Security Threats and Attacks

Group 1:
Tirth Kamlesh Kothari, Matthew Harper, Anirudh Sunil

There are a number of considerations that are necessary when implementing any system in a secure manner. There are even more when this system is communicating over an insecure medium such as the internet or with any wireless system. There are a number of attacks that we can consider, both those that are realistic, which we can counter, and those that are more out there that we may not be able to counter.

Network Attacks on an Insecure Implementation (realistic):

Sniffing Attacks: For systems that communicate over a potentially insecure network, this can be a surprisingly common issue. If weak cryptographic methods (DES, MD5, RSA 512), weak and flawed systems (WEP…), or the use of unencrypted protocols (Telnet, HTTP). As we are **implementing** the system we are primarily concerned with **unencrypted communications** and **weak cryptographic methods** being used to ascertain privileged information. This could be done using tools like Wireshark, TCPDump, or more complicated attacks on the system affecting routing (ARP poisoning, DNS cache poisoning etc.) so they can directly receive our packets.

Replay Attacks: We are concerned that registration, ping, pong, and any later packets can be replayed to compromise the system or gather information on the overlay network. If an advisory can replay registration packets, it may be possible to clutter the system and lead to an unintended number of pings affecting the system

Reflection Attacks: Depending on the scheme that is implemented - Primarily with challenge-response-based methods we may be concerned with attacks that force another entity to solve the authentication challenge. This is done by making the entity (server in most cases) solve its own challenge, which can then be used in another ongoing connection.

Impersonation Attacks: Additional concerns are related to the server or other client devices being impersonated. If the server is impersonated (or compromised…) the attacker can do whatever they would like with clients, giving them faulty information on where packets should be sent, and if were able to control the clients in some way - change their behavior (This is in a more general sense). If clients are impersonated, attackers can be disruptive and have a method of gaining additional information or access to the system (possible avenue of lateral movement)

Man in the Middle (MITM): This is essentially a more advanced form of Impersonation. We are concerned that an advisory can “sit” in the middle of a connection analyzing packets; the information contained within then the attacker can choose to change the message, drop the messages, and of course, save sensitive information. All done without the two communicating parties knowing a third (or more) party is also included

Denial of Service (DoS) and Distributed Denial of Service (DDoS): Like most services exposed to a network, and possibly the wider internet as a whole, we are concerned that an advisory is able to consume resources, or communicate with the server in some way (send specially formed packets) which

would prevent it from responding to benign or normal clients. This could be done by crashing the server with a specific input, consuming resources by making connections (and not closing them), crashing the host system (Syn Flood, Botnet, etc.…) to name a few.

Key management attacks :

These attacks involve compromising the security of the key management process, such as improper key generation, storage, or distribution. For example, if the private key is not properly protected or stored securely, it could be stolen or compromised, allowing an attacker to decrypt the encrypted messages.

There are various ways to give this type of attacks a chance to break in, some of them are as mentioned:

-Weak keys
-Incorrect use of keys
-Re-use of keys
-Non-rotation of keys
-Insecure movement of keys, and many more.

Race conditions:
This is basically the situation when the device or system tries or makes an attempt to perform two or more operations at the same time. In other words, this condition is executed when multiple requests are sent in a small time frame.

Perfect Forward Secrecy:
Users of an application may be concerned that all messages, or at least those after a given point, can be compromised when a key from a previous message is compromised. This is the lack of Perfect forward secrecy that is often achieved using some form of Diffie Hellman.

Injection/Overflow Attacks:
This is the use of specially crafted packets to alter the behavior of a system in unintended ways, leading to the leakage of data/information or remote execution of code.

Attacks on an Insecure Implementation (Outlandish):

Side Channel Attacks: This is the use of other methods such as emissions and electrical usage through electron microscopes or other attacks to determine the characteristics and possibly keys (or some bits of) the keys used by the system.

Root Kit/Malware: Rootkits and malware are not the same, the main difference is the malware is located in the userspace of the system, and the rootkit is in the kernel space of the system. When either is operating within a system, you can no longer trust (especially in the case of rootkits) what the system tells you. They can

Justin Marwad:
He is… um… scary?