The importance of Information Integrity, Security, Networking and Data Protection

Rajashri S.Limaye
Department of CS & IT
Yeshwant Mahavidyalaya Nanded

Abstract - Information technology is widely recognized as the engine that drives the INDIA. economy, giving industry a competitive advantage in global markets, enabling the federal government to provide better services to its citizens, and facilitating greater productivity as a nation. Organizations in the public and private sectors depend on technology-intensive information systems to successfully carry out their missions and business functions. Information systems can include diverse entities ranging from high-end supercomputers, workstations, personal computers, cellular telephones, and personal digital assistants to very specialized systems (e.g., weapons systems, telecommunications systems, industrial/process control systems, and environmental control systems).

Information systems are subject to serious threats that can have adverse effects on organizational operations (i.e., missions, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation by exploiting both known and unknown vulnerabilities to compromise the confidentiality, integrity, or availability of the information being processed, stored, or transmitted by those systems. Threats to information and information systems can include purposeful attacks, environmental disruptions, and human/machine errors and result in great harm to the national and economic security interests of the United States. Therefore, it is imperative that leaders and managers at all levels understand their responsibilities and

are held accountable for managing information security risk—that is, the risk associated with the operation and use of information systems that support the missions and business functions of their organization.

I. INTRODUCTION

A.What is information Integrity?

System integrity is concerned with security, completeness, trustworthiness, timeliness, up-to-date and relevant.We define information integrity (I*I) with there dimensions:

Accuracy, consistency and reliability. It is concerned with how information flows in the organization and how it impacts processes and outcomes.

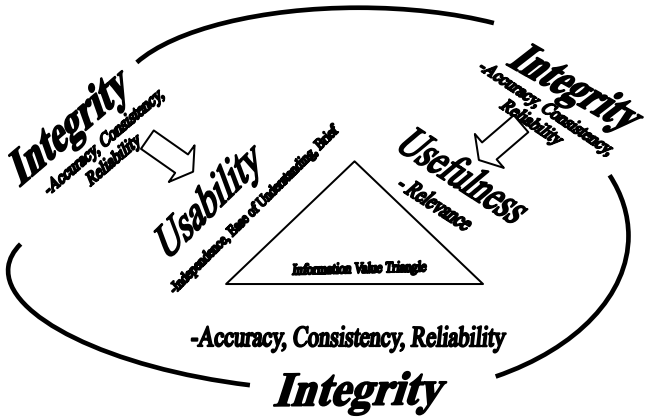
Important concerns in integrity are privacy and disaster recovery. Privacy deals with rights of individuals to protect themselves from unauthorized disclosure of information about them. Disaster recovery deals with to get back to normalcy after an accident or damage. Integrity of the overall system is ensured only if the integrity of all part of the system is ensured. Information Integrity (I*I) is dependability and trustworthiness of information and controlling. It is a key factor determining strategic business advantage. Its attributes are accuracy, consistency and reliability of information system . Value of information is governed by three factors.

Usefulness, its Usability and its Integrities.

System integrity is concerned with security, completeness, trustworthiness, timeliness, up-to-date and relevant.

We define information integrity (I*I) with there dimensions:

Accuracy, consistency and reliability. It is concerned with how information flows in the organization and how it impacts processes and outcomes. Value of information is governed by three factors. Usefulness, its Usability and its Integrities.



B. UUI (Usefulness, Usability and Integrity)

1. Requirement of useful information in usable form.
2. Definition of I*I is the inverse amount of distortion and noise present. I*I is thus concerned with correctness and exactness aspect of the information.
3. Information should be useful and usable.

Information integrity is thus seen as the problem of data integrity and other sub fields are confidentiality and privacy.

Securing data in public and private sectors is challenging because participants may behave maliciously, and because their remote systems are outside the control of the data owner.

. To provide confidentiality, a flexible fine-grained encryption framework is proposed which allows data owners to construct, from a set of access policies, a single encrypted database that can be stored and exchanged by all parties. Access is granted by separately disseminating keys. To provide integrity, an efficient authentication mechanism is described which can be used to detect tampering when data is stored by an untrusted database. Together these techniques can significantly advance the security of distributed data exchange.

C. Defining information Security

Security relates to the protection of valuable assets against unavailability, loss, misuse, disclosure or damage. In this context, valuable assets are the information recorded on, processed by, stored in, shared by, transmitted from or retrieved from any medium. The information must be protected against harm from threats leading to different types of impacts, such as loss, inaccessibility, alteration or wrongful disclosure. Threats include errors and omissions, fraud, accidents, and intentional damage.

II. Importance of Information Security for the Corporate Environment

Information security is a key aspect of IT governance, and it is an important issue for all computer users to understand and address. As computer systems have become more and more commonplace in all walks of life, from home to school and the office, unfortunately, so too have the security risks.

The widespread use of the Internet, handheld and portable computer devices, and mobile and wireless technologies has made access to data and information easy and affordable. On the other hand, these developments have provided new opportunities for IT-related problems to occur, such as theft of data, malicious attacks using viruses, hacking, denial-of-service (DoS) attacks and even new ways to commit organized crime. These risks, as well as the potential for careless mistakes, can all result in serious financial, reputational and other damages.

III. The Business Value of Information Security

Generally speaking the business value of information security can be calculated on the basis of risk reduction, security as a (decreasing) cost of doing business and return on investment via enhanced trust relationships and improved business opportunity. Few enterprises that have strong security will brag about it publicly. Instead, code words such as "risk" and "trust" will be used to signal superior security to markets, trading partners and customers. In any case, unsecured enterprises will face higher costs from poorly administered, expensive security programs, intellectual property losses, theft and lawsuits. Superior security is a competitive advantage, and poor security will be increasingly disadvantageous. Good security allows you to achieve a primary goal of the e-business era: reaching a greater number of customers with enhanced products and services.

IV. Data protection requirements

The number one item on the 2008 information security agenda is data protection. The practice of protecting the confidentiality, integrity and availability of data is not new—passwords, encryption and data classification structures have been around for years. What has changed is the type of data that's now considered valuable. From the external attacker perspective, intellectual property and insider information were once the most sought-after data asset. Now, the data currency of choice is identity, e-mail addresses, social security numbers and credit card information. Corporate espionage is still a significant threat, but the new underground deals in volume, where success is being measured in thousands and millions of identities.

V. Insider Threat requirements

While data protection provides the challenge, and compliance will consume a majority of the time, the most relevant trend for 2008 is information security's emergence as a strategic business-level issue that plays an increasing role in achieving business objectives. For years, the term IT security has been very appropriate, since activities were focused around antivirus, firewall rules, intrusion detection and the like, with the need for specialized skills to implement and manage specific security technologies. These technologies will continue to flourish and improve, but the mysticism associated with managing them has all but gone away. The operational roles to support these tools are being integrated into the organization's infrastructure team, which is where the roles belong. Antivirus software should be a standard part of a desktop operating system build and supported by the desktop management team; firewall management should be included as part of the network management team, etc.

VI. Privacy

Privacy is a valuable aspect of personality. Data or information protection forms an element of safeguarding a person’s right to privacy. It provides for the legal protection of a person in instances where his or her personal information is being collected, stored, used or communicated by another person or institution. The constitutional

right to privacy is, like its common law counterpart, not an absolute right but may be limited in terms of law of general application and has to be balanced with other rights entrenched in the Constitution. In protecting a person's personal information consideration should, therefore, also be given to competing interests such as the administering of national social programs, maintaining law and order, and protecting the rights, freedoms and interests of others, including the commercial interests of industry sectors such as banking, insurance, direct marketing, and health care, pharmaceuticals and travel services. The task of balancing these opposing interests is a delicate one.

VII. U DIRECTIONS REGARDING INFORMATION SECURITY TECHNOLOGIES

EU defines a number of Emerging Security Technologies for which research projects are funded. For the year 2007 EU defines the Work Programmed for the ICT theme of the FP7 Specific Program "Cooperation" which defines the priorities for the calls for proposals to be launched in 2007. One of the Calls for 2007 is related to information security and has the title "Challenge 1: Pervasive and Trusted Network and Service Infrastructures". The particular objective of this challenge which deals with information security technologies is called "Secure, dependable and trusted Infrastructures".

VIII. THE NEW WAVE OF INFORMATION SECURITY TECHNOLOGIES

The information security industry is in transition. It is experiencing rapid change in business processes, the types of transactions that need securing, the threat profile, the legal and regulatory landscape, the vendor-side industry structure, security product types, delivery mechanisms and the security standards framework. Those changes are tightly coupled with the new paradigm of business models which includes openness, unbounded, dynamic, interconnected actors that need to share content and resources and where security should become an enabler and not a disabler. Related to this is the need for a practical yet rigorous approach to information security in large distributed systems as well as models and mechanisms for secure and trusted inter-enterprise cooperation and cooperation in virtual organizations.

IX. MARKET OVERVIEW

Despite the various business, operational, and regulatory hurdles that must be overcome, federated identity is building real momentum. The standards and technologies developed during the past several years have moved beyond the hypothetical into real-world deployments. Federated identity management technology is considered to be mature, as standards have been produced and used by the industry.

In September 2005, the Radicati Group, a technology market research firm, forecast that the revenues from Identity Management products will be increased from $374 in 2005 millions to $2,462 millions by the 2009.

X. END POINT SECURITY

Enterprises today face many IT challenges. Key among these are combating ever more frequent security incidents and striving to maintain regulatory compliance. A common thread among these challenges is the need to ensure protection and control of the endpoint. End point security solutions are a process designed to reduce security incidents and increase compliance by enforcing IT security policies as a prerequisite for network access. End point security technologies address this problem by auditing the security stance of endpoints before they connect and

making appropriate updates before there is a connection to the standard corporate network. This keeps worms and viruses off the network and also allows enforcement of application level security policy.

Endpoint security is a hot topic with myriad hardware and software solutions, the reality is that there are no standards, many current solutions are proprietary, and solutions are costly and complex to implement. Combined with the fact that there are not a lot of experts in the field, organizations are trying to figure out how to best future proof their endpoint security investments.

XI. Security Compliance Software

From an IT perspective, the key to compliance is the documentation, monitoring, and management of compliance control architecture. The architecture contains operational policy and technical controls aligned to business and regulatory requirements. It also establishes accountability, responsibility, and risk management principles ultimately mapped to the specific controls. In developing control architecture, enterprises should follow a recognized control framework, such as COSO, COBIT, or ISO17799.

XII. Investment Strategies

Investment strategies play a significant role in organizational risk management efforts. These strategies generally reflect the long-term strategic goals and objectives of organizations and the associated risk management strategies developed and executed to ensure mission and business success. Underlying all investment strategies is the recognition that there is a finite amount of resources available to invest in helping organizations effectively manage risk—that is, effectively addressing risk to achieve on-going mission/business success.

XIII. Limitations on Strategic Investments

The ability of organizations to provide strategic information security investments is limited. Where the desired strategic investment funding or strategic resources are not available to address specific needs, organizations may be forced to make compromises. For example, organizations might extend the time frame required for strategic information security objectives to be accomplished. Alternatively, organizations might prioritize risk management investments, opting to provide resources (financial or otherwise) to address some critical strategic needs sooner than other less critical needs. All investment decisions require organizations to prioritize risks and to assess the potential impacts associated with alternative courses of action.

XIV. Information Security Architecture

The *information security architecture* is an integral part of the organization's enterprise architecture. It represents that portion of the enterprise architecture specifically addressing information system resilience and providing architectural information for the implementation of security capabilities. The primary purpose of the information security architecture is to ensure that mission/business process-driven *information security requirements* are consistently and cost-effectively achieved in organizational information systems and the environments in which those systems operate consistent with the organizational risk management strategy.

XV. Trust and Trustworthiness

Trust is an important concept related to risk management. How organizations approach trust influences their behaviors and their internal and external trust relationships. This section introduces some conceptual ways of thinking about trust, defines the concept of *trustworthiness*, and shows how the concept of trustworthiness can be used in developing *trust relationships*. Appendix G describes several *trust models* that can be applied in an organizational context, and considers how trust can be measured. The importance of organizational governance, culture, and transparency are also considered with regard to trust and its affect on risk management.

XVI. Establishing Trust among Organizations

Parties enter into trust relationships based on mission and business needs. Trust among parties typically exists along a continuum with varying degrees of trust achieved based on a number of factors. Organizations can still share information and obtain information technology services even if their trust relationship falls short of complete trust.

XVII. Organizational Culture

Organizational *culture* refers to the values, beliefs, and norms that influence the behaviors and actions of the senior leaders/executives and individual members of organizations. Culture describes the way things are done in organizations and can explain why certain things occur. There is a direct relationship between organizational culture and how organizations respond to uncertainties and the potential for near-term benefits to be the source for longer-term losses.

XVIII. Threat Sources

Threat sources cause events having undesirable consequences or adverse impacts on organizational operations and assets, individuals, other organizations, and the Nation. Threat sources include: (i) hostile cyber/physical attacks; (ii) human errors of omission or commission; or (iii) natural and man-made disasters. For threats due to hostile cyber attacks or physical attacks, organizations provide a succinct characterization of the types of tactics, techniques, and procedures employed by adversaries that are to be addressed by safeguards and countermeasures (i.e., security controls) deployed .

XIX. Vulnerabilities

Organizations identify approaches used to characterize vulnerabilities, consistent with the characterization of threat sources and events. Vulnerabilities can be associated with exploitable weakness or deficiencies in: (i) the hardware, software, or firmware components that compose organizational information systems (or the security controls employed within or inherited by those systems; (ii) mission/business processes and enterprise architectures (including embedded information security architectures) implemented by organizations; or (iii) organizational governance structures or processes. Vulnerabilities can also be associated with the susceptibility of organizations to adverse impacts, consequences, or harm from external sources.

XX. Consequences and Impact

Organizations provide guidance on how to assess impacts to organizational operations (i.e., mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation .

XXI. Assessing Risk

Risk assessment identifies, prioritizes, and estimates risk to organizational operations (i.e., mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation and use of information systems. Risk assessments use the results of threat and vulnerability assessments to identify and evaluate risk in terms of likelihood of occurrence and potential adverse impact (i.e., magnitude of harm) to organizations, assets, and individuals.

XXII. Confidentiality and Integrity in Distributed Data Exchange

The distributed exchange of structured data has emerged on the World Wide Web because it promises efficiency, easy collaboration, and—through the integration of diverse data sources—the discovery of new trends and insights. Along with these benefits, however, there is also the danger that exchanged data will be disclosed inappropriately or modified by unauthorized parties.

XXIII. Integrity in data exchange

Hash trees are a key technology for supporting such annotations, and can also be used to provide integrity of data in conventional database systems that may be vulnerable or untrusted. Although hash tree techniques are well-known, they do not always permit efficient operations, particularly in a database system.

XXIV. Views and access control

A view is a virtual table whose rows are determined by a view definition referencing stored tables (and possibly other views). A view definition is an expression in SQL that can combine information from multiple tables, apply logical selection conditions, remove columns, compute aggregates, etc. Views can be used like base tables when querying the database, and in some cases can also be updated.

XXV. Approaches to information security governance

Three approaches to information security governance can be used to meet organizational needs: (i) a *centralized* approach; (ii) a *decentralized* approach; or (iii) a *hybrid* approach.

XXVI. Conclusion

Information security has been transformed to a vital business issue and it is treated like that both from Enterprises as well as service providers & vendors. The benefits of good information security are not just a reduction in risk or a reduction in the impact should something go wrong. Good security will improve an enterprise's reputation, build its confidence and increase the trust from others with whom business is conducted, and can even improve efficiency by making it possible to avoid wasted time and effort recovering from a security incident. Having a good security posture can allow an organization to more successfully embrace new opportunities. The challenge for information security today is to serve the needs of the next generation of ubiquitous and converged network and service infrastructures for communication, computing and media.

To provide confidentiality, a flexible fine-grained encryption framework is proposed which allows data owners to construct, from a set of access policies, a single encrypted database that can be stored and exchanged by all parties. Access is granted by separately disseminating keys. To provide integrity, an efficient authentication mechanism is to

be described which can be used to detect tampering when data is stored by an untrusted database. Together these techniques can significantly advance the security of distributed data exchange.

REFERENCES

[1] Mart´ın Abadi and Phillip Rogaway. Reconciling two views of cryptography (the computational soundness of formal encryption). In IFIP International Conference on Theoretical Computer Science, Sendai, Japan, 2000.

[2] Mart´ın Abadi and BogdanWarinschi. Security analysis of cryptographically controlled access to xml documents. In Principles of Database Systems (PODS), 2005.

[3] Nabil R. Adam and John C. Wortmann. Security-control methods for statistical databases. ACM Computing Surveys, 21(4):515–556, Dec. 1989.

[4] Gagan Aggarwal, Mayank Bawa, Prasanna Ganesan, Hector Garcia-Molina, Krishnaram Kenthapadi, Rajeev Motwani, Utkarsh Srivastava, Dilys Thomas, and Ying Xu. Two can keep a secret: A distributed architecture for secure database services. In Conference on Innovative Data Systems Research (CIDR), pages 186–199, 2005.

[5] Rakesh Agrawal, Alexandre Evfimievski, and Ramakrishnan Srikant. Information sharing across private databases. In SIGMOD Conference, pages 86–97, 2003.

[6] Ross Anderson. Security Engineering: A Guide to Building Dependable Distributed Systems. Wiley Computer Publishing, 2001.

[7] Kazumaro Aoki and Helger Lipmaa. Fast Implementations of AES Candidates. In The 3rd Advanced Encryption Standard Candidate Conference, pages 106–120. NIST, 13–14 2000.

[8] Berkeley db xml. Available at www.sleepycat.com.

[9] Michael Backes, Birgit Pfitzmann, and MichaelWaidner. A composable cryptographic library with nested operations. In Conference on Computer and Communications Security (CCS), pages 220–230, New York, NY, USA, 2003. ACM Press.

[10] Fran¸cois Bancilhon and Nicolas Spyratos. Protection of information in relational data bases. In Conference on Very Large Databases (VLDB), pages 494–500, 1977.

[11] Fran¸cois Bancilhon and Nicolas Spyratos. Algebraic versus probabilistic independence in data bases. In Principles of Database Systems (PODS), pages 149–153, 1985.

[12] Josh Benaloh and Jerry Leichter. Generalized secret sharing and monotone functions. In CRYPTO, pages 27–35, 1988.

[13] E. Bertino, S. Castano, and E. Ferrari. Securing XML documents with Author-X. IEEE Internet Computing, May/June 2001.

[14] Elisa Bertino, Barbara Carminati, and Elena Ferrari. A temporal key management scheme for secure broadcasting of xml documents. In Conference on Computer and Communications Security (CCS), pages 31–40, New York, NY, USA, 2002. ACM Press.

[15] Elisa Bertino and Elena Ferrari. Secure and selective dissemination of xml documents. ACM Transactions on Information and System Security (TISSEC), 5(3):290– 331, 2002.

[16] Mandke vijay v.,center for information integrity research.A CIIR white paper by CIIR/TRAQUAINITSCOMSTA2FEB04

[17] www.ciir.org.in