



Relatório da segurança do SSL sobre dados

Nalbert Gabriel Melo Leal

13-10-2017

Contents

1	Introdução	1
2	SSL	2
2.1	Oque é SSL ?	2
2.2	Como o SSL funciona ?	2
2.3	É o SSL a prova de hackers ?	2
3	Problemas do SSL	3
3.1	Prpblemas do SSL	3
3.2	Como funcioan o ataque "man in the middle" ?	3
3.3	O ataque "Man in the middle" e o SSL	4
4	O experimento	5
4.1	Requisitos	5
4.2	Passo-a-passo	5
5	Conclusão	6
5.1	Como se defender do "Man in the middle" sobre o SSL ?	6
5.2	Considerações finais	6

1 Introdução

2 SSL

2.1 Oque é SSL ?

No ano de 1994 a Netscape criou um protocolo de segurança chamado SSL (secure socket layer) que cria um tunel lógico entre dois computadores para que a comunicação entre eles não possa ser compreendida por terceiros. Entenda o tunel lógico como uma comunicação sendo feita com uso de criptografia.

Esse canal criptografado entre é muito utilizado nos dias de hoje entre servidores e clientes para aumentar a segurança durante a troca de dados. Durante o acesso a um site para saber se existe o uso de SSL basta verificar se ao lado da URL da pagina existe o simbolo de um cadeado fechado, indicando uma conexão segura.

2.2 Como o SSL funciona ?

O SSL como protocolo é bem simples. Para ativar o SSL em um sevidor é nescessário responder a algumas questões sobre identidade de quem esta sendo certificado (o servidor) e assim gerar um certificado que apos algum tempo definido irá ser invalidado.

Quando um servidor é requisitado por um cliente ele usa o certificado gerado para criar uma chave privada e uma publica. A chave privada vai servir para descriptografar os dados vindos do cliente, já a chave publica server para o cliente ter certza que a informação vem do servidor. Essas duas chaves permitem a troca de chaves unicas para que a comunicação atravez do canal criptografado possa acontecer.

2.3 É o SSL a prova de hackers ?

Já mencionamos que o SSL foi desenvolvido para aumentar a segurança entre cliente e servidor, entretanto isso não significa que seja impossivel de burlar ou de descriptografar. Com pesquisas e com a insistencia de hackers é comum que em algum mommento se descubra vulnerabilidades.

No caso do SSL existe maneiras de se interceptar a comunicação no momento que ela esta sendo iniciada e assim interceptar os dados da comunicação. Esse metodo de invasão é chamado de "man in the middle", traduzido para "o homem no meio".

Esse ataque é potencialmente perigoso e permite que um atacante possa descobrir dados sensiveis de usuarios/servidor, sendo assim vamos demonstrar o quanto é fácil fazer um ataque "man in the middle" e como ele pode ser devastador, tanto para o usuário que pode ser colocado em grande risco e para o servidor, pois a baixa segurança pode fazer o numero de usuários cair.

3 Problemas do SSL

Discutimos brevemente na sessão anterior um ataque que pode ocorrer ao SSL, mas esse não é o unico problema envolvendo o uso do SSL.

3.1 Prpblemas do SSL

Se olharmos esse protocolo por sí só podemos achar que os motivos para não usa-lo são fracos, entretanto após olharmos um acumulo desse motivos podemos acabar vendo se vale ou não a pena usar.

1. O SSL causa um incremento no custo computacional. Isso ocorre pois esse protocolo faz uso de criptografia, e a criptografia requer que sejam usados algoritmos custosos para encriptar e desencriptar.
2. Aparentemente o SSL inpede que alguns tipos de cache, por exemplo o proxy transparente de ISP (Internet Service Provider ou em português Provedor de Serviço Internet). Com isso é nescessário um aumento no consumo de banda do servidor.

3.2 Como funcioan o ataque "man in the middle" ?

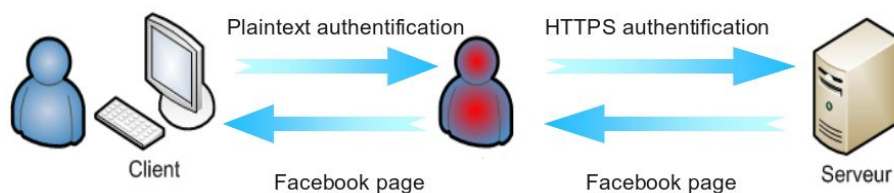
Em uma conexão normal de troca e informações dois computadores trocam dados sem a interferência de terceiros. O termo "man in the middle" é uma referência a um ataque em que o atacante intercepta os dados entre duas pessoas (por exemplo o usuário e o facebook), registra esses dados e em alguns casos até os altera sem que as vítimas percebam.

Esse ataque claramente é extremamente perigoso por conta do atacante ter acesso aos dados que estão criptografados. Ocorre da seguinte forma:

1. O usuário faz uma requisição a um servidor.
2. O atacante finge que é o servidor e assim intercepta a requisição.
3. O atacante tem acesso aos dados do usuário em texto limpo.
4. com esses dados pode-se fazer uma requisição ao servidor e receber a resposta.
5. envia a resposta de volta ao usuario.
6. usuário recebe a resposta e pensa que está em uma conexão segura.

3.3 O ataque "Man in the middle" e o SSL

Como foi visto esse ataque é fácil de se entender, a maneira como ele funciona com o SSL é igual com modificações para que o ataque funcione nesse protocolo. Com o SSL o atacante ao interceptar a conexão força um "downgrade" do HTTPS (HTTP sobre SSL) para HTTP e assim tem acesso aos dados do cliente em texto limpo, com isso pode fazer a conexão com o servidor e retornar a resposta ao usuário. Abaixo uma imagem:



Na próxima sessão tem um passo-a-passo de como fazer o um ataque "man in the middle" e assim demonstrar que é um ataque completamente de ser executado com um conhecimento extremamente básico de redes de computadores possível.

4 O experimento

Nessa sessão vamos demonstrar o quão fácil é para interceptar dados SSL e assim ter acesso a dados dos usuários. Será também demonstrado que o nível de conhecimento necessário é muito baixo, visto que usaremos ferramentas já prontas, assim podemos dizer que "lamers" podem facilmente fazer esse ataque, mostrando ser um ataque que nas mãos de hackers experientes pode acabar causando grandes danos ao serviço.

4.1 Requisitos

Os requisitos para fazer o experimento são os mesmos utilizados na hora da montagem para garantir que não haverá problemas quando for replicado pelo leitor.

1. Usar o sistema operacional Ubuntu:
2. Instalar as bibliotecas necessárias com o comando: `$ sudo apt-get install build-essential ruby-dev libcap-dev`
3. Instalar a gema (software escrito na linguagem ruby) usando o gerenciador de pacotes "gem": `$ sudo gem install bettercap`
4. Possuir o programa "virtual machine" da oracle para rodar duas máquinas virtuais, uma será o servidor e a outra o cliente. Os links para baixar as máquinas estão abaixo (as máquinas virtuais já possuem os softwares necessários para rodar o experimento):
 - (a) Servidor:
 - (b) Cliente:

4.2 Passo-a-passo

5 Conclusão

5.1 Como se defender do "Man in the middle" sobre o SSL ?

5.2 Considerações finais