Evolution of Information Technology in Computer

Rouf Ali*

Department of Computer Application, Government Degree College Boys Sopore, Jammu and Kashmir, India

Commentary

Received: 05-Sep-2022, Manuscript No. GRCS-22-76646; **Editor assigned:** 07-Sep-2022, Pre QC No. GRCS-22-76646 (PQ); **Reviewed:** 21-Sep-2022, QC No. GRCS-22-76646; **Revised:** 26-Sep-2022, Manuscript No. GRCS-22-76646 (A); **Published:** 05-Oct-2022, DOI: 10.4172/2229-371X.10.3.002

***For Correspondence:**

Rouf Ali, Department of Computer Application, Government Degree College Boys Sopore, Jammu and Kashmir, India

E-mail: alirou@gmail.com

ABOUT THE STUDY

The protection of computer systems and networks from information disclosure, theft of their hardware, software, or electronic data, as well as from the disruption or misdirection of the services they offer is known as computer security, cyber security or Information Technology security (IT security).

This field has gained importance as a result of the increased use of computer systems, the Internet, wireless network protocols like Bluetooth and Wi-Fi as well as the expansion of smart devices like smartphones, televisions and other items that make up the Internet of Things (IoT). Due to the complexity of information systems in today's world, both technologically and politically, cybersecurity is another major concern. The main objective is to guarantee the dependability, integrity and data privacy of the system.

The National Security Agency (NSA) is in charge of gathering foreign intelligence as well as safeguarding American information systems. These two responsibilities are at variance with one another. Information systems must be protected by analysing software, spotting security problems, and taking defensive measures to fix the errors. Exploiting security weaknesses to extract information is an offensive technique in intelligence gathering. Security weaknesses can no longer be exploited by the NSA after being fixed.

The agency examines widely used software to identify for security problems, which also maintains for offensive purposes against American competitors. Rarely does the government engage in defensive action by informing software developers of problems so they can fix them.

The aggressive approach initially succeeded, but later other countries such as China, North Korea, Iran, and Russia acquired their own offensive capabilities and tended to employ them against the United States. "Click-and-shoot" attack tools were developed and sold by NSA contractors to U.S. agencies and close allies, but eventually the tools reached foreign adversaries. The NSA's own cyber tools were compromised in 2016, and North Korea and Russia have since used them. Adversaries eager to compete in cyber security have recruited NSA staff and contractors at premium wages.

For instance, starting in 2007, the United States and Israel started attacking and harming machinery used in Iran to refine nuclear materials by taking advantage of security holes in the Microsoft Windows operating system. Iran's response was to make significant investments in their own cyber ware capabilities, which they then started, use against the US. The way employees behave can have a significant impact on an organization's information security.

The least privilege principle states that each component of the system should only have the privileges necessary to carry out its purpose. In this manner, even if a hacker manages to access that portion, their access to the entire system will be restricted. Automated theorem is proving to improve the correctness of crucial software subsystems.

Unit testing and code reviews are methods for increasing module security when formal correctness proofs are not feasible.

Defence in depth refers to a system's design where it takes the compromising of multiple subsystems to endanger the integrity of the system and the data it contains. When a security breach occurs, the technique and severity of the breach can be identified according to audit trails that keep track of system activity. Audit trails can be protected from becoming erased by being stored remotely.