

~ COLORADO TECHNICAL UNIVERSITY ~

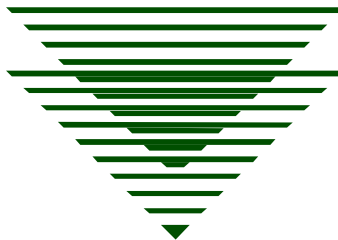
Planning For System Security

Designing IT Systems with Information Security in Mind

**Professor Roger Stemp
Submitted in Partial Fulfillment of the Requirements for
IT-501
Foundations in Information Technology**

By

**William P. Flinn
Fort Collins, Colorado
October, 2004**



Abstract

Information technology (IT) system consists of identifying user needs, automated processes that need to be performed, and how humans will interface and use the system. One aspect of the system analysis and design process that should also be considered up front is the planning for various types of disasters, whether they are naturally occurring, intentionally propagated by humans, or unintentionally caused by authorized system users. This paper looks at designing systems with security and fault tolerance in mind, and illustrates certain aspects of the certification and accreditation process that systems in the federal government must undergo to be authorized for use.

Planning for System Security:
Designing IT Systems with Information
Security in Mind

Information technology (IT) systems are typically designed using a variety of standardized project planning methods, and are implemented for a variety of automated data processing purposes. The primary consideration is given to solving a problem and that the customer is able to use the system to efficiently do business or carry out a business function. Things that are often looked at when designing a system are such things as inputs and outputs, data flow processes, user interfaces, and what processes are to be performed. As seen in the object oriented (OO) methods for designing systems, for instance, much time is spent in various design tasks. A system must be thought of in terms of how it will be used. People, or “actors,” and their “roles” must be considered in terms of what input tasks they will perform, what outputs they will receive, and what functions they will perform when interfacing with the system. A system consists of subsystems that will perform specific tasks within the whole process, and has relationships which exist between those processes. A detailed description will need to be developed showing the flow of events, including any preconditions, post conditions, and exceptions. When the system is then completed, the user will have a finished product that can be used to perform automated work.

But, designing functionality and interfaces into a system, along with all of the other considerations as mentioned above is not enough to ensure that the system will be robust and fault tolerant. In fact, fault tolerance and the ability to recover from disasters is an important aspect of a system’s overall effectiveness and longevity. Many organizations, such as the federal government and health care agencies, for instance, even have to adhere to various regulations and standards for their systems to become certified and accredited for use. The purpose of this

paper is to focus on the security aspects of designing a system. Examples will be given of processes and activities (Certification and Accreditation) that organizations such as government agencies use to ensure that their systems will withstand disasters, virus attacks, and other events that could jeopardize a system's availability. It will be shown how a system must be designed with security and recovery in mind, and how these aspects of system design are important to the system's ability to meet the needs of its users. There are many aspects of system security that should be considered as well. The scope of this paper will be to use the following sections to further discuss risk assessments for system design, as well as security categorizations that should be considered. Three aspects of the Certification and Accreditation process will be discussed in this paper: risk assessment, testing plans, and security plans, all of which should be designed in to the system from the beginning, instead of as an afterthought after the system is in production.

Significant Background

There are a variety of threats to which IT systems are vulnerable. Some are naturally occurring, such as floods, severe weather, earthquakes, and other similar natural disasters. Yet others are intentional and human-made, such as viruses and worms, hacker attacks from outside the organization, and even unauthorized access to systems from inside the organization. Then, there are other threats that can be attributed to unintentional acts of users, such as accidentally deleting data, not knowing how to use a system and corrupting system operation, or simply forgetting to back up (or automating backup of) important data. All of these potential threats must be taken into account. These threats can effect virtually every aspect of a system, including software, hardware, telecommunications infrastructures, information, and people. In fact, government agencies have several regulations and directives in place to ensure that a system has

protective measures to help safeguard all of these things. These protective measures must be in place and verified before the system is authorized for use.

There are generally three areas of importance for which a system must have safeguards in place. This is often referred to as the “C-I-A” triad of Confidentiality, Integrity, and Availability (USDA ISSM Training Seminar, 2004). The first is confidentiality, meaning that the data contained in a system is secure from unauthorized use or disclosure. The purpose of ensuring confidentiality is to protect privacy and proprietary information. An example would be social security numbers or other personal data that should not be released to unauthorized person who do not have a legal or valid use for obtaining that data. Proprietary corporate information, or sensitive classified information, as is the case in a government agency, are other examples. The second aspect system data that must be safeguarded is that of integrity. Data integrity simply means that the data will be accurate and free from being corrupted or inaccurately stored. Examples of this would include the idea that data, once entered into the system, would not be corrupted by system processes. The system would accurately display data, accurately manipulate data, and accurately display any results from the manipulations. Finally, there is the concept of availability. System availability refers to the idea that the system will be available when the users need it, regardless of system faults and errors, disasters, and other problems. Fault tolerance and methods to ensure that the system has redundant measures to keep it operating in cases of lost power, a hardware error, or even a disaster are important to this concept. An example would be that a router that helps the server housing the database communicate with the rest of the network fails. Another router is always in a “hot standby” mode to take over if the primary router fails. Or having generators and backup power supplies available would be another example of this concept.

Certification and Accreditation: Risk Categorization

When government systems are designed for use, a process of certification and accreditation of systems has to be undertaken. This process is part of the system development lifecycle as it takes a look at system design, with respect to meeting security requirements, and continues through system changes and the system being taken out of service. Most importantly, certification and accreditation process is vital during the requirements definition and development stages (FIPS PUB 102, 1983, pg. 8). What this means, then, is that ideally, a system will not be placed into operation until it has been certified. When the system requirements are being developed, not only must this design take stakeholders, users, and processes into consideration, but also meeting the needs for security in terms of confidentiality, integrity, and availability as mentioned above.

Part of the certification and accreditation process is to identify security and risk categories or risk ratings of the system being put into use. The system being certified is rated based on levels of risk, labeled low, medium, and high (FIPS Pub 199, 2003, pg. 5). Low risk means that loss of data or loss of access to data would have a limited effect on the agency's ability to conduct business. The term "limited" is defined here as limited harm to individual privacy if the data were exposed to unauthorized persons and limited damage to availability and mission criticality of systems. If a system is rated as having medium risk, it is said to mean that exposure of data to unauthorized persons could have a serious adverse effect on an agency's ability to carry out its mission. This level of risk means that a system could experience a serious business disadvantage, or suffer from major damage to assets or data if the system is not available. Finally, a high risk means that data compromise could have a severe or catastrophic effect on an agency's ability to conduct its mission. Non-availability of a system under this rating would

cause a loss of system availability for a period of time that could even be serious enough to threaten human life (FIPS PUB 199, 2003, pg. 6).

Certification and Accreditation: System Testing Plans

Once a system is categorized under one of the above severity ratings, another aspect of certification and accreditation is the design of testing measures. Several testing measures are pre-existing, and can be called in as part of the system requirements for implementation of ongoing testing throughout the lifecycle of the system. Some examples of system testing include network scanning, vulnerability scanning, password cracking, log reviews, and penetration testing (NIST PUB 800-42, 2003, pg. 3-1). Each of these can be used to test various types of system equipment, multiple tests can be run on a part of the system, and the results can be combined to get an overall picture of system security. For instance, network scanning can be used to detect what traffic is being allowed or denied by firewalls, routers, and even individual servers and work stations. This will tell the organization if any configuration changes are needed so that unauthorized or malicious traffic cannot eventually find its way to a server with critical data, or cause a denial of service to that data.

Another type of testing, vulnerability scanning, can be used to detect systems on the network that have not been updated with all of the necessary critical security patches. An instance of even one single un-patched computer can leave the entire network open to exploitation. The un-patched computer can be exploited and cause an overload of network traffic leading to a denial of service for the rest of the network, or be taken over by unauthorized persons to later use to exploit other systems. The critical system design aspect of this type of vulnerability would be to look for ways to implement a system that has minimal vulnerabilities. For instance, if a system

design involves the use of a web server, perhaps choosing a UNIX or Linux based web server (as opposed to a Windows based sever) might minimize the risk of exploitation.

With all of the testing methods identified during the system analysis and design process, determination of testing roles also has to be outlined. Since of the key aspects of system requirements identification involves communicating with and involving stakeholders, it would be important to identify network support and server administrator personnel in the testing plan. This will ensure that they are aware of the new system coming online, and will know their new responsibilities with regard to this system's operation. Testing of systems add costs in terms of the size and complexity of the system to be tested, cost of staff to perform testing, and the feasibility of doing testing samples (NIST PUB 800-42, 2003, pg. 4-2). In addition, the costs of testing the system throughout its lifecycle should be determined up front so that all stakeholders are aware of the overall system costs, and weigh that against the anticipated benefits. This is critical to helping the project team determine overall costs of the system throughout the lifecycle, and to be able to compare alternative systems that may be used.

Certification and Accreditation: System Security Plans

Major applications and general support systems are required to be covered by a security plan. For example, a database that is used for agency financial management is considered a major application, whereas a word processing program is not. General support systems included office automation systems and local area network (LAN) equipment (NIST PUB 800-18, 1998, pg. 1). System owners are responsible for maintaining required security plans. The requirements of the security plan should be integrated into the system analysis and design process so that a plan for review and maintenance can be incorporated into the overall system lifecycle and costs. Additionally, the system security plan takes into account the same risk management concepts

that were previously introduced in this paper – looking at whether a system is rated as low, medium, or high risk. System boundaries must be determined as well. This includes determining the definition of a “system,” to include what software and hardware makes up the system, as well as what other assets are used by the system. System boundaries also define who owns the system, and general similarities between components of the system, such as operating in the same operating environment, having the same (or similar) functions, and who manages or controls the system. These system boundaries will help determine how the security plan should be developed. Additionally, some individual parts of the system may not normally require a security plan, but some parts of the system do. The minor parts of the system that would not normally require a security plan on their own, but now being part of a larger system, would then come under security plan requirements (NIST PUB 800-18, 1998, pg. 5).

The security planning aspect of the system design process would indicate that there would need to be a very thoroughly thought out analysis of what components would make up a system, and what security needs would exist to protect all of those components within the system. The owners of the system would need to be identified, as well as the operating environment and mission objectives. As is true with project plans, if there is a template from a previous system that can be applied to the new system, then the security plan template from a prior system can be used and modified to meet the needs of the new system. This would help minimize new tasks and allow the work of system design to progress more efficiently.

Conclusion

When beginning a project to implement a new automated data processing system, several factors must be taken into consideration. User needs, stakeholder requirements, software and hardware requirements, and overall system operation are all things that must be considered in the

project planning activities. The security of the system must also be thought about early on in the planning as well. Once the system is in place, the software, hardware, and data will have to be protected and be able to be recovered from events such as natural disasters, intentional attacks, human errors, and equipment failures. The three aspects of data confidentiality, data integrity, and system availability must be optimized through a system of access protective measures, data backups, and system redundancies and fail-over points. Systems should be categorized according to their risk level, according to the expected impact if they should experience a disaster, to determine what protective measures are needed. These protective measures will be based largely upon the importance of the system, and the consequence of losing data.

Continuous testing to expose system vulnerabilities and security weaknesses should be conducted. The system must be covered by a security plan to ensure that all criteria set forth by applicable regulations are being met. Security plans can be templates based on previous similar systems, but should be tailored to meet the needs and description of the specific system being secured. All of these things need to be done in the planning phase of a project to implement a new system, rather than being an after thought once the system is in place. By properly planning for system security (and other) risks in the beginning of the project, the system will be more likely to survive disaster events throughout its lifecycle.

References

Evans, D.L., Bond, P.J., and Bement, A. L. (2003) Federal Information Processing Standards Publication 199: Standards for Security Categorization of Federal Information and Information Systems.

Evans, D.L., Bond, P.J., and Bement, A. L. (2003) National Institute of Standards and Technology (NIST) Special Publication 800-42: Guideline on Network Security Testing

Swanson, Marianne (1998). National Institute of Standards and Technology (NIST) Special Publication 800-18: Guide for Developing Security Plans for Information Technology Systems

USDA ISSM Training Seminar, 2004.

U.S. Department of Commerce. (1983). Federal Information Processing Standards (FIPS) Publication 102.