Short Communication

iMedPub Journals
www.imedpub.com

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

2023
Vol.6 No.1:069

Protection of Computer Systems and Networks from Information Disclosure

Barbara Weber*

Department of Computer Science, University of St Gallen, St Gallen, Switzerland

***Corresponding author:** Barbara Weber, Department of Computer Science, University of St Gallen, St Gallen, Switzerland; E-mail: Weber234@gmail.com

Received date: October 18, 2022, Manuscript No. IJAREEIE-22-14821; **Editor assigned date:** October 21, 2022, PreQC No. IJAREEIE-22-14821 (PQ); **Reviewed date:** November 07, 2022, QC No. IJAREEIE-22-14821; **Revised date:** January 27, 2023, Manuscript No. IJAREEIE-22-14821 (R); **Published date:** February 02, 2023, DOI: 10.36648/IJAREEIE.6.1.69

Citation: Weber B (2023) Theoretical and Practical Fields of Hardware and Software Design in Computer Science. Int J Adv Res Vol:6 No:1

Introduction

The protection of computer systems and networks from information disclosure, theft, damage to their hardware, software or electronic data, as well as from the disruption or misdirection of the services they provide, is referred to as computer security, cyber security (cyber security) or Information Technology security (IT security). The growth of smart devices, including smartphones, televisions and the various devices that make up the Internet of Things (IoT), as well as the increased reliance on computer systems, the internet and wireless network standards like bluetooth and Wi-Fi, has given rise to the importance of the field. Due to the complexity of information systems, both in terms of political usage and technology, cyber security is also one of the major challenges facing the modern world. The system's dependability, integrity and data privacy are its primary objectives.

Description

The topic of cyber security has become ingrained in both our professional and personal lives ever since the introduction of the internet and the digital transformation that has been underway in recent years [1]. Over the course of the past 50 years of technological advancement, cyber threats and cyber security have remained constant. Computer security was mostly practiced in academic settings in the 1970's and 1980's until the internet was created, when computer viruses and network intrusions started to spread. The institutionalization of cyber threats and cyber security in the 2000's was a significant event following the spread of viruses in the 1990's. The Ware report and the April 1967 session that Willis Ware organized at the spring joint computer conference were pivotal junctures in the history of computer security. Material, cultural, political and social issues came together in Ware's work [2]. The "CIA triad" of Confidentiality, Integrity and Availability was introduced in a 1977 NIST publication as a clear and straightforward method for describing key security objectives. Numerous more complex frameworks have been proposed since then. However, because computers and the internet were still in their infancy and security threats were readily apparent, there were no significant computer threats in the 1970's or 1980's. Threats were typically posed by malicious insiders who gained unauthorized access to confidential files and documents. While malware and network breaches were present in the beginning, they were not used for financial gain. Established computer companies like IBM began offering commercial access control systems and computer security software by the second half of the 1970's. Creeper was the first in 1971. Bob Thomas at BBN wrote the experimental computer program Creeper. It is thought to be the first computer virus. Reaper was the name of the first anti-virus software that was developed in 1972. Ray Tomlinson developed it to traverse the ARPANET and eliminate the Creeper worm [3].

The first known case of cyber espionage was carried out by a group of German hackers in September 1986 and June 1987 [4]. The group sold the gathered data to the Soviet KGB by hacking into the networks of American defense contractors, universities and military bases. Markus Hess, who was arrested on June 29, 1987, was the leader of the group. On February 15, 1990, he and two other co-conspirators were found guilty of espionage. The Morris worm, which was one of the first computer worms, was spread *via* the internet in 1988. It received a lot of attention from the mainstream media. Shortly after the National Center for Supercomputing Applications (NCSA) launched Mosaic 1.0, the first web browser, in 1993, Netscape began developing the protocol SSL. In 1994, Netscape had SSL version 1.0 ready, but due to numerous serious security flaws, it was never made available to the general public. Replay attacks and a flaw that allowed hackers to alter user sent unencrypted communications were among these flaws. However, Netscape released Version 2.0 in February 1995 [5]. The National Security Agency (NSA) is in charge of gathering foreign intelligence and protecting American information systems. There is a conflict between these two responsibilities. Evaluation of software, identification of security flaws and defensive action to rectify the flaws are all part of protecting information systems. Exploiting security flaws to obtain information is an offensive action in intelligence gathering. When security flaws are fixed, they can't be used by the NSA. The agency looks at software that is used a lot to find security flaws. It uses these flaws to attack US competitors in an offensive way. The agency rarely takes defensive action by notifying software manufacturers of flaws so that they can be fixed. The offensive strategy worked for a while, but other countries, such as China, Russia, Iran and North Korea, eventually developed their own offensive capabilities and have typically used them against the United States. The "click and shoot" attack tools were made and sold by contractors at the NSA to US agencies and close allies, but the

tools eventually got to foreign adversaries. Russia and North Korea have utilized the NSA's own hacking tools that were compromised in 2016 and were used by them. In order to compete in cyber warfare, adversaries have hired NSA employees and contractors at high wages. For instance, in 2007, Israel and the United States began taking advantage of security flaws in the Microsoft Windows operating system to attack and destroy Iranian nuclear material refinery equipment. Iran responded by beginning to employ cyber warfare against the United States and investing heavily in their own capability. A flaw in internal control, implementation, operation or design is vulnerability [6].

Conclusion

The Common Vulnerabilities and Exposures (CVE) database contains documentation for the majority of the vulnerabilities that have been discovered. A vulnerability that can be exploited requires at least one successful attack or exploit to be present. Utilizing automated tools or custom scripts, vulnerabilities can be researched, reverse-engineered, hunted or exploited. Any secret way to get around standard authentication or security controls is known as a backdoor in a computer system, cryptosystem or algorithm. They could be there for a variety of reasons, including a bad design or configuration. They could have been added by an authorized party to give some legitimate access or they could have been added by an attacker for bad reasons; however, despite the reasons for their existence, they create an opening. Backdoors are typically discovered by someone who has access to the application source code or intimate knowledge of the computer's operating system. Backdoors can be extremely difficult to identify.

References

1. de Souza Z, Dick GN (2008) Information disclosure on MySpace-the what, the why and the implications. Pastoral Care in Education 26:143-157
2. Christofides E, Muise A, Desmarais S (2019) Information disclosure and control on Facebook: are they two sides of the same coin or two different processes? Cyberpsychol Behav 12:341-345
3. Mohammadi A, Hamidi H (2018) Analysis and evaluation of privacy protection behavior and information disclosure concerns in online social networks. Int J Eng 31:1234-1239
4. Kisekka V, Bagchi-Sen S, Rao HR (2013) Extent of private information disclosure on online social networks: An exploration of Facebook mobile phone users. Comput Human Behav 29:2722-2729
5. Shibchurn J, Yan X (2015) Information disclosure on social networking sites: An intrinsic–extrinsic motivation perspective. Comput Hum Behav 44:103-117
6. Hey Tow WN, Dell P, Venable J (2010) Understanding information disclosure behaviour in Australian Facebook users. J Inf Technol 25:126-136