Cybersecurity

Attacks, Threats, and Vulnerabilities

1.2.16 Cryptographic Attacks

What are the different types of cryptographic attacks and how do they differ from one another?

Overview

Given a scenario, the student will analyze potential indicators to determine the type of attack.

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).

CYBER.ORG

Teacher Notes:

CompTIA SY0-601 Security+ Objectives

Objective 1.2

- Given a scenario, analyze potential indicators to determine the type of attack.
    - Cryptographic Attacks
        - Birthday
        - Collision
        - Downgrade

Cryptographic Attacks

The aim of a cryptographic attacker is to break the security of the encryption algorithm and decrypt the ciphertext (encrypted message), or even better, learn the private key. There are numerous types of attacks that have been created against numerous types of cryptosystems each with varying levels of effectiveness, difficulty, and speed. The following cryptographic attacks are popular methods.

Happy Birthday to You!

The ***Birthday*** attack is a form of cracking using collisions. The birthday attack is based on the birthday paradox (or the birthday problem), which states that the probability of two people sharing the same birthday is actually far higher than it seems. For a group of 23 people, the probability is actually just above 50%! In a similar fashion, the probability of detecting a collision among a hash function is much higher than expected. The attacker generates multiple versions of plaintext to hash and then checks for matching outputs.

Collision

A ***collision*** is when the output of a hashing algorithm (the message digest) is the same for two unique inputs. This creates a problem because hash values are supposed to be unique – different input values should never create the same output result. The intention of using a hash algorithm is to ensure the integrity of data. Collisions make it difficult for a user to be confident that data received has not been modified.

Downgrade

A ***downgrade*** attack is when a malicious actor is able to attack a system by

Teacher Notes:

using older version of software. When software is updated, vulnerabilities are patched making the newer version more secure than the older. However, if the newer versions still cooperate with older versions, they may be susceptible to an attack because of the older vulnerabilities. Thus, even if a person keeps their software up to date, they still might be at risk if that software allows backward compatibility. Always be wary of software that allows backward compatibility to help keep your system more secure.