Applied Cryptography
Individual Project: PKI-TLS

Objective

This lab is designed to help students understand the practical implementations of Public Key Infrastructure (PKI) and Transport Layer Security (TLS), including mutual TLS (mTLS). Students will configure a server and a client to communicate securely using TLS and mTLS and discuss the implications. You may have done some labs on TLS in other classes. The focus here is to understand the certificates and how they are being used in practice.

Steps to Implement the experiments.

Setup:

1. Create two Linux VMs, call one Client and the other Server.
2. On Server
    a. Install NGINX (an HTTP web server) to serve web contents
    b. Install easy-rsa to manage PKI
3. On the Client
    a. Install cURL to make HTTP requests.
    b. Install tcpdump to capture network traffic.

TLS Configuration:

4. On the Server
    a. Create a basic website hosted on NGINX.
    b. Configure NGINX to use HTTPS with self-signed Elliptic Curve Cryptography (ECC) certificates.
    c. Set the server to accept connections only using TLS version 1.3 (Version 1.2 is OK but discouraged).
5. On the client
    a. Start tcpdump to capture traffic.
    b. Use cURL to make a secure request to the server.
    c. Stop tcpdump.
    d. Analyze the pcap file with Wireshark to verify the TLS handshake, ensuring the correct protocol and certificates were used.

mTLS Configuration:

6. On the Server
    a. Create a Certificate Authority (CA) using easy-rsa, opting for ECC over RSA for the certificate type.
    b. Generate and sign certificates for both the Server and Client.
    c. Configure NGINX to require client certificate verification (mTLS) before serving the webpage.
7. On the Client
    a. Start tcpdump and attempt to connect to the server using cURL without the client certificate to observe the failure.

b. Stop tcpdump and review both the pcap in Wireshark and the NGINX logs to analyze why the connection failed.
c. Restart tcpdump, this time using cURL with the client certificate to attempt access.
d. Stop tcpdump and review the pcap and NGINX logs to confirm successful mTLS connection.

8. On the Server
    a. revoke the existing client certificate.
    b. Issue a new Client certificate
    c. How do you inform the server that the Client's old certificate should be rejected?

Discussions

1. PKI Security: How should you protect the PKI setup on the server?
2. Certificate Revocation List (CRL): How frequently should you regenerate the CRL?
3. TLS vs. mTLS: What differences do you observe in the TLS handshake process between standard TLS and mTLS?
4. Cipher Suites: What might happen if a client configured only to use RSA cipher suites tries to connect?

Submission

1. Document Your Experiments:
    - Capture and include screenshots during each experiment to visually document the process. Place at least one screenshot under each step to illustrate key actions and results. Aim to include screenshots of intermediate steps where significant changes or outcomes occur. However, ensure that each screenshot adds value and avoids redundancy.
    - Accompany each screenshot with a concise description that explains what the screenshot represents and why it is significant. This will help clarify the context and relevance of each image.
    - A zip for all the PCAP files.
2. Write-Up Discussions:
    - The discussions should reflect your analysis, insights, and conclusions based on the experiments conducted.
3. Overall Presentation:
    - Organize your submission into clearly defined sections corresponding to each task. Use headings and subheadings to structure your document logically.
    - Write clearly and concisely, focusing on the relevance to the project objectives. Ensure your language is precise and your arguments are well-supported with evidence from your experiments.
4. Submission Format:
    - Submit your documentation and discussions in a PDF format. Ensure that all images are clear and adequately sized within the document. Your file name should start with your name.

Additional notes

1. You can use wireshark & nmap/zenmap (GUI's) instead of tcpdump
2. You may spin up a NGINX server on Docker than using multiple VM instances.
3. You may use Let's encrypt instead of 'easy-rsa'. Easy-RSA sometimes is not easy.

4. Some students suggested using the reference to know curl, libcurl and the cURL. https://everything.curl.dev/usingcurl/tls/sslkeylogfile.html
5. Seek clarification or help from CAs and/or class slack

Grading Rubrics

Total 12

Setup (1)

NOTE: This may be done on two different VMs, containers or on the same host. As far as students have a means of starting NGINX and a means of using cURL to connect to NGINX.

TLS (3)

4. On the Server (1.5): a(0.5), b (0.5), c(0.5)
5. On the client (1.5): a,b,c, d(1.5). Remember that the certificate exchange may occur after encryption has been established. What do you need to do to see the certificate exchange in Wireshark? This applies if it's TLS 1.3.

mTLS (4)

6. On the Server (1.4): a, b(0.7), c(0.7)
7. On the Client (1.4): a, b(0.7), c, d(0.7)
8. On the Server (1.2): a(0.4), b(0.4), c(0.4)

Discussion (4):