Cybersecurity

Architecture and Design

2.8.3 Quantum Cryptography and Ephemeral Keys

How does quantum computing affect current cryptography?

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.
    - Quantum
        - Communications
        - Computing
    - Post-quantum
    - Ephemeral

Quantum Cryptography and Ephemeral Keys

A Different Kind of Quant

As technology improves, the desire (and arguably need) for quantum computing increases. To start, ***quantum*** is a physics term relating to a discrete quantity of energy proportional in magnitude to the frequency of the radiation it represents (that's a lot to process). Simply put, a quantum is the least amount of any physical entity required for an interaction.

Since so much of the computer sciences rely on physics and mathematics, we should quickly discuss quantum information science and then relate that to our field. Quantum information science is area of study relating information science to quantum effects.

Communications

Quantum communications is a specific subset of quantum information science. It is a field of applied quantum physics related to both quantum information processing and quantum teleportation. This is useful (in our field) because it helps protect information channels against eavesdropping via quantum cryptography.

Computing

Quantum computing is the next major step in computing. Quantum computing uses quantum phenomena to perform computations. These quantum phenomena include entanglement and superposition (do not

Teacher Notes:

stress on understanding these physics principles, taking one from Einstein's book, it gets spooky). If a computer performs quantum computations, it is called a quantum computer. There are current limitations (particularly time and temperature) that quantum computers should help solve that current computers currently can't within a reasonable amount of time.

Quantum and Post-quantum Cryptography

Quantum cryptography refers to the science of using quantum phenomena to perform cryptography. One of the most obvious examples is quantum key distribution. Theoretically, this provides an information secure solution to the key exchange problem. The main draw to quantum cryptography is with the fact that it can do certain tasks that are currently proven or thought to be impossible using classic cryptography.

Post-quantum cryptography refers to cryptographic algorithms thought secure against attacks orchestrated by a quantum computer. As of 2020, the fear is that the most popular public-key algorithms would be quickly cracked by a sufficient quantum computer. A quantum computer running "Shor's algorithm" would quickly dissect the integer factorization problem, the discrete logarithm problem, or the elliptic-curve discrete logarithm problem (the three problems that popular algorithms rely on). Currently, the experimental quantum computers do not have the necessary processing power to do this.

Ephemeral Keys

A cryptographic key is called ***ephemeral*** if it is generated for **each** execution of a key establishment process. The term ephemeral means lasting a very short amount of time. This is different from a ***static key***, which is expected to be used for a long amount of time. Occasionally, ephemeral keys are used more than once but only within a single session, where the sender generates one ephemeral key pair per message and private key.

Diffie-Hellman

The ***Diffie-Hellman key exchange***, published in 1976 (patented in 1977 by Witfield Diffie, Martin Hellman, and Ralph Merkle), is a popular key exchange that allows the transfer of a symmetric key over an insecure channel. It's important to understand that Diffie-Hellman is a form of asymmetric

Teacher Notes:

cryptography, not asymmetric encryption.

Diffie-Hellman key exchange is used in various ways. One application is using ***Perfect Forward Secrecy*** provided by ***Ephemeral Diffie-Hellman*** keys, EDH or DHE. When combined with elliptic curve cryptography, we get ECDHE or ECDH, ***Elliptic Curve Diffie-Hellman key exchange***.

There is a common example used when describing Diffie-Hellman (key exchange). Since this is asymmetric cryptography, we know we have a public and a private key. Alice (It's always Alice) and Bob (It's always Bob) will keep individual private keys to themselves. Both Alice and Bob have public keys as well. If Alice combines her private key with Bob's public key, she will get a symmetric key, and if Bob does the same with Alice's public key, he will get the exact same symmetric key! The symmetric keys never needed to be ***sent*** to each other – they can each be used internally to encrypt the messages being sent over an insecure channel.