Optional Homework 10

SSL/TLS Certificates and Their Role

An **SSL/TLS certificate** is a digital file used to secure communication across networks. It contains a **public key**, details about the **issuer**, and the **domain** it's issued for. The primary goals are to authenticate the server's identity and to enable encrypted connections.

Public Key Cryptography and Key Length

Certificates rely on **public key algorithms**, most commonly RSA or ECC (Elliptic Curve Cryptography). Key length measures the computational complexity required to break encryption:

- 2048-bit RSA keys remain standard, though 4096 bits are sometimes employed.
- Shorter ECC keys (e.g., 256 bits) can offer security comparable to longer RSA keys.

In a PKI context, key lengths indicate how resistant a certificate is to brute-force attacks. Longer key lengths usually mean better security (though they may affect performance).

Validity Periods and Lifespans

Certificates include **validity periods** defined by the not_before and not_after fields. The duration—commonly measured in days—represents how long the certificate remains valid. Industry rules often limit certificates to maximum lifespans of 398 days for publicly trusted entities. Shorter-lived certificates reduce the window for exploits or vulnerabilities, enhancing security posture.

Issuers and Trust

A **certificate issuer** (also known as a Certification Authority, or CA) vouches for the authenticity of the certificate. Each CA belongs to a "trust store" managed by operating systems and browsers. The $C = US$, $O = Let's Encrypt$, etc., structure in the issuer name references the **country** (C) and organization (O). This code's approach to analyzing certificate data includes extracting country-level distribution to visualize global issuer presence.

Certificate Transparency and Logging

Modern web security initiatives advocate logging certificates in **Certificate Transparency** databases. This helps users, researchers, and browser vendors to track newly issued certificates for potential misuse. By analyzing logs and certificate data programmatically, one can:

- Identify suspicious patterns (e.g., unexpected issuers or short-lifespan certificates)
- Track the usage of specific key lengths or algorithms
- Evaluate compliance with evolving security standards

Statistical Analysis of Certificates

Statistical insights—such as the **mean** or **median** certificate validity—reveal usage trends. **Histograms** or **bar charts** of key lengths highlight cryptographic preferences, while **pie charts**

can capture issuer or geographic distributions:

- Common key lengths of 2048 bits or 4096 bits
- Popular public key algorithms (e.g., RSA, ECC)
- Most frequent issuer countries, extracted from metadata ($C = \ldots$)

Understanding these distributions guides best practices: if the data suggests widespread adoption of strong cryptography, it affirms alignment with current security norms.