essas medidas são implementadas de forma integrada, elas criam uma defesa robusta contra-ataques *Man-in-the-Middle* em redes IoT, garantindo a segurança e a integridade das comunicações. A conscientização sobre essas práticas é crucial para manter um ambiente digital seguro.

CONCLUSÃO

Em um mundo cada vez mais conectado, as redes IoT desempenham um papel crucial em diversas aplicações, desde a automação residencial até a gestão de veículos inteligentes. No entanto, a segurança dessas redes é uma preocupação crescente, especialmente com a ascensão de ataques do tipo *Man-in-the-Middle* (MitM), que podem comprometer não apenas a privacidade, mas também a segurança física dos usuários. Os exemplos recentes de ataques a veículos, como demonstrado pelos pesquisadores Talal Haj Bakry e Tommy Mysk, ilustram a vulnerabilidade desses sistemas e a necessidade urgente de implementação de medidas de segurança robustas.

Ao aplicar essas práticas de segurança, é possível criar um ambiente inteligente mais seguro e confiável, permitindo que os usuários aproveitem os benefícios das tecnologias IoT com maior tranquilidade. A conscientização dos processos de segurança pode garantir um ambiente mais seguro para todos os usuários da rede, evitando o sucesso de ataques como o do tipo MitM nas comunicações.

REFERÊNCIAS

BAKRY, Talal Haj; MYSK, Tommy. *MiTM phishing attack may allow attackers to unlock and steal Tesla car*. Medium, 2024. Disponível em: https://medium.com/@zakpatrikcz/mitm-phishing-attack-may-allow-attackers-to-unlock-and-steal-tesla-car-29595f7a0ed0. Acesso em: 7 out. 2024.

OGUNDARE, Emmanuel. *Security of Internet of Things (IoT) Devices and Systems*. TECHiT, 2024. Disponível em: https://www.researchgate.net/publication/379430395. Acesso em: 07 out. 2024.

ABED, Ali Kamil; ANUPAM, Angesh. *Review of security issues in internet of things and artificial intelligence-driven solutions*. *Security and Privacy*, v. 6, n. 3, 2022. Disponível em: https://doi.org/10.1002/spy2.285. Acesso em: 07 out. 2024.