Module 2 Glossary

New terms and their definitions: Course 5 Week 2

Advanced Encryption Standard (AES): The first and only public cipher that's approved for use with top secret information by the United States National Security Agency

Asymmetric encryption: Systems where different keys are used to encrypt and decrypt

Authentication: A crucial application for cryptographic hash functions

Block ciphers: The cipher takes data in, places that into a bucket or block of data that's a fixed size, then encodes that entire block as one unit

CA (Certificate authority): It's the entity that's responsible for storing, issuing, and signing certificates. It's a crucial component of the PKI system

Caesar cipher: A substitution alphabet, where you replace characters in the alphabet with others usually by shifting or rotating the alphabet, a set of numbers or characters

CBC-MAC (Cipher block chaining message authentication codes): A mechanism for building MACs using block ciphers

Central repository: It is needed to securely store and index keys and a certificate management system of some sort makes managing access to storage certificates and issuance of certificates easier

Certificate fingerprints: These are just hash digests of the whole certificate, and aren't actually fields in the certificate itself, but are computed by clients when validating or inspecting certificates

Certificate Revocation List (CRL): A means to distribute a list of certificates that are no longer valid

Certificate Signature Algorithm: This field indicates what public key algorithm is used for the public key and what hashing algorithm is used to sign the certificate

Certificate-based authentication: It is the most secure option, but it requires more support and management overhead since every client must have a certificate

Certificate Signature Value: The digital signature data itself

CMACs (Cipher-based Message Authentication Codes): The process is similar to HMAC, but instead of using a hashing function to produce a digest, a symmetric cipher with a shared keys used to encrypt the message and the resulting output is used as the MAC

Code signing certificates: It is used for signing executable programs and allows users of these signed applications to verify the signatures and ensure that the application was not tampered with

Cryptanalysis: Looking for hidden messages or trying to decipher coded message

Cryptography: The overarching discipline that covers the practice of coding and hiding messages from third parties

Cryptology: The study of cryptography

Cryptosystem: A collection of algorithms for key generation and encryption and decryption operations that comprise a cryptographic service

Cryptographic hashing: It is distinctly different from encryption because cryptographic hash functions should be one directional

Data binding and sealing: It involves using the secret key to derive a unique key that's then used for encryption of data

Decryption: The reverse process from encryption; taking the garbled output and transforming it back into the readable plain text

DES (Data Encryption Standard): One of the earliest encryption standards

Deterministic: It means that the same input value should always return the same hash value

DH (Diffie-Hellman): A popular key exchange algorithm, named for its co-inventors

DSA (Digital Signature Algorithm): It is another example of an asymmetric encryption system, though its used for signing and verifying data

ECDH & ECDSA: Elliptic curve variants of Diffie-Hellman and DSA, respectively

Elliptic curve cryptography (ECC): A public key encryption system that uses the algebraic structure of elliptic curves over finite fields to generate secure keys

Encapsulating security payload: It's a part of the IPsec suite of protocols, which encapsulates IP packets, providing confidentiality, integrity, and authentication of the packets

Encryption: The act of taking a message (plaintext), and applying an operation to it (cipher), so that you receive a garbled, unreadable message as the output (ciphertext)

Encryption algorithm: The underlying logic or process that's used to convert the plaintext into ciphertext

End-entity (leaf certificate): A certificate that has no authority as a CA

Entropy pool: A source of random data to help seed random number generators

FIPS (Federal Information Processing Standard): The DES that was adopted as a federal standard for encrypting and securing government data

Forward secrecy: This is a property of a cryptographic system so that even in the event that the private key is compromised, the session keys are still safe

Frequency analysis: The practice of studying the frequency with which letters appear in ciphertext

Full disk encryption (FDE): It is the practice of encrypting the entire drive in the system

Hash collisions: Two different inputs mapping to the same output

Hashing (Hash function): A type of function or operation that takes in an arbitrary data input and maps it to an output of a fixed size, called a hash or a digest

HMAC (Keyed-Hash Message Authentication Codes): It uses a cryptographic hash function along with a secret key to generate a MAC

HTTPS: Hypertext Transfer Protocol Secure is a secure version of HTTP that ensures the communication your web browser has with the website is secured through encryption

Intermediary (subordinate) CA: It means that the entity that this certificate was issued to can now sign other certificates

IPsec (Internet Protocol security): A VPN protocol that was designed in conjunction with IPv6

Issuer Name: This field contains information about the authority that signed the certificate

Kerckhoff's principle: A principle that states that a cryptosystem, or a collection of algorithms for key generation and encryption and decryption operations that comprise a cryptographic service should remain secure, even if everything about the system is known except for the key

Key: A crucial component of a cipher, which introduces something unique into your cipher

Key length: It defines the maximum potential strength of the system

Key signing parties: Organized by people who are interested in establishing a web of trust, and participants perform the same verification and signing

Key size: It is the total number of bits or data that comprises the encryption key

L2TP (Layer 2 Tunneling Protocol): It is typically used to support VPNs

MACs (Message Authentication Codes): A bit of information that allows authentication of a received message, ensuring that the message came from the alleged sender and not a third party masquerading as them

MD5: A popular and widely used hash function designed in the early 1990s as a cryptographic hashing function

MIC (Message Integrity Check): It is essentially a hash digest of the message in question

NIST: National Institute of Standards and Technology

Password salt: Additional randomized data that's added into the hashing function to generate the hash that's unique to the password and salt combination

PGP (Pretty Good Privacy) encryption: An encryption application that allows authentication of data along with privacy from third parties relying upon asymmetric encryption to achieve this

PKI system: A system that defines the creation, storage and distribution of digital certificates

Pseudo-random: Something that isn't truly random

Public key authentication: A key pair is generated by the user who wants to authenticate

Public key signatures: Digital signature generated by composing the message and combining it with the private key

RA (Registration Authority): It is responsible for verifying the identities of any entities requesting certificates to be signed and stored with the CA

Rainbow table attacks: To trade computational power for disk space by pre-computing the hashes and storing them in a table

Rainbow tables: A pre-computed table of all possible password values and their corresponding hashes

Random numbers: A very important concept in encryption because it avoids some kind of pattern that an adversary can discover through close observation and analysis of encrypted messages over time

RC4 (Rivest Cipher 4): Asymmetric stream cipher that gained widespread adoption because of its simplicity and speed

Remote attestation: The idea of a system authenticating its software and hardware configuration to a remote system

Root certificate authority: They are self signed because they are the start of the chain of trust, so there's no higher authority that can sign on their behalf

RSA: One of the first practical asymmetric cryptography systems to be developed, named for the initials of the three co-inventors: Ron Rivest, Adi Shamir and Leonard Adleman

Secure channel: It is provided by IPsec, which provides confidentiality, integrity, and authentication of data being passed

Secure element: It's a tamper resistant chip often embedded in the microprocessor or integrated into the mainboard of a mobile device

Secure Shell (SSH): A secure network protocol that uses encryption to allow access to a network service over unsecured networks

Security through obscurity: The principle that if no one knows what algorithm is being used or general security practices, then one is safe from attackers

Self-signed certificate: This certificate has been signed by the same entity that issued the certificate

Serial number: A unique identifier for their certificate assigned by the CA which allows the CA to manage and identify individual certificates

Session key: The shared symmetric encryption key using TLS sessions to encrypt data being sent back and forth

SHA1: It is part of the secure hash algorithm suite of functions, designed by the NSA and published in 1995

Shannon's maxim: It states that the system should remain secure, even if your adversary knows exactly what kind of encryption systems you're employing, as long as your keys remain secure

SSL 3.0: The latest revision of SSL that was deprecated in 2015

SSL/TLS Client Certificate: Certificates that are bound to clients and are used to authenticate the client to the server, allowing access control to a SSL/TLS service

SSL/TLS Server Certificate: A certificate that a web server presents to a client as part of the initial secure setup of an SSL, TLS connection

Steganography: The practice of hiding information from observers, but not encoding it

Stream ciphers: It takes a stream of input and encrypts the stream one character or one digit at a time, outputting one encrypted character or digit at a time

Subject: This field contains identifying information about the entity the certificate was issued to

Subject Public Key Info: These two subfields define the algorithm of the public key along with the public key itself

Substitution cipher: An encryption mechanism that replaces parts of your plaintext with ciphertext

Symmetric key algorithm: Encryption algorithms that use the same key to encrypt and decrypt messages

TLS 1.2: The current recommended revision of SSL

TLS 1.2 with AES GCM: A specific mode of operation for the AES block cipher that essentially turns it into a stream cipher

TLS Handshake: A mechanism to initially establish a channel for an application to communicate with a service

TPM (Trusted Platform Module): This is a hardware device that's typically integrated into the hardware of a computer, that's a dedicated crypto processor

Transport mode: One of the two modes of operations supported by IPsec. When used, only the payload of the IP packet is encrypted, leaving the IP headers untouched

Trusted execution environment (TEE): It provides a full-blown isolated execution environment that runs alongside the main OS

Tunnel: It is provided by L2TP, which permits the passing of unmodified packets from one network to another

Tunnel mode: One of the two modes of operations supported by IPsec. When used, the entire IP packet, header, payload, and all, is encrypted and encapsulated inside a new IP packet with new headers

Username and password authentication: Can be used in conjunction with certificate authentication, providing additional layers of security

Validity: This field contains two subfields, Not Before and Not After, which define the dates when the certificate is valid for

Version: What version of the X.509 standard certificate adheres to

VPN (Virtual Private Network): A secure method of connecting a device to a private network over the internet

Web of trust: It is where individuals instead of certificate authorities sign other individuals' public keys

X.509 standard: It is what defines the format of digital certificates, as well as a certificate revocation list or CRL

Terms and their definitions from previous weeks

A

Adware: Software that displays advertisements and collects data

Attack: An actual attempt at causing harm to a system

Availability: Means that the information we have is readily accessible to those people that should have it

B

Backdoor: A way to get into a system if the other methods to get in a system aren't allowed, it's a secret entryway for attackers

Baiting: An attack that happens through actual physical contact, enticing a victim to do something

Botnet: A collection of one or more Bots

Bots: Machines compromised by malware that are utilized to perform tasks centrally controlled by an attacker

Brute force attacks: A common password attack which consists of just continuously trying different combinations of characters and letters until one gets access

C

CIA Triad: Confidentiality, integrity, and availability. Three key principles of a guiding model for designing information security policies

Confidentiality: Keeping things hidden

Cross-site scripting (XSS): A type of injection attack where the attacker can insert malicious code and target the user of the service

D

Denial-of-Service (DoS) attack: An attack that tries to prevent access to a service for legitimate users by overwhelming the network or server

Dictionary attack: A type of password attack that tries out words that are commonly used in passwords, like password, monkey, football

Distributed Denial-of-Service (DDoS) attack: A DoS attack using multiple systems

DNS Cache Poisoning Attack: It works by tricking a DNS server into accepting a fake DNS record that will point you to a compromised DNS server

E

Evil twin: The premise of an evil twin attack is for you to connect to a network that is identical to yours but that is controlled by an attacker. Once connected to it, they will be able to monitor your traffic

Exploit: Software that is used to take advantage of a security bug or vulnerability

H

Hacker: Someone who attempts to break into or exploit a system

Half-open attacks: A way to refer to SYN floods

I

Injection attacks: A common security exploit that can occur in software development and runs rampant on the web, where an attacker injects malicious code

Integrity: Means keeping our data accurate and untampered with

K

Keylogger: A common type of spyware that's used to record every keystroke you make

L

Logic bomb: A type of Malware that's intentionally installed

M

Malware: A type of malicious software that can be used to obtain your sensitive information or delete or modify files

Meddler in the middle (formerly known as Man in the Middle): An attack that places the attacker in the middle of two hosts that think they're communicating directly with each other

P

Password attacks: Utilize software like password crackers that try and guess your password

Phishing attack: It usually occurs when a malicious email is sent to a victim disguised as something legitimate

Ping flood: It sends tons of ping packets to a system. If a computer can't keep up with this, then it's prone to being overwhelmed and taken down

R

Ransomware: A type of attack that holds your data or system hostage until you pay some sort of ransom

Risk: The possibility of suffering a loss in the event of an attack on the system

Rogue Access Point (AP) Attack: An access point that is installed on the network without the network administrator's knowledge

Rootkit: A collection of software or tools that an admin would use

S

Screen lock: A security feature that helps prevent unwanted access by creating an action you have to do to gain entry

Session hijacking (cookie hijacking): A common meddler in the middle attack

Social engineering: An attack method that relies heavily on interactions with humans instead of computers

Spear phishing: Phishing that targets individual or group - the fake emails may contain some personal information like your name, or the names of friends or family

Spoofing: When a source is masquerading around as something else

Spyware: The type of malware that's meant to spy on you

SQL injection Attack: An attack that targets the entire website if the website is using a SQL database

SYN flood: The server is bombarded with SYN packets

T

Tailgating: Gaining access into a restricted area or building by following a real employee in

Threat: The possibility of danger that could exploit a vulnerability

Trojan: Malware that disguises itself as one thing but does something else

V

Viruses: The best known type of malware

Vulnerability: A flaw in the system that could be exploited to compromise the system

W

Worms: They are similar to viruses except that instead of having to attach themselves onto something to spread, worms can live on their own and spread through channels like the network

Z

0-Day Vulnerability (Zero Day): A vulnerability that is not known to the software developer or vendor, but is known to an attacker

Mark as completed

Like **Dislike** **Report an issue**