NASA USRP – Internship Final Report

Computer Network Security-

The Challenges of Securing a Computer Network

Vincent Scotti Jr

Brevard Community College, Cocoa, Fl 32922

Computer Network Security-

The Challenges of Securing a Computer Network

Vincent Scotti Jr.[1]
Brevard Community College, Cocoa, Fl 32922

This article is intended to give the reader an overall perspective on what it takes to design, implement, enforce and secure a computer network in the federal and corporate world to insure the confidentiality, integrity and availability of information. While we will be giving you an overview of network design and security, this article will concentrate on the technology and human factors of securing a network and the challenges faced by those doing so. It will cover the large number of policies and the limits of technology and physical efforts to enforce such policies.

Nomenclature

AO	=	*Authorizing Official*
Attacker	=	*A person or system trying to gain illegal access to a system*
C&A	=	*Certification & Accreditation*
CERT	=	*Computer Emergency Response Team*
CIO	=	*Chief Information Officer*
Compromise	=	*an event for which an attacker has tried or succeeded in gaining access to the system*
Event	=	*an observable occurrence in a network or system*
False Positive	=	*when antivirus software wrongly classifies a harmless file as a virus*
Firewall	=	*Physical or logical device to prevent unwanted intrusion to Computer networks*
Full-Duplex	=	*allows communication in both directions*
FISMA	=	*Federal Information Security Management Act of 2002*
Hostile Probe	=	*A program, run by a hacker, which checks for possible security holes on your system*
Incident	=	*A violation of computer security policies, acceptable use policies, or standard computer security practices*
Incident Detection	=	*Discover or determine the existence or presence of an incident*
Incident Response	=	*Incident confinement, recovery, and notification of others*
NIST	=	*National Institute of Standards and Technology*
OSI	=	*A standard way of sub-dividing a communications system into smaller parts called layers.*
PII	=	*Personal Identifying Information*
PKI	=	*Public Key Infrastructure*
POA& M	=	*Plan of Action and Milestones*
Router	=	*Network distribution hardware*
Sensor	=	*A device that converts measurable elements of a physical process into data meaningful to a computer*
IT	=	*Internet Technology*
ITSM	=	*IT Security Manager*
VPN	=	*Virtual Private Network*
Vulnerability	=	*A weakness in a computer system which allows an attacker to reduce a system's information assurance*

[1] Intern, CIO & IT Security, Kennedy Space Center, Brevard Community College.

I. What is Computer Security

Computer security is a section of Information Technology known as information security as it is applied to computers and computer networks. The point of computer security includes protection of information and property from theft, corruption, or natural disaster, while at the same time, allowing the information and property to remain accessible and useful to its intended users. Computer system security is the combined processes and mechanisms by which sensitive and valuable information or services are protected from exploitation, tampering or destruction by unauthorized activities instituted by untrustworthy or even authorized individuals or unplanned events respectively. The strategies and methodologies of computer security, known as best practices outlined in the NIST documents[2] or Defense in Depth[3]Methodology often differ from most other computer technologies because of its somewhat elusive objective of preventing unwanted computer behavior instead of enabling wanted computer behavior.

Both of these methodologies use the risk management method when designing a computer system lifecycle, which should be applied to all computer systems. The better the design, the easier it is to implement the best practices or methods. The System Design Life Cycle design process starts with:

1. Initiation Phase- what is the need for the system.
2. Development or Acquisition Phase – the system is designed, bought, developed, and constructed.
3. Implementation Phase – system security is configured and enabled.
4. Operation and Maintenance Phase – The system is put in operation with ongoing support.
5. Disposal – this is the phase where information, hardware, software may be discarded.

The disposal phase is the last phase of the risk management best practices methodology. We will discuss the risk management methods later on in this article and its application of best practices.

II.

III. Introduction – Why the Need for Computer Security

The need for computer security is one of the most important issues to be considered when planning on using a computer system for personal use or business. Most people today take computer security for granted; they just think by installing anti-virus software on the computer and the system will be protected. The reality is far from the truth. Computer security has multiple aspects to the vulnerabilities facing computers. The first is the design aspect of the system. A system should be designed from the beginning with computer security in mind. By using the best practices[4] mentality towards computer security, it will go a long way to helping secure a system.

Next is the most challenging by far: the human aspect of computer security. The human factor has to deal with people not following guide lines set forth by NIST[5] or the host system administrator. A person not changing his password regularly or securing her password is a big problem in computer security. Another is social engineering attacks, where people ask you for personal information which to you seems harmless, but helps an attacker guess your password and gain access to your system. This is a big problem with people who use social networks such as Face book and Twitter. Hackers surf these site looking for information, which will help them infiltrate your computer system.

Another in the list of challenges is the technological aspect of Computer Security; we live in a world where technology grows by leaps and bounds. Every time a company comes out with a new piece of hardware to help you secure your computer network against intrusions, there is another piece of hardware or software which enables hackers to gain access to your system. This is a cat and mouse game in which the mouse (Hackers) seems to be winning. The effort it takes to keep up with the latest technology seems insurmountable at best.

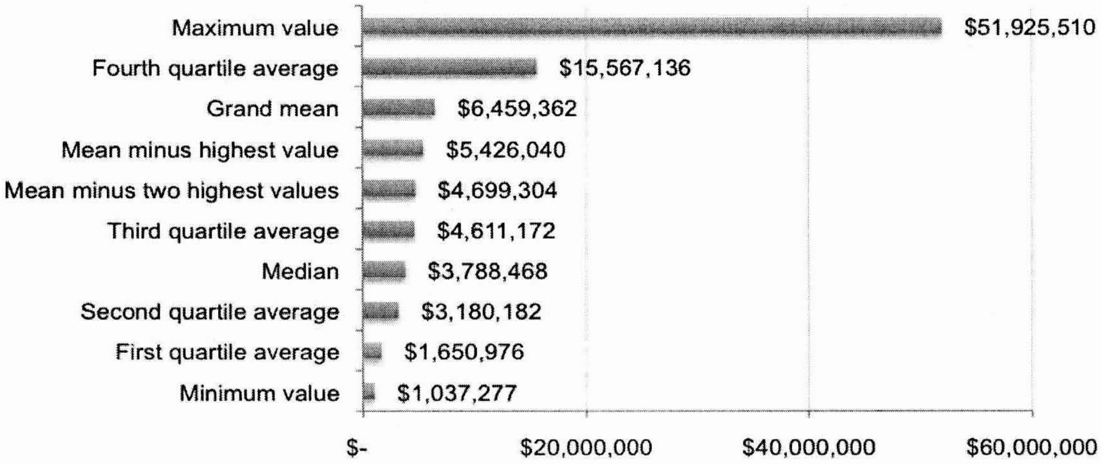
This brings us to the last topic, which is the implementation of policies and the effects of the IT network Budget. We all know that by following the policies suggested by NIST that it would make it much easier to secure a computer network, but as I mentioned above, there are a couple of different areas, which makes it hard to follow. Whether it takes training for the users, purchases of new equipment or implementing policies; it all comes down to

[2] (National Institute of Standards and Technology, 2011)
[3] (NSA:Information Assurance Solutions Group, 2000)
[4] (National Institute of Standards and Technology, 2011)
[5] (Technology, 1995)

the budget and the resources it takes to insure the confidentiality, integrity and availability of information. This includes correcting all the vulnerabilities. We all know in this economy, the IT budget seems to keep shrinking all the time, while at the same time the threats seem to keep getting more sophisticated and frequent.

In the first ever study on the annual cost of cyber crime done by the Ponemon Institute July 2010[6], it was found that out of the 45 companies it surveyed in the study, the average annualized cost of cyber crime of the 45 organizations in our study is $3.8 million per year, but can range from $1 million to $52 million per year per company.

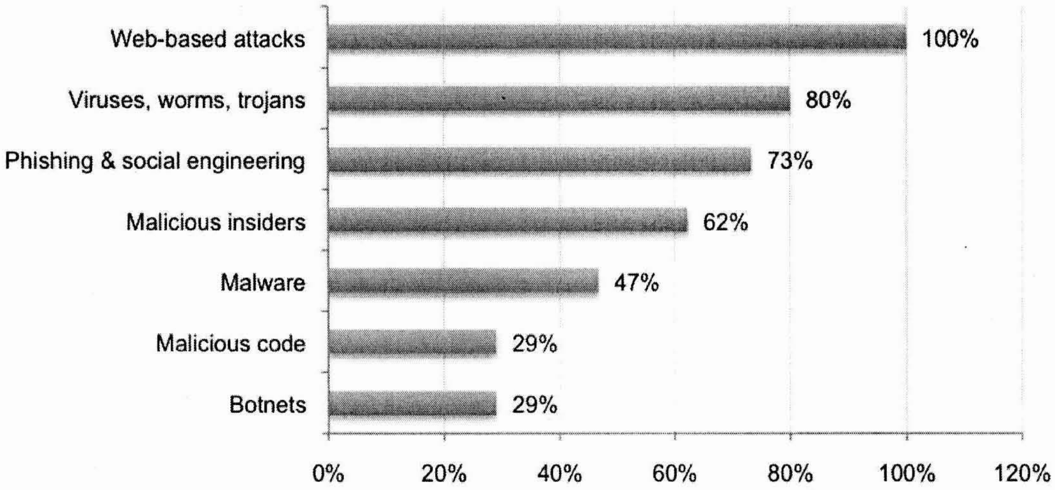
Key benchmark sample statistics on the annualized cyber crime cost[7]



The average occurrence of attacks in our survey was 50 per week, with the most costly cyber crimes being those caused by web attacks, malicious code and malicious insiders.[8] These attacks are being perpetrated by nation states, terrorists, criminals, corporate spies, general hackers, and even malicious insiders.

Frequency of cyber attacks experienced by benchmark sample[9]

The percentage frequency defines a type of attack categories experienced.



So you see, the cost to an organization's bottom line is severely impacted by security breaches, and the IT budgets proposed do not start to fill the needs of the IT security department. Nor do they take into effect the cost of the breach. The saying is not if your computer network will be breached, but when?

[6] (Ponemon Institute LLC, 2010)

[7] (Ponemon Institute LLC, 2010)

[8] (Ponemon Institute LLC, 2010)

[9] (Ponemon Institute LLC, 2010)

The following chart will take us through the different phases (cycles) of the best practices method of risk management. This system of cycles will continue at different phases during the life of the computer Network. See Below:

Table 2-1 Integration of Risk Management into the SDLC

SDLC Phases	Phase Characteristics	Support from Risk Management Activities
Phase 1—Initiation	The need for an IT system is expressed and the purpose and scope of the IT system is documented	• Identified risks are used to support the development of the system requirements, including security requirements, and a security concept of operations (strategy)
Phase 2—Development or Acquisition	The IT system is designed, purchased, programmed, developed, or otherwise constructed	• The risks identified during this phase can be used to support the security analyses of the IT system that may lead to architecture and design trade-offs during system development
Phase 3—Implementation	The system security features should be configured, enabled, tested, and verified	• The risk management process supports the assessment of the system implementation against its requirements and within its modeled operational environment. Decisions regarding risks identified must be made prior to system operation
Phase 4—Operation or Maintenance	The system performs its functions. Typically the system is being modified on an ongoing basis through the addition of hardware and software and by changes to organizational processes, policies, and procedures	• Risk management activities are performed for periodic system reauthorization (or reaccreditation) or whenever major changes are made to an IT system in its operational, production environment (e.g., new system interfaces)
Phase 5—Disposal	This phase may involve the disposition of information, hardware, and software. Activities may include moving, archiving, discarding, or destroying information and sanitizing the hardware and software	• Risk management activities are performed for system components that will be disposed of or replaced to ensure that the hardware and software are properly disposed of, that residual data is appropriately handled, and that system migration is conducted in a secure and systematic manner

[10]

Now that we have the design process explained, we next must address risk assessment. Risk assessment is the process in which you take all the different variables into account when trying to prevent a security breach into your computer network, by preventing risks that may impact your operations. It is much harder trying to prevent a security breach than to try to react to one. The difference is when you successfully implement your policy on risk assessment; you can prevent and eliminate the opportunity for breaches to occur.

[10] (National Institute of Standards and Technology, 2011)

The alternative is having your system breached and compromised with the loss of valuable information, time and resources and reputation trying to correct the situation. There are numerous factors involved; for the purpose of this paper, see the cause and effect chart below:

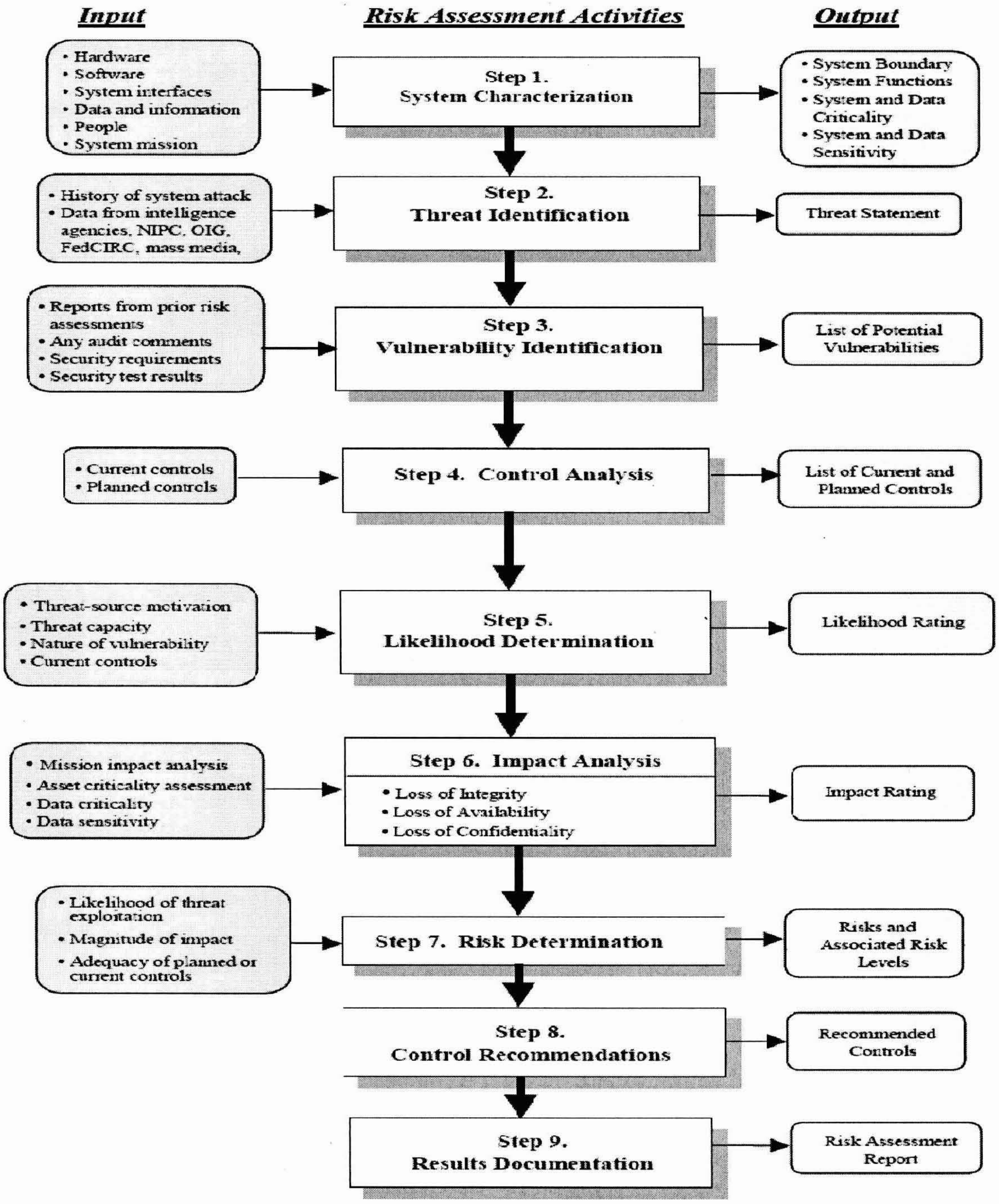


Figure 3-1. Risk Assessment Methodology Flowchart [11]

[11] (National Institute of Standards and Technology, 2011)

III. Related Technologies

A. Hardware

To provide good computer network security, you would start with the type of hardware you purchase and where you store it. Now most people would not consider a secure building and/or room to be hardware, but where you set up a data network is just as important as which hardware you purchase. You need a secure room to house servers, firewalls and intrusion detection devices, which are hooked to the network. What good is it to have a list full of policies like environmental and physical controls in place with the best anti-virus software, if you are not going to keep the potential intruders away from the very thing you are trying to protect. Doors should be locked, allowing entrance to authorized personnel only, rooms should have redundant cooling systems if one should fail (overheated servers can bring down a system just as fast as a virus), and a back-up electrical supply should also be considered.

Firewalls are an important part of network security; they are your first line of defense when it comes to deterring intruders. A firewall is a network device or set of devices designed to allow or prevent network traffic based upon a set of rules, and it is frequently used to protect computer networks from unauthorized access while permitting legitimate communications to occur. Firewalls can be hardware based, software based, or a combination of both.

Hardware related firewalls are connected between the network and the outside WAN (Wide Area Network); there are three generations[12] in use as of today, depending on the IT budget and business. The three are:

1. The First Generation is a packet filtering firewall, which works mainly on the first three layers of the OSI reference model, which means most of the work is done between the network and physical layers.
2. The Second Generation is an application firewall, which is much more secure and reliable compared to the packet filter firewalls, because it works on all seven layers of the OSI model, from the application down to the physical Layer.
3. The Third Generation firewall combines both of the technologies above with "stateful" filters or what they call "stateful packet inspection", because it maintains the records of all the connections passing through the firewall and it is able to determine whether the packet is the start of a new connection, a part of an existing connection, or is an invalid packet.

Firewalls can also use software to prevent unwanted traffic by disabling specific ports, limiting the type of traffic permitted through the firewall and also connecting only to those specific IP addresses which it is set up to allow. I will discuss aspects of firewalls in the software section of this paper.

Routers are devices, which forward data packets between different computer networks. Routers perform the traffic cop duties of "directing data traffic" functions on the Internet. When multiple routers are used to inter-connect multiple networks, the routers exchange data about destination addresses, using a dynamic routing protocol to construct their router table. Each router builds up a table listing the preferred routes between any two systems on the interconnected networks. A router has the ability to connect to different physical types of network connections, (such as copper cables, fiber optic, or wireless). It also contains a small program (software) called firmware for different networking protocol standards. Each network interface uses this specialized computer software to enable data packets to be forwarded from one protocol transmission system to another.

Routers can also use these protocols to secure a computer network, network address translation (NAT) is sometimes thought of as a firewall technology, but it is actually a routing technology[13]. Global computer network traffic must be carefully taken into consideration as part of the overall security strategy. Separate from the router may be a firewall or VPN networking device, or the router may include these and other security functions. Many companies produced security-oriented routers, including Cisco Systems, Juniper and Palo Alto.

A network tap appliance is a hardware device which provides a way to access and monitor the data flowing across a computer network. It is usually installed between the firewall and the computer network. Network taps are usually used for network intrusion detection systems, network probes, packet sniffers, and other types of monitoring and collection devices. These taps run software which requires access to a computer network segment. A network tap is used in security applications because they are non-obtrusive and are not detectable on the Computer network (They have no physical or logical address). Network taps can handle full-duplex_and non-shared networks, and will usually allow (pass-through) traffic even if the tap stops working or loses power.

[12] (Stephanie Forrest, 2002)
[13] (Paul Hoffman, 2009)

B. Software

Software plays a big part of the network security equation. Software like operating systems, browsers settings, firewall software, packet sniffing software, and security patches for Operating systems, and applications all are an integral part of computer security using software as a means to control unauthorized access to a computer network. The Software plays a big part of a layered defense[14] against intruders. Examples of layer defenses, which utilize software, are listed below:

Examples of Layered Defenses[15]

Class of Attack	*First Line of Defense*	*Second Line of Defense*	*Defense Mechanisms Deployed*
1.Passive	*Link & Network Layer Encryptions and Traffic Flow Security*	*Security Enabled Applications*	*NAT Translation* *Telnet* *Virtual Private Network*
2.Active	*Defend the Enclave Boundaries*	*Defend the Computing Environment*	*Firewalls, Routers*
3.Insider	*Physical and Personal Security*	*Authenticated Access Controls, Audit*	*Passwords, Smart Card Readers, Audit &Security logs*
4.Close-In	*Physical and Personal Security*	*Technical Surveillance Countermeasures*	*Security Cameras, Biometric Scanners, Keypad Smart Locks*
5.Distribution	*Trusted Software Development and Distribution*	*Run Time Integrity Controls*	*Apply all the latest updates to operating systems, Applications, Anti-Virus signatures, Spyware signatures*

In the passive attack, we would use one or all of the following protocols:

NAT (Network Address Translation), which is like a receptionist in an office who uses one public telephone number. All phone calls made from the office all appear to come from the same telephone number. But, all incoming calls have to be transferred to the correct private extension by an operator/ receptionist asking the callers who they'd like to speak with; private extensions cannot be dialed directly from outside.

VPN(Virtual Private Network) is a protocol which encapsulates data traffic using a secure cryptographic method between two or more networked routers or devices which are not on the same private network to keep the transferred data private from other devices on one or more of the other LANs (local area networks) or WANs (wide area networks). There are many different uses, classifications, and implementations for VPNs.

Telnet is a network protocol used on the local area networks to provide a two-way interactive text-based communication facility using a virtual terminal connection. User data is combined with Telnet control information in an 8-bit (byte oriented) data connection over port 23, TCP (Transmission Control Protocol). Telnet can also describe the software that implements the client part of the Client –Server protocol used over TCP.

In the active attacks, we would use software provided by companies making the operating systems, routers, firewalls to limit the open ports, types of traffic based on IP addresses, headers, and protocols. We could limit the types of traffic by denying specific addresses and applications from running on the network. Using Anti-virus and anti-malware/spyware software also would be used at this point to protect the network.

Insider attacks refer to attacks by disgruntled or untrustworthy employees. Insider attacks involve employees using social engineering to get colleagues' passwords or information to gain unauthorized access to the network, or using authorized access in an unauthorized manner. Disgruntled employees may steal information, or destroy files and information from the network to get back at the company. The extreme case could involve selling the information to other companies or countries.

Close-In attacks refer to attacks by individuals on the infrastructure of the network, by gaining access to the data centers, servers, routers and any other part of the network. To prevent these types of attacks, you would use Security cameras in the data center, secure the router closets and servers, smart card access locks to secure areas, and secure log-ins on all parts of the network, like Biometrics Scanners.

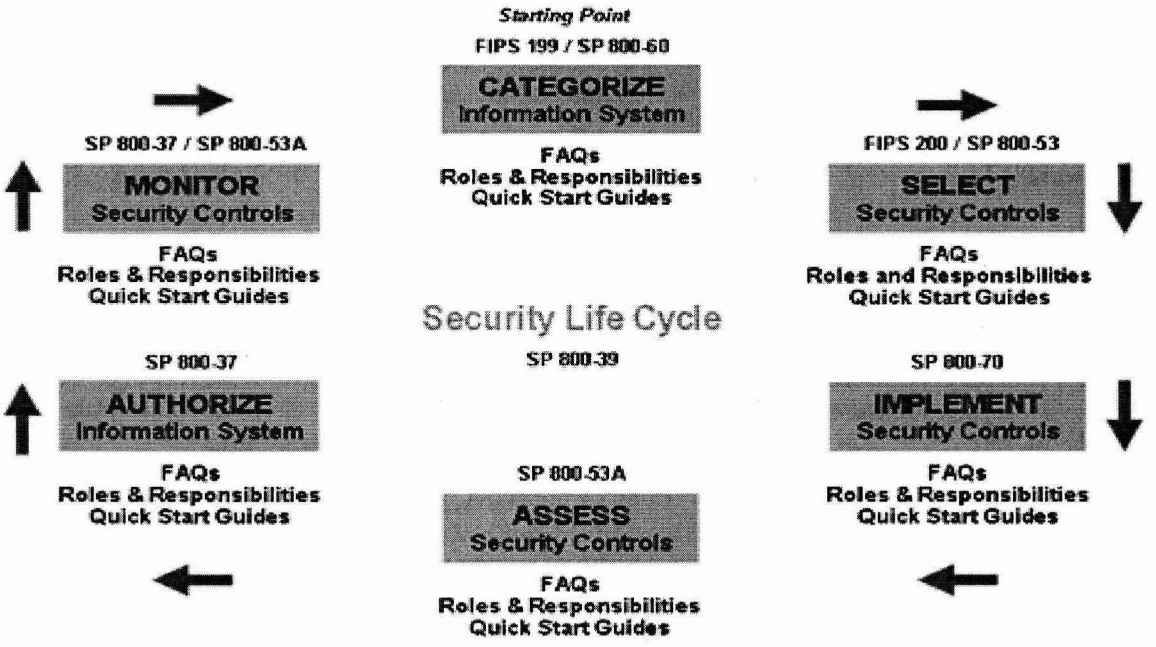
Distribution attacks can be prevented by insuring that all your anti-virus signatures and updates for applications and operating systems are properly done in a timely manner. By insuring this is done, you prevent unauthorized access to the computer Network due to vulnerabilities found in software not up-to-date on patches.

[14] (NSA:Information Assurance Solutions Group, 2000)

[15] (NSA:Information Assurance Solutions Group, 2000)

IV. Policies and Procedures

Policies and procedures is another component of controls used to allow the computer network to function in a standard and efficient manner. The controls are put in place to allow computer administrators to control how, who and what has access to the network. The computer policies can be derived from NIST documents, which are used as best practices and a requirement for Federal Information Systems.[16] Other standards such as ISO270001, HIPAA, SOX or COBIT may also be in used. Not all policies will apply to all computer networks, computer network administrators and Computer Information officers will decide which policies and controls will be implemented depending on the use for the network and the cost to implement such policies. Some, no matter what the cost, will be implemented, such as audit controls, system security hardware, personnel training and the use of application patches. See the chart[17] below as to the different policies needed to be considered to protect a federal computer network system:



As you can see, there are a multitude of factors needed to be taken into account, when designing and implementing security controls on a computer network. You have NIST special publications18 which start with categorizing a network using SP 800-60, selecting controls SP 800-53, and Implement controls SP 800-70, Assess Controls (audit) SP 800-53, Authorize to operate SP 800-37 and finally Monitor SP 800-53A. These are just some of the basic policies (controls) needed to operate a computer network; other would or should be used depending on the network application. Some of these controls might be cost prohibitive depending on the size of the computer network.

SP800-60 is a guide for matching the different types of computer information and information systems to the applicable security categories. The proper identification of the information used on information systems is very critical to the proper choice of security controls and ensuring the confidentiality, integrity, and availability of the system and its information19. SP 800-60 is intended to help federal agencies consistently match the security impact

[16] (National Institute of Standards and Technology, 2011)
[17] (National Institute of Standards and Technology, 2010)
[18] (National Institute of Standards and Technology, 2011)
[19] (William C. Barker, 2008)

levels(risks) to types of information (privacy, medical, proprietary, financial, corporation sensitive, industrial secret, investigation, etc); and information systems (mission critical or support, administrative, etc.).[20]

SP800-53 is the guide for "Recommended Security Controls for Federal Information Systems and Organizations."[21] The proper selection and implementation of the appropriate *security controls* for an information system or a collection of systems is a very important task, which can have major implications on the operations and assets of an organization or agency, as well as the welfare of individuals and the nation. "Security controls are the management, operational, and technical safeguards or countermeasures employed within an organizational information system to protect the confidentiality, integrity, and availability of the system and its information."[22] Some questions which should be answered are: what is the security controls needed to properly defend against the risk, what is the required base-line level of confidence needed to insure the desired controls are working as Intended, and have the selected security controls been implemented in a timely manner or is there a plausible plan for their implementation in the near future?

SP800-70 is titled the National Checklist Program for IT Products: Guidelines for Checklist Users and Developers[23], this publication helps the network administrator and security personnel design a check list to insure all the security settings and policies are implemented in the environment for which they were designed. Securing networks and hosts continues to increase in importance, while at the same time the complexity to secure such networks is increasing each and every day. Hardware, operating systems and applications have inherent vulnerabilities by default and the check list is designed to help the administrator and security personnel ensure that the appropriate security policies and controls are in place.

SP800-53A is the Guide for Assessing the Security Controls in Federal Information Systems, Organizations, and Building Effective Security Assessment Plans[24]. This is one of the most important publications that will be referenced, when auditing a security plan and system. "Security control assessments are not about checklists, assessments are the principal vehicle used to verify that the implementers and operators of information systems are meeting their stated security goals and objectives".[25]

It is very important to note that this is an on-going process to insure and maintain a secure environment in a computer network. The challenges simple pass-fail results, or generating paperwork to pass inspections or audits—rather, security controls change from day to day as the methods used by individuals trying to gain unauthorized access to the network develops. This is where the cat and mouse game I referenced earlier comes into play. Because of the ever-increasing size and complexity of today's computer systems, it is safe to say that it is daunting task to secure a network in real time, so the securing of the network is always behind the threats.

All that can be done is identify potential problems, system weaknesses and deficiencies, Prioritize risk mitigation decisions and activities, Confirm that identified weaknesses and deficiencies have been addressed, continuous monitoring activities for security situational awareness, implement security authorization decisions and lastly, make inform budgetary decisions in the capital investment process. Note that this is a never ending cycle.

SP800-37 is the Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach.[26] This is a system wide approach which integrates information security into the enterprise architecture and system development lifecycle and links the risk management processes at the information system level to risk management processes at the organizational level. It also promotes the use of automation to provide senior level leaders the necessary information to make cost-effective, risk-based decisions and provides guidance on the selection, implementation, assessment, and monitoring of security controls. This promotes the best practices concept of near real-time risk management and ongoing information system and the authorization of the system through the implementation of pro-active continuous monitoring processes[27].

[20] (William C. Barker, 2008)

[21] (Initiative, 2010)

[22] (Initiative, 2010)

[23] (Melanie Cook, 2011)

[24] (Initiative, Guide for Assessing the Security Controls in Federal Information Systems and Organizations, Building Effective Security Assessment Plans, 2010)

[25] (Initiative, Guide for Assessing the Security Controls in Federal Information Systems and Organizations, Building Effective Security Assessment Plans, 2010)

[26] (Initiative, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach, 2010)

[27] (Initiative, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach, 2010)

V. Human Factors

The human factor takes into account the different habits, personalities, computer proficiencies and education which tend to cause the greatest challenges to network security administrators. Any security system, no matter how well-designed and implemented, will have to depend on people to manage the network, and use it as intended. We can implement all the technical solutions we want, but it will all fail, if we do not take into account the human factor[28]. The human factor plays a crucial part in most security incidents affecting computer networks and is a troubling feature of the modern "security know-how" best practices.

The human personality is by far the hardest challenge to Network Security; most people who hold a high office in organizations have been with the organizations for a long time and some were there before the advent of computers. The normal response to request from the network security administrator to implement a policy is "This is not the way we have always done it" and herein lies the problem. Most people do not want to learn new ways of doing things and some, if not most, take offense to being told that policies need to change.

The other problem is most people are not up on the new technology due to the lack of formal training. When a company utilizes a new program or operating system, there is a time curve to learn the new system and that time curve is a prime opportunity for system compromises. This is not due to malice, but is the normal process of learning how to use the new system. Companies need to increase the training of their employees to help insure the integrity of the computer system. People need to be taught to break old habits and implement a best practices approach to computer security while working with the system. One problem to training everyone is the limitations of the IT budgets of most system administrators, as well as the belief that this training does not contribute to the bottom line of an organization, but is seen as a cost.

VI. Conclusion

In summation, the goal of computer network security has many varied challenges to the implementation of the policies and controls needed to secure a network. While there is new hardware and software being produced all the time, the limitations of the IT budget limits the timely implementation of the new hardware and software. In addition to the technological limitations to computer security, by far the biggest limitation is the people, who use the computers every day. People need to account for their actions when using the computer network by changing their passwords regularly, staying off the social websites at work, and not clicking on links to unknown e-mails. Administrators need to implement the latest controls and not just keep things the way they always have been!

The best possible solution is education; computer security should be taught at the most basic level to ensure that when employees finally enter the job market, they have the necessary tools to help ensure computer network security in the organizational environment. This is the only way to insure the confidentiality, integrity and availability of information.

[28] (JOSE J GONZALEZ, 2002)

Works Cited

Initiative, J. T. (2010, February 1). *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach.* Retrieved March 28th, 2011, from National Institute of Standards and Technology: http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf

Initiative, J. T. (2010, June 1). *Guide for Assessing the Security Controls in Federal Information Systems and Organizations, Building Effective Security Assessment Plans.* Retrieved March 28th, 2011, from National Institute of Standards and technology: http://csrc.nist.gov/publications/nistpubs/800-53A-rev1/sp800-53A-rev1-final.pdf

Initiative, J. T. (2010, May 1). *Recommended Security Controls for Federal Information Systems and Organizations.* Retrieved March 28th, 2011, from Natinal Institute of Standards and Technology: http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf

JOSE J GONZALEZ, A. S. (2002). *A Framework for Human Factors in Information Security.* Retrieved March 29th, 2011, from Dept. of Information and Communication Technology Agder University College: http://ikt.hia.no/josejg/Papers/A%20Framework%20for%20Human%20Factors%20in%20Information%20Security.pdf

Melanie Cook, S. D. (2011, February 1). *National Checklist Program for IT Products: Guidelines for Checklist Users and Developers.* Retrieved March 28th, 2011, from National Institute of Standards and Technology: http://csrc.nist.gov/publications/nistpubs/800-70-rev2/SP800-70-rev2.pdf

National Institute of Standards and Technology. (2011, March 1st). *Publications : Special Publications (800 Series).* Retrieved March 23rd, 2011, from Computer Security Devision - Computer Security Resource Center: http://csrc.nist.gov/publications/PubsSPs.html

National Institute of Standards and Technology. (2011, March 1st). *Publications.* Retrieved March 4th, 2011, from Computer Security Division/Computer Security Resource Center: http://csrc.nist.gov/publications/PubsSPs 800-30.html

National Institute of Standards and Technology. (2010, August 17th). *Risk management framework (RMF) ---frequently asked questionS (FAQ's), Roles and responsibilities & quick start guides* . Retrieved March 23rd, 2011, from NIST: Computer Security Devision- Computer Security Resource Center: http://csrc.nist.gov/groups/SMA/fisma/Risk-Management-Framework/index.html

National Institute of Standards and Technology. (2002, August). *Security Guide for Interconnecting Information Technology Systems.* Retrieved March 4th, 2011, from Nist.Gov/NIST Special Publication 800-47: http://csrc.nist.gov/publications/nistpubs/800-47/sp800-47.pdf

National Security Agency Attention:Information Assurance Solutions Group – STE 6737. (2000, September 1st). *Defense in Depth.* Retrieved March 3rd, 2011, from A practical strategy for achieving Information Assurance in today's highly networked environments.: http://www.nsa.gov/ia/_files/support/defenseindepth.pdf

NSA:Information Assurance Solutions Group. (2000, September 11). *Defense in Depth.* Retrieved March 15th, 2011, from National Security Agency: http://www.nstissc.Gov/Assets/pdf/4009.pdf

Paul Hoffman, K. S. (2009, September 11th). *National Institute of Standards and Technology.* Retrieved March 16th, 2011, from Guidelines on Firewalls and Firewall Policy, Special Publication 800-41 Revision 1: http://csrc.nist.gov/publications/nistpubs/800-41-Rev1/sp800-41-rev1.pdf

Ponemon Institute LLC. (2010, July 4th). *First Annual Cost of Cyber Crime Study:Benchmark Study of U.S. Companies.* Retrieved March 18th, 2011, from Ponemon Institute: http://www.arcsight.com/collateral/whitepapers/Ponemon_Cost_of_Cyber_Crime_study_2010.pdf?elq=933f1109acb8449b97ab0ff4abb6ec23

Stephanie Forrest, K. I. (2002, March 7th). *A History and Survey of Network Firewalls.* Retrieved March 16th, 2011, from The University of New Mexico Computer Science Department Technical Report 2002-37.: http://www.cs.unm.edu/~treport/tr/02-12/firewall.pdf

Technology, N. I. (1995, October). *An Introduction to Computer Security:The NIST Handbook.* Retrieved March 18th, 2011, from Special Publications (800 Series): http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf

William C. Barker, J. F. (2008, August 1). *National Institute of Standards and Technology.* Retrieved March 28th, 2011, from Guide for Mapping Types of Information and Information Systems to Security Categories: http://csrc.nist.gov/publications/nistpubs/800-60-rev1/SP800-60_Vol1-Rev1.pdf