Computer security software

Computer security software or **cybersecurity software** is any computer program designed to influence information security. This is often taken in the context of defending computer systems or data, yet can incorporate programs designed specifically for subverting computer systems due to their significant overlap, and the adage that the best defense is a good offense.

The defense of computers against intrusion and unauthorized use of resources is called *computer security*. Similarly, the defense of computer networks is called *network security*.

The subversion of computers or their unauthorized use is referred to using the terms *cyberwarfare*, *cybercrime*, or *security hacking* (later shortened to *hacking* for further references in this article due to issues with *hacker*, *hacker culture* and differences in white/grey/black 'hat' color identification).

Types

Below, various software implementations of Cybersecurity patterns and groups outlining ways a host system attempts to secure itself and its assets from malicious interactions, this includes tools to deter both passive and active security threats. Although both security and usability are desired, today it is widely considered in computer security software that with higher security comes decreased usability, and with higher usability comes decreased security.[1]

Prevent access

The primary purpose of these types of systems is to restrict and often to completely prevent access to computers or data except to a very limited set of users. The theory is often that if a key, credential, or token is unavailable then access should be impossible. This often involves taking valuable information and then either reducing it to apparent noise or hiding it within another source of information in such a way that it is unrecoverable.

- Cryptography and Encryption software
- Steganography and Steganography tools

A critical tool used in developing software that prevents malicious access is *Threat Modeling*.[2] Threat modeling is the process of creating and applying mock situations where an attacker could be trying to maliciously access data in cyberspace. By doing this, various profiles of potential attackers are created, including their intentions, and a catalog of potential vulnerabilities are created for the respective organization to fix before a real threat arises.[3] Threat modeling covers a wide aspect of cyberspace, including devices, applications, systems, networks, or enterprises. Cyber threat modeling can inform organizations with their efforts pertaining to cybersecurity in the following ways:[4]

- Risk Management
- Profiling of current cybersecurity applications
- Considerations for future security implementations

Regulate access

The purpose of these types of systems is usually to restrict access to computers or data while still allowing interaction. Often this involves monitoring or checking credential, separating systems from access and view based on importance, and quarantining or isolating perceived dangers. A physical comparison is often made to a shield. A form of protection whose use is heavily dependent on the system owners preferences and perceived threats. Large numbers of users may be allowed relatively low-level access with limited security checks, yet significant opposition will then be applied toward users attempting to move toward critical areas.

- Access control
- Firewall
- Sandbox

Monitor access

The purpose of these types of software systems is to monitor access to computers systems and data while reporting or logging the behavior. Often this is composed of large quantities of low priority data records / logs, coupled with high priority notices for unusual or suspicious behavior.

- Diagnostic program
- Intrusion detection system (IDS)
- Intrusion prevention system (IPS)
- Log management software
- Records Management
- Security information management
- Security event management
- Security information and event management (SIEM)

Surveillance monitor

These programs use algorithms either stolen from, or provided by, the police and military internet observation organizations to provide the equivalent of a police Radio scanner. Most of these systems are born out of mass surveillance concepts for internet traffic, cell phone communication, and physical systems like CCTV. In a global perspective they are related to the fields of SIGINT and ELINT and approach GEOINT in the global information monitoring perspective. Several instant messaging programs such as ICQ (founded by "former" members of Unit 8200), or WeChat and QQ (rumored 3PLA/4PLA connections[5][6]) may represent extensions of these observation apparati.

Block or remove malware

The purpose of these types of software is to remove malicious or harmful forms of software that may compromise the security of a computer system. These types of software are often closely linked with software for computer regulation and monitoring. A physical comparison to a doctor, scrubbing, or cleaning ideas is often made, usually with an "anti-" style naming scheme related to a particular threat type. Threats and unusual behavior are identified by a system such as a firewall or an intrusion detection system, and then the following types of software are used

to remove them. These types of software often require extensive research into their potential foes to achieve complete success, similar to the way that complete eradication of bacteria or viral threats does in the physical world. Occasionally this also represents defeating an attackers encryption, such as in the case of data tracing, or hardened threat removal.

- Anti-keyloggers
- Anti-malware
- Anti-spyware
- Anti-subversion software
- Anti-tamper software
- Antivirus software

See also

- Computer security
- Data security
- Emergency management software
- Cloud Workload Protection Platforms
- Computer Antivirus Software

References

1. *Barragán, Claudio Casado (2017). Information Technology - New Generations. Springer International Publishing. pp. 395–398. ISBN 9783319549774.*
2. *Bodeau, Deborah J.; McCollum, Catherine D.; Fox, David B. (2018-04-07). "Cyber Threat Modeling: Survey, Assessment, and Representative Framework" (https://apps.dtic.mil/sti/citations/AD1108051) . Archived (https://web.archive.org/web/20210929040958/https://apps.dtic.mil/sti/citations/AD1108051) from the original on September 29, 2021.*
3. *"Threat Modeling: 12 Available Methods" (https://insights.sei.cmu.edu/blog/threat-modeling-12-available-methods/) . SEI Blog. Retrieved 2021-10-04.*
4. *Jones, Andy (2005). Risk management for computer security : Protecting your network and information assets (https://www.worldcat.org/oclc/159937634) . Debi Ashenden. Amsterdam, Netherlands: Elsevier Butterworth-Heinemann. ISBN 978-0-08-049155-4. OCLC 159937634 (https://www.worldcat.org/oclc/159937634) .*

5. *O'Neill, Patrick Howell (3 May 2017). "Under tough surveillance, China's cybercriminals find creative ways to chat" (https://www.cyberscoop.com/chinese-cybercriminals-speak-in-code-to-hide-from-government-surveillance/) . SNG. cyberscoop. Retrieved 22 October 2020.*

6. *Dasgupta, Binayak (1 July 2020). "Mass surveillance risk real with Chinese apps: Experts" (https://www.hindustantimes.com/india-news/mass-surveillance-threat-real-with-chinese-apps-says-cybersecurity-experts/story-HphmVO6k2D8kiRMqoD4NgI.html) . Hindustan Times, New Delhi. Retrieved 22 October 2020.*

Last edited 2 months ago by GreenC bot