Cybersecurity

Architecture and Design

2.8.4 Cryptography Modes of Operation and Blockchains

What are 3 cryptography modes of operation and what do they do?

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).

Teacher Notes:

CompTIA SY0-601 Security+ Objectives

Objective 2.8

- Summarize the basics of cryptographic concepts.
    - Modes of operation
        - Authenticated
        - Unauthenticated
        - Counter
    - Blockchain
        - Public ledgers

Cryptography Modes of Operation and Blockchains

Modes of Operation

There are two forms of authenticated modes of operations: single-sided and mutual. A mode of operation is an algorithm used with a block cipher to make an encryption algorithm. One of the most common forms of single-sided authentication occurs when someone browses a website that presents an x.509 certificate. The browser validates (or invalidates) the certificate and then you can navigate the site. Mutual authentication relies on x.509 certificates but both ways.

Regardless of the type of authenticated mode, authenticated modes of encryption validate the integrity of the ciphertext, verifying it has not been modified. Unauthenticated modes do NOT validate the integrity of the ciphertext.

Another mode is the counter mode (CTR) which changes block ciphers into stream ciphers by generating successive blocks in the stream using a nonrepeating counter.

Blockchain

The *blockchain* is a distributed and immutable public ledger. Simply put, it can store records in a way that distributes records among different systems worldwide while preventing tampering. This growing list of records, called blocks, are linked via cryptography. Every block contains a hash of the

Teacher Notes:

previous block, a timestamp, and transaction data. Because of the repetitive hashing, a blockchain is highly resistant to data alteration. Any individual change will compound quickly to a drastically different chain.