Universidade de Brasília Faculdade UnB Gama

Laboratório sobre Certificados Digitais e Autoridades Certificadoras

Fundamentos de Redes de Computadores - Turma 1

Prof. : Fernando William Cruz

Engenharia de Software

Alunos

Ana Carolina Rodrigues Leite - 19/0101792

Ricardo de Castro Loureiro - 20/0043111

1. Introdução

A proposta deste laboratório é fornecer aos alunos a oportunidade de expandir os conhecimentos sobre Certificados Digitais por meio de atividades práticas. Durante o curso, foram explorados tópicos como a criação de Certificados Digitais, o estabelecimento de uma Autoridade Certificadora (AC) para assinar os certificados, o uso do OpenSSL para gerar e manipular chaves criptográficas, além da configuração de servidores web para oferecer suporte a conexões HTTPS.

Os Certificados Digitais desempenham um papel fundamental na segurança das comunicações online, permitindo a autenticação das partes envolvidas e a criptografia dos dados transmitidos. Eles são emitidos por Autoridades Certificadoras confiáveis, que garantem a validade e a integridade dos certificados.

A utilização do OpenSSL, uma biblioteca de software de código aberto, permite realizar uma série de operações relacionadas à criptografia e ao gerenciamento de certificados digitais. Através do OpenSSL, é possível gerar pares de chaves criptográficas, criar solicitações de certificados (CSR) e assinar certificados usando uma AC.

Além disso, a configuração de servidores web, como o Apache2, para suportar conexões HTTPS é essencial para oferecer uma experiência segura aos usuários. Isso envolve a instalação de certificados digitais válidos no servidor, a ativação do módulo SSL/TLS e a configuração correta do VirtualHost para habilitar o suporte HTTPS.

Ao realizar atividades práticas nesse laboratório, os alunos terão a oportunidade de aprofundar seus conhecimentos sobre Certificados Digitais, Autoridades Certificadoras, OpenSSL e configuração de servidores web. Essas habilidades práticas serão valiosas para a implementação de comunicações seguras e a proteção de informações sensíveis em ambientes online.

2. Passo 1: Criação um Certificado Digital e como criar uma Autoridade Certificadora para assinar o próprio certificado

Para criar um Certificado Digital e uma Autoridade Certificadora (AC) para assinar o próprio certificado, você precisará seguir alguns passos específicos. Antes de seguir os passos, iremos entender mais sobre o que é um Certificado Digital e uma Autoridade Certificadora (AC).

Certificados Digitais:

Um Certificado Digital é um arquivo eletrônico que contém informações sobre a identidade de uma entidade, como nome, organização e chave pública. Ele é usado para autenticar e criptografar comunicações online, garantindo a confidencialidade, integridade e autenticidade dos dados transmitidos.

Os certificados digitais são emitidos por Autoridades Certificadoras confiáveis (ACs) que atuam como terceiros confiáveis. Essas ACs são responsáveis por verificar a identidade do titular do certificado e garantir sua validade. Cada certificado é assinado digitalmente por AC, tornando-se um meio confiável de autenticação online.

Autoridades Certificadoras (ACs):

Uma Autoridade Certificadora (AC) é uma entidade confiável responsável por emitir e assinar certificados digitais. Ela estabelece uma cadeia de confiança na qual uma AC superior valida e emite certificados para outras ACs. Isso cria uma hierarquia de confiança, onde os certificados emitidos pelas ACs inferiores são confiáveis devido à confiança nas ACs superiores.

Uma AC possui uma Chave Privada, que é usada para assinar digitalmente os certificados que emite. A AC também possui um Certificado Digital próprio, que é usado para verificar sua autenticidade. Esse certificado é emitido por uma AC superior ou por uma Autoridade de Registro (AR), que realiza a verificação da identidade da AC.

Agora vamos definir a parte prática via comandos openssl:

1. Criar uma Chave Privada para a AC:

   openssl genpkey -algorithm RSA -out ca.key

Explicação: O comando openssl genpkey é usado para gerar uma Chave Privada para a Autoridade Certificadora. Neste exemplo, estamos usando o algoritmo RSA para gerar a chave e salvá-la no arquivo "*ca*.key". A chave privada deve ser mantida em segredo absoluto, pois é usada para assinar os certificados.

2. Gerar um certificado auto assinado da Atividade Certificadora (AC):

   openssl req -new -x509 -key ca.key -out ca.crt

   Explicação: O comando openssl req é usado para gerar um Certificado Digital auto-assinado para a Autoridade Certificadora. Neste caso, estamos criando um certificado autoassinado (self-signed) com validade de 365 dias. O certificado é gerado usando a Chave Privada da AC e é salvo no arquivo "*ca.crt*". Esse certificado será usado para assinar outros certificados.

3. Criar uma chave privada para o Certificado Digital:

   openssl genpkey -algorithm RSA -out cert.pem

   Explicação: O comando openssl genpkey é utilizado novamente para gerar uma Chave Privada para o Certificado Digital que desejamos emitir. Essa chave privada será usada para criptografar e descriptografar os dados durante as comunicações.

4. Gerar uma Solicitação de Assinatura de Certificado (CSR):

   openssl req -new -key cert.key -out cert.csr

   Explicação: A Solicitação de Assinatura de Certificado (CSR - Certificate Signing Request) é um arquivo que contém informações sobre a entidade e sua chave pública. Essa solicitação é enviada à Autoridade Certificadora para solicitar a assinatura do certificado. O comando openssl req é usado para gerar a CSR, com base na Chave Privada do Certificado e salvando-a no arquivo "*cert.pem*".

5. Assinar o certificado digital para a Atividade Certificadora AC:

   openssl x509 -req -in cert.csr -CA ca.crt -CAkey ca.key -CAcreateserial -out cert.crt

Explicação: O último comando openssl x509 é usado para assinar o Certificado Digital com a Autoridade Certificadora. A opção -req indica que estamos assinando um CSR. O certificado é assinado usando a Chave Privada da AC e é salvo no arquivo "*cert.crt*". A opção -CA especifica o Certificado Digital da AC que será usado para assinar o certificado, enquanto a opção -CAkey especifica a Chave Privada da AC. A opção -CAcreateserial indica que o OpenSSL deve criar um arquivo serial para rastrear os certificados assinados.

3. Passo 2: Configuração do servidor Apache2 para atender requisições HTTPS

Para configurar o servidor Apache2 para atender requisições HTTPS, você precisa seguir alguns passos. Aqui está um resumo do processo:

1. Instalar o Apache2:

   sudo apt-get update

   sudo apt-get install apache2

2. Certificar que o módulo SSL esteja habilitado no Apache2:

   sudo a2enmod ssl

3. Crie um diretório para guardar o certificado e a chave privada do servidor:

   sudo mkdir /etc/apache2/ssl

4. Copie o certificado digital (cert.crt) e a chave privada (cert.key) para o diretório criado acima.
5. Edite o arquivo de configuração do Apache para habilitar o suporte HTTPS:

   sudo nano /etc/apache2/sites-available/default-ssl.conf

6. Dentro do arquivo, localize as linhas ´SSLCertificateFile´ e ´SSLCertificateKeyFile´ e atualize os caminhos para apontar os arquivos de certificado e chave privada que você copiou anteriormente:

SSLCertificateFile /etc/apache2/ssl/cert.crt

SSLCertificateKeyFile /etc/apache2/ssl/cert.key

7. Ative o site padrão SSL:

   sudo a2ensite default-ssl.conf

8. Reinicie o Apache2 para aplicar as alterações:

   sudo service apache2 restart

Agora, o servidor está configurado para atender as requisições HTTPS usando o certificado digital gerado. Você pode acessar o site usando `https:// <seu_endereco_ip>` ou o famoso `https: //localhost`.

4. Passo 3: Configuração do cliente WWW (Firefox ou Chrome) para acessar o servidor WWW via HTTPS

Para configurar o cliente WWW (Firefox ou Chrome) para acessar um servidor WWW via HTTPS, siga as instruções abaixo:

Google Chrome:

1. Abra o Google Chrome e digite "*chrome://settings*" na barra de endereços.
2. Role para baixo e clique em "Avançado" para expandir as configurações avançadas.
3. Localize a seção "Privacidade e segurança" e clique em "Configurações de site".
4. Na nova página, clique em "Cookies e dados do site".
5. Certifique-se de que a opção "Bloquear cookies de terceiros" esteja desativada.
6. Volte para a página anterior de configurações de site e clique em "Permissões".
7. Clique em "Localização" e verifique se o acesso à localização está ativado para o site que você está tentando acessar.
8. Volte para a página anterior de configurações de site e clique em "Segurança".
9. Certifique-se de que a opção "Usar HTTPS" esteja ativada.

Mozilla Firefox:

1. Abra o Mozilla Firefox e digite "about:preferences" na barra de endereços.
2. Na página de preferências, clique em "Privacidade e Segurança" no painel esquerdo.
3. Role para baixo até a seção "Permissões" e clique em "Configurações".
4. Certifique-se de que a opção "Bloquear cookies de terceiros e site data" esteja desativada.
5. Volte para a página de preferências e clique em "Privacidade e Segurança" novamente.
6. Na seção "Histórico", selecione a opção "Usar configurações personalizadas para o histórico".
7. Certifique-se de que a opção "Aceitar cookies de sites" esteja ativada.
8. Volte para a página de preferências e clique em "Geral".
9. Role para baixo até a seção "Rede de Conexão" e clique em "Configurações".
10. Selecione "Configurações de Proxy" e verifique se as configurações de proxy estão corretas para acessar o site via HTTPS.

Após configurar as opções relevantes, feche e reabra o navegador. Agora você poderá acessar o servidor WWW via HTTPS usando o cliente WWW configurado. Certifique-se de digitar o URL completo, incluindo "https://" no início, para garantir que a conexão seja estabelecida por meio do protocolo HTTPS seguro.

Aqui estão os passos necessários para importar e exportar certificados digitais nos navegadores Firefox e Chrome:

Firefox:

Importar Certificado Digital:

1. Abra o Firefox e vá para "Preferências" no menu.
2. Na seção "Privacidade e Segurança", role até "Certificados" e clique em "Ver Certificados".
3. Na janela "Gerenciador de Certificados", vá para a guia "Seus Certificados".
4. Clique em "Importar" e localize o arquivo do certificado digital que deseja importar.
5. Siga as instruções para importar o certificado e, se necessário, insira a

senha associada ao arquivo.
6. O certificado será importado e estará disponível para uso.

Exportar Certificado Digital:

1. Abra o Firefox e vá para "Preferências" no menu.
2. Na seção "Privacidade e Segurança", role até "Certificados" e clique em "Ver Certificados".
3. Na janela "Gerenciador de Certificados", vá para a guia "Seus Certificados".
4. Selecione o certificado que deseja exportar e clique em "Fazer Backup".
5. Escolha um local para salvar o arquivo de backup e forneça um nome para ele.
6. O certificado será exportado para o local especificado.

Chrome:

Importar Certificado Digital:

1. Abra o Chrome e vá para "Configurações" no menu.
2. Role para baixo e clique em "Avançado" para expandir as configurações avançadas.
3. Na seção "Privacidade e segurança", clique em "Gerenciar Certificados".
4. Na janela "Gerenciador de Certificados", vá para a guia "Pessoal".
5. Clique em "Importar" e localize o arquivo do certificado digital que deseja importar.
6. Siga as instruções para importar o certificado e, se necessário, insira a senha associada ao arquivo.
7. O certificado será importado e estará disponível para uso.

Exportar Certificado Digital:

1. Abra o Chrome e vá para "Configurações" no menu.
2. Role para baixo e clique em "Avançado" para expandir as configurações avançadas.
3. Na seção "Privacidade e segurança", clique em "Gerenciar

Certificados".

4. Na janela "Gerenciador de Certificados", vá para a guia "Pessoal".
5. Selecione o certificado que deseja exportar e clique em "Exportar".
6. Siga as instruções para exportar o certificado e escolha um local para salvá-lo.
7. O certificado será exportado para o local especificado.

5. Passo 4: Pesquisa sobre o protocolo SSL/TLS

O protocolo SSL/TLS (Secure Sockets Layer/Transport Layer Security) é um protocolo de segurança utilizado para estabelecer comunicações seguras na Internet. Ele fornece criptografia e autenticação para proteger a integridade e a confidencialidade dos dados transmitidos entre um cliente e um servidor.

O SSL foi desenvolvido pela Netscape Communications nos anos 1990 e, posteriormente, foi substituído pelo TLS. Atualmente, o termo SSL é frequentemente usado de forma genérica para se referir a ambas as versões do protocolo.

A principal função do SSL/TLS é garantir que a comunicação entre o cliente e o servidor seja segura, protegendo os dados sensíveis contra interceptação e manipulação por terceiros. Isso é alcançado por meio de três componentes principais:

1. Criptografía: O SSL/TLS utiliza algoritmos criptográficos para criptografar os dados transmitidos. Isso significa que os dados são convertidos em um formato ilegível durante a transmissão e só podem ser decifrados pelo destinatário correto. Isso protege a confidencialidade das informações.
2. Autenticação: O SSL/TLS permite a autenticação do servidor e, opcionalmente, do cliente. Isso garante que o cliente esteja se comunicando com o servidor correto e vice-versa, evitando ataques de phishing e garantindo a identidade das partes envolvidas.
3. Integridade dos dados: O SSL/TLS utiliza funções de hash criptográfico para verificar se os dados não foram alterados durante a transmissão. Isso permite detectar qualquer manipulação dos dados durante o transporte, garantindo a integridade dos dados transmitidos.

O processo de estabelecimento de uma conexão segura SSL/TLS envolve

várias etapas, incluindo negociação de algoritmos criptográficos, troca de chaves, verificação de certificados digitais e estabelecimento de uma sessão segura. Uma vez estabelecida a conexão segura, todos os dados transmitidos entre o cliente e o servidor são protegidos pela criptografia.

O SSL/TLS é amplamente utilizado em aplicativos web, como sites de comércio eletrônico, serviços bancários online, redes sociais e qualquer outra aplicação que exija a transmissão segura de informações confidenciais. A implementação correta do SSL/TLS é essencial para garantir a segurança das comunicações online e proteger os dados dos usuários.

6. Conclusão

6.1 - Resultado do projeto

Neste laboratório, discutimos vários tópicos relacionados à segurança e criptografia na Internet, incluindo Certificados Digitais, Autoridades Certificadoras, OpenSSL e o protocolo SSL/TLS.

Certificados Digitais garantem segurança nas comunicações online, autenticado e criptografando dados. O OpenSSL é uma biblioteca de software para segurança, gerenciando certificados e operações criptográficas. O protocolo SSL/TLS estabelece conexões seguras na Internet, protegendo dados contra interceptação. Segurança na Internet é crucial para proteger informações e evitar ataques.

Eu, Ana Carolina, pude aprender muito mais sobre o conceito de protocolo SSL/TLS e os Certificados digitais, achei difícil poder configurar o apache e antes disso fazer a criptografia funcionar no qual também tive dificuldades, mas gostei e pude conhecer mais sobre criptografia no geral e especificar o conceito de segurança na internet por um todo.

Fiquei focada na parte de protocolo SSL/TLS e os Certificados digitais, lendo e colhendo informações através das minhas pesquisas na internet e tentando fazer o certificado digital e assinar ele na minha própria máquina.

Tive problemas ao fazer isso pois consegui apenas na quarta vez entre comandos e comandos, consegui achar o certo. Gostei muito de poder conhecer mais sobre as bibliotecas na implementação da openssl.

Outro ponto de dificuldade foi poder fazer a configuração do apache na máquina, que levou tempo e muitas pesquisas no stackoverflow. Considero minha participação muito ativa nas partes de certificado digital e assinatura e na execução de configuração do apache, me avaliando com nota 8.

Eu, Ricardo, fui capaz de integrar os conhecimentos teóricos da aula com a prática desenvolvida no laboratório. Compreendi profundamente o conceito do protocolo SSL/TLS, bem como a importância dos certificados digitais.

Inicialmente, encontrei algumas dificuldades para gerar os certificados e associá-los ao servidor do Apache2. Contudo, esse desafio ajudou-me a entender melhor como funciona um sistema de criptografia e segurança.

Apesar de ter encontrado diferenças no sistema Mac, consegui efetivamente

realizar o laboratório no ambiente Debian Ubuntu. A interpretação de cada comando do OpenSSL demandou esforço, e a configuração do servidor Apache2 apresentou alguns problemas. Essas dificuldades eram esperadas, dado que eu nunca havia trabalhado com essas tecnologias antes. Sendo necessário pesquisar para entender como utilizar.

No entanto, ao final, consegui gerar meu próprio certificado para responder às solicitações HTTPS e criar uma página com o certificado digital. Portanto, considero minha participação bastante ativa e, avaliando meu desempenho, acredito merecer uma nota 9.

Portanto, podemos dizer que conseguimos entender muito mais sobre o fato de como funciona a criptografia e como ela pode auxiliar no processo de segurança na própria internet. Tivemos dificuldade em pode executar as chaves de criptografia e configurar o apache, mas conseguimos reter conhecimento teórico sobre esse laborátorio.

Certificado

ricardo

Nome do sujeito

País	br
Estado/Província	distrito federal
Localidade	brasilia
Organização	unb
Unidade organizacional	engenharia de software
Nome da empresa	ricardo
Endereço de email	ricardoloureiro75@gmail.com

Nome do emissor

País	br
Estado/Província	distrito federal
Localidade	brasilia
Organização	unb
Unidade organizacional	engenharia de software
Nome da empresa	ricardo
Endereço de email	ricardoloureiro75@gmail.com

Validade

Não antes de	Tue, 11 Jul 2023 20:11:15 GMT
Não após	Thu, 10 Aug 2023 20:11:15 GMT

Informações da chave pública

Algoritmo	RSA
Tamanho da chave	2048
Expoente	65537
Módulo	C8:40:76:8A:F3:60:0D:9E:B2:EB:78:79:EA:D8:DE:43:B7:3F:90:CD:0F:E4:0B:2C…

7. Referências

DEVMEDIA. Gerando um certificado digital você mesmo. Disponível em: https://www.devmedia.com.br/gerando-um-certificado-digital-proprio/31506. Acesso em: 10/07/2023

SERASA.O que é certificado digital e para que serve. Disponível em: https://serasa.certificadodigital.com.br/blog/certificado-digital/o-que-e-certificado-digital-e-para-que-serve/. Acesso em: 10/07/2023

REMESSAONLINE.Certificado digital aprenda como obter e instalar. Disponível em: https://www.remessaonline.com.br/blog/certificacao-digital-aprenda-como-obter-e-instalar// . Acesso em: 10/07/2023

MICROSOFT.Obter um certificado digital e criar uma assinatura digital. Disponível em: https://support.microsoft.com/pt-br/office/obter-um-certificado-digital-e-criar-uma-assinatura-digital-e3d9d813-3305-4164-a820-2e063d86e512. Acesso em: 10/07/2023

CCUEC.Comandos úteis openssl. Disponível em: https://www.ccuec.unicamp.br/ccuec/material_apoio/comandos-uteis-openssl. Acesso em: 10/07/2023

FREECODECAMP.Comandos úteis openssl. Disponível em: https://www.freecodecamp.org/portuguese/news/dicas-de-comandos-do-openssl/. Acesso em: 10/07/2023

UFPR.Certificados digitais. Disponível em: https://wiki.inf.ufpr.br/maziero/doku.php?id=sc:certificados_digitais. Acesso em: 10/07/2023

UFRGS.Certificados de segurança. Disponível em: https://www.inf.ufrgs.br/admrede/tutoriais/certificados-de-seguranca/. Acesso em: 10/07/2023

SOFTWELL.Certificado Digital ambiente web. Disponível em: https://suporte.softwell.com.br/Manual/Maker2_6/dicas_e_truques/webrun/certificacao_digital_ambiente_webrun.htm. Acesso em: 10/07/2023

SIMPLIFICANDOREDES.Apache https server configurar. Disponível em: https://simplificandoredes.com/apache-https-server-configurar/. Acesso em: 10/07/2023

IMASTERS.Servidor apache hospedando diversos sites com e sem ssl. Disponível em: https://imasters.com.br/devsecops/servidor-apache-hospedando-diversos-sites-com-e-sem-ssl. Acesso em: 11/07/2023

DIGITALOCEAN.How to create a self signed ssl certificate for apache in ubuntu 20-04. Disponível em: https://www.digitalocean.com/community/tutorials/how-to-create-a-self-signed-ssl-certificate-for-apache-in-ubuntu-20-04-ptl. Acesso em: 11/07/2023

PUCPR.Guia foca GNU/Linux - Apache. Disponível em: https://www.ppgia.pucpr.br/pt/arquivos/techdocs/linux/foca-avancado/ch-s-apache.html. Acesso em: 11/07/2023

MOZILLA.Configurações de conexão no firefox. Disponível em: https://support.mozilla.org/pt-BR/kb/configuracoes-de-conexao-no-firefoxl. Acesso em: 11/07/2023

GOOGLE.Configurar a inspeção TLS (ou SSL) em dispositivos Chrome. Disponível em: https://support.google.com/chrome/a/answer/3505249?hl=pt-br. Acesso em: 11/07/2023

UNIFESSPA.Instalar ou importar o certificado no navegador mozilla firefox. Disponível em: https://helpdesk.unifesspa.edu.br/wiki-unifesspa/instalar-ou-importar-o-certificado-no-navegador-mozilla-firefox/. Acesso em: 11/07/2023

UNIFESSPA.Exportar o certificado do navegador google chrome. Disponível em: https://helpdesk.unifesspa.edu.br/wiki-unifesspa/exportar-o-certificado-do-navegador-google-chrome/. Acesso em: 11/07/2023

CONTEUDOFISCAL.Exportar o certificado do navegador google chrome. Disponível em: https://conteudo.fiscal.io/blog/como-instalar-certificado-digital-a1-no-chrome-internet-exporer-ie-firefox/. Acesso em: 11/07/2023

UNIPAMPA.Como exportar seu certificado do google chrome. Disponível em: https://sites.unipampa.edu.br/certificadosdigitais/como-exportar-seu-certificado-do-google-chrome/. Acesso em: 11/07/2023

HOSTINGER.O que é SSL/TLS. Disponível em: https://www.hostinger.com.br/tutoriais/o-que-e-ssl-tls-https. Acesso em: 11/07/2023

VALIDCERTIFICADORA.SSL ou TLS quais são as diferenças entre esses protocolos. Disponível em: https://blog.validcertificadora.com.br/ssl-ou-tls-quais-sao-as-diferencas-entre-esses-protocolos/. Acesso em: 11/07/2023

UFRJ.Segurança - Protocolo SSL/TLS. Disponível em: https://www.gta.ufrj.br/ensino/eel879/trabalhos_vf_2010_2/bernardo/tls.html. Acesso em: 11/07/2023

CRYPTOID.Explicando os protocolos de segurança ssl e tls. Disponível em: https://cryptoid.com.br/ssl-tls/explicando-os-protocolos-de-seguranca-ssl-e-tls/. Acesso em: 11/07/2023