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).

Replacement cypher (monoalphabetic substitution)

Substitute each letter with another letter. Fixed cipher, each encrypted letter always corresponds univocally to the same unencrypted letter.

Brute force cipher breaking is highly complex, however:

- letters change their individual identity but not their groupings
- the cipher can be broken by matching the relative frequency of letters with the ones in the unencrypted alphabet

Nulls

Using least frequent symbols in positions that do not alter the meaning, e.g. instead of spaces. The symbol itself can be called through some sort of escape sequence, like repeating it twice.

Homophones

Use of a sequence of several symbols to substitute singular frequent characters. This changes the distribution of symbols to make it less recognizable.

Code words

Whole word substitution. The code word needs to be diffused along with the message, which might fall into the attacker's hands. No significant increase of protection over monoalphabetic substitution.

More complex approaches

Two possible lines:

- multiple encrypting alphabets
  - Leon Battista Alberti
  - Vigenère (predecessor of modern encryption)
- encryption of multiple letters as a unit
  - Porta
  - Playfair

Alberti cypher disk

Uses a rotating disk with letters both inside and outside the disk. Rotating the inner disk changes the cipher. For example, two different ciphers may be alternated for even and odd letters.

Porta cipher

It encrypts letters in pairs through a 26×26 encryption matrix that assigns each pair to its cell number. The key can be changed by changing the cipher numbers (even by substituting them with symbols) or the letters on row and column headers.

Vigenère cipher

Treat letters as numbers and sum them the cipher, mod 26.

If the key has t letters, the text will be stripped from blank spaces and broken up into groups of t letters. After that, each letter will be summed (mod 26) to the corresponding letter in the key.

It was considered unbreakable for a long time. The possible keys are 26^t where t is the key size.

It's resistant to frequency analysis. Babbage and Kasiski realized that the length of the key can be deduced from repeating letters.

Grids

Girolamo Cardano. Even-sized grid with holes in certain points. By alternatively rotating the grid in its four possible positions, the message can be read.

Playfair cipher

5×5 matrix, with the key at the beginning and the rest of the alphabet, in order, following it. It considers letters in pairs. Digrams with repeating letters add an "X" in between. Each digram marks the vertices of the diagonal of a rectangle on the matrix. The digram gets substituted by choosing the letters on the other diagonal.

It's better than a monoalphabetic cipher but easy to break using digram frequency analysis.

One-time pad (Vernam Cipher)

Perfect cipher: the encrypted and unencrypted messages are independent. The key is a set of n random independent binary bits, that are XOR-ed with the message itself, also n-sized.