TESTE DE INVASÃO EM PROTOCOLOS DE AUTENTICAÇÃO PARA AMBIENTES DE INTERNET DAS COISAS

Horus Cristian da Silva Barbosa (PIC/UEM), Luciana Andréia Fondazzi Martimiano (Orientadora), e-mail: ra103948@uem.br, lafmartimiano@uem.br

Universidade Estadual de Maringá / Centro de Tecnologia/Maringá, PR

Ciências Exatas e da Terra / Ciência da Computação

Palavras-chave: protocolo de autenticação, vulnerabilidades, Internet das Coisas (IoT)

Resumo:

O Teste de Invasão permite examinar, sob determinadas circunstâncias, o comportamento de sistemas computacionais para identificar vulnerabilidades que possam ser exploradas. Tais testes são executados em ambientes controlados com o intuito de evitar futuros problemas com ataques de pessoas mal-intencionadas. Em ambientes de Internet das Coisas (*IoT*), os dispositivos que fazem parte desses ambientes precisam, muitas vezes, se autenticar antes de serem autorizados a executar ações. Para tal, diversos protocolos de autenticação têm sido desenvolvidos ao longo dos anos. Para garantir que esses protocolos sejam seguros e não possuam vulnerabilidades que podem ser exploradas para comprometer o processo de autenticação, testes de invasão podem ser realizados. Neste contexto, este projeto tinha como principal objetivo executar testes de invasão em um protocolo de autenticação para ambientes de *IoT*. No entanto, como houve problema no desenvolvimento do protocolo em si, foi possível fazer uma análise de alguns dos ataques que podem ser comprometer um protocolo de autenticação.

Introdução

A crescente preocupação por segurança está diretamente relacionada ao fato de que, atualmente, o bem mais precioso das organizações ser a informação. Uma vez que o conhecimento é gerado a partir dessa informação, tornou-se crucial que sejam estabelecidos meios que auxiliem na proteção dos sistemas computacionais contra

ações não autorizadas. Segundo a norma NBR ISO/IEC 27002 (ABNT, 2013), "segurança da informação é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócios".

A segurança da informação é alcançada a partir da implementação de um conjunto de controles adequados, como políticas, processos, procedimentos, hardware e software. Esses controles podem ser estabelecidos, implementados, monitorados e mantidos a fim de garantir os objetivos de negócio (ABNT, 2013).

Para que a segurança da informação seja efetiva, é preciso uma gestão de riscos adequada. Infelizmente, não existe segurança total ou risco zero. Assim, é preciso aumentar o esforço dos atacantes, estabelecer níveis de risco toleráveis e gerenciar os riscos. Para tal, é importante avaliar constantemente as possíveis vulnerabilidades existentes em um ambiente.

Diversos estudos têm sido conduzidos no sentido de reduzir ou mitigar riscos por meio de testes de invasão (WEIDMAN, 2014). O Teste de Invasão envolve a simulação de ataques reais para avaliar os riscos associados a potenciais vulnerabilidades de segurança. O *pentester* (profissional que realiza o teste de invasão) identifica as vulnerabilidades que podem ser exploradas pelo atacante, mas também explora essas vulnerabilidades para avaliar o que poderia ser acessado ou obtido com a exploração (WEIDMAN, 2014).

Ambientes de *IoT* geram dados e informações. Portanto, também estão suscetíveis a vulnerabilidades de segurança, principalmente quanto à autenticação dos dispositivos que são utilizados no ambiente, conforme apontam Granjal, Monteiro, e Sa Silva, 2015.

Dessa forma, o principal objetivo deste trabalho era analisar um protocolo de autenticação desenvolvido por um aluno em seu trabalho de iniciação científica, de forma a avaliar o nível de segurança do protocolo para dispositivos *IoT*. No entanto, o aluno desistiu do trabalho antes de concluir a implementação do referido protocolo. Assim, o objetivo deste trabalho foi redefinido para analisar alguns dos ataques que podem ser comprometer um protocolo de autenticação em ambientes *IoT*.

Materiais e Métodos

Para o desenvolvimento deste projeto, foram estudados conteúdos sobre Internet das Coisas (*IoT*), protocolos de autenticação e os métodos mais comuns para sua implementação (como senha, *token*, criptografia), ataques conhecidos para protocolos de autenticação em ambientes IoT, e as principais ferramentas utilizadas em teste de invasão para protocolos de autenticação disponíveis no sistema operacional Kali Linux (2022). Neste resumo, são descritos alguns métodos de autenticação e alguns dos ataques que um protocolo pode sofrer.

Resultados e Discussão

IoT se trata de toda tecnologia que segue o conceito de conectar dispositivos que são utilizados diariamente entre si e podem se comunicar através da Internet. Dessa forma, um dispositivo *IoT* é qualquer dispositivo físico que recebe e transfere dados em redes sem fio e entre si através de sensores em um determinado ambiente sem intervenção humana.

Entende-se por protocolo de autenticação, as regras que regem o sistema para a validação da identidade de usuários e de dispositivos relacionados ao tráfego de dados, reduzindo os riscos de vazamento de dados e acessos indevidos. Os métodos de autenticação mais são: o par *login* e senhas, que permite ao usuário fornecer uma combinação de códigos já armazenada em um servidor para se autenticar no ambiente; o t*oken*, que utiliza uma estrutura parecida com o protocolo de senha, divergindo ao ser um código muitas vezes temporário utilizado para autenticar a sessão do usuário; a biometria, na qual o sistema faz uso de características humanas físicas, como córnea ou digital para autenticar o usuário; a criptografia, que faz uso de uma senha secreta para codificar ou decodificar alguma informação fornecida pelo usuário; e a autenticação multifatorial, que se dá ao unir um ou mais protocolos de autenticação, tornando assim o processo mais seguro.

Os principais tipos de ataques que podem comprometer à autenticação em ambientes *IoT*, foram levantados os seguintes: *Masquerade Attack,* no qual o atacante se passa por um usuário por meio do roubo de sua identidade; *Man in The Middle,* no qual o atacante se infiltra no meio da comunicação entre dois usuários de uma rede podendo observar ou adulterar dados; *Denial of Service Attack,* no qual o atacante envia um enorme número de requisições de acesso a um serviço alvo visando sobrecarregar e impedir que novas conexões e autenticações sejam feitas; *Forging Attack,* no qual o atacante se passa por algum componente do sistema para interceptar a conexão do usuário com o servidor, podendo utilizar desses dados para conexões posteriores; *Guessing Attack,* que se trata do atacante tentar adivinhar a senha do usuário por meio de múltiplas tentativas; *Physical Attack*, no qual o atacante causa danos físicos e materiais aos componentes do sistema; e *Routing Attack*, no qual o atacante se infiltra no roteamento dos dados, podendo repassar indevidamente ou impedir que solicitações cheguem ao destino final. Todos esses ataques visam a comprometer os pilares da segurança da informação, sendo eles a confidencialidade, integridade, disponibilidade dos dados e autenticação das entidades (usuários e dispositivos).

Conclusões

Este projeto contribuiu com a coleta de informações relacionadas a ambientes *IoT*, protocolos de autenticação, segurança da informação, bem como a identificação dos principais ataques que podem ocorrer para comprometer um protocolo de autenticação em ambientes *IoT*. Porém, não foram obtidos resultados satisfatórios quanto à contribuição para o desenvolvimento de um novo protocolo de autenticação seguro e eficiente para ambientes IoT devido à não conclusão de um trabalho de

iniciação científica correlacionado, uma vez que não foi possível realizar os testes de invasão propriamente ditos.

Referências

ABNT. Tecnologia da Informação – Técnicas de segurança - Código de prática para a gestão da segurança da informação. Associação Brasileira de Normas Técnicas – NBR ISO/IEC 27002. 2013.

G. WEIDMAN. Testes de Invasão: Uma introdução prática ao *hacking*. Novatec Editora. 2014. 576 p.

J. Granjal, E. Monteiro e J. Sá Silva. "Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues". In IEEE Communications Surveys & Tutorials, vol. 17, no. 3, pp. 1294-1312, 2015. DOI: 10.1109/COMST.2015.2388550.

KALI LINUX. https://www.kali.org/. Acesso em Agosto de 2022.