UNIT IV

TECHNICAL SECURITY

Cryptographic Techniques-Threat and Incident Management

CRYPTOGRAPHIC TECHNIQUES

Cryptographic techniques concern themselves with three basic purposes: **Authentication Verifying the identity of a user or computer**. Confidentiality Keeping the contents of the datasecret. Integrity Ensuring that data doesn't change between the time it leaves the source and thetime it reaches its destination.

Three types of cryptographic techniques used in general.

- Symmetric-key cryptography.
- The **security token** or the authentication Hash functions.
- Public-key cryptography.

Token is the one that is considered as the cryptography tool. Using the security token, one can authenticate the user.It is also used to provide statefulness to the HTTP protocol. The security token has to be encrypted to allow the secure exchange of data

Need Data Encryption?

If anyone wonders why organizations need to practice encryption, keep these four reasonsin mind:

- **Authentication:** Public key encryption proves that a website's origin server owns theprivate key and thus was legitimately assigned an SSL certificate. In a world where so many fraudulent websites exist, this is an important feature.
- **Privacy:** Encryption guarantees that no one can read messages or access data except the legitimate recipient or data owner. This measure prevents cybercriminals, hackers, internet service providers, spammers, and even government institutions from accessingand reading personal data.
- **Regulatory Compliance:** Many industries and government departments have rules inplace that require organizations that work with users' personal information to keep that data encrypted. A sampling of regulatory and compliance standards that enforce encryption include HIPAA, PCI-DSS, and the GDPR.
- **Security:** Encryption helps protect information from data breaches, whether the data isat rest or in transit. For example, even if a corporate-owned device is misplaced or stolen, the data stored on it will most likely be secure if the hard drive is properly encrypted. Encryption also helps protect data against malicious

activities like man-in- the-middle attacks, and lets parties communicate without the fear of data leaks.

Let us now find out the important types of data encryption

methods.

The Three Important Types of Data Encryption

Techniques Hashing

Hashing generates a unique signature of fixed length for a data set or message. Each specific message has its unique hash, making minor changes to the information easily trackable. Data encrypted with hashing cannot be deciphered or reversed back into its original form. That's whyhashing is used only as a method of verifying data.

Specific Encryption Algorithms

There's a host of different encryption algorithms available today. Here are five of the more common ones.

- **AES.** The Advanced Encryption Standard (AES) is the trusted standard algorithm used by the United States government, as well as other organizations. Although extremely efficient in the 128-bit form, AES also uses 192- and 256-bit keys for verydemanding encryption purposes. AES is widely considered invulnerable to all attacksexcept for brute force.
.
- **Triple DES.** Triple DES is the successor to the original Data Encryption Standard (DES)algorithm, created in response to hackers who figured out how to breach TripleDES applies the DES algorithm three times to every data block and is commonly used to encrypt UNIX passwords and ATM PINs.

- **RSA.** RSA is a public-key encryption asymmetric algorithm and the standard for encrypting information transmitted via the internet. RSA encryption is robust and reliable because it creates a massive bunch of gibberish that frustrates would-be hackers,causing them to expend a lot of time and energy to crack into systems.

- **Blowfish.** Blowfish is another algorithm that was designed to replace DES. This symmetric tool breaks messages into 64-bit blocks and encrypts them individually.Blowfish has established a reputation for speed, flexibility, and is unbreakable.

- **Twofish.** Twofish is Blowfish's successor. It's license-free, symmetric encryption that deciphers 128-bit data blocks. Additionally, Twofish always encrypts data in 16 rounds,no matter what the key size. Twofish is perfect for both software and hardware environments and is considered one of the fastest of its type.

- **Rivest-Shamir-Adleman (RSA).** Rivest-Shamir-Adleman is an asymmetric encryptionalgorithm that works off the factorization of the product of two large prime numbers. Only a user with knowledge of these two numbers can decode the message successfully.Digital signatures commonly use RSA, but the algorithm slows down when it encrypts large volumes of data.

THREATS AND INCIDENT MANAGEMENT:

Threat management is a process used by cyber security professionals to prevent cyber attacks,detect cyber threats and respond to security incident.

Some cyber security threats are ,

Cybersecurity threats are acts performed by individuals with harmful intent, whose goal is tosteal data, cause damage to or disrupt computing systems.

Threats can be classified according to their type and origin:[13]

- Types of threats:
  - Physical damage: fire, water, pollution
  - Natural events: climatic, seismic, volcanic
  - Loss of essential services: electrical power, air conditioning, telecommunication
  - Compromise of information: eavesdropping, theft of media, retrieval ofdiscarded materials
  - Technical failures: equipment, software, capacity saturation,
  - Compromise of functions: error in use, abuse of rights,

denial ofactions **A threat type can have multiple origins:**

- Deliberate: aiming at information asset
  - spying
  - illegal processing of data
- Accidental
  - equipment failure
  - software failure
- Environmental
  - natural event
  - loss of power supply
- Negligence: Known but neglected factors, compromising the network safetyand sustainability

Threat classification

The threat classification called STRIDE, as follows

- **S**poofing of user identity
- **T**ampering
- **R**epudiation
- **I**nformation disclosure
- **D**enial of Service (D.o.S.)
- **E**levation of privilege

The security threats have five categories in a classification called DREAD.,

- **D**amage – how bad would an attack be?
- **R**eproducibility – how easy it is to reproduce the attack?
- **E**xploitability – how much work is it to launch the attack?
- **A**ffected users – how many people will be impacted?
- **D**iscoverability – how easy it is to discover the threat?

Few concepts under threat management includes,

Threat action, Threat analysis, Threat consequence. **Threat action** an assault on system security.

Threat analysis is the analysis of the probability of occurrences and consequences of damagingactions to a system.

Threat consequence is a security violation that results from a threat action.[1] Includes **disclosure, deception, disruption, and usurpation.**

Example:

Threat actions that are accidental events are marked by "*"."Unauthorized disclosure" (a threat consequence)

"Human error"

Human action or inaction that unintentionally results in an entity gainingunauthorized knowledge of sensitive data.

* "Hardware/software error"

System failure that results in an entity gaining unauthorized knowledge of sensitive data.

"Traffic analysis"

Gaining knowledge of data by observing the characteristics of communications that carrythe data.

"Signals analysis"

Threat landscape or environment

A collection of threats in a particular domain or context, with information on identifiedvulnerable assets, threats, risks, threat actors and observed trends.

Threat management

Threats should be managed by operating an ISMS, performing all the IT riskmanagement activities foreseen by laws, standards and methodologies.

Very large organizations tend to adopt business continuity management plans in order to protect,maintain and recover business-critical processes and systems. Some of these plans foreseen to set up **computer security incident response team** (CSIRT) or **computer emergency responseteam** (CERT)

There is some kind of verification of the threat management process:

- Information security audit
- Penetration test

Most organizations perform a subset of these steps, adopting countermeasures based on a non-systematic approach: computer insecurity studies the battlefield of computer security exploits and defences that results.

Cyber threat management

- Cyber threat management (CTM) is the process of identifying, analyzing, evaluating andaddressing an organization's cyber security requirements.

- It enables early identification of threats, data- driven situational awareness, accuratedecision-making, and timely threat mitigating actions.

CTM includes:

- Manual and automated intelligence gathering and threat analytics.
- Comprehensive methodology for real-time monitoring including advancedtechniques.
- Use of advanced analytics to optimize intelligence, generate security intelligence,and provide Situational Awareness.
- Technology and skilled people leveraging situational awareness to enable rapid decisionsand automated or manual actions