Fábio Henrique Alves Fernandes
19.1.4128
Link YouTube: https://youtu.be/Ho2MYeMEjqM
OBS: Vídeo grande demais para ser postado diretamente no Moodle!!!!!!

Com o avanço da tecnologia, ciberataques estão cada vez mais focados em dados financeiros e outras informações valiosas. Podemos distinguir os ataques de forma ativa ou passiva. Um ataque passivo envolve alguém ouvir as trocas de telecomunicações ou gravar de forma passiva atividade do computador. Já ataques ativos envolvem o uso de informações obtidas durante um ataque passivo, como IDs de usuário e senhas, ou um ataque imediato com o uso de crackers de senhas, ataques de negação de serviço, e-mail phishing, worms e outros ataques de malware.

Um exemplo de ataque é o conhecido Man-In-The-Middle. Nesse ataque, como o próprio nome propõe,o criminoso se posiciona entre as duas partes envolvidas em uma comunicação, podendo ser a partir de um router WiFi corrompido, interceptando-a. Com isso, ele passa a ter acesso a dados vulneráveis, como senhas e e-mails, dados bancários e afins. A partir disso, o criminoso parte para ataques ativos, obtendo acesso a contas de bancos, ou aplicando outros golpes utilizando o nome da vítima. Uma versão mais recente do ataque MITM é chamada man-in-the-browser. Nesta variável o agressor usa um dos inúmeros métodos para implementar um código daninho no navegador do computador de suas vítimas. O malware silenciosamente grava informações enviadas a vários sites.

Um dos métodos de evitar este tipo de ataque é criptografando os dados até que eles cheguem no receptor, único com a capacidade de realizar a descriptografia. O sistema operacional usa a criptografia em muitos lugares: para transmitir dados com segurança através da rede, armazenar arquivos com segurança em disco, embaralhar as senhas em um arquivo de senhas etc. O endurecimento de programa também é usado por toda parte, evitando que atacantes injetem códigos novos em softwares em execução, certificando-se de que cada processo tem exatamente os privilégios de que ele precisa para fazer o que deve fazer e nada mais, entre outros métodos.

Uma outra solução dentro da criptografia é uma ferramenta bem utilizada atualmente chamada OpenSSL. Com a campanha “HTTPS Everywhere”, a demanda para a criação de

certificados SSL aumentou bastante. O OpenSSL é uma biblioteca open source criada em 1998 que permite a criação de chaves CSR, parte dos requisitos para se obter um certificado SSL, e também permite instalar arquivos SSL em servidores. Com isso, os dados podem ser criptografados e só conseguem ser acessados por quem possui um certificado SSL válido (não pode estar vencido).

SSL significa Secure Sockets Layer, um tipo de segurança digital que permite a comunicação criptografada entre um site e um navegador. Atualmente a tecnologia se encontra depreciada e está sendo completamente substituída pelo TLS. O TLS é uma sigla que representa Transport Layer Security e certifica a proteção de dados de maneira semelhante ao SSL. Como o SSL não está mais de fato em uso, esse é o termo correto que deveria ser utilizado.

Quando um site tem o certificado SSL/TLS, isso o torna mais seguro para os usuários fazerem acessarem, afinal, os dados serão criptografados e não poderão ser acessados por ninguém. Isso, aplicado ao sistema operacional, incluído a outros sistemas de segurança, permite uma navegação mais segura ao usuário, negando possíveis golpes.

Referências:

http://ptcomputador.com/Networking/network-security/75586.html
https://www.kaspersky.com.br/blog/what-is-a-man-in-the-middle-attack/462/
https://www.ssldragon.com/blog/what-is-openssl-and-how-it-works/
https://www.openssl.org/