SSL

Herivelton Coelho, Pedro Brentan, Renato da Motta Bustamante

23 de junho de 2013

1 Introdução

O Trabalho em Grupo, TG, feito com objetivo de obtenção de aprovação na disciplina de Segurança em Computação, teve diversos temas das mais variadas vertentes da área de segurança. Nosso grupo - formado por Pedro Brentan, Herivelton Coelho e Renato da Motta Bustamante - Aborda o tema SSL, que é um protocolo para criação e manutenção de um canal criptográfico entre um cliente e um servidor.

O tema é bem difundido e conta com uma vasta quantidade de documentação na Internet, o que é uma vantagem e uma desvantagem ao mesmo tempo. A vantagem é óbvia, não seria por falta de material que o trabalho seria inviabilizado. A desvantagem é justamente a grande quantidade de informação, o que faz com que seja difícil sintetizar o conteúdo e não perder o foco, além de obrigar a fazer um trabalho completo e bem estruturado.

2 Fundamentação Teórica

A base para pesquisa sobre o tema foi o [RFC 6101]. À partir desse material foi possível conhecer a fundo a estrutura e o funcionamento do protocolo SSL. Neste RFC encontra-se, além da definição básica do protocolo, a descrição completa da implementação do protocolo, sua estrutura física, com seus registros e campos, e a sequência de passos que regem o protocolo.

Após conhecer o protocolo tecnicamente, buscamos informações mais descritivas e históricas para complementar o embasamento teórico, para tal confessamos que a fonte principal foi a [Wikipedia]. Nela também foi possível complementar informações técnicas de mais alto nível do ponto de vista da engenharia por trás do protocolo.

Feito isso buscamos listar algumas aplicações, além da principal que é comunicação entre navegador e servidor.

Para a implementação prática do protocolo tivemos que criar uma coisa simples, que seja didática e possível de demonstrar num curto espaço de tempo. SSL/TLS tem diversas implementações das mais varias linguagens de programação em todos os sistemas operacionais. Não era nosso intuito reinventar a roda e criar algo que de fato seja utilizado algum dia, o propósito da implementação

prática é meramente didático e ilustrativo.

3 Protótipo. Neste capítulo descrever o protótipo, ou seja, o experimento prático realizado.

O experimento pratico foca em uma das partes do protocolo SSL chamado handshake, este é um acordo entre as partes interessadas em estabelecer um canal de segurança, no passo inicial é aplicada a criptografia assimétrica, usando o método de RSA, em seguida é iniciado o acordo de chaves, diffie-hellman foi usado no nosso trabalho, pois é de domínio de todos os integrantes do trabalho, assim como da turma em geral, sendo mais didático para os interessados, após o diffie-hellman estiver concluído, iniciasse então a transmissão de dados simétricos , pelo método AES .
Na interface depois de realizado o handshake, nosso programinha permite que o usuário envie mensagens a outra entidade , seja pelo servidor ou pelo cliente enviando uma mensagem (um numero) que é cifrado, e ao chegar na outra entidade e é exibido cifrado, demonstrado como ela navega no canal de comunicação, e depois então ele decifra e exibe a mensagem.

4 Considerações Finais

O TG, que por ser um trabalho em que se espera grande qualidade e conteúdo, dados os recursos e o tempo disponíveis, parecia a princípio apenas mais uma entre tantas tarefas universitárias. Porém ao longo do trabalho a equipe conseguiu se integrar e criar uma identificação com o tema.

SSL faz parte do dia a dia de qualquer pessoa que tenha acesso à internet, foi muito bom conhecer melhor o assunto e poder ter uma melhor consciência da importância desse protocolo. Saber como funciona faz com que a confiança aumente e induz nós mesmos a usarmos a tecnologia quando confrontarmos uma possibilidade de uso.

Um dos integrantes do grupo, inclusive, se interessou tanto pelo assunto que conseguiu convencer os diretores da empresa em que trabalha a deixá-lo implementar segurança nos servidores da empresa. Havia uma vontade mas não saía do papel, após conhecer o protocolo a fundo foi possível usar argumentos sólidos que zeram com que a proposta fosse irrecusável. Tendo feito esse trabalho foi obtida a confiança necessária por ambos os lados para a concretização desse projeto.

Referências

[RFC 6101] A. Freier; P. Karlton; P. Kocher. The Secure Sockets Layer (SSL) Protocol Version 3.0. Disponível em:

http://tools.ietf.org/html/rfc6101. 30/04/2013

[Wikipedia] Wikipedia. Transport Layer Security. Disponível em : https://en.wikipedia.org/wiki/Transport_Layer_Security. 30/04/2013.