Computer Network Security

Lesson 2

Principles of Computer Network Security

Lecturer: Dr Msagha J Mbogholi, PhD

Flashback from Lesson 1

- Network security is concerned with the CIA dimensions: Confidentiality, Integrity & Availability
- The OSI model explains the different security issues in the 7 layers
- The challenges in network security lie mostly with 3 issues: how will the network be attacked, what type of attack will it be, who is attacking us.
- The 5 defense principles upon which all defense mechanisms are based: layering, limiting, diversity, obscurity, simplicity
- Security services used to counter different categories of attacks: Confidentiality, Integrity, Availability. The X.800 document adds more categories and relates them to the OSI model
- There are 2 models proposed by IDC as generic security service models: Secure Channel Communication and Network Access Security Model
- Threat modeling is the process by which threats to the network can be identified.

Content

- Complexities of Network Security
- Major Security Controls
- Integrals of Computer Network Security
- Security Requirements
- Design Principles
- Network Security Strategy

Part 1

Complexities of Network Security

Importance of Network Security

- When designing for network security there are many principles that need to be taken into account. In lesson 1 the types of attacks and general defense mechanisms were discussed.
- So, in a network what is the key component we are trying to protect? Of course every component is important, but there is no component more important than the information itself? After all is it not the main reason we have the network in the first place? To exchange and find information, right?
- Thus primarily with network security we wish to prevent the theft or modification of information, allow users to exchange and find information, protect the organization from liability and any other legal issues that may arise due to the tampering of information, and keep cyber criminals at bay.

Complexities of Network Security

- Network security is intricate. At face value the study of the 3 dimensions of security appears simple. However, implementation mechanisms require a certain level of professional knowledge.
- Who will protect the mechanisms themselves? Often the attacker might attack the network after finding the first weakness, which might be a weakness in the defense mechanism itself. Paradoxical.
- More often than not one simple defense mechanism is not enough. A threat needs to be properly assessed in order to determine the best defense mechanism(s) to implement.
- Where to place a defense mechanism both physically and logically is a complexity in itself. Some of these need to be placed in more than one location or defend in more than one logical layer.
- In the case of the information channel the use of channel defense mechanisms might collide with communication protocols or their native defense mechanisms. A possible solution to this is to test before live implementation.

Complexities of Network Security (cont'd)

- An attacker needs to find only one weakness in the network in order to penetrate it. A designer on the other hand has to design against all perceived weaknesses of the system; this essentially makes it a harder task for the designer.
- Management is sometimes reluctant to invest in network security. This rapidly changes when a breach actually occurs. The network team needs to impress on management the cost of protecting the network is negligible compared to the potential damage a breach can cause.
- With the complexities of today's network environments it is difficult for network administrators to effectively monitor the entire network. It calls for more monitoring tools and possibly personnel.
- Considering the SDLC (Software Development Life Cycle) it is evident that the implementation of security is more of an afterthought than a key component.
- Recall the defense principle of simplicity discussed in lesson 1? Yes, complexity (read too much security) makes it difficult for the users of the network. A balance between complexity and ease of use needs to be found by the designer.

Part 2

Major Security Controls

Security Controls

- A control in network security is defined as "An action, device, procedure, or other measure that reduces risk by eliminating or preventing a security violation, by minimizing the harm it can cause, or by discovering and reporting it to enable corrective action." (Stallings & Brown, 2018 pg.. 512).
- In any given network there are 3 major security controls that need to be considered. These controls encompass the whole network, i.e., the hardware, the software and the users. These controls collectively protect the entire network. They are:
    - Technical Controls
    - Operational Controls
    - Management Controls
- We simply call them TOM (of controls)

Management Controls

- Generally list of controls are provided by different standardization bodies: in this particular instance reference can be made to ISO 27001/13335 and NIST SP800-53. These documents are available in the public domain.
- Adapting from NIST SP800-53 Stallings and Brown (2018, pg. 514) list management controls as: Planning, program management, Risk assessment, Security assessment and authorization, System and services acquisition.
- For the purposes of this course we classify management controls as:
  - Management of Risk
  - Policy design and Implementation
- These two effectively discuss all the listed management controls within them.

1. Risk Management

- A risk was defined earlier as an assessment of the likelihood of an attacker or a threat using an exploit to attack or compromise the network. In this instance the attacker is referred to as an agent. Further from the steps of an attack we also learnt that the agent needs access to the system in order to attack it; moreover every agent is motivated by a different end in their pursuit of attacking the network system.
- Risks are generally categorized as:
    - Low
    - Medium
    - High
- Depending on the likelihood of it happening, and the potential damage the attack may cause

Risk Management (cont'd)

- Since it is impossible to totally eliminate risk in the network system, it is desirable to keep the levels of risk at a bare minimum. This is what risk management is all about: identifying and categorizing the risk, determining what mechanisms if any to put in place to control the risk, and implementing it.
- Risks to the network system are everywhere from insiders (employees) to vulnerability points in the network.
- Our desire is to make risk manageable.

Risk Management (cont'd)

- To manage risk the organization must strike a balance between implementing risk aggressively and keeping users satisfied and protected on one hand; appeasing users and risk exposing the system to attack agents. If the organization is a business that deals with both internal and external users then this makes the balance more complicated as at the end of the day management has to align the risks with business objectives; the latter can not suffer.
- Risk management involves three steps: assessment of the risk, mitigating (reducing) the risk, and uncertainty analysis

Assessment of the Risk

- In order to assess risk the first step is to identify what threats and vulnerabilities exist in the network.
- Vulnerabilities are weaknesses or defects found in the network system.
- Threats are the people or things that can exploit the vulnerabilities.
- The first place to identify vulnerabilities are where attacks can take place, and this is always where there are entries to the system. From a software perspective this will mean the connections, namely internet connections, connections via extranet, remote access points. From a hardware perspective this would mean physical access to network devices and infrastructure.

Assessment of the Risk (cont'd)

- After identifying the vulnerabilities the next step is to identify likely threats. The threats will be in the form of employees or business partners. The employees present the insider threat while partners can be both insider or outsider threat. It may make more sense to simply categorize the threats in relation to the users of the system. Is it necessary to know why they want to attack the system?
- Next the existing environment defenses are examined. This gives an idea as to how the current environment is protected from threats. These defenses may include antivirus, firewalls, smart card readers, biometric devices, network and file access control, and so on.
- After collecting all the information regarding vulnerabilities, threats and environment defenses the next step is to analyze the information with a view to categorizing the risk. It is only when the risk is categorized that mitigation measures can be identified and put in place.

Assessment of the Risk (cont'd)

- In analyzing risk it is important to ask a question regarding the likelihood of a particular threat occurring; this is referred to as likelihood assessment. It examines the likelihood of any given threat occurring and its frequency. This makes it easier to classify the threat.
- Analysis of threats enables classification/categorization of the threat either qualitatively or quantitatively.
- Qualitative classification/categorization example: low, medium, high. Alternatively a Likert scale may be used (scale from 1 to 5, with 1 being low risk and 5 being high risk)
- Quantitative classification/categorization example: quantitative analysis in terms of cost to repair, cost of damaged goods, cost of lost income, and so on.
- Classification/categorization will then assist in determining the mitigation measures to put in place.

Risk Mitigation

- Mitigation steps are the ones that will be put in place to contain the risk should it occur.
- These steps are based on a sensitivity analysis of defense mechanisms put in place to mitigate the risk.
- The sensitivity analysis is based on what –if analyses that will measure the difference should the defense mechanism be put in place in terms of impact on the network, users and applications.

Uncertainty Analysis

- In this step the model acknowledges the sources of uncertainty in its development. This is because even in the assessment of risk there are still many unknowns which may have different effects on the mitigation measures taken.

2. Policy Design & Implementation

- A policy is a document that specifies goals and objectives and how they will be implemented. This refers to the organization's goals and objectives.
- It is the work of senior management to define the organization's goals and objectives; for this reason all organizational policies start from the top and trickle down to the lower management levels.
- Senior management will develop a policy that establishes the computer and network security program, its goals and objectives.
- An information security policy is the document from senior management that represents their view on how overall security program, controls and users should be implemented.
- The network and computer policy contains documentation on all matters network and computer that will guide users on the use of the network and computers, goals and objectives of the network, and protect the network from potential attacks.

Policy Design & Implementation (cont'd)

- The network and computer policy (NCP) program is established by management.
- Arising from the NCP there will be 2 other types of policies that will be developed:
- *Issue-specific policies* are made for specific issues that the organization wishes to address.
- *System-specific policies* are made by management to protect certain particular systems.

Policy Design & Implementation (cont'd)

- The Information Security Policy from management will contain the following details: Authority, Purpose, Scope, Roles and Responsibilities, Definitions and (optionally) Revision History.
- Additionally all policies require standards, guidelines and procedures to guide in their implementation. These are defined next.

Policy Design & Implementation (cont'd)

- Standards – They give support to policies by providing the mechanisms to make the policies effective.
- Guidelines – they provide general frameworks with which the implementation of policies is achieved.
- Procedures – they specifically show how the policies, guidelines and standards will be implemented in a configured network environment.

Policy Design & Implementation (cont'd)

- The General Policy/ Information Security Policy (ISP) is developed by senior management and can be said to contain the vision of the organization in terms of security.
- From the general policy several Issue-specific policies can be developed, in alignment with the ISP. The issue – specific policies examine one issue at a time.

Policy Design & Implementation (cont'd)

Issue – specific policy contains the following:

- Goals and objectives of the policy
- Application area / relevance – when and how it is to be applied, and where
- Roles/Responsibilities – who is responsible for the implementation of the policy?
- Compliance – how users are expected to comply with the policy.

An example of an issue – specific policy is on the use of the Internet in the office.

Policy Design & Implementation (cont'd)

System – specific policies address specific systems at a time. The content is basically the same; however, the following should also be taken into consideration:

- Build system specific policies based on the organization's goals and objectives – this most importantly helps the organization determine the applications it needs, and consequently the specific policies to be developed.
- The policies will have specifics on the who, when and how of the targeted systems.
- Can what is being put in the policy be automated by an existing application?

Operational Controls

- Adapting from NIST SP800-53 Stallings and Brown (2018, pg. 514) list operational controls as: awareness and training, configuration management, contingency planning, incident response, maintenance, media protection, personnel security, physical and environmental protection, and system and information integrity.
- These are also explained in detail in the NIST document but for the purposes of this course we categorize them into 3 broad groups:
    - Personnel
    - Computer/Network
    - Physical and Environment

Operational Controls (cont'd)

- Personnel - operations that deal with staff awareness and training. This also includes staffing (the right person for the right job).
- Computer/ Networking – this refers to all system administration and support activities external to the system itself, for example user and software support. Software support refers to the maintenance and monitoring of all software on the network (system), for example configuration management, media control measures, and so on.
- Physical and Environment – all measures put in place to protect the organizational infrastructure as relates to the system.

Technical Controls

- Adapting from NIST SP800-53 Stallings and Brown (2018, pg. 514) list technical controls as: access control, audit and accountability, identification and authentication, and systems and communication protection.
- Technical controls are the different ways in which the system is protected from threats. As the first point of entry is normally some form of logon most of the controls purpose to restrict access to the system. The remaining threats in the system and between devices is handled by the systems and communication protections controls.

Part 3

Integrals of Network Computer Security

Integrals of Network Computer Security

- Network Computer Security should support the mission, vision, goals and objectives of the organization. – this means that development of the network system should help the organization in the pursuit of its goals.
- Network computer security is an integral component that supports management in the day to day running of the organization.
- Network computer security should be cost effective. – the investment cost must justify the risks that the system is being protected from.
- The roles of all players in the computer network security environment should be made clear. – this may be done by the use of effective policies.

Integrals of Network Computer Security (cont'd)

- Network computer security owners have the responsibility of showing all users, internal and external, that the system has appropriate controls in place. – this can be made evident when users first access the system via messages regarding some of the controls, before the user accesses the system.
- Network computer security requires an encompassing approach. – every department should be involved and the benefit impact analysis should be made clear.
- Network computer security should be periodically reassessed. – this is to ensure it satisfies the changing requirements of the organization.
- Network computer security should allow for cultural disparities. – for multiple site organizations spread across different cultures policies should allow for customization in line with the individual cultures.

Part 4

Security Requirements

Security Requirements

- These are based on FIPS 200 which is available freely online at:
- https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.200.pdf
- In this course the importance of the requirements from a functional perspective are analyzed. FIPS 200 standard describes 17 defense mechanisms that relate to the CIA of enterprise wide information systems.

Functional Requirements

Name	Function
Access control	Limited to authorized users only.
Awareness and training	Ensuring all users are made aware of risks and policies across the enterprise. Training users on how to execute security related tasks.
Audit and accountability	Ensuring the system retains proper audit records to enable timely monitoring and accountability of users.
Certification, accreditation and security assessments	Making timely assessment of implemented controls to ensure their continued effectiveness.
Configuration management	Enforcement of security configuration settings
Contingency planning	Ensuring availability of the network and its continuity in times of crisis/attack.
Identification and authentication	Knowing the identity of all users and verifying them and their processes before they take place
Incident response	Procedures on how incidents should be handled and their documentation.

Functional Requirements (cont'd)

Name	Function
Maintenance	Timely maintenance of the system. Includes use of a maintenance schedule
Media protection	Protection of all the system information media by limiting access to authorized users.
Physical and environmental protection	Physical protection of the system and from environmental hazards.
Planning	Development of security plans
Personnel security	Protection of the system and its personnel. Having procedures dealing with when personnel are terminated and how to deal with complicity with security policies and procedures.
Risk assessment	Periodical assessment of risk
System and services acquisition	Acquisition of sufficient resources to protect the system as a whole.

Functional Requirements (cont'd)

Name	Function
System and communications protection	Protecting the system communication both within the organizational boundaries and at its external boundaries
System and information integrity	Ensuring the integrity of information on the system, and ensuring corrective mechanisms in place in the case of a breach.

- All the above requirements ensure the CIA of information in the network.
- Exercise: Can you classify the functional requirements in the table as managerial, technical, or operational controls?

Part 5

Design Principles

Security Design

- It has been acknowledged in several sources of literature and even in lesson 1 of this course that it is near impossible to create a foolproof security environment. Some of the reasons for this were discussed.
- However, with certain design principles in mind it is possible to cover most if not all the bases when designing a security system for the network.
- The National Center of Academic Excellence in Information Assurance (NCAE) have described 13 principles that assist in this pursuit.

Security Design Principles (cont'd)

- Economy of mechanism – keep the design as simple as possible. Paradoxically complex design allows for more vulnerabilities.
- Fail – safe defaults – let the default be maximum protection
- Complete mediation – every access must be checked repeatedly against an access control mechanism
- Open design – think open source vs proprietary. It is recommended to make the design open to public scrutiny
- Separation of privilege – allowing parts of the program to run on separate threads based on the privileges allocated.
- Least privilege – all users and/or processes should only be allowed enough privileges to carry out the tasks that they have to.
- Least common mechanism – sharing of functions by users on the network should be minimized. This makes it easier to isolate incidents and find their source(s).

Security Design Principles (cont'd)

- Psychological acceptability – similar to the concept of fair use. The network should offer as much transparency as possible to the users while still maintaining an optimal level of security
- Isolation – isolation of public parts of the system from internal data and resources. Isolation of users and their files (think user profiles in windows environment). Isolation of security mechanisms to prevent unauthorized access.
- Encapsulation – protection of the data objects (think OO) and only allowing access via select procedures and at designated entry points.
- Modularity – same as the OO principle of modularity. Designing functionality as separate modules in the system.
- Layering – using multiple layers to protect the system….recall layering as a defense principle in lesson 1?
- Least astonishment – system defense mechanisms such as authorization access should not surprise the user; rather they should be clear and easy to understand.

Part 6

Network Security Strategy

Parts of the Strategy

- The development of a security strategy is done by examining or rather asking 3 pertinent questions:
  - What is the security service supposed to do?
  - How does it do it?
  - Does the service actually work?

Implementing the Strategy

- What is the service supposed to do? – This is best implemented using a policy. Policies have been described as security program, issue – specific and system – specific.
- How does it do it? – There are 4 courses related to defense mechanisms and their implementation (PDRR), i.e., prevention, detection, response and recovery.
- Does the service actually work? – Mechanisms put in place to evaluate and monitor the service, such as audits.

Summary

- There are several complexities to address with network security.
- The 3 major security controls are Technical, Operational and Managerial (TOM)
- There are 8 integrals of network computer security.
- FIPS 200 standard describes 17 defense mechanisms that relate to the CIA of enterprise wide information systems.
- The National Center of Academic Excellence in Information Assurance (NCAE) have described 13 principles that assist in the design of the optimal security system.
- The development of a security strategy is done by examining or rather asking 3 pertinent questions – what is the service supposed to do, how does it do it, and does it actually work?

References

- Ciampa, M. (2012). *Security+ Guide to Network Security Fundamentals* (4th ed.). Course Technology.
- Maiwald, E. (2001). *Network Security: A Beginner's Guide* (1st ed.). Osborne_McGraw Hill.
- Peltier, T. R. (2002). *Information Security Policies, Procedures, and Standards: Guidelines for Effective Information Security Management*. Auerbach, NY.
- Stallings, W., & Brown, L. (2018). *Computer security: Principles and practice* (5th ed.). Pearson.
- https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.200.pdf
- National Centers of Academic Excellence in Information Assurance/Cyber Defense (2013). *NCAE IA/CD Knowledge Units.*