Discussion-4 The goal of cryptography is to ensure the confidentiality and integrity of any information technology system

Discussion Topic:

The goal of cryptography is to ensure the confidentiality and integrity of any information technology system. Workplaces are employing more and more remote workers. How can cryptography be used to secure the lines of network communications between a remote worker and the corporate servers?

My Post:

Hello Class,

Many of the software engineering jobs are remote or partially remote; most online university jobs (e.g., CSU Global), from teaching to administration, are remote. This is also true for a good portion of office jobs in corporate businesses. This massive shift to partial to full remote work has created a need for secure servers and network systems, and cryptography is the technology that is used to protect the information shared within communications between a remote worker and corporate servers.

Cryptography addresses issues like eavesdropping and Man-in-the-Middle (MitM) attacks by providing solutions like encryption, cryptographic hashing, and Public Key Infrastructure (PKI).

Encryption is the process of converting readable data (plaintext) into an unreadable format (ciphertext) (uCertify, n.d.). Encryption provides confidentiality services by transforming plaintext into an unreadable ciphertext. Security protocols leverage encryption by using processes like asymmetric encryption (using a public/private key pair) to safely exchange a single-use symmetric key, or, for faster processing, they use a symmetric key (like AES) to encrypt the actual bulk data of the communication session.

Cryptographic hashing uses a hash function to create a unique, fixed-length "digital fingerprint" (called a message digest) of the original data (uCertify, n.d.). Cryptographic hashing provides authenticity/integrity services by comparing the received message digest with a new digest calculated from the received data. For example, if the two digests used by the sender and receiver match, the data has not been altered, verifying the integrity of the communication/data. Note that when the hash is combined with a secret key, as in a Hashed Message Authentication Code (HMAC), it authenticates the source of the message.

Public Key Infrastructure (PKI) within a server comes as a digital certificate that is generated/provided by a trusted third party called a Certificate Authority (CA), binding the server's identity to its public key (uCertify, n.d.). Note that the client operating system (e.g., your PC's OS) and browser trust a list of major CAs. Thus, PKI is used to provide authentication (Trust) services.

-Alex

References: uCertify (n.d). Lesson 7: Cryptography. *(ISC)² SSCP Certification Training Guide*. uCertify. ISBN: 976164493776.