PKI & SSL/TLS

Overview

The fundamental Diffie-Hellman key exchange is susceptible to a Man-in-the-Middle (MITM) attack because it lacks a mechanism for participants to authenticate each other's identity, allowing an attacker to establish two separate secret keys and decrypt all communication. This critical security gap is filled by Public Key Infrastructure (PKI), which introduces trust by using digital certificates signed by a universally trusted third party called a Certificate Authority (CA). Consequently, modern protocols like HTTPS rely on the client's ability to verify the server's certificate signature, ensuring that the initial key exchange and subsequent encrypted communication are indeed with the legitimate intended party.

Key Information

- Diffie-Hellman (DH) Flaw: The standard DH key exchange lacks authentication, leaving it vulnerable to Man-in-the-Middle (MITM) attacks.
- MITM Attack: An attacker can intercept public values and establish two separate secret keys (one with Alice, one with Bob), allowing them to read and modify all communication.
- PKI Solution: Public Key Infrastructure (PKI) resolves this by providing an identity verification mechanism.
- Digital Certificates: PKI uses digital certificates which cryptographically bind a public key to an identity.
- Trusted CAs: These certificates are signed by a Certificate Authority (CA) (a trusted third party), enabling protocols like HTTPS to ensure clients are communicating with the genuine server.

Notes

Creating a certificate with openssl

```
openssl req -new -nodes -newkey rsa:4096 -keyout key.pem -out cert.csr
```

- `req -new` create a new certificate signing request
- `-nodes` save private key without a passphrase
- `-newkey` generate a new private key
- `rsa:4096` generate an RSA key of size 4096 bits
- `-keyout` specify where to save the key
- `-out` save the certificate signing request

Viewing a certificate and its information

```
openssl x509 -in cert.pem -text
```

- `x509` Specifies that you want to perform operations related to X.509 digital certificates
- `-in` Specifies the input file
- `-text` output the certificate content in a human-readable, detailed text format, rather than the raw encoded form

---

Task

1. What is the size of the public key in bits?
    1. `openssl x509 -in cert.pem -text`
    2. **Public Key: (4096 bits)**
2. Till which year is this certificate valid?
    1. `Not After : Feb 25 11:34:19 2039 GMT`
    2. **2039**

Conclusion

The inherent lack of identity verification in the basic Diffie-Hellman key exchange leaves it vulnerable to a crippling MITM attack where all communication is compromised. This fundamental flaw is securely mitigated by PKI, which leverages CA-signed digital certificates to authenticate the

server's identity, thereby guaranteeing the integrity and confidentiality of modern communication protocols like HTTPS.

Resources

- **TryHackMe**: Intro to Cryptography

Revision #6
Created 2025-11-25 18:40:18 UTC by David Rizzo
Updated 2025-12-01 16:09:12 UTC by David Rizzo