Course Outline

SSL and TLS Deep Dive

Course Summary

Description

This course is designed to provide a very thorough understanding of Transport Layer Security and Secure Sockets Layer (TLS and SSL) – the protocols which are used to secure the vast majority of the Internet. The class will start with an overview of SSL, which will lead into a discussion of the Cryptography necessary to understand how TLS/SSL provides security to Internet communication; including a real example of the math behind RSA Key Generation, Encryption, and Signing.

The class will then be introduced to the whole SSL Process, from establishing a Public and Private Key pair to getting a signed Certificate from a Certificate Authority. Following that, we will take a closer look at the contents of a Certificate, a Private Key, and a Certificate Signing request. The student will then complete a collaborative lab where they set up their own Certificate Authority and use it to sign their certificates from the other students in the class.

Afterwards, the class will take a close look at exactly how a Client validates a Server's Certificate – the heart of Public Key Infrastructure. The class will then discuss the concept of Certificate Chains: why they are important and how they work. Then we take a quick look at the different types of Certificates available (DV, OV, EV), before continuing with an explanation of the two primary means of revoking a compromised certificate.

Lastly, the class will tie everything together with a comprehensive look at what happens in the first few milliseconds of browsing to any HTTPS website… the SSL Handshake. Each message in the SSL Handshake and their contents are illustrated and explained. The lecture concludes with a look at the different variations of the SSL Handshake which allows for different features, extensions, and levels of security.

Finally, the students complete two additional labs. The first is designed to make them experts at determining complete, proper certificate chains. And the second one is a manual look at the Certificate Revocation process: how it works and its effectiveness.

Topics

- Explain the overarching process of securing a website using HTTPS
- Understand the role of the Client and Server in an SSL Handshake
- Understand the role of the Certificate Authority and intermediate CAs
- Discuss the cryptography involved in SSL and how it is used to provide secured communication
- Describe the contents of an X509 Certificate, RSA Private Key, and Certificate Signing Request (CSR)
- Explain and Convert Certificates and Keys between the three major versions (PEM/DER/PFX)
- Illustrate what a Client checks to validate a Server's Certificate
- Understand the purpose and functional operation of a Certificate Chain
- Describe the various messages in an SSL Handshake
- Know, Understand, and be able to define and explain the following concepts and terms:
    - Certificate Chains, Certificate Revocation List (CRL), Certificate Signing Request (CSR), Change Cipher Spec, Cipher Suites, Common Name, Distinguished Named, Domain Validation (DV), End Entity Certificate, Ephemeral Key Exchanges, Export grade ciphers, Extended Validation (EV) Certificate, Handshake Messages, Intermediate Certificates, Issuer, Message Signing, OCSP Stapling, Online Certificate Status Protocol (OCSP), Organization Validation (OV) Certificate, Perfect Forward Secrecy, Root Certificate, Server Name Indication (SNI), SSL Records, Subject, Subject Alternative Name (SAN) Cert.

Course Outline

SSL and TLS Deep Dive

Course Summary

Audience

This course is designed for students with some exposure to SSL.

Prerequisites

This is an Advanced level, Deep Dive class that is built to take a student with some exposure to SSL and make them SSL Experts – students SHOULD have at least some exposure to SSL and/or SSL Certificates before attending this class

The labs make use of certain Linux commands. Each student SHOULD have a basic understanding of what each of these commands do and hopefully have used these commands at least once before.

Duration

Three days

Course Outline

SSL and TLS Deep Dive

Course Outline

I. TLS/SSL Overview
A. What is SSL? What is TLS?
B. How do SSL/TLS Protect your Data?
C. Anti-Replay and Non-Repudiation
D. Key Players
E. TLS / SSL Versions - Part 1`
F. TLS / SSL Versions - Part 2
G. Module 1 Review Questions

II. Cryptography
A. Hashing
B. Data-Integrity
C. Encryption
D. Public and Private Keys
E. How TLS and SSL use Cryptography
F. Public Key Infrastructure (PKI)
G. RSA
H. Diffie-Hellman
I. Digital Signature Algorithm
J. Module 2 Review Questions

III. x509 Certificates and Keys
A. Overview of the SSL Process
B. What is in a Certificate?
C. Inspecting a Certificate
D. Certificate Extensions
E. LAB 3.0 - Setting up your Lab Environment
F. LAB 3.1 - Inspecting the certificate of your favorite website
G. What is in a Private Key?
H. LAB 3.2 - Matching Certificates to Private Keys
I. What is in a CSR?
J. File Formats
K. LAB 3.3 - Creating a Certificate Authority and two Signed Certificates
L. LAB 3.4 - File Conversions
M. Module 3 Review Questions

IV. Security through Certificates
A. Overview of the SSL Process, part 2
B. Certificate Validation - Part 1
C. Certificate Validation - Part 2
D. Certificate Chains - Part 1
E. Certificate Chains - Part 2
F. LAB 4.1 - Certificate Chains
G. Basic Constraints
H. Certificate Types (DV, OV, EV)
I. Certificate Revocation
J. Checking Revocation Status
K. LAB 4.2 - Certificate Revocation
L. Module 4 Review Questions

V. Cipher Suites
A. Cipher Suites
B. CS - Key Exchange - Part 1
C. CS - Forward Secrecy - Key Exchange - Part 2
D. CS - Authentication
E. CS - Encryption - Part 1
F. CS - Encryption - Part 2
G. CS - Hashing
H. Cipher Suites - Avoid, Accept, Prefer
I. Enumerating Cipher Suites
J. LAB 5.1 - Cipher Suite Enumeration

VI. TLS/SSL Handshake
A. Records - Part 1
B. Records - Part 2
C. TLS Handshake
D. LAB 6.1 - Inspecting a TLS Handshake in Wireshark
E. Handshake: Ephemeral Diffie-Hellman
F. Handshake: Session Resumption
G. Handshake: Mutual Authentication
H. LAB 6.2 - Inspecting TLS Handshake Variants
I. TLS Extensions
J. Extension: OCSP Stapling
K. Extension: Server Name Indication (SNI)
L. Extension: Session Tickets
M. LAB 6.3 - Inspecting Handshake Extensions
N. Decrypting TLS
O. LAB 6.4 - Decrypting TLS

VII. TLS Defenses
A. Major SSL/TLS Failures over the Years
B. HTTP Strict Transport Security
C. Certificate Authority Authorization
D. Certificate Transparency - Part 1 - Overview
E. Certificate Transparency - Part 2 - Process and Demonstration
F. Certificate Transparency - Part 3 - Merkle Hash Trees

VIII. Bonus Content
A. Free access to OpenSSL Training Course

IX. TLS 1.3 Live Session Recordings
A. Recording - Differences with TLS 1.3 - 2022 0830
B. Recording - Middleboxes, Forward Secrecy, Decrypting TLS 1.3 - 2022 0922
C. Recording - Key Schedule, Part 1
D. Recording - TLS 1.3 Handshake
E. Recording - Key Schedule, Part 2