

~ COLORADO TECHNICAL UNIVERSITY ~

Information Security Management

Implementing Network Access Controls Using the Information Systems Architecture

**Professor Karl Seifert
Submitted in Partial Fulfillment of the Requirements for
CS-654
Information Systems Security**

By

**William P. Flinn
Fort Collins, Colorado
March, 2006**

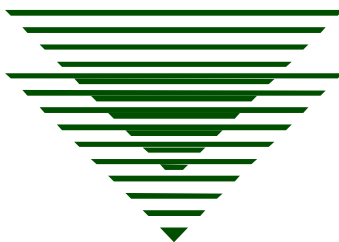


Table of Contents

Hypothesis 3
Implementing Network Access Controls..... 4
Significant Background Information:..... 5
Network Access Controls: 6
Why Is an Information Security Architecture Model Needed? 7
Organization and Infrastructure:..... 8
Policies, Standards, and Procedures: 9
Security Baselines and Risk Assessments:..... 10
User Awareness and Training:..... 11
Compliance: 12
Conclusion: 13
References..... 14

Hypothesis

A network access control (NAC) system will provide a large organization with enhanced network security and information assurance. Implementing such a system, however, requires adherence to an Information Systems Architecture (ISA) framework and sound project management principles. Using this type of framework will provide key elements to the project such as infrastructure analysis. Risk assessment, user awareness, proper system maintenance, and continued compliance. A NAC system is large enough in scope that particular attention is going to have to be paid to ensure that adequate resources are available to the implementation and maintenance of this system.

Implementing Network Access Controls

Network Access Control (NAC), also known as port security, or “quarantining,” allows the enhanced security of the organization’s network by inspecting each computer as it attempts to attach to the network. The extent of the inspection can be defined by the security team using established security policies, and can include such things as verifying the installation of enterprise standard antivirus programs, patch management system software, and the presence of current security patches. If a computer fails to meet these requirements it can be denied access to the network. Implementing such a process is usually done to mitigate a number of potential risks caused by “unhealthy” computers connecting to the corporate network

Implementing such an aggressive security measure, however, can also lead to a number of consequences and business related risks. For example, this type of security measure can result in preventing people from being able to access information and even the network itself until their computers are remediated. Avoiding this type of potential problem requires that the implementation include appropriate levels of planning of the overall architecture and required resources to ensure its success. The five-element Information Security Architecture (ISA) as presented in the Tudor text (Tudor, 2001, pg. xvi) outlines a necessary framework for implementing such a system. Proper use of the components contained in the ISA such as project management and risk analysis are important to ensure that this system is successfully implemented, and can be successfully maintained in the future.

The purpose of this paper is to discuss how implementing such an aggressive security measure ties in with a framework methodology, such as can be achieved by

using the ISA framework. The general aspects of network access controls will be described, along with potential business implications. Then, the implementation steps will be discussed, and how they integrate with each of the five points of Tudor's Information Security Architecture (ISA) model. A conclusion will be based on whether or not the ISA model provides any advantages in implementing this type of security measure in a large organization.

Significant Background Information:

Large enterprises with numbers of end users reaching into the thousands are often challenged with a variety of computer security issues. For one thing, it can be safely assumed that close to one hundred percent of all employees have computers. It is also a safe assumption that one hundred percent of these computers communicate with a corporate network, even if for no other reason than to authenticate with a server so that permission to network resources can be obtained. Because of the ubiquitous nature of connecting computers to a network (and ultimately the Internet) there is an increasing need to ensure security and protection from viruses and other threats. The use of wireless technologies has broadened as well, leading to a variety of yet additional security and access concerns (Lopez, et al, 2005, ¶ 1).

Because so many users are accessing the network, and because the risk of online virus threats is so widespread, and because so many computers are accessing the network from such a wide geographical base, network access controls have become an important consideration. Not only are the threats widespread, but the mitigations for these threats have become so numerous that the typical end user can easily be overwhelmed if they are the ones on the hook for ensuring that they are all implemented

and working. For these as well as other reasons, it has become critical for a more automated solution to be put in place to ensure that user empathy, lack of user awareness, and plain outright refusal to cooperate with corporate policies are eliminated as contributors to an unsecured computing environment.

To put the specific project and environment being described into perspective, this paper will discuss implementing a network access control solution based on a large enterprise of approximately 9,000 desktop and 300 server computers connected to a world-wide network. A large portion of the user population uses laptop computers to access the corporate LAN from remote locations, including home offices, hotels, and various other remote locations. Wireless technologies, broadband access technologies, and a corporate virtual private network (VPN) are all used to enable these remote connections. The remaining population of employees accesses the corporate network using a variety of desktop and laptop computers from offices and data centers around the world. There is a wide area network (WAN) that interconnects all of the field office locations to the corporate network, and the data centers are all interconnected as well.

Network Access Controls:

Network access control (NAC) is used to describe the type of security that is put in place to ensure that only “healthy” systems are able to access the network. Synonymous with NAC are such terms as “quarantining,” “port security,” “endpoint security,” and “secure network access.” All of these technologies typically ensure system health by performing an inspection of the computer (to look for required system software) as it is trying to access the network. By “healthy” the typical definition is a computer that has all of the required items described by the corporate computer security

policy, which includes the enterprise standards for anti-virus protection, any prescribed automated patch management agents, up to date security patches and even that the computer itself is a member of a domain or other corporate directory structure. Other requirements can be specified by the security policy and implemented by the security team configuring the NAC system.

As alluded to previously, the need to implement such measures are many, including user unawareness, user empathy, or just plain uncooperative attitudes. As will be discussed later, some of these attitudes introduce human risks along side the technical risks into the equation. But some of the more concrete reasons for being so aggressive with network security include adherence to compliance and other federal regulations such as Gramm-Leach-Bliley, HIPAA, and Sarbanes-Oxley Acts (Infoblox, 2006, ¶1). A NAC solution, therefore, is assumed to help take some of the security compliance requirements out of the hands of end users and place them with an automated solution that provides objective, electronic enforcement of corporate security policies.

Why Is an Information Security Architecture Model Needed?

The type of security measure being discussed in this paper is extremely aggressive. In many cases it requires a large budget to implement, and a large number of resources to configure and manage. Just these attributes alone indicate a clear need for sound project management principles and project organization to be used in implementing a technology such as this one. There will be a number of risks involved. There will be risks present not only in not implementing this technology, but in the very fact that a new technology is coming into play. For instance, while not implementing the NAC solution involves the risk of increased vulnerability to network attacks, putting this type of a

system in place will introduce business risks such as preventing legitimate users from accessing data and doing work. Unless all of the risks are properly evaluated, the project will fail. Additionally, other project management processes will have to be considered, such as time and budget management, allocation of resources, and definition of scope, just to name a few. Using project management techniques and practices will help ensure success of the project, as well as ensuring that all of the stakeholders (customers) expectations are met (Kerzner, 2003, pg. 61). This also helps ensure that their business needs are not hindered or disrupted as well.

The following sections of this paper will briefly discuss each of the elements of the ISA, as outlined in the Tudor text, and how each contributes to the NAC implementation project and follow-on program. The five points of the ISA, according to Tudor are Organization/Infrastructure; Policies, Standards and Procedures; Security Baselines and Assessments; User Awareness and Training; and Compliance. Each of the elements has at least some key feature that should be considered when implementing a technology such as NAC. Each of the five ISA elements will be discussed as they relate specifically to the implementation of a NAC system in a large enterprise.

Organization and Infrastructure:

Before implementing any new technology or changing an existing environment, it is important to assess the organization and infrastructure. In this case, it is important to have a clear picture of how the enterprise is made up in terms of numbers and types of devices (computers) and the types of platforms that are running. In this particular example, the network is large, and the user base is spread out over a world-wide geographical area. The number of computers that has to connect to this network is over

nine thousand. There are two key factors involving the infrastructure. First, there is the matter of how many routers, switches, and other server devices will be needed to support the requirements of port security. Some processing resources will be required by these devices to carry out host inspections. Secondly, there is the matter of how many additional staff will be required to support the extra equipment and software. There is even discussion of how much cross training will be required so that all of the staff already in place can support and troubleshoot initial problems as they occur.

For example: Right after the implementation of a NAC system, users will likely call in to report that they are having problems connecting to the network. The Windows Engineers will have to be cross trained to perform network troubleshooting. Likewise, the network engineers will have to be cross trained to perform Windows troubleshooting to ensure that the proper certificates are in place and that the problem isn't being caused by the system doing what it was designed to do – block access to unhealthy computers.

Policies, Standards, and Procedures:

Prior to implementing such a system, it will be important to ensure that the requirement for having this system operate in the corporate environment is contained in the organization security policy. In order to require people to adhere to this system and its operational requirements, there has to be a stated policy to ensure that this requirement cannot be argued against. Standards will also play an important role in this system's implementation. The system should be chosen so that it presents a set of conventions and agreed upon sets of standards to allow the system to operate more efficiently (Tudor, 2000, pg. 91). This will help to ensure that the system conforms to

standards that are easy to support and easy to maintain. In other words, there will be minimized risks due to consistent operating standards that adhere to security standards.

There will be a number of procedural items for a system such as this. Since a number of staff members and resources will be required to maintain this system, and given that a great deal of cross training will be needed to ensure system support, procedure guides will have to be developed to cover all of the required tasks. As Tudor mentions, procedure guides should be written well enough and detailed enough so that the staff can perform the tasks without having to ask for a great deal of clarification or assistance (Tudor, 2001, pg. 97). Having well written procedure guides in place will help support personnel perform their tasks without having to seek unnecessary assistance.

Security Baselines and Risk Assessments:

While base lining this type of system will be a fairly straightforward process, doing the risk assessments for implementation will be a very detailed process. The baseline issues simply consist of measuring how well a user is able to connect to the network and access resources before the system is implemented, then comparing that performance after implementation. Network switches and routers will be required to handle some of the processing required for end node inspection, so these units will also have to be monitored for performance after implementation to see if they are using significantly higher levels of processing power. Pre-implementation testing will help to determine how much processing requirements are placed on this equipment.

Risk analysis will be a very important aspect of implementation. At the heart of this project is analyzing the risks of implementing versus not implementing the system. On

one hand, by not implementing such a system would increase the risks that an unhealthy computer would connect to and infect the network. On the other hand, the risk of implementing the system is that users would be impeded in their attempt to do their work. There are a variety of other risks that should be weighed as well, such as the risks involved in there not being enough resources to manage the system, or the risk of it costing more than anticipated in training the staff to support the system.

Overall, however, all of these risks have to be weighed using a “calculated risk strategy” to determine if the realized benefits of either choice would outweigh the potential risks and losses of selecting that choice (Barkley and Saylor, 2004,pg. 428).

User Awareness and Training:

Users have to know why their access to the network will potentially be limited. When implementing a system such as this, it will be important for users to be aware of why it is being implemented, and what’s in it for them. If users are given more awareness training in security matters in general and the reasons for this system specifically, they are more likely to accept its introduction. Once the system is in place, the end users are going to be required to know how the system affects them, and what might happen to cause their access to the network to be precluded. When these types of events happen, it will be important for the user to know what basic steps they can take to get connected, and whom to call to help them solve the problems they are experiencing. An annual requirement for security awareness training alone, which is what many corporations require, will not be adequate for ensuring that the users are prepared for this system. Overall security awareness and training in how to interact with this system specifically will be important to ensuring that they are able to do business with minimal

interruption. User awareness can help overcome empathy by helping the end users to see the need for security, helping them to see how they impact security, and allowing them to realize that they have responsibilities when it comes to information security.

In fact, this point in the ISA framework specifies user awareness and training as a separate element of the five-pointed ISA star, when it could be argued that training and awareness should be considered an important element throughout the implementation and through system maintenance. A system such as NAC is large enough in scope and complexity that user awareness and training will need to be covered through various means. User awareness and training will call into play a variety of techniques such as on-line documentation, resident experts, the help desk, and other technical support personnel (Satzinger, et al, 2004, pg. 660). All of these resources will be necessary to help ensure that an ongoing training and awareness program is carried out. Training and awareness, therefore, is an important part of planning for resource utilization as well.

Compliance:

Compliance helps to measure how well an organization is following and complying with defined policies, standards, and procedures (Tudor, 2001, pg. 165). As mentioned previously, a system such as this is being considered by a number of organizations to help them meet compliance requirements with respect to federal on other legal requirements and laws. One important tie-in of the compliance aspect of the project with that of the risk assessment aspects is that part of the risk of not implementing such a system is that the organization might have a more difficult time meeting its requirements with respect to various laws. In other words, a system such as this would

help mitigate threats to potentially sensitive data. Selling the implementation of the system to management might very well involve making the case that this system will help reduce the risks and difficulties in meeting compliance requirements.

Also as important to realize it that a NAC system is the type of system that will (or at least should be) be scalable, meaning that continued growth and expansion of the system will take place in the future. This means that continued analysis of added components will be required to ensure that they do not make the system behave contrary to compliance requirements.

Conclusion:

A network access control system represents an aggressive security measure for an organization to consider. The implementation of such a system should be treated like a project in that a formalized method for ensuring proper resources, risk analysis, and schedule and budget are all considered. This type of system will require the support of management as well as end users in order to be successful. Management will need to know all of the risks involved with choosing or not choosing implementation. End users will need to be aware of why it is being implemented and how the system will change their interaction with their network and their data. All of the other elements of an Information Security Architecture (ISA) will play an important part. By using a framework provided by the ISA, system implementation will be more organized and better thought out. This will result in a NAC system that provides a large pay back in terms of added security benefit and minimized risk in terms of the business needs of the organization.

References

- Barkley, B. and Saylor, J., (2004). *Customer Driven Project Management: Building Quality into Project Processes. Second Edition.* New York, NY: McGraw Hill.
- Infoblox, (2006), *Building a Solid Network Access Control Foundation with the Infoblox ID Aware DHCP Solution.* Whitepaper: Infoblox, Inc., February 2006.
- Kerzner, H. (2003). *Project Management: A Systems Approach to Planning, Scheduling, and Controlling. Eighth Edition.* Hoboken, NJ: John Wiley & Sons.
- Lopez, G., Gomez, A. and Marin, R., (2005), *A Network Access Control Approach based on the AAA Architecture and Authorization Attributes.* White Paper: Proceedings of the 19th IEEE International Parallel and Distributed Processing Symposium, (IPDPS'05). Downloaded from CTU Online Library on March 10, 2006.
- Satzinger, J., Jackson, R., and Burd, S., (2004), *System Analysis and Design in a Changing World. Third Edition.* Boston, MA: Thomson Course Technology.
- Tudor, J.K., (2001), *Information Security Architecture: An Integrated Approach to Security in the Organization.* Boca Raton: Auerbach Publications.