Network Security Common Attack Types

Target Course

Networks

Learning Goals

A student shall be able to:

1. Describe security design principles and identify security issues associated with common threats and attacks.

IAS Outcomes

IAS Knowledge Topic	Outcome
Cryptography	4. Explain how public key infrastructure supports digital signing and encryption and discuss the limitations/vulnerabilities. [Familiarity]
Network Security	1. Describe the different categories of network threats and attacks. [Familiarity]
Threats and Attacks	1. Describe likely attacker types against a particular system. [Familiarity] 3. Identify instances of social engineering attacks and Denial of Service attacks. [Familiarity] 4. Discuss how Denial of Service attacks can be identified and mitigated. [Familiarity] 6. Discuss the concepts of covert channels and other data leakage procedures. [Familiarity]

Dependencies

- Cover after the ***Network Security Overview*** module.
- We covered this material before going into details on any of the network layers. We also highlighted some of the risks and attack types while covering each network layer.

Summary

Introduce common network attack types.

Estimated Time

This module took approximately 45 lecture minutes to cover.

Materials

What are the common types of threats and attacks on a computer system?

According to [1], the types of threats and attacks include:

- Eavesdropping – intercepting information that is in transit and intended for someone else.
- Alteration – unauthorized modification of information (in transit or at rest).
- Denial-of-service – the interruption or degradation of an information service.
- Masquerading – fabrication of information that is alleged to be from someone, but the information is not from the supposed author.
- Repudiation – someone denies that they performed an action or obtained information.
- Correlation and traceback – integrating information from multiple sources to determine the source of a particular piece of information; this is an attack on anonymity.
- Man-in-the-middle attack – intercepting and altering information that is in transit, resulting in the sender and receiver receiving modified data.
- Brute-force decryption attack – someone uses each possible decryption key value and then tries to determine which of the resulting plaintext is the one that was encrypted.

- Dictionary attack – try each word in a dictionary to attempt to break into a password-protected entity.
- Social engineering – a broad category of attacks that involve trickery to obtain data or access to a service. These types of attacks include: pretexting (someone masquerades as someone else to obtain the credentials e.g., password of the victim); baiting (use a "gift" to encourage someone to install malware); and quid pro quo (the malicious actor offers something to the victim and then tries to get the victim to "return the favor" by sharing their information with the malicious actor).
- Vulnerabilities in software code – some software vulnerabilities may be known privately (i.e., not by the software vendor), when this vulnerability is used it is called a zero-day attack. Other software vulnerabilities may be known by the software vendor but have not yet been fixed or have been fixed but may not have been updated at each site that uses the software.

According to [2], the types of threats and attacks include:

- Worms – a piece of malware (i.e., malicious software) that will replicate itself to have it spread across a network to other hosts.
- Denial-of-service in VoIP – a flood of SIP (Session Initiation Protocol) traffic registration requests are made which slows down the services ability to respond to valid requests.
- Spoofing web services – a malicious actor develops software that acts like a real web service, providing fake responses to valid requests.

According to [3], the types of threats and attacks include:

- Attacks based on psychology – examples are pretexting (described above) and phishing.
- Social engineering attacks – described above.

Are there other types of attacks?

- Side channel attacks – these attacks take advantage of information obtained through physical devices. For example, a CPU performing a cryptographic algorithm will likely consume more power and produce more heat. These physical characteristics may be used to identify the type of algorithm being used, the key length, or other information that may weaken the use of cryptography.
- Covert channel attacks – these attacks use command and control information flowing through a network to ascertain what the network is doing. An example is the phone phreaking that was done in landline phones by mimicking the tones used to make long-distance phone calls.

What are the limitations and vulnerabilities associated with using public key cryptography?

- Speed. Asymmetric cryptography is significantly slower than symmetric cryptography. When a large volume of data or high rate of transactions need to be encrypted/decrypted, using a single secret key will be much faster than using a public-private key pair.
- Use of a certificate authority (CA). A CA is used to certify that a public key is owned by a particular organization. When a CA gets compromised, the digital certificates provided by the CA can be spoofed, convincing an organization to send their data to a malicious actor.

Assessment Methods

None used.

References

[1] M.T. Goodrich & R. Tamassia, (2011). *Introduction to Computer Security*. Addison Wesley.

[2] E.B. Fernandez, (2013). *Security Patterns in Practice: Designing Software Architectures Using Software Patterns*. Wiley.

[3] R. Anderson, (2008). *Security Engineering, Second Edition*. Wiley.