Cybersecurity

Architecture and Design

2.8.2 Elliptic Curves and Perfect Forward Secrecy

Why is it important to frequently change encryption keys?

Overview
The student will summarize the basics of cryptographic concepts.

Grade Level(s)
10, 11, 12

Cyber Connections

- Threats & Vulnerabilities
- Networks & Internet
- Hardware & Software

This content is based upon work supported by the US Department of Homeland Security's Cybersecurity & Infrastructure Security Agency under the Cybersecurity Education Training and Assistance Program (CETAP).

Copyright © 2023 Cyber Innovation Center
All Rights Reserved. Not for Distribution.

Teacher Notes:

CompTIA SY0-601 Security+ Objectives

Objective 2.8

- Summarize the basics of cryptographic concepts.
    - Elliptic-curve cryptography
    - Perfect forward secrecy

Elliptic Curves and Perfect Forward Secrecy

Curve Cryptography

Elliptic Curve Cryptography, ECC, is an approach to asymmetric encryption based on the algebraic structure of elliptic curves over finite fields. Do not let the wordiness of that definition intimidate you. The important thing to know about asymmetric encryption is that the encryption uses extremely large integers made from the product of two or more large prime numbers. ECC uses curves of the form y^2 = x^3 + ax + b to generate numbers used for the encryption. ECC are more resistant to attacks, allowing for the integers to be smaller (only 256-bit, which is still huge) than general asymmetric encryption.

SSL vs. TLS

When studying ***cryptographic protocols*** it is inevitable to come across the terms SSL and TLS. Cryptographic protocols encrypt data exchanged between a webserver and a user. SSL stands for ***Secure Sockets Layer***, while TLS stands for ***Transport Layer Security***. SSL and TLS are very similar. They both authenticate data transfer between the user and the applications or server.

During the establishment of an SSL/TLS session, an RSA key is used for authentication along with a symmetric key exchange. Traditionally, this one key encrypts all symmetric keys. Hopefully, you can see the weakness in this design. This one key IS KEY! If a hacker is able to access this server's private key, they can get ALL the other data and decrypt it. This is referred to as a single point of failure (SPOF).

Copyright © 2023 Cyber Innovation Center
All Rights Reserved. Not for Distribution.

Teacher Notes:

Perfect Forward Secrecy

Perfect forward secrecy refers to a piece of encryption that automatically (and frequently) changes the key it uses to encrypt and decrypt information. The purpose behind this is that if the latest key is compromised, only a small portion of the user's data will be revealed. Encryption tools using perfect forward secrecy change their keys every time a user loads or reloads an encrypted webpage. Other examples include changing keys after every message in a text-based conversation or after every phone call within an encrypted calling application. If this encryption method isn't in place, all previous data can be easily decrypted all at once.

Copyright © 2023 Cyber Innovation Center
All Rights Reserved. Not for Distribution.