Criptografia - SSL/TLS
Trabalho Teórico

Autor:
Vasco Barnabé - nº42819

Setembro de 2021

1 Introdução

No âmbito da unidade curricular de Segurança Informática, e proposto pelo professor Pedro Patinho, este trabalho procura explorar o tema da criptografia, aprofundando especificamente o sub-tema "**SSL/TLS**".

2 Criptografia

Em Segurança Informática, a criptografia consiste na conversão de dados de um formato legível para um formato codificado. Os dados resultantes desta operação, ou seja, criptografados ou encriptados, perdem a sua utilidade quando se encontram neste formato, podendo apenas ser lidos ou processados novamente após serem desencriptados, ou seja, passarem pelo processo inverso, passando o seu formato de codificado para legível.

A criptografia é utilizada por elementos individuais ou grandes entidades que pretendem tornar seguros os dados que navegam entre cliente e servidor, sendo por isso, a forma mais simples e importante de garantir que os dados existentes num computador ou numa base de dados não são legíveis caso estes sejam roubados (ex: passwords de usuários, dados de contas bancárias, etc...) por terceiros que não têm autorização para ter acesso a esses dados, de modo a que estes não possam ser utilizados para fins maliciosos.

Apesar do tema geral deste trabalho ser a criptografia, não tem como objetivo avançar em detalhe sobre o modo como esta funciona, quais as suas técnicas mais comuns (chaves simétricas ou assimétricas), quais os algoritmos utilizados para encriptar dados ou benefícios da sua utilização e exemplos de aplicação. No entanto, será apresentada a diferença entre criptografia de dados em trânsito e criptografia de dados em repouso, sendo a criptografia de dados em trânsito o foco principal deste trabalho.

2.1 Criptografia de dados em repouso

São considerados dados em repouso aqueles que se encontram num dispositivo de armazenamento de dados (ex: guardados em disco rígido), não estando a ser utilizados ou transferidos.

Comparativamente aos dados em trânsito, estes podem ser considerados mais seguros, uma vez que, além da descodificação necessária dos dados para que estes possam estar legíveis, o hacker tem ainda de passar pela segurança do dispositivo onde estes dados estão guardados, que restringe o acesso a estes.

2.2 Criptografia de dados em trânsito

Dados em trânsito é a designação atribuída aos dados que são transmitidos entre redes na Internet, que navegam entre dispositivos. No início do processo de transferência destes dados, estes são encriptados de modo a que, mesmo que sejam intercetados por terceiros (hackers) durante a transferência, estes continuam privados e ilegíveis para o intercetor. Naturalmente, estes dados encriptados não são impossíveis de desencriptar por parte dos intercetores, mas as probabilidades destes ficarem de facto em sua posse em formato legível, e por isso, disponíveis para serem utilizados para fins maliciosos, são muito reduzidas.

Assim, e chegando finalmente ao objetivo principal deste trabalho, serão apresentados dois protocolos criptográficos utilizados nas transferências de dados encriptados na Internet, **SSL** e **TLS**.

3 SSL/TLS

SSL e **TLS** são protocolos criptográficos que fornecem autenticação e criptografia dos dados que circulam entre servidores e dispositivos na Internet.

Mas o que significa SSL e TLS? SSL (*Secure Sockets Layers*) e TLS (*Transport Layer Security*) são, como já foi referido, ambos protocolos criptográficos que encriptam dados e autenticam uma ligação, por exemplo, entre cliente e servidor web, para que os dados possam navegar entre eles. E em que diferem? De forma breve e resumida, o protocolo TLS é apenas uma versão mais recente e mais segura do SSL.

Histórico de lançamentos de versões de SSL e TLS:

- SSL 1.0 - devido a grandes falhas de segurança, esta versão nunca foi oficialmente lançada.
- SSL 2.0 - lançada em 1995. Devido a problemas de segurança detetados, esta versão foi desacreditada em 2011.
- SSL 3.0 - lançada em 1996, mas desacreditada em 2015 devido igualmente a problemas de segurança.
- TLS 1.0 - Surgiu então como uma atualização ao protocolo SSL 3.0, em 1999. Esta versão ainda se encontra em vigor, apesar de se estimar a sua retirada em 2020.
- TLS 1.1 - Lançada em 2006, com retirada igualmente prevista para 2020.
- TLS 1.2 - Lançada em 2008.
- TLS 1.3 - lançada em 2018.

4 Proteção de dados com SSL e TLS

Quando um usuário visita determinado site, o seu navegador procura o certificado SSL/TLS desse site. Quando este certificado está presente, é realizado um "Handshake"(aperto de mão, que será explorado mais à frente neste trabalho) para que este seja validado. Assim, quando o navegador de um usuário determina que o certificado é válido e autentica o seu servidor, é criado um link criptografado entre si e o servidor para que os dados sejam transportados em segurança.

É neste passo que entra a designação tão conhecida, **HTTPS** (*Hyper Text Transfer Protocol Secure*), que significa "HTTP over SSL/TLS".

É conhecido que **HTTP** (*Hyper Text Transfer Protocol*) é um protocolo que desempenha um papel essencial na transferência de dados pela Internet, mas, apenas com HTTP, os dados encontram-se vulneráveis a ataques. Com HTTPS, os dados são criptografados e autenticados durante o transporte, o que os torna seguros.

A diferença entre HTTP e HTTPS é: ambos são o mesmo protocolo, no entanto, HTTPS é HTTP sobre SSL ou TLS.

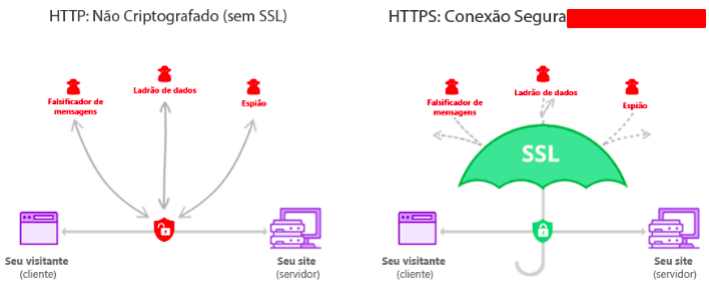

Figura 1: HTTP(não seguro) vs HTTPS(seguro).

5 Handshake

O Handshake resume-se à concordância de um segredo compartilhado entre cliente e servidor, e o tipo de criptografia que será usado nos dados em trânsito.

5.1 Handshake com SSL

O protocolo SSL usa uma porta para realizar as conexões, processo este apelidado de **conexão explícita**. É utilizada a porta padrão para HTTPS, a porta 443.

5.2 Handshake com TLS

Por outro lado, o protocolo TLS utiliza **conexão implícita**. Esta conexão pode ser ilustrada na seguinte imagem:

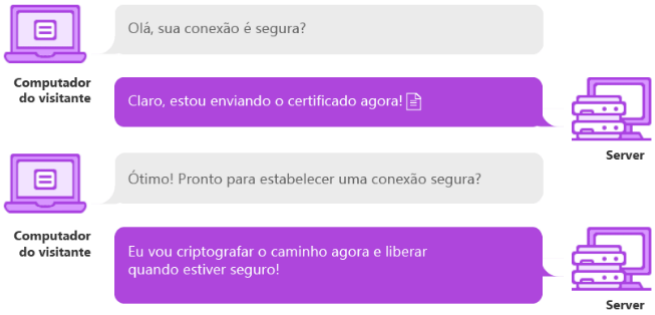

Figura 2: Handshake model.

O cliente envia uma primeira mensagem ao servidor, por um canal inseguro para dar a conhecer que quer estabelecer ligação. De seguida, é o servidor a responder ao cliente. Após acontecer este Handshake entre cliente e servidor, a ligação passa a ocorrer por um canal seguro, pela porta padrão, 443, ou qualquer outra que tenha sido designada no início do processo pelo usuário.

Tanto SSL como TLS, funcionam através de chaves públicas e privadas, utilizadas para criar uma chave de sessão durante a conexão inicial, sendo então esta chave utilizada para encriptar e desencriptar os dados transferidos, mantendo-se válida apenas para a sessão criada.

6 Curiosidade

Na Figura 1 é possível verificar que na ligação em **HTTPS** se encontra apenas "SSL". Posto isto, porque se dá o nome de certificado SSL se o protocolo SSL foi desacreditado?

Primeiro, é preciso ter em atenção que certificado não é o mesmo que o protocolo utilizado pelo servidor, e por isso, a explicação: é uma questão de marca, uma vez que que os principais fornecedores destes certificados ainda se referem a eles como certificados SSL, sendo todos estes certificados na realidade, certificados SSL/TLS. Por isso, ambos os protocolos SSL e TLS são suportados, não tendo o usuário que se preocupar em utilizar um certificado SSL para usar protocolo SSL e um certificado TLS para um protocolo TLS.

7 Conclusão

Quanto maior for a importância e exposição dos nossos dados, maior terá de ser o cuidado e a proteção destes. Podemos ter estes dados em repouso, num disco rígido por exemplo, ou em tráfego pela Internet, situação esta que é mais perigosa e exige maior atenção da nossa parte.

Para a transferência destes dados, foi visto que os protocolos TLS e SSL são ambos protocolos para autenticar e criptografar a transferência de dados na Internet, sendo o TLS uma versão mais atualizada e segura do SSL.

Não é demais insistir no facto de que certificado não é o mesmo que protocolo, e por isso, não é necessário mudar o certificado SSL existente, uma vez que este certificado suporta tanto o protocolo SSL como o TLS, sendo até o TLS já mais utilizado por ser o protocolo com as versões mais recentes e mais seguras.

Para concluir, salienta-se a importância dos assuntos envolvidos e tratados neste trabalho, uma vez que dizem respeito à segurança dos dados pessoais de cada um de nós, alguns deles que expostos por terceiros podem causar-nos apenas algum incómodo, e outros que podem de facto alterar a nossa vida.