Information System Security

Anil Chhangani
Head of Department, Computer Engineering
Lokmanya Tilak College of Engineering
Navi Mumbai, India
Anil_chhangani@rediffmail.com

Akanksha Chaturvedi
Student, M.E Computer Engineering
Lokmanya Tilak College of Engineering
Navi Mumbai, India
Chaturvedi.akanksha7@gmail.com

Abstract—Information, a valuable resource in any business entity, has become an important driver which supports organizational operations and systems. Any firm that holds confidential information in an electronic format is exposed to threat of data loss and breaching federal and state privacy laws. This paper presents a high level view of threats that exist in information system environment and focuses on best security practices to mitigate them.

Index Terms—Protocols SSL/TLS, Information systems (IS), SQL injection, Firewall, IDS/IPS Cryptography.

I. Introduction

Information systems store, process and transmit information critical to drive organizations business operations. Each organization depending on their mission and business objectives, implement information systems, either as decision support systems, transaction processing system, knowledge management systems, database management systems or learning management systems. Information systems streamline processes, increases the speed of performing regular business functions and influence the quality of work.

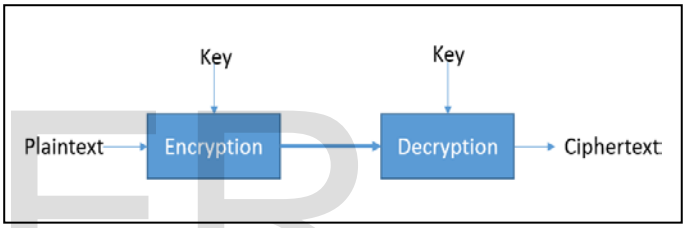
Along with opportunities, the reliance on information systems has given rise to new threats. Information technology is one of the main components of IS, which is now embedded in the operations and management of organizations. With emergence of new technology, focus is now drawn on keeping this systems secure and maintain the competitive edge along with business reputation. Information has "Value", it may be a new product information, employee records or Intellectual property. There is a need to protect information kept in computer based systems and controlling its access via authorized means only.

II. Principles of Informations systems Security

Security can only be achieved through constant change, through discarding old ideas that have outlived their usefulness and adapting others to current facts. [1] The core principles of information system security consist of confidentiality, integrity and availability. Confidentiality is preventing information from being obtained by unauthorized person, and integrity is preventing unauthorized changes to information. Availability is the aspect that information resources will be available to authorized users whenever they are authorized to use them.

III. ROLE OF CRYPTOGRAPHY

Cryptography is science of secure communications. It is the mathematical scrambling of data to hide the original message. It is the art of coding and decoding messages, often implemented via application of mathematical algorithm. Encryption is conversion of plaintext into cipher text, where plaintext is clear text and cipher text is coded message.



Cryptography finds its application in an enterprise, securing contents of the database, where confidential information can be stored in encrypted form, e.g., passwords as one way hash, or for additional protection, salted hash. Not everything needs to be encrypted, sometimes only a particular row or column of a database needs to be protected, field level encryption can be applied, where only the chosen field is encrypted, e.g. bank account Numbers, SSN numbers. File-level encryption protects file on a logical file-by-file basis, whereas full drive encryption encrypts the entire drive.

Many organizations use email as primary means of communication. From information security perspective, e-mails contain confidential information, maintaining their integrity and confidentiality is important. One way to securely transmit and receive email is by implementing application of cryptography, known as PKI (Public key infrastructure). PKI enables users to sign and encrypt email. A digital signature prevents masquerading by authenticating the sender, and alerts the recipient to any modifications made to the email, during transit. It also makes it difficult for a user to deny having sent the email (non-repudiation). Encrypting the email prevents it being read by anyone other than the intended recipient (provided confidentiality).

PKI also provides authentication (in virtual private networks, wireless LANs) and controls the distribution of information with digital rights management.

For transfer of sensitive information over internet, use of TLS (transport layer security), which is a cryptographic protocol, provides communication security. Cryptography is an essential part of today's information systems. It provides validity for e-commerce transactions, prevents alteration of organization's webpage by vandals and also provides a competitive edge by protecting company's trade secrets. Information systems cannot be secured by cryptographic techniques alone. A layered, defense in depth approach is essential to advance towards a secure and reliable system.

IV. SECURITY CONTROLS

Controls are a key element in the process area to implement security. The security controls can be categorized into three categories, technical, management and operational. Depending on information criticality, information that drives success or failure of an organization, security controls are selected and implemented. Security controls can also be categorized as either preventive, reactive or detective controls.

Security controls consist of:

Technical
Access control
Audit and Accountability
Identification and authentication
System and communications protection

Management
Risk assessment
System and services acquisition
Certification, accreditation and security assessment

Operational
Planning
Maintenance
Media Protection
Incident response
Personnel security
Contingency planning
Awareness and training
Configuration management
System and information integrity
Physical and environmental protection

Access control is control of logical, physical and remote access to information and resources; including identification and authentication, authorization, password and user management on applications, operating systems and within networks. Audit and accountability control aids systems in capturing sufficient information in audit records to establish what events occurred, the sources of events and outcomes of the event. Identification and authentication control determines and validates user identity. System and communication protection control prevents disruption of services and ensures the authenticity of information handled by telecommunications systems.

Risk assessment is an integral part of risk management and consist of identifying threats and vulnerabilities, determining their impact and deciding what actions should be taken to mitigate security related risks. System and services acquisition control is aimed at producing policies and procedures that are required for effective implementation of selected security controls in organizational environment. Certification, accreditation and security assessment certifies that an information system meets documented security requirements before the information system is "accredited" into operations.

Planning includes generating a high level policy aligning security objectives with business critical mission and objectives. Media protection control addresses the need for protecting media throughout its lifecycle. Incident response plays an important role in information security, it is crucial to define what constitutes as an incident;

- Loss of information confidentiality (data theft)
- Compromise of information integrity (damage to data or unauthorized modification)
- Theft of physical IT asset including computers, storage devices, printers, etc.
- Damage to physical IT assets including computers, storage devices, printers, etc.
- Denial of service.
- Misuse of services, information, or assets.
- Infection of systems by unauthorized or hostile software.
- An attempt at unauthorized access.
- Unauthorized changes to organizational hardware, software, or configuration.
- Reports of unusual system behavior (deviation from normal behavior)

Incident can be identified through logs generated from firewall (device that segregates traffic based on rules) intrusion prevention alarms or intrusion detection alerts. Once incident is recognized, incident response team can take action contain/eradicate it. Personnel security addresses administrative processes and requirements for personnel within the organization, e.g. Background checks, access levels. Contingency planning encompasses business continuity and disaster recovery planning. It prioritizes mission-essential functions and resources to be restored in the event of actual contingency. Continuous security awareness is essential in instilling security into the organization's business culture. The organization's security policy should address the frequency and types of security training needed for users, technical staff, and senior management.

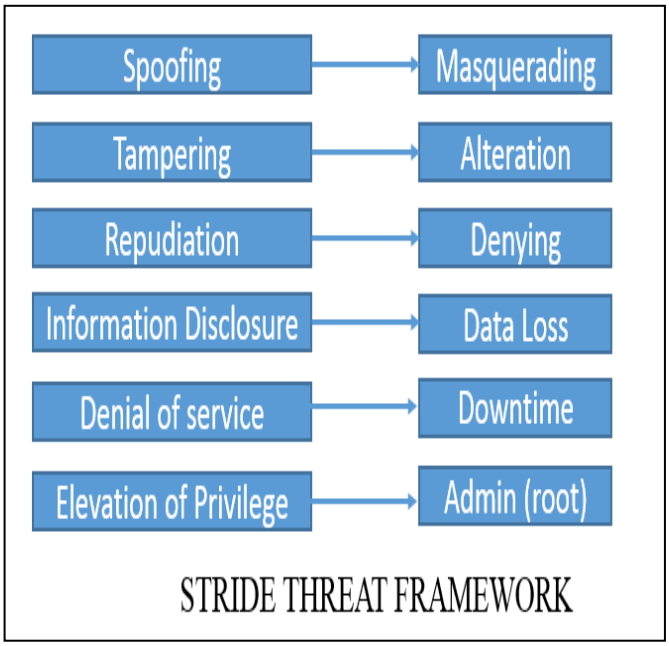
Configuration management ensures that changes will not have a negative impact on the organization. It addresses testing requirements for implementation, and requirements for updates to system diagrams and inventories when changes occur. System and information integrity ensures that systems are not tampered with and the security measures implemented are effective. Physical security concerns can directly benefit or hurt an organization's technical security posture. Locked doors, alarms, and armed guards can reduce the overall threat to an organization, therefore reducing the overall risk. Implementation of physical security measures should be an integral part of the security posture analysis of an organization. Common examples for which physical security can help improve information security include:

- Locked server room doors to prevent physical access to servers
- Locked gates to reduce the threat of unauthorized internal security problems
- Guards to prevent theft of hardware or software assets

V. RISKS, THREATS AND VULNERABILITIES

Risk is possibility of suffering a loss from an uncertain event. e.g., damage to physical infrastructure during flooding. Threat can be defined as a potential to cause harm by exploiting the weakness, that exists in system or system environment, where information resides. e.g. SQL injection, the SQL injection attack consist of insertion of a SQL query via the input data from client to application, a successful SQL injection can read sensitive data from database, modify database, delete contents of database. Another example is, cross-site scripting commonly found in web applications, where attackers can inject a client-side script into web pages viewed by other users.

The mitigation efforts can only begin with first identifying the threats that exist and their impact. Threat model such as STRIDE can be used to identify threat and vulnerabilities.



Spoofing is threat action aimed at unauthorized access by using another's authorized user's credentials, such as user name and password. Tampering is threat action aimed at unauthorized modification of data and alteration of data in transit over an open network, such as internet. Repudiation is threat action aimed to perform illegeal operation in a system that lacks the ability to trace it back to source which performed the illegal operation in first place. Information disclosure is a threat action aimed to read a file which a user does not have authorized access to, or read data in transit resulting in data loss. Denial of service is a threat action aimed at denying authorized users access to service they require e.g. deny access to web server. Elevation of priviliege is a threat aimed to gain unauthorized privileged access to compromise a system.

Once the threats are identified, their impact level is determined, and a decision is made to either accept, transfer, avoid or mitigate risk. The decision depends on organization's individual risk appetite.

VI. CONCLUSION

It is essential to understand ,why it is important to protect our information systems, what value they add to our organization, and what are the risks they are facing .One key point to address is as technology evolves, so does the risk environment. Threats need to be monitored continuously, and security controls implemented need to assessed for effectiveness.

Perfect security is not possible, attackers do not break crypto, they bypass it. Focus should be on designing secure applications that are deployed within organization. User awareness and training is a key aspect often ignored when it comes to protecting our systems, it is users who interact with systems, enabling them with secure best practices, further strengthens our information security approach.

BYOD (bringing your own device), where organizations allow employees to connect their personnel device on the network, significantly impacts the traditional security model that organization use. By integrating a mix of above defined security controls, policies and procedures, a right balance can be set which will assist organizations to increase their productivity and maintain their security posture.

REFERENCES

[1] William O. Douglas, U.S. SUPREME COURT JUSTICE (1898–1980).

[2] Open web application security project

[3] 'Principles of Information system and security', by Vincent Nestler, Gregory White, Wm. Arthur Conklin, Matthew Hirsch, Corey Schou

[4] Security Assessment: Case Studies for Implementing the NSA by Russ Rogers , Greg Miles , Ed Fuller