Tools to Secure Cyber Threats

Goutam K Saha

Senior Member IEEE <gksahaATrediffmail.com>

Apart from using various type of security protection like firewall, antivirus, strong passwords, protecting Wi-Fi connection to secure the data, other few ways to protect the data information and improve security level need to be deployed.

Digital Signature (a type of electronic signature) — is to protect electronic data in such a way that the originality of data and integrity of data can be checked. It is a mathematical algorithm routinely used to validate the authenticity and integrity of a message for example, an email, a credit card transaction, a digital document. Digital signatures are more secure than other forms of electronic signatures. A digital signature is created using hash algorithms or a scheme of algorithms like DSA and RSA that use public key and private key encryptions. The sender uses the private key to sign the message digest (not the data), and when they do, it forms a digital thumbprint to send the data. The client can create key match by utilizing the particular crypto programming. The Certifying Authority issues Digital Signature Certificate for an application when an individual approach to a certifying authority.

Encryption- is to encode the sensitive records and messages in travel and capacity. It is a means of securing digital data using one or more mathematical techniques, along with a password or "key" used to decrypt the information. For example, websites that transmit credit card and bank account numbers should always encrypt this information to prevent identity theft and fraud. This is the process of translating plain text data (plaintext) into something that appears to be random and meaningless (cipher text). Decryption is a process of converting cipher text back to plaintext.

Security Audits- is a practice of an effective evaluation of the security of an organization data framework by estimating on how the arrangement is going well in creating up the criteria. This is to discover the vulnerabilities that an association is looking for its IT framework. The security of the structure’s physical setup and condition, programming, information dealing with systems can be overviewed by a thorough audit. A security audit is a systematic evaluation of the security of a company's information system by measuring how well it conforms to an established

set of criteria. Security audits measure an information system's performance against a list of criteria. Four main security audits that every business should be conducting on a regular basis: Risk Assessment, Vulnerability Assessment, Penetration Testing, Compliance Audit.

Cyber Forensics – is the solution in investigating the computerized violations. Digital legal sciences are nothing but the revelation, examination, and remarking of confirmation extricated from any component of computer frameworks, systems, media, and peripherals that enable specialists to unravel a wrongdoing (Iqbal, 2016). Computer forensics involves imagery storage media, restoring deleted files, finding slacks and free space and maintaining the data that being collected for prosecution purposes. Forensic networking is a consistent forensic in terms of the network.

Cryptography- is based on strong mathematical reasoning and it aims to guarantee more the nature of confidentiality only. It provides tools for protecting integrity and legitimacy of the message. It is the technique of securing information and communications through use of codes so that only those person for whom the information is intended can understand it and process it. Thus preventing unauthorized access to information. The prefix “crypt” means “hidden” and suffix “graphy” means “writing”. In Cryptography the techniques which are used to protect information are obtained from mathematical concepts and a set of rule based calculations known as algorithms to convert messages in ways that make it hard to decode it. These algorithms are used for cryptographic key generation, digital signing, verification to protect data privacy, web browsing on internet and to protect confidential transactions such as credit card and debit card transactions.

Cryptanalysis- is to understand the threats to security of the existing primitives in order to be ahead of malicious (Roca et. Al., 2019). An empirical measure of security thanks to a thorough and never-ending scrutiny, searching for possible weaknesses. In-depth Cryptanalysis is the backbone for the design of secure primitives. Cryptography which focuses on creating secret codes and Cryptanalysis which is the study of the cryptographic algorithm and the breaking of those secret codes. The person practicing Cryptanalysis is called a Cryptanalyst. It helps us to better understand the cryptosystems and also helps us improve the system by finding any weak point and thus work on the algorithm to create a more secure secret code. For

example, a Cryptanalyst might try to decipher a cipher text to derive the plaintext. It can help us to deduce the plaintext or the encryption key.