ISSN 2278-8808 SJIF 2014 = 4.889
An International Peer Reviewed & Referred
SCHOLARLY RESEARCH JOURNAL
FOR INTERDISCIPLINARY STUDIES

DATA PROTECTION, INFORMATION SECURITY SYSTEM & NETWORKS

Surushe Ankita Vasantrao[1] & Anurag Tripathi[2], Ph. D.

Abstract

Information technology is widely recognized as the engine that drives the Indian 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 India.

INTRODUCTION

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.

Data integrity is a fundamental component of information security. In its broadest use, “data integrity” refers to the accuracy and consistency of data stored in a database, data warehouse, data mart or other construct. The term – Data Integrity - can be used to describe a state, a process or a function – and is often used as a proxy for “data quality”. Data with “integrity” is said to have a complete or whole structure. Data values are standardized according to a data model and/or data type. All characteristics of the data must be correct – including business rules, relations, dates, definitions and lineage – for data to be complete.

Data integrity is imposed within a database when it is designed and is authenticated through the ongoing use of error checking and validation routines. As a simple example, to maintain data integrity numeric columns/cells should not accept alphabetic data.

Software developers must also be concerned with data integrity. They can define integrity constraints to enforce business rules on data when entered into an application. Business rules specify conditions and relationships that must always be true, or must always be false. When a data integrity constraint is applied to a database table, all data in the table must conform to the corresponding rule.

SECURITY PROGRAM FOR THE COMPANY

No matter how large or small your company is, you need to have a plan to ensure the security of your information assets. Such a plan is called a security program by information security professionals. Whether yours is five or 200 pages long, the process of creating a security program will make you think holistically about your organization's security. A security program provides the framework for keeping your company at a desired security level by assessing the risks you face, deciding how you will mitigate them, and planning for how you keep the program and your security practices up to date.

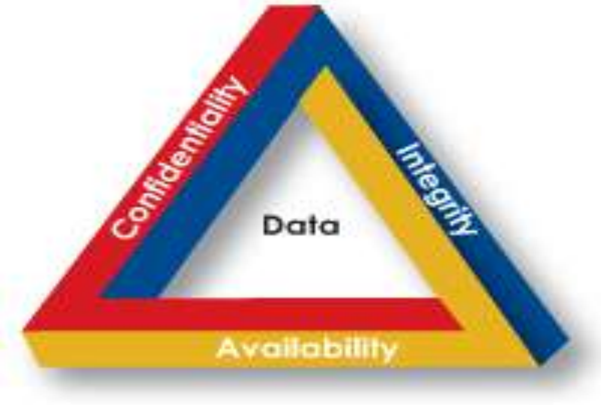
Your company's value is its data

Think you don't have anything of value to protect? Think again. The key asset that a security program helps to protect is your data — and the value of your business is in its data. You already know this if your company is one of many whose data management is dictated by governmental and other regulations — for example, how you manage customer credit card data. If your data management practices are not already covered by regulations, consider the value of the following:

- Product information, including designs, plans, patent applications, source code, and drawings
- Financial information, including market assessments and your company's own financial records
- Customer information, including confidential information you hold on behalf of customers or clients

BUSINESSVALUEOFINFORMATIONSECURITY

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 andservices.



DATA PROTECTIONREQUIREMENTS

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.

INSIDER THREATREQUIREMENTS

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.

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 constitutionalright 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.

THE NEW WAVE OF INFORMATION SECURITYTECHNOLOGIES

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 virtualorganizations.

ARCHITECTUREOF INFORMATION SECURITY

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 managementstrategy.

ESTABLISHMENT OF TRUST AMONGORGANIZATIONS

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.

THREATSOURCES

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 .

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.

CONFIDENTIALITYANDINTEGRITYINDISTRIBUTEDDATAEXCHANGE

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.

APPROACHES TO INFORMATION SECURITYGOVERNANCE

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.

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 tobe 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

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

Mart´ınAbadi 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.

Berkeley db xml. Available atwww.sleepycat.com.

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. ACMPress.

RakeshAgrawal, AlexandreEvfimievski, and RamakrishnanSrikant. Information sharing across private databases. In SIGMOD Conference, pages 86–97,2003.

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

Mart´ınAbadi and BogdanWarinschi. Security analysis of cryptographically controlled access to xml documents. In Principles of Database Systems (PODS),2005.

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

E. Bertino, S. Castano, and E. Ferrari. Securing XML documents with Author-X. IEEE Internet Computing, May/June2001.

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. ACMPress.

Elisa Bertino and Elena Ferrari. Secure and selective dissemination of xml documents.

GaganAggarwal, MayankBawa, PrasannaGanesan, Hector Garcia-Molina, KrishnaramKenthapadi, Rajeev Motwani, UtkarshSrivastava, 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.

Kazumaro Aoki and HelgerLipmaa. Fast Implementations of AES Candidates. In The 3rd Advanced Encryption Standard Candidate Conference, pages 106–120. NIST, 13–142000.

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

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

ACM Transactions on Information and System Security (TISSEC), 5(3):290– 331,2002.

Mandkevijayv.,center for information integrity research.A CIIR white paper byCIIR/TRAQUAINITSCOMSTA2FEB04