Computer Security

2024-2025

Threats, exploits and attacks

A *threat* is any potential violation of security that could cause harm to the asset. It may be a person, an insecure service or some unacknowledged piece of information, service or system.

An *exploit* is any software or tool used to take advantage of vulnerabilities.

An *attack* is any intentional or unintentional event that harms, or tries to harm, an asset.

CVE (Common Vulnerability and Exposure).

Untargeted threats: worms and other malware trying to access any computer they find on the net. *Targeted attacks*: deliberate attack on a single, specific machine.

Bot network: network of hacked machines, owned by unknowing individuals but controlled by a single hacker, used for malevolent purposes such as DDoS attacks. Most common in the US where static IPv4 addresses are the norm. To mitigate this issue, ISPs try to identify both the single machines (by cutting off their connection and notifying the owners) and the control systems (to shut them down).

APT (Advanced Persistent Threat): a persistent, patient and well-prepared enemy that is constantly looking for a way to harm a specific asset. It can cause a high emotional impact. An APT may infiltrate, wait patiently while gathering information in the most discrete way possible, and finally unleash an attack only when fully ready.

Building a system that handles complexity in a simple way, and that is also safe, is a hard task. As the system grows in complexity, the amount of components that cannot be fully trusted increases, along with the necessity of redundancy to maintain it reliable.

A *risk* is the product of the probability of a threat of taking advantage of a vulnerability, multiplied by the size of the potential damage.

The value assessment of assets may be asymmetrical (for example, personal data is highly valuable to the owner and of very little value to attackers, except for ransom) or symmetrical (money is equally valuable to both the thief and the victim).

Insecure applications on the asset, conflicting security policies and insecurely configured systems enlarge the exposed surface. Having a myriad of internet-connected devices around us all day also enlarges the exposed surface. To solve this, strong authentication is needed on both sides, services and users. Authorization and access control systems need to be reliable. Abuse control (detection of suspicious activity) must be effective. Protocols, OSs and applications need to have a secure design. The implementations need a bug-free implementation. Security policies must be perfect. Users need to be "perfect" as in not falling for simple attacks.

IDS: Intrusion Detection System, log-based abuse control. Machine learning algorithms are beginning to be used for log checking, for their ability to detect patterns and discern normal patterns from malicious patterns.

In the real world, effective security protections are not deployed. Patches are not applied in a timely manner. Websites do not properly monitor and restrict access to their internal hosts and resources. Organizations do not allocate enough resources and manpower to security tasks. Users are uneducated about security issues. Sites do not implement the policies they define, if they even have any.

Absolute security does not exist. It is a tradeoff between functionality, security and usability. Rather than reducing attacks, it is more advisable to reduce their rate of success and limit the scope of their potential damage. An excess of security reduces the usability and performance of the system. Security has a cost and so does the lack of it.

Minimum viable security: intersection between what customers will buy and what the security team demands.

Non-technological security: logical security (access control), organizational security (assignment of critical roles), physical security (guards, locks, surveillance over the physical infrastructure).