African Virtual University

Applied Computer Science: CSI 4104

ADVANCED COMPUTER SECURITY

Richard Musabe

Foreword

The African Virtual University (AVU) is proud to participate in increasing access to education in African countries through the production of quality learning materials. We are also proud to contribute to global knowledge as our Open Educational Resources are mostly accessed from outside the African continent.

This module was developed as part of a diploma and degree program in Applied Computer Science, in collaboration with 18 African partner institutions from 16 countries. A total of 156 modules were developed or translated to ensure availability in English, French and Portuguese. These modules have also been made available as open education resources (OER) on oer.avu.org.

On behalf of the African Virtual University and our patron, our partner institutions, the African Development Bank, I invite you to use this module in your institution, for your own education, to share it as widely as possible and to participate actively in the AVU communities of practice of your interest. We are committed to be on the frontline of developing and sharing Open Educational Resources.

The African Virtual University (AVU) is a Pan African Intergovernmental Organization established by charter with the mandate of significantly increasing access to quality higher education and training through the innovative use of information communication technologies. A Charter, establishing the AVU as an Intergovernmental Organization, has been signed so far by nineteen (19) African Governments - Kenya, Senegal, Mauritania, Mali, Cote d'Ivoire, Tanzania, Mozambique, Democratic Republic of Congo, Benin, Ghana, Republic of Guinea, Burkina Faso, Niger, South Sudan, Sudan, The Gambia, Guinea-Bissau, Ethiopia and Cape Verde.

The following institutions participated in the Applied Computer Science Program: (1) Université d'Abomey Calavi in Benin; (2) Université de Ougagadougou in Burkina Faso; (3) Université Lumière de Bujumbura in Burundi; (4) Université de Douala in Cameroon; (5) Université de Nouakchott in Mauritania; (6) Université Gaston Berger in Senegal; (7) Université des Sciences, des Techniques et Technologies de Bamako in Mali (8) Ghana Institute of Management and Public Administration; (9) Kwame Nkrumah University of Science and Technology in Ghana; (10) Kenyatta University in Kenya; (11) Egerton University in Kenya; (12) Addis Ababa University in Ethiopia (13) University of Rwanda; (14) University of Dar es Salaam in Tanzania; (15) Universite Abdou Moumouni de Niamey in Niger; (16) Université Cheikh Anta Diop in Senegal; (17) Universidade Pedagógica in Mozambique; and (18) The University of the Gambia in The Gambia.

Bakary Diallo

The Rector

African Virtual University

Production Credits

Author

Richard Musabe

Peer Reviewer

Ashenafi Kassahun

AVU - Academic Coordination

Dr. Marilena Cabral

Overall Coordinator Applied Computer Science Program

Prof Tim Mwololo Waema

Module Coordinator

Robert Oboko

Instructional Designers

Elizabeth Mbasu

Benta Ochola

Diana Tuel

Media Team

Sidney McGregor

Barry Savala

Edwin Kiprono

Kelvin Muriithi

Victor Oluoch Otieno

Michal Abigael Koyier

Mercy Tabi Ojwang

Josiah Mutsogu

Kefa Murimi

Gerisson Mulongo

Copyright Notice

Supported By

AVU Multinational Project II funded by the African Development Bank.

Table of Contents

Course Overview

Welcome to Introduction to Advanced Computer Security

There are both practical and theoretical reasons to study algorithms. From a practical standpoint, you have to know a standard set of important algorithms from different areas of computing; in addition, you should be able to design new algorithms and analyze their efficiency. From the theoretical standpoint, the study of algorithms, sometimes called algorithmics, has come to be as the cornerstone of computer science.

This course aim to provide an in-depth understanding of the fundamental algorithmic techniques for design and analysis, in turn impart knowledge and practical competence in use of advanced data structures and the design and Welcome to Advanced computer Security Module. This module provides a study of high-level computer security issues in computer networks and advanced methods of data encryption. It focuses on advanced aspects of computer security, such as encryption, security practices, system security, security for authentication on the Web and password management techniques. Finally this module, students should be able to create secure network architectures adapted to the investment level and required security. Take responsibility for installation, configuration and network security maintenance.

The module aims to give IT infrastructure management skills, where the role of computer security is critical to ensure the integrity of data and the normal operation of the various systems: computer networks, servers and personal computers in the organization. The course will also explore various Information Security controls, how to handle various risk assessment in an organization and finally creating a security policy in organization.

Today, we note that the information is considered the key business of an organization / company due to its usefulness and importance, however, the issue of the company's Information Security is a priority task for managers, because they recognize the value it has and therefore organizations must make sure that it is managed effectively. For this reason, this module is important because you will learn the methods and tools for computer security that can ensure the confidentiality of information in organizations and also learn how to protect their information and systems in a network environment.

Prerequisites

- Introduction to Computer Security
- Communication of Information and Computer Networks

Materials

The materials required to complete this course are:

- server or personal computer
- Smart phones (smart phones)
- Network Infrastructure ;
- Server and client operating system
- Open Source Softwares Like Wireshark, Nmap,OpenVAS

Books

- Pfleeger , Charles P. Pfleeger , Shari L. , " Security in Computing" , Fourth Edition, Prentice Hall PTR , 2006 .
- Malik , S., " Network Security Principles and Practices " . Cisco Press. 2002 .
- Mark - Ousley Rhodes , et al . " Network Security : The Complete Reference, " in 2003
- Kaufman , C. , et al , " Network Security : Private Communication in a Public World ." . 2nd edition , Prentice Hall, 2002 .
- Gert DeLaet , Gert Schauwers , " Network Security Fundamentals ," Cisco Press Fundamentals Series 2004 .
- Oliveira, Victor . Information Security - Techniques and Solutions , 1 edition , Lisbon, 2001

Course Goals

Upon completion of this course the learner should be able to:

- Identify the information security concepts and the main architectures used to protect networks and services;
- Apply the principles and features of encryption techniques, authentication and access control management;
- Create secure network architectures adapted to the level of investment required and security;
- Design and develop authentication and security systems;
- Design and develop encryption algorithms and de-encryption for security systems;

Units

Unit 1: General Concepts Computer Security

In this unit you will learn the general concepts of computer security. We define the IT security concept, the main objectives that lead the study of security. Further on we discuss the safety study of the causes and aspects to be taken into account for the computer security implementation on a computer network.

Unit 2: Cryptography

In this unit we will address the existing security techniques. We speak of the concept Hashing function that is very involved when encryption speech, this encryption method most commonly used in digital signatures. We will also explore methods of authentication encryption algorithms messages.

Unit 3: Network Security and Security Tools

In this unit we will address the concept of security in computer networks. We will also see that network security begins with the existence of the organization's security policy, this policy should be set by the higher of the organization in coordination with technical team. We will address information security protocols in computers network.

Unit 4: Web Security

It is in this unit, which will cover the services and the main Web threats ways and preventing these threats mechanisms. We will address the SSL and TLS, providing a layer of security for two communicating applications (client and server). In the end, we discuss the concept Virtual Private Network (VPN), which will discuss security on a VPN network, your engine runs for tunneling, where we address the main security tools in VPN's, such as encryption, digital certificates, and RADIUS IPSec.

Assessment

In each unit are included formative assessment tools to check the progress of the student.

At the end of each module are presented summative assessment tools, such as testing and final works, which comprise the knowledge and skills studied in the module.

The implementation of summative assessment tools is at the discretion of the institution offering the course. The suggested evaluation strategy is as follows:

1	Unit 1: Assessments	10%
2	Unit 2: Assessments	10%
3	Unit 3: Assessments	10%
4	Unit 4: Assessments	10%
5	MINI-Test	20%
6	Final Exam	30%
7	Laboratory	10%
Total		100%

Schedule

Unit	Activities	Estimated time
General concepts of information security	Activity 1-1: Information Security Management and Risk Assessment	6 hrs
	Activity 1-2: Information Security Management issues	6 hrs
	Activity 1.3: Information Security Planning	6 hrs
Cryptography	Activity 2.1 - Encryption Techniques	6 hrs
	Activity 2.2 - Hash function	2 hrs
	Activity 2.3: Message Authentication and Digital Signature	4 hrs
Network security and security tools	Activity 3.1 - Protocols and safety standards on the Internet	2 hrs
	Activity 3.2 - Wireless Network Security	3 hrs
	Activity 3.3 - Internet Authentication Applications	4 hrs
Web Security	Activity 4.1 - Web Services Security	4 hrs
	Activity 4.2 - Major web protocols	2 hrs
	Activity 4.3 - Virtual Private Network (VPN)	2 hrs

Readings and Other Resources

Extra reading resources

- Oliveira, Victor . Information Security - Techniques and Solutions , 1ed , Lisbon, 2001
- Kaufman , C. , et al , " Network Security : Private Communication in a Public World ." 2nd ed . , Prentice Hall, 2002 .
- Malik , S., " Network Security Principles and Practices " . Cisco Press. 2002 .
- Pfleeger , Charles P. Pfleeger , Shari L. , " Security in Computing" , Fourth Edition, Prentice Hall PTR , 2006 .

The readings and other resources in this course are:

Unit 1

Required readings and other resources:

- Wadlow , Thomas . Network Security . Publisher Campus . Rio de Janeiro, 2000 .
- Rezende , Denis Alcides and ABREU , Aline France . Applied Information Technology to Business Information Systems. Editora Atlas . São Paulo, 2000 .
- DAYS , Claudia. Security and Audit of Information Technology . Axcel Books. Rio de Janeiro, 2000 .
- KRAUSE , Micki and TIPTON , Harold F. Handbook of Information Security Management . Auerbach Publications, 1999 .
- Information Systems Management Issues for the 1990s , Fred Niederman , James C. Brancheau and James C. Wetherbe , MIS Quarterly, Vol . 15, No. 4 (Dec. , 1991) , pp . 475-500

Unit 2

Required readings and other resources:

- Garfinkel , Simson . PGP : Pretty Good Privacy . O'Reilly & Associates. 1995 .
- Khanna , Raman . Distributed Computing Implementation and Management Strategies. Prentice Hall, 1993 .
- Gradient Technologies White Paper - Encryption Security in the Enterprise. URL: http://www.gradient.com/Products/NetCrusader/WhitePaper/wp_pbkey.htm
- White Paper on the impact of the Public Key technology and Digital Signatures on CAD . URL: http://www.datakey.com/SignaSURE-EDM_white_paper.htm .

Unit 3

Required readings and other resources:

- SOARES, Luiz Fernando Gomes; LEMOS , Guido ; Colcher Sergio . computer networks LANs , MANs and WANs to ATM networks . 2.ed. Rio de Janeiro :, 2015 .
- Kurose , James ; ROSS , Keith . Computer network and the Internet : Umaabordagem top-down . 3.ed. Sao Paulo : Pearson Addison Wesley , 2006 .
- McCumber , John. Assessing and Managing Security Risk in IT Systems : A Structured Methodology. 1.ed. Auerbach, 2005 .
- Andrew S. Tanenbaum , Computer Networks Campus, 4th Edition, 2003 .
- James F. Kurose , Keith W. Ross , Computer Networking and the Internet: A Top-Down Approach , 3rd Edition , 2006 .
- Luiz Fernando Soares, Guido Lemos, Sérgio Colcher , Computer Networks , LANs , MANs and WANs to ATM Networks , 2nd Edition , 1995 .
- Osborne , McGraw -Hill, Networks Security , The complete reference , 2004. http://cartilha.cert.br/redes/

Unit 4

Required readings and other resources:

- A. D. Rubin , D. Geer , and M. J. Ranum , Web Security Sourcebook , John Wiley & Sons , New York , 1997 .
- A. D. Rubin , D. Geer , A Survey of Web Security , Computer, September 1998 , pp 34-41 .
- Laurie B. and P. Laurie , Apache : The Definite Guide, 2nd Edition , O'Reilly , 1999. http : //www.gta.ufrj.br/grad/04_1/vpn/Script/RDIIntroducao.html
- Scott , Charlie ; Wolfe , Paul ; Erwin , Mike.Virtual Private Networks, Second Edition. O'Reilly , 1999
- Brian Browne , " Best Practices For VPN Implementation , " Business Communication Review, March2001 .
- Hanks , S., Editor, "Generic Routing Encapsulation over IPv4 ", RFC 1702, October 1994

Unit 1. General concepts of information security

Unit Introduction

The term security is not new for us and even young children have heard this term in radio, television etc., applied in other areas including: military, food, public, road and others. However in computers the term security is exclusively dedicated to protecting information.

Currently the concept of Information Security is standardized by ISO / IEC 17799: 2005, influenced by the Standard English (British Standard) BS 7799. The series of ISO / IEC 27000 have been reserved for dealing with security standards of information. The ISO / IEC 27002: 2005 is still considered formally as 17799: 2005 for historical purposes. The content of the Net Workshop is protected under the Creative Commons license (CC BY-NC-ND). You can play it as long as insert credits WITH LINK to ORIGINAL CONTENT and do not make commercial use of our production. In this lesson, the concept of computer security will be used to refer to the protection of the information. This unit introduces the Information Security Management and risk assessment, Information security management issue, as well as Information security plan.

Unit Objectives

Upon completion of this unit you should be able to:

- Identify different information security management issues
- Perform an information security risk assessment
- Perform an information security plan

Key Terms

Security: Set of measures taken to protect the information.

Information: Information is an organized set of data, which is a message about a particular phenomenon or event.

Learning Activities

Activity 1 - Information Security Management and Risk Assessment

Introduction

In order to control the computer system threats, we need to first be able to manage the computer systems and also be able to assess the possible risks that can harm the organization's computer and network resources. In this activity, we are going to learn the computer security management system and how the organizations implement the security policy and also some risk assessment factors.

Information Security Management

Computer Security Management is a process used to achieve and maintain appropriate levels of confidentiality, integrity, availability, accountability, authenticity, and reliability.

Computer Security Management can be divided into the following:

- Determining organizational computer security objectives, strategies, and policies
- Determining organizational computer security requirements
- Identifying and analyzing security threats to computer assets within the organization
- Identifying and analyzing risks
- Specifying appropriate safeguards
- Monitoring the implementation and operation of safeguards that are necessary in order to cost effectively protect the information and services within the organization
- Developing and implementing a security awareness program detecting and reacting to incidents

The Computer security management process is shown in the figure below, with a particular focus on the internal details relating to the risk assessment process.

It is important to emphasize that computer security management needs to be a key part of an organization's overall management plan. Together with computer security management, computer security risk assessment process should be included into the wider risk assessment of all the organization's assets and business processes. Not until the senior management in an organization are aware of, and support, the computer security management plan, it would be difficult that the desired security objectives will be met and contribute appropriately to the organization's business outcomes.

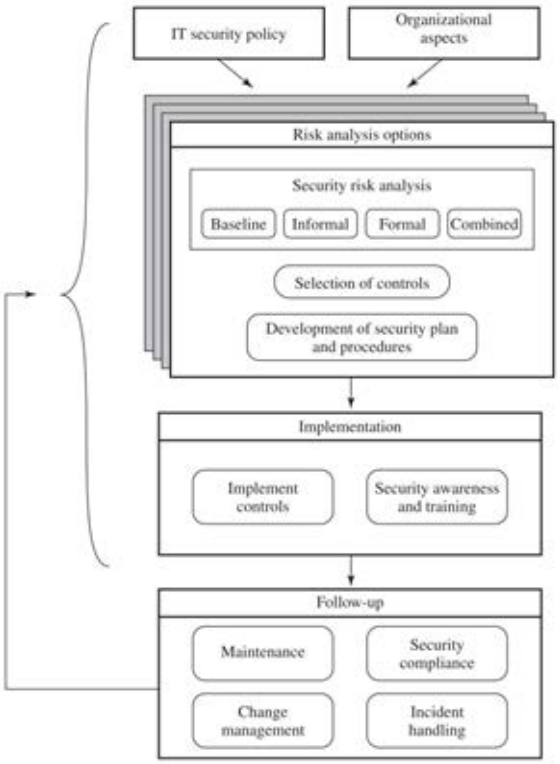


Fig2: Computer security management process (adapted from computer security principles and practice 2nd edition)

Organizational Context and Security Policy

Organizational Context:

The initial step in the IT security management process comprises an examination of the organization's IT security objectives, strategies, and policies in the context of the organization's general risk profile. This can only occur in the context of the wider organizational objectives and policies, as part of the management of the organization. Organizational security objectives identify what IT security outcomes should be achieved. They need to address individual rights, legal requirements, and standards imposed on the organization, in support of the overall organizational objectives.

Organizational security strategies identify how these objectives can be met. Organizational security policies identify what needs to be done. These objectives, strategies, and policies need to be maintained and regularly updated based on the results of periodic security reviews to reflect the constantly changing technological and risk environments.

Implementation of a Security Policy

Definition of a Security Policy:

A security policy is a formal statement of the rules by which people who are given access to an organization's technology and information assets must abide." (RFC 2196, Site Security Handbook)

Why Create a Security Policy?

- To create a baseline of your current security posture
- To set the framework for security implementation
- To define permitted and non permitted behaviors
- To help determine necessary tools and procedures
- To communicate consensus and define roles
- To define how to handle security incidents

Implementation of a security policy as a continuous process

Network security is a continuous process built around a security policy it involves four steps which are:

- Step 1: Secure
- Step 2: Monitor
- Step 3: Test
- Step 4: Improve

Step 1: Secure the Network

Implement security solutions to stop or prevent unauthorized access or activities , and to protect information. It involves the following processes

- Authentication
- Encryption
- Firewalls
- Vulnerability patching

Step 2: Monitor Security

This step detects violations to the security policy. It involves system auditing and real-time intrusion detection. It validates the security implementation in Step 1

Step 3: Test Security

This step validates the effectiveness of the security policy through system auditing and vulnerability scanning.

Step 4: Improve Security

This step uses information from the monitor and test phases to make improvements to the security implementation. It adjusts the security policy as security vulnerabilities and risks are identified.

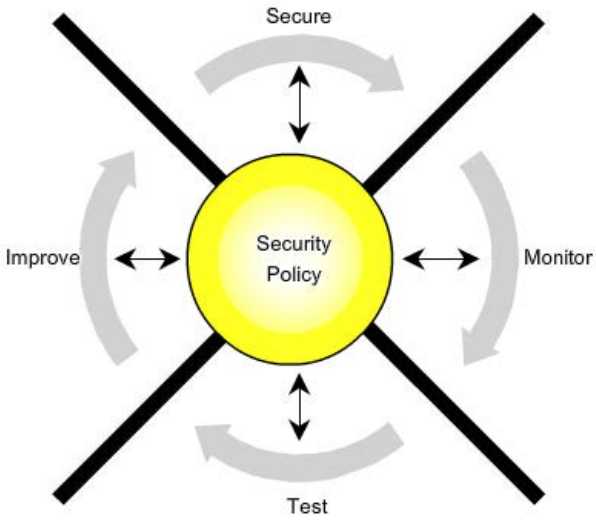


Fig 3: Four steps of security policy

Risk Assessments

This stage is critical, because without it there is a significant chance that resources will not be deployed where most effective. The result will be that some risks are not addressed, leaving the organization vulnerable to threats such as computer threats, while other protection may be deployed without enough reasons, hence wasting time and money.

If a risk is judged to be too much, then appropriate counteractive controls are deployed to reduce the risk to an acceptable level. In practice this requires much time and effort to achieve it due to the rapid rate of change in both computer security technologies and the wider threat environment. In an ideal world the goal would be to eliminate all risks completely.

There are a range of formal standards that detail suitable Computer security risk assessment processes, including [ISO13335], [ISO27005], and [NIST02]. In particular, [ISO13335] recognizes four approaches to identifying and mitigating risks to an organization's IT infrastructure:

- Baseline approach
- Informal approach
- Detailed risk analysis
- Combined approach

The choice among these will be determined by the resources available to the organization and from an initial high-level risk analysis that considers how valuable the computer security systems are and how critical to the organization's business objectives. Legal and regulatory constraints may also require specific approaches. This information should be determined when developing the organization's IT security objectives, strategies, and policies.

1.Baseline Approach:

The baseline approach to risk assessment aims to implement a basic general level of security controls on systems using baseline documents, codes of practice, and industry best practice.

Advantage of Baseline Approach

It does not require the expenditure of additional resources in conducting a more formal risk assessment and that the same measures can be replicated over a range of systems.

Disadvantage of Baseline Approach

No special consideration is given to variations in the organization's risk exposure based on who they are and how their systems are used.

The baseline level may be set either too high, leading to expensive or restrictive security measures that may not be warranted, or set too low, resulting in insufficient security and leaving the organization vulnerable.

2.Informal Approach:

The informal approach involves conducting some form of informal, pragmatic risk analysis for the organization's IT systems. This analysis does not involve the use of a formal, structured process, but rather exploits the knowledge and expertise of the individuals performing this analysis. These may either be internal experts, if available, or, alternatively, external consultants.

Advantage of Informal Approach

The individuals performing the analysis require no additional skills. Hence, an informal risk assessment can be performed relatively quickly and cheaply.

The organization's systems are being examined, judgments can be made about specific vulnerabilities and risks to systems for the organization that the baseline approach would not address. Thus more accurate and targeted controls may be used than would be the case with the baseline approach.

Disadvantage of Informal Approach

Because a formal process is not used, there is a chance that some risks may not be considered appropriately, potentially leaving the organization vulnerable.

Because the approach is informal, the results may be skewed by the views and prejudices of the individuals performing the analysis.

It may also result in insufficient justification for suggested controls, leading to questions over whether the proposed expenditure is really justified.

Lastly, there may be inconsistent results over time as a result of differing expertise in those conducting the analysis.

3.Detailed Risk Analysis:

The third and most comprehensive approach is to conduct a detailed risk assessment of the organization's IT systems, using a formal structured process. This provides the greatest degree of assurance that all significant risks are identified and their implications considered. This process involves a number of stages, including identification of assets, identification of threats and vulnerabilities to those assets, determination of the likelihood of the risk occurring and the consequences to the organization should that occur, and hence the risk the organization is exposed to. With that information, appropriate controls can be chosen and implemented to address the risks identified.

Advantage of Detailed Risk Analysis

It provides the most detailed examination of the security risks of an organization's IT system, and produces strong justification for expenditure on the controls proposed.

It also provides the best information for continuing to manage the security of these systems as they evolve and change.

Disadvantage of Detailed Risk Analysis

The major disadvantage is the significant cost in time, resources, and expertise needed to perform such an analysis. The time taken to perform this analysis may also result in delays in providing suitable levels of protection for some systems.

4.Combined Approach:

The last approach combines elements of the baseline, informal, and detailed risk analysis approaches. The aim is to provide reasonable levels of protection as quickly as possible, and then to examine and adjust the protection controls deployed on key systems over time. The approach starts with the implementation of suitable baseline security recommendations on all systems. Next, systems either exposed to high risk levels or critical to the organization's business objectives are identified in the high level risk assessment. A decision can then be made to possibly conduct an immediate informal risk assessment on key systems, with the aim of relatively quickly tailoring controls to more accurately reflect their requirements. Lastly, an ordered process of performing detailed risk analyses of these systems can be instituted. Over time this can result in the most appropriate and cost-effective security controls being selected and implemented on these systems.

Advantage of Combined Approach

The use of the initial high-level analysis to determine where further resources need to be expended, rather than facing a full detailed risk analysis of all systems, may well be easier to sell to management.

It also results in the development of a strategic picture of the IT resources and where major risks are likely to occur. This provides a key planning aid in the subsequent management of the organization's security.

Disadvantage of combined Approach

If the initial high-level analysis is inaccurate, then some systems for which a detailed risk analysis should be performed may remain vulnerable for some time.

Conclusion

This activity introduced the computer security management system and how the organizations implement the security policy and also some risk assessment factors.

Assessment

1. Provide the advantages and disadvantages of the following approaches;
   - Detailed risk analysis approach
   - Combined approaches
   - Informal approach
2. What is a security Policy?
3. Briefly describe the four steps of a security Policy

Activity 2 - Information Security Management issues

Introduction

Today the business world is increasingly on the Internet, however it is essential that each organization takes care of their information security and privacy. Security threats, vulnerability and risk of privacy are challenging all organizations today, these risks should be identified, understood and overcome.

Often organizations do not know what risks they face and not how to manage these risks as identified. However according to the ITIL (Information Technology Infrastructure Library) is important, good security and privacy practices can provide the organization's growth opportunities through proper management of the security of the organization's information system.

For this reason, in this lesson we will address security management discussing ways of planning, policy and legal practices of implementation of information security systems.

Activity Details

Currently, security is a priority issue for organizations concerned with the confidentiality of your information. However best practices should be incorporated in these modern organizations to ensure continuous monitoring of the data and the integrity of corporative information.

For this reason, for good safety management information an organization begins with the planning of actions to be implemented..

Computer Security Management Implementation

Having seen computer security management process in the previous activity, in this activity, we focus on the latter stages, which include selecting controls, developing an implementation plan, and the follow-up monitoring of the plan's implementation. Details of these steps are illustrated in **Figure 3 adapted from (computer security principles and practice 2nd edition)**.

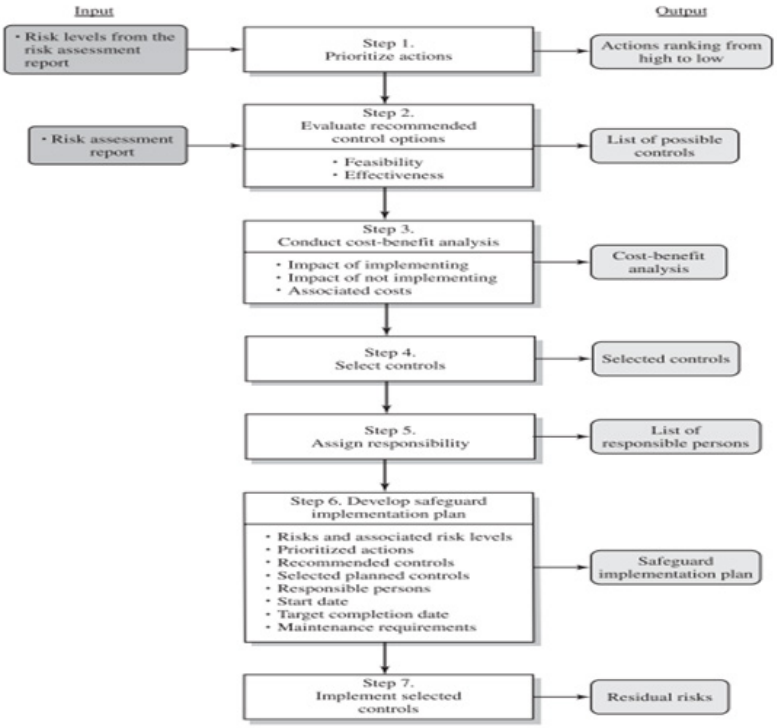


Fig 4: Information Security Management Controls and Implementation

Information Security Controls

A risk assessment on an organization's computer systems identifies areas needing treatment. The next step on risk analysis options, is to select suitable controls to use in this treatment. computer security control helps to reduce risks.

Definition:

Computer Security control: a means of managing risk, including policies, procedures, guidelines, practices, or organizational structures, which can be of administrative, technical, management, or legal nature.

Some controls address multiple risks at the same time, and selecting such controls can be very cost effective. Controls can be classified as belonging to one of the following classes:

Management controls: Focus on security policies, planning, guidelines, and standards that influence the selection of operational and technical controls to reduce the risk of loss and to protect the organization's mission. These controls refer to issues that management needs to address.

Operational controls: Address the correct implementation and use of security policies and standards, ensuring consistency in security operations and correcting identified operational deficiencies. These controls relate to mechanisms and procedures that are primarily implemented by people rather than systems. They are used to improve the security of a system or group of systems.

Technical controls: Involve the correct use of hardware and software security capabilities in systems. These range from simple to complex measures that work together to secure critical and sensitive data, information, and IT systems functions

In turn, each of these control classes may include the following:

Supportive controls: Pervasive, generic, underlying technical IT security capabilities that are interrelated with, and used by, many other controls.

Preventative controls: Focus on preventing security breaches from occurring, by inhibiting attempts to violate security policies or exploit a vulnerability.

Detection and recovery controls: Focus on the response to a security breach, by warning of violations or attempted violations of security policies or the identified exploit of a vulnerability and by providing means to restore the resulting lost computing resources.

Conclusion

This activity addressed the security management issues discussing ways of planning, policy and legal practices of implementation of information security systems.

Assessment

1. Define computer Security control
2. Describe different categories of computer Security control

Activity 3 - Information Security Planning

Introduction

This activity is the continuation of the previous activity, and it will focus mainly on the security planning as well as the ethical and legal aspects of security.

Security Planning:

Planning is critical and at the same time success for the initiative to manage information security. This plan is that it will point the way and steps (activities) that will point and meet the organization's security needs. The plan should be built taking into account all organizational levels: Physical, Logical and Administrative.

According to Wadlow, you can not buy a device or software that makes your business safe, and you can not buy or create a software that can secure your computer to 100%. Security is a process and follows a cycle after its implementation, which means that security expert must:

- Analyze the problem taking into consideration everything you know about safety;
- Synthesize a solution to the problem from its analysis;
- Evaluate the solution and evaluate what aspects did not meet your expectations.

There are several techniques and standards for Management and Security Planning, including Information Security Management Maturity Model (ISM3), Information Security Forum's Standard of Good Practice "(sOGP), Control Objectives for Information and Related Technology (COBIT), infornation Technology Infrastructure Library (ITIL) and Plan-Do-Check-Act (PDCA) among others, which will cover the last.

If we take one technique such as Plan-Do-Check-Act method (PDCA), it is currently the main management method for quality improvement in four stately homes, having been created in the late 20 by Walter A. Shewhart. It is based on control processes, but can be adapted for using an information system security verification process cycle.

The PDCA initials are an acronym for Plan, Do, Check, Act (Plan, Do, Check / Control, Act).

Plan: Define what you want, plan what will be done, set goals and define ways and means to achieve the proposed targets. In the case of security of an information system, this activity can match the assessment of information security risks and selecting appropriate controls.

Do: It is a phase that involves the implementation and operation of controls, implement and execute planned according to the defined goals and methods. In the case of a security information system, this activity may correspond methods defined in the planning.

Check: Check the efficiency and effectiveness of the results achieved, continually check the work to see if they are running as planned. In the case of security of an information system, this activity may correspond to the analysis of generated reports and evaluation of effectiveness of methods taken.

Act: At this stage take place changes, where necessary, to take the set goals, take corrective or improvement actions, if it was found in the previous phase the need to correct or improve any process. In the case of security of an information system, this activity can meet the necessary adjustments or continuity of the methods that have produced positive results.

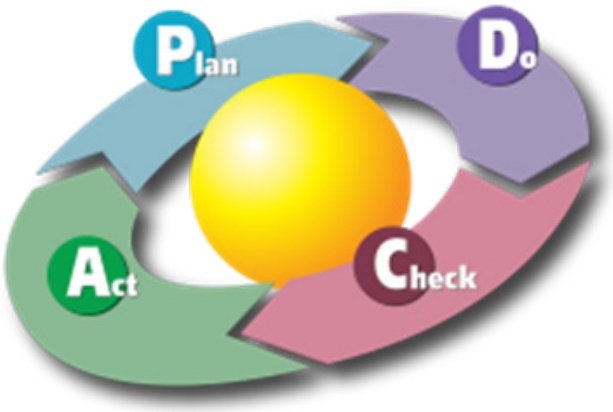


Fig6: PDCA cycle.

Having identified a range of possible controls from which management has selected some to implement, a computer security plan should then be created. This is a document that provides details as to what will be done, what resources are needed, and who will be responsible. The goal is to detail the actions needed to improve the identified deficiencies in the organization's risk profile in a timely manner. This plan should include details of:

- Risks (asset/threat/vulnerability combinations)
- Recommended controls (from the risk assessment)
- Action priority for each risk
- Selected controls (on the basis of the cost-benefit analysis)
- Required resources for implementing the selected controls
- Responsible personnel
- Target start and end dates for implementation
- Maintenance requirements and other comments

Implementation of Security Plan

The computer security plan documents what needs to be done for each selected control, along with the personnel responsible, and the resources and time frame to be used. The identified personnel then undertake the tasks needed to implement the new or enhanced controls, be they technical, managerial, or operational. This may involve some combination of system configuration changes, upgrades, or new system installation. It may also involve the development of new or extended procedures to document practices needed to achieve the desired security goals. Note that even technical controls typically require associated operational procedures to ensure their correct use. The use of these procedures needs to be encouraged and monitored by management. The implementation process should be monitored to ensure its correctness.

This is typically performed by the organizational security officer, who checks that:

- The implementation costs and resources used stay within identified bounds.
- The controls are correctly implemented as specified in the plan, in order that the identified reduction in risk level is achieved.
- The controls are operated and administered as needed.

When the implementation is successfully completed, management needs to authorize the system for operational use. This may be a purely informal process within the organization. Alternatively, especially in government organizations, this may be part of a formal process resulting in accreditation of the system as meeting required standards. This is usually associated with the installation, certification, and use of trusted computing system.

In these cases an external accrediting body will verify the documented evidence of the correct design and implementation of the system.

Implementation Follow Up

The computer security management process does not end with the implementation of controls and planning. it is a cyclic process, constantly repeated to respond to changes in the computer systems and the risk environment. The various controls implemented should be monitored to ensure their continued effectiveness. Any proposed changes to systems should be checked for security implications and the risk profile of the affected system reviewed if necessary.

Unfortunately, this aspect of computer security management often receives the least attention and in many cases is added as an afterthought, if at all. Failure to do so can greatly increase the likelihood that a security failure will occur. This follow-up stage of the management process includes a number of aspects:

- Maintenance of security controls
- Security compliance checking
- Change and configuration management
- Incident handling

Any of these aspects might indicate that changes are needed to the previous stages in the IT security management process. An obvious example is that if a breach should occur, such as a virus infection of desktop systems, then changes may be needed to the risk assessment, to the controls chosen, or to the details of their implementation. This can trigger a review of earlier stages in the process.

Maintenance of Security Controls

The first aspect concerns the continued maintenance and monitoring of the implemented controls to ensure their continued correct functioning and appropriateness. It is important that someone has responsibility for this maintenance process, which is generally coordinated by the organization's security officer.

The maintenance tasks include ensuring that:

- Controls are periodically reviewed to verify that they still function as intended.
- Controls are upgraded when new requirements are discovered.
- Changes to systems do not adversely affect the controls.
- New threats or vulnerabilities have not become known.

This review includes regular analysis of log files to ensure various system components are functioning as expected, and to determine a baseline of activity against which abnormal events can be compared when handling incidents. The goal of maintenance is to ensure that the controls continue to perform as intended, and hence that the organization's risk exposure remains as chosen. Failure

to maintain controls could lead to a security breach with a potentially significant impact on the organization.

Security Compliance Checking:

Security compliance checking is an audit process to review the organization's security processes. The goal is to verify compliance with the security plan. The audit may be conducted using either internal or external personnel. It is generally based on the use of checklists, which verify that the suitable policies and plans have been created, that suitable controls were chosen, and that the controls are maintained and used correctly.

This audit process should be conducted on new computer systems and services once they are implemented; and on existing systems periodically, often as part of a wider, general audit of the organization or whenever changes are made to the organization's security policy.

Change and configuration management:

Change management is the process used to review proposed changes to systems for implications on the organization's systems and use. Changes to existing systems can occur for a number of reasons, such as the following:

- Users reporting problems or desired enhancements
- Identification of new threats or vulnerabilities
- Vendor notification of patches or upgrades to hardware or software
- Technology advances
- Implementation of new computer system features or services, which require changing existing systems
- Identification of new tasks, which require changing existing systems

Configuration management is concerned with specifically keeping track of the configuration of each system in use and the changes made to each. This includes lists of the hardware and software versions installed on each system.

This information is needed to help restore systems following a failure (whether security related or not) and to know what patches or upgrades might be relevant to particular systems. Again, this is a general systems administration process with security implications and must interact with IT security management.

Incident handling:

The procedures used to respond to a security incident comprise the final aspect included in the follow-up stage of IT security management.

Safety Procedures

Security in technology infrastructure should be treated with priority within organizations. To be addressed effectively is necessary for organizations to adopt a set of rules that enable the reduction of vulnerabilities, risks and threats to the technological infrastructure of the organization. These procedures range from passwords cloned through fire and theft of confidential information, in this scenario an appropriate security policy is the differential for the continuity of the network.

Follow some of the actions that represent security procedures for the technological infrastructure of the organization.

Physical Security

Physical security is directly related to aspects associated with physical access to information resources, in addition, it is also related to the techniques of preservation and retrieval of information and their support and storage media.According Wadlow (2000) emphasizes, "Physical security is an important part of the overall network security, but it is one of the most poorly understood aspects of network security."

To ensure system security to inform some aspects should be considered as the following:

- Ensure that there doors, locks, shield, guards in the equipment room.
- Protection for communication links, network equipment and computers,
- Monitoring and control input and output equipment room and whenever possible keep locked location;
- Monitoring of video cameras in the equipment room;
- Alarm systems for equipment rooms;
- Do not allow the entry of unauthorized persons;
- Cable networks in secure locations;
- Systems of uninterrupted power supply

Logical Security

Logic Security is comprehensive and complex aspect, requiring consequently a much more accurate and detailed study. However, we can define the logic control as barriers that prevent or limit access to information, usually electronic, and that otherwise would be exposed to unauthorized access by malicious elements. The security directly related to the confidentiality, integrity and availability (CIA) of the technological infrastructure of the organization.

There are various logical security mechanisms, namely:

- Intrusion detectors programs (antivirus, firewall, anti-span filters, etc.);
- Encryption mechanisms;
- Access control mechanisms for keywords;
- Certification mechanisms and use of secure protocols;
- Disable booting drive A: or CD-ROM on the primary computer;
- Mechanisms for remote access restrictions by VPN (virtual private network);
- Disable or delete unused user accounts;
- Set a backup policy;
- Keep the machine park with upgraded operating systems;
- Keep trained users;

Ethical and legal aspects of security

Professional ethics is defined as a set of rules of conduct that should be put in place in the exercise of any profession. Ethics in Information Security also is related to concepts Privacy integrity, availability and confidentiality are the three attributes that define an information security, however, the code of ethics of computing professionals include some basic aspects of ethical obligations linked to these concepts.

The basic requirements are:

- Computer systems users (hardware and software) must ensure the safety, privacy and economic interests of the organization;
- Each user must enter / change / delete the reports which access is permitted;
- Never destroy maliciously or modify programs, files or data of another person;
- Never violate the privacy of an individual, group or organization;
- Never invade a system for profit or sport;
- Never create or spread computer viruses;
- Never use technology to facilitate discrimination or harassment.

Conclusion

In this lesson you studied the mechanisms for security management. We affirm that planning is critical and at the same time success for the initiative to manage information security. This plan is that it will point the way and steps (activities) that will point and meet the organization's security needs. Further down we approach the Plan-Do-Check-Act method (PDCA) that allows control processes, but can be adapted for use in an information system security verification process cycle. We also discussed the physical and logical procedures for information security. At the end we were discussed some ethical about safety.

Assessment

1. What is the importance of security planning in the organization?
2. What are the detailed items that make up a security plan document ?
3. What does the acronym PDCA mean in full?

Unit Summary

We reached the end of the unit. In this unit you studied the general concepts of computer security. We set the computer security concept, the main objectives that lead the study of security.

You also studied the mechanisms for security management. We affirm that planning is critical and at the same time success for the initiative to manage information security. This plan is that it will point the way and steps (activities) that will point and meet the organization's security needs.

Further down we approach the Plan-Do-Check-Act method (PDCA) that allows control processes, but can be adapted for use in an information system security verification process cycle.

Unit Evaluation

To verify that understands the issues discussed in this unit, answer the following questions:

Instructions

In case of doubt read the corresponding content or query again on the Internet.

Unit Assessment

Check your understanding!

1. Provide the advantages and dis-advantages of the following approaches;
   - Detailed risk analysis approach
   - Combined approaches
   - Informal approach
2. What is a security Policy?
3. Briefly describe the four steps of a security Policy
4. Define computer Security control
5. Describe different categories of computer Security control
6. What is the importance of security planning in the organization?
7. What are the detailed items that make up a security plan document ?
8. What does the acronym PDCA mean in full ?

Assessment Criteria:

For the examination setting and marking the AVU generic marking criteria will be used.

For the assignment, criteria will be drawn up appropriate to the skills assessed , based on the AVU generic marking criteria

Grading Scheme

Refer to the course assessment Table above

Activity 1.1: 14 Marks

Activity 1.2: 8 marks

Activity 1.3; 11 marks

Answers

.Provide the advantages and dis-advantages of the following approaches;

A.Detailed risk analysis approach

Advantage of Detailed Risk Analysis(2 marks)

- It provides the most detailed examination of the security risks of an organization's IT system, and produces strong justification for expenditure on the controls proposed.
- It also provides the best information for continuing to manage the security of these systems as they evolve and change.

Disadvantage of Detailed Risk Analysis(1 mark)

- The major disadvantage is the significant cost in time, resources, and expertise needed to perform such an analysis. The time taken to perform this analysis may also result in delays in providing suitable levels of protection for some systems.

B.Combined approaches

Advantage of Combined Approach (2 marks)

- The use of the initial high-level analysis to determine where further resources need to be expended, rather than facing a full detailed risk analysis of all systems, may well be easier to sell to management.
- It also results in the development of a strategic picture of the IT resources and where major risks are likely to occur. This provides a key planning aid in the subsequent management of the organization's security.

Disadvantage of combined Approach (1 mark)

- If the initial high-level analysis is inaccurate, then some systems for which a detailed risk analysis should be performed may remain vulnerable for some time.

C.Informal approach

Advantage of Informal Approach (2 marks)

- The individuals performing the analysis require no additional skills. Hence, an informal risk assessment can be performed relatively quickly and cheaply.
- The organization's systems are being examined, judgments can be made about specific vulnerabilities and risks to systems for the organization that the baseline approach would not address. Thus more accurate and targeted controls may be used than would be the case with the baseline approach.

Disadvantage of Informal Approach (1 mark)

- Because a formal process is not used, there is a chance that some risks may not be considered appropriately, potentially leaving the organization vulnerable.
- Because the approach is informal, the results may be skewed by the views and prejudices of the individuals performing the analysis.
- It may also result in insufficient justification for suggested controls, leading to questions over whether the proposed expenditure is really justified.
- Lastly, there may be inconsistent results over time as a result of differing expertise in those conducting the analysis

What is a security Policy? (1 mark)

A security policy is a formal statement of the rules by which people who are given access to an organization's technology and information assets must abide

Briefly describe the four steps of a security Policy (4 marks)

Network security is a continuous process built around a security policy it involves four steps which are:

Step 1: Secure

Step 2: Monitor

Step 3: Test

Step 4: Improve

Step 1: Secure the Network

Implement security solutions to stop or prevent unauthorized access or activities , and to protect information. It involves the following processes

- Authentication
- Encryption
- Firewalls
- Vulnerability patching

Step 2: Monitor Security

This step detects violations to the security policy. It involves system auditing and real-time intrusion detection. It validates the security implementation in Step 1

Step 3: Test Security

This step validates the effectiveness of the security policy through system auditing and vulnerability scanning

Step 4: Improve Security

This step uses information from the monitor and test phases to make improvements to the security implementation. It adjusts the security policy as security vulnerabilities and risks are identified.

Activity 1: Information Security Management issues

1. Define computer Security control (2 mark)

   Computer Security control: a means of managing risk, including policies, procedures, guidelines, practices, or organizational structures, which can be of administrative, technical, management, or legal nature.

2. Describe different categories of computer Security control (6 marks)

   Management controls: Focus on security policies, planning, guidelines, and standards that influence the selection of operational and technical controls to reduce the risk of loss and to protect the organization's mission. These controls refer to issues that management needs to address.

   Operational controls: Address the correct implementation and use of security policies and standards, ensuring consistency in security operations and correcting identified operational deficiencies. These controls relate to mechanisms and procedures that are primarily implemented by people rather than systems. They are used to improve the security of a system or group of systems.

Technical controls: Involve the correct use of hardware and software security capabilities in systems. These range from simple to complex measures that work together to secure critical and sensitive data, information, and IT systems functions

Activity 3: Information Security Planning

1. 1What is the importance of security planning in the organization? (2 marks)

   Planning is critical and at the same time success for the initiative to manage information security. This plan is that it will point the way and steps (activities) that will point and meet the organization's security needs. The plan should be built taking into account all organizational levels: Physical, Logical and Administrative

2. What are the detailed items that make up a security plan document ?(8 marks)

   - Risks (asset/threat/vulnerability combinations)
   - Recommended controls (from the risk assessment)
   - Action priority for each risk
   - Selected controls (on the basis of the cost-benefit analysis)
   - Required resources for implementing the selected controls
   - Responsible personnel
   - Target start and end dates for implementation
   - Maintenance requirements and other comments

3. What does the acronym PDCA? (1 mark)

   - Plan, Do, Check, Act

Unit Readings and Other Resources

The readings in this unit are to be found at course level readings and other resources.

- Information Systems Management Issues for the 1990s, Fred Niederman, James C. Brancheau and James C. Wetherbe, MIS Quarterly, Vol. 15, No. 4 (Dec., 1991), pp. 475-500
- Wadlow, Thomas. Network Security. Publisher Campus. Rio de Janeiro, 2000.
- Rezende, Denis Alcides de ABREU, Aline France. Applied Information Technology to Business Information Systems. Editora Atlas. São Paulo, 2000.
- DIAS, Claudia. Security and Audit of Information Technology. Axcel Books. Rio de Janeiro, 2000.
- KRAUSE, Micki e TIPTON, Harold F. Handbook of Information Security Management. Auerbach Publications, 1999.
- KATZAM JR, Harry. Security in Computing. Publisher LTC. Rio de Janeiro, 1977

Unit 2. Cryptography

Unit Introduction

This unit focuses on cryptography and different encryption techniques used in cryptography.

Cryptography is a collection of mathematical techniques for protecting information using encryption and decryption techniques. There two main techniques used in Cryptography which are:

- Symmetric encryption (symmetric key encryption): This technique encrypt/ decrypt a message using the same key. Where the Key is a piece of information or sequence of bits
- Asymmetric encryption (asymmetric key encryption): This technique uses one key for encryption (public key), another key used for decryption (private key)

Unit Objectives

Upon completion of this unit you should be able to:

- Apply key encryption techniques;
- Create principles of encryption, authentication and access control management;
- Apply the encryption technology, authentication and access control management;
- Apply the main encryption algorithms.

Key Terms

Encryption: Encryption can be understood as a set of methods and techniques to encrypt or encode information readable by means of an algorithm, converting an original text m an unreadable text, is possible through the reverse process to recover the original information.

Algorithim: Algorithm is a finite set d and rules which provides a sequence of logical and mathematical operations to solve a specific type of problem.

Key: In computer science, key are key elements that interact with the algorithms for encryption / decryption of messages.

Function: A function is a relationship between two or more sets, established by a law of formation. The elements of a group must be related to the elements of the other group, through this law

Ciphertext (**ciphertext**): Garbled generated by coding a clear / readable text to the user.

Encode (**encrypt**): The act of transforming a plain text into an encrypted text.

Decode (**decrypt**): The act of turning a ciphertext in a clear text.

Learning Activities

Activity 1 - Encryption Techniques

Introduction

Encryption considered as the science and art of writing messages in encrypted form or in code, is one of the main security mechanisms that you can use to protect themselves from the risks associated with the use of information and communication technologies.

At first glance, seems to be difficult to implement an encryption technique, however currently there are many techniques to ensure the encryption mechanisms and some are already installed on the computer operating system.

However, this section will address the concept encryption, its importance and key encryption techniques (symmetric and asymmetric).

Activity Details

Encryption is considered as the science and art of writing messages in encrypted form or in code, it is one of the main security mechanisms that you can use to protect themselves from the risks associated with the use of technological communication resources.

You can encrypt information primarily through codes or ciphers. The codes protect the information exchanging parts for these preset codes. All persons authorized to have access to certain information must know the codes used

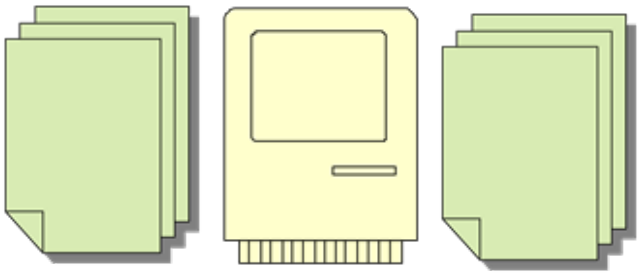


Fig 7: General scheme for encryption text

Why we need to Encrypt our Information:

- Protect sensitive data stored on your computer;
- Create an area (partition) specific to the computer, in which all of the information stored there will automatically be encrypted;
- Protect your backups against unauthorized access;
- Secure communications made over the Internet, such as e-mails sent / received and the banking and commercial transactions.

According to the type of key used, cryptographic methods can be divided into two broad categories:

1. Symmetric key cryptography and Asymmetric keys cryptography.
2. Symmetric encryption

And also called symmetrical encryption secret or private key encryption, uses the same key both to encode and to decode information, that is, the password is used both by the sender to encode the message and the recipient to decrypt it. This model is considered the oldest encryption.

The main advantage is simplicity, this technique provides ease of use and speed to perform cryptographic processes.

The main resident problem in using this encryption system is that when ciframento key is the same used for deciphering, or the latter can easily be obtained from knowledge of the first, both must be previously shared between source and destination before to establish the desired cryptographic channel, and during the process of sharing the password can be intercepted, so it is essential to use a secure channel for sharing.

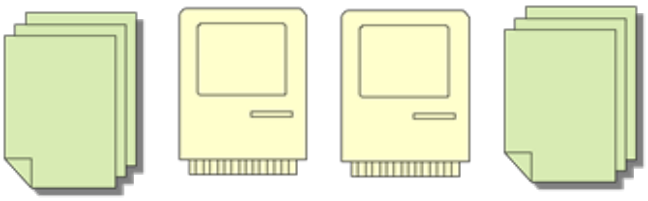


Fig 8: symmetric encryption scheme

Elements of Symmetric Encryption

- Plaintext
- Encryption algorithm
- Secret key
- Ciphertext (encrypted text)
- Decryption algorithm

Principle of Symmetric Encryption

Security of symmetric encryption depends on the secrecy of the key. It does not depend on the secrecy of the algorithm. Because It is difficult to invent new algorithms and keep them secret but It is relatively simple to produce keys.

Requirements for Symmetric Encryption

Strong encryption algorithm: The attacker should be unable to decrypt encrypted text, even if he/she knows several matching pairs of plaintext and encrypted plaintext.

The private key must be kept secret: Sender and receiver must have obtained copies of the secret key (private key) in a secure way and must keep the key secure.

Examples of cryptographic methods that use symmetric key

1. **Data Encryption Standard (DES)**: A standardized encryption algorithm approved by the U.S. government in 1977. It uses a 56-bit key, which is sometimes stored with additional parity bits, extending its length to 64 bits. DES is a block cipher and encrypts and decrypts 64-bit data blocks. It is now considered insecure.In 1998, a cracker could crack the key in 3 days
2. **Advanced Encryption Standard (AES)**: AES replaced DES. A fast block cipher, with variable key length and block sizes (each can be independently set to 128, 192 or 256 bits). An official U.S. government standard since 2002. Now widely used for commercial and private encryption purposes. The algorithm is public, and its use is unrestricted, with no royalties or license fees owed to the inventors or the government.

3. **The Blowfish Encryption Algorithm**: Blowfish is a keyed, symmetric block cipher, designed in 1993 by Bruce Schneier and included in a large number of cipher suites and encryption products. Blowfish is a symmetric block cipher that can be used as a drop-in replacement for DES or IDEA. (Bruce Schneier) . Blowfish was designed in 1993 by Bruce Schneier as a fast, free alternative to existing encryption algorithms. It takes a variable-length key, from 32 bits to 448 bits, making it ideal for both domestic and exportable use.

   Since then it has been analyzed considerably, and it is slowly gaining acceptance as a strong encryption algorithm. Blowfish is unpatented and license-free, and is available free for all uses. While no effective cryptanalysis of Blowfish has been found to date, more attention is now given to block ciphers with a larger block size, such as AES or Two fish. There are two parts to this Blowfish algorithm;

   - A part that handles the expansion of the key.
   - A part that handles the encryption of the data.

   The expansion of the key: break the original key into a set of subkeys. Specifically, a key of no more than 448 bits is separated into 4168 bytes. There is a P-array and four 32-bit S-boxes. The P-array contains 18 32-bit subkeys, while each S-box contains 256 entries.

4. **The encryption of the data**: 64-bit input is denoted with an x, while the P-array is denoted with a Pi (where i is the iteration).

5. **RC5 Algorithm**: In cryptography, RC5 is a symmetric-key block cipher notable for its simplicity. Designed by Ronald Rivest in 1994, RC stands for "Rivest Cipher", or alternatively, "Ron's Code" (compare RC2 and RC4). The Advanced Encryption Standard (AES) candidate RC6 was based on RC5. RC5 has a variable block size (32, 64 or 128 bits), key size (0 to 2040 bits) and number of rounds (0 to 255).

   The original suggested choice of parameters were a block size of 64 bits, a 128-bit key and 12 rounds. A key feature of RC5 is the use of data-dependent rotations; one of the goals of RC5 was to prompt the study and evaluation of such operations as a cryptographic primitive.

   RC5 also consists of a number of modular additions and exclusive OR (XOR)s. The general structure of the algorithm is a Feistel-like network. The encryption and decryption routines can be specified in a few lines of code

Asymmetric encryption

In asymmetric encryption also known as public key encryption uses two separate keys: a public, which can be freely disseminated, and one private, which must be kept secret by its owner. When information is encrypted with one key, only the other pair of the key can decode it. It is with the private key that the recipient can decrypt a message that was encrypted.

The great advantage of this system is to allow anyone to send a secret message using the public key.

As a disadvantage, it takes message confidentiality only when the private key is safe. Otherwise, who have access to the private key will have access to

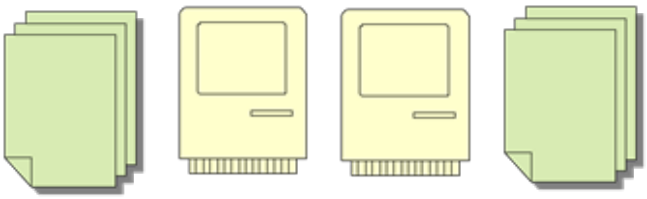


Fig 9: Asymmetric encryption scheme

Examples of cryptographic methods that use asymmetric key

RSA: By Rivest, Shamir & Adleman of MIT in 1977 , Best known & widely used public-key scheme: Each user has a pair of keys: Public key (for encryption) and Private key (for decryption). Based on exponentiation in a finite field over integers modulo a prime . Uses large integers (eg. 1024 bits). Security due to cost of factoring large numbers

Diffie-Hellman: The Diffie-Hellman protocol is a method where two computer users generate a shared private key with which they can then use to exchange information across an in secure channel.

Types of operations used by both symmetric and asymmetric algorithms

There are two types of operations used by these algorithms which are:

Substitutions where Each element of the plaintext (bit, letter, group of bits) is mapped to another element and **Transpositions** where Elements of the plaintext are re-arranged.There are also two ways in which the plain text is processed, which are:

A block cipher where a block of elements is transformed to the output block in one go and a **Stream cipher** where the input elements are processed continuously one element at a time

Block Ciphers v Stream Ciphers

Block ciphers use algorithms to encrypt and decrypt a fixed-size block of plaintext and ciphertext, respectively, usually a multiple of 64 bits where as Stream ciphers continuously encrypt any amount of data as it is presented, usually by mathematically combining the data with a keystream, an infinitely long key sequence that is generated based on a finite key starting value.

Conclusion

Encryption can only be effective if the basic principles of confidentiality, authentication, data integrity are followed and offered. This is why encryption is such an important feature in the transmission of information over the network, and even then it is not able to guarantee 100% security.

One question you should be asking is that what the encryption model that we use, symmetrical or asymmetrical? The answer is simple, we must use both a model called hybrid.

In summary, the encryption mechanisms discussed in this lesson, although employees provide the desired protection to information, increasing data security and minimizing the impact of the attacks submitted to the information that travels through computer networks.

Unit Assessment

1. Search the Internet, landmarks / historic events of related to the use of encryption, according to the following table.

Year	Event

2. Search on the Internet, the main algorithms of symmetric and asymmetric encryption, according to the following table.

Year	Event

3. Differentiate Symmetric Cryptography Asymmetric.
4. Differentiate Block ciphers from stream ciphers

Activity 2 - Hash function

Introduction

With the increasing use of computer networks for organizations to conduct business and the mass use of the Internet, there is a need to use the best transaction security mechanisms and confidential information. Because of this concern, the protection of information has become one of the primary interests of those responsible for systems administrators. The most common way to stop these attacks is the encryption of information. Encryption offers techniques to encode and decode data, so they can be stored, transmitted and retrieved without their modification or disclosure. However, in this lesson we will address some of the functions implemented in encryption algorithms.

Hash function

Technical symmetric or asymmetric encryption can unfortunately not be used in practice in an isolated form, the use of a key mechanism for proper use of digital signatures is required. This mechanism is the hashing function.

This function has the main control the integrity ensuring that the received message is sent by the other party and has not been manipulated.

A hash function is an encryption function that generates a fixed-size output (usually 128-256 bits) regardless of the size of the input. The result of this output is called the message hash.

The hash is a message generated such that it is not possible to perform the inverse processing to obtain the original information and that any change in the original data produces a hash.

Properties of a HASH Function

A hash function is a mathematical function that generally has the following three properties:

Condenses arbitrary long inputs into a fixed length output: In general this hash is much smaller than the data that was put into the function. Because the hash is a smaller thing that represents a larger thing, it sometimes referred to as a digest, and the hash function as a message digest function.

Is one-way:The hash function should be easy to compute, but given the hash of some data it should be very hard to recover the original data from the hash.

It is hard to find two inputs with the same output: It should be hard to find two different inputs (of any length) that when fed into the hash function result in the same hash (collision free). Note that it is impossible for a hash function not to have collisions. If arbitrarily large inputs are all being reduced to a fixed length hash then there will be lots of collisions. (For example - it is impossible to give each of 60 million people a different 4 digit PIN.) The point is that these collisions should be hard to find.

Hash function applications

Digital signatures with appendix: hash-functions are used to bind data together and make the signature process more efficient.

Password storage: hash-functions are sometimes used to store highly confidential data such as passwords.

Cryptographic protocols: hash-functions are often used within cryptographic protocols (including entity authentication protocols) to bind different data items together.

Hash-functions can be used as components from which to construct other cryptographic primitives.

Well Known HASH Function:

MD2 (Message Digest Algorithm RDA-MD2) & MD4

Designed for computers with 8-bit processor, and today hardly used. They know there are many attacks on partial versions of MD2. The MD4 demonstrated to be slower and enables the existence of collisions.

MD5 (Message Digest Algorithm RDA-MD5)

It is an improved version of MD4. At the moment it is considered safe. The algorithm is designed to be fast, simple and secure. Your details are public and free, and have been analyzed by the cryptographic community. It was discovered a weakness, but so far it has not affected the overall security of the algorithm.

SHA-1 (Secure Hash Algorithm)

It is very similar in its mode of operation, with MD5. This algorithm is slightly slower than MD5, but the greater length of the message hash, makes it safer forward looking collision.

SHA-2 (Secure Hash Algorithm)

This is very similar to SHA-1, in its mode of operation. This algorithm is slightly faster than the SHA-1, but the greater length of this algorithm is to use two similar hash functions, different sizes, one different block of 256 bits and 512 other bits.

Conclusion

In this activity, we discussed one of the most used functions in safety technology with data encryption. We also defined the hash function as the encryption function that generates a fixed-size data output regardless of the input size. Addressed key hashing algorithms being the most used at present the MD5 and SHA-2.

Assessment

1. Briefly describe the properties of a hash function.
2. What kind of applications that Hash function can be applied to?
3. Describe four well known Hash Functions

Activity 3 - Message Authentication and Digital Signature

Introduction

In this activity, we will discuss, two mechanisms which can be used to prove that the information within a document have not been modified. These two mechanisms are: Message Authentication and Digital Signature.

Message Authentication

Sometimes, we do not need to encrypt documents. What we need is simply to prove the information in this document has not been modified. For these particular cases, authentication and data integrity services are required and can be performed by two mechanisms: Message Authentication Code (Message Authentication Code - MAC) and Digital Signatures. Half a MAC or a digital signature is to make it possible to send information from one part to another, with the receptor able to demonstrate that fact that information came from the sender it claims to have sent it and that the same has not been tampered with in transmission .

Many people confuse MACs and digital signatures with checksums. A typical checksum is a mechanism whose function is to find errors that are the result of noise or other unintended sources. On the other hand, a digital signature or MAC is a cryptographic checksum that is ordered to detect attacks initiated by intentional or accidental sources.

Message Authentication Codes are mechanisms used with symmetric encryption systems, in order to protect the information. When run on information, this generates a value (small piece of data) that serves as a code for the document.

Obviously, the attacker can also modify the MAC the same way you can modify the data. But without knowledge of the key used to create the MAC, it is not possible to modify this information sent.

Limitation of Using Hash Functions for Authentication

Require an authentic channel to transmit the hash of a message: Without such a channel, it is insecure, because anyone can compute the hash value of any message, as the hash function is public. Such a channel may not always exist

How to address this?

- Use more than one hash functions
- Use a key to select which one to use

Digital signatures

A digital signature is a specific type of MAC (Message Authentication Code) that results from asymmetric encryption systems. To sign a message, a Message Digest function (MD) is used to process the document, producing a small piece of data called a hash. An MD is a mathematical function that refines all the information of a file in a single piece of fixed length data. Once computed one message digest, hash generated if encrypts it with a private key. The result of this procedure is called a digital signature information.

The digital signature is a guarantee that the document is a true and correct copy of the original. The entire process of generation and digital signature verification can be seen in figure 6, using the RSA asymmetric encryption algorithm.

To be possible that a document or tampered signature is not detected, the attacker must have access to private key who signed this document. What makes different digital signatures of MACs is that while the latter require private keys for verification, digital signatures are able to be verified using public key. The digital signature is also valuable because you can sign information in a computer system and then prove its authenticity without worrying about the security of the system that stores it

Security requirements for Digital Signature

A digital signature on a message should provide:

Data origin authentication of the signer : A digital signature validates the message in the sense that assurance is provided about the integrity of the message and of the identity of the entity that signed the message.

Non-repudiation : A digital signature can be stored by anyone who receives the signed message as evidence that the message was sent and of who sent it. This evidence could later be presented to a third party who could use the evidence to resolve any dispute that relates to the contents and/or origin of the message

Input to a digital signature

The message: Since a digital signature needs to offer data origin authentication (and non-repudiation) it is clear that the digital signature itself must be a piece of data that depends on the message, and cannot be a completely separate identifier. It may be sent as a separate piece of data to the message, but its computation must involve the message.

A secret parameter known only by the signer: Since a digital signature needs to offer non-repudiation, its calculation must involve a secret parameter that is known only by the signer. The only possible exception to this rule is if the other entity is totally trusted by all parties involved in the signing and verifying of digital signatures.

Properties of a digital signature

Easy for the signer to sign a message : There is no point in having a digital signature scheme that involves the signer needing to use slow and complex operations to compute a digital signature.

Easy for anyone to verify a message: Similarly we would like the verification of a digital signature to be as efficient as possible.

Hard for anyone to forge a digital signature : It should be practically impossible for anyone who is not the legitimate signer to compute a digital signature on a message that appears to be valid. By "appears to be valid" we mean that anyone who attempts to verify the digital signature is led to believe that they have just successfully verified a valid digital signature on a message.

Conclusion

In this activity, we discussed Message Authentication and digital certification, which in essence assume that is a kind of identification technology that allows electronic transactions are carried out considering its integrity, authenticity and confidentiality in order to prevent tampering, private information capture or other wrongdoing occur.

Assessment

1. What are the limitations of Using Hash Functions for Authentication?
2. What do you understand by digital signatures?
3. Provide the security requirements for digital signatures

Unit Summary

This is why existing security techniques are improved every day and others are created. In cryptography Hashing function concepts is very involved, this encryption method most commonly used in digital signatures.

also addressed message authentication methods of encryption algorithms that a quick analysis and assuming that all algorithms operating in conjunction with the hash function, leads us to conclude that

In summary, the cryptographic algorithms can be combined to implement the cryptographic three basic mechanisms: encryption, hashing and signing. These mechanisms are components of cryptographic protocols, built-in security architecture.

For those who want to work with computers, encryption is an interesting area. Obviously, you must have a lot of affinity with calculations; after all, as can be noted in the article, mathematics is the basis for concepts involving encryption.

Unit Evaluation

Instructions

In case of doubt read the text again of related activities or make the Internet consultation.

Unit Assessment

Check your understanding

1. Differentiate Symmetric Cryptography Asymmetric.
2. Differentiate Block ciphers from stream ciphers
3. Briefly describe the properties of a hash function.
4. What kind of applications that Hash function can be applied to?
5. Describe four well known Hash Functions
6. What are the limitations of Using Hash Functions for Authentication?
7. What do you understand by digital signatures?
8. Provide the security requirements for digital signatures

Assessment Criteria

- For the examination setting and marking the AVU generic marking criteria will be used.
- For the assignment, criteria will be drawn up appropriate to the skills assessed , based on the AVU generic marking criteria

Grading Scheme

Refer to the course assessment Table above

Activity 2.1; 10 marks

Activity 2.2: 11 marks

Activity 2.3: 8 marks marks

Answers

1. Differentiate Symmetric Cryptography Asymmetric. (4 m arks)

   Symmetrical encryption secret or private key encryption, uses the same key both to encode and to decode information, that is, the password is used both by the sender to encode the message and the recipient to decrypt it

   In asymmetric encryption also known as public key encryption uses two separate keys: a public, which can be freely disseminated, and one private, which must be kept secret by its owner. When information is encrypted with one key, only the other pair of the key can decode it. It is with the private key that the recipient can decrypt a message that was encrypted.

2. Differentiate Block ciphers from stream ciphers (4 marks)

   Block ciphers use algorithms to encrypt and decrypt a fixed-size block of plaintext and ciphertext, respectively, usually a multiple of 64 bits where as Stream ciphers continuously encrypt any amount of data as it is presented, usually by mathematically combining the data with a keystream, an infinitely long key sequence that is generated based on a finite key starting value

3. Briefly describe the properties of a hash function. (3 marks)

Condenses arbitrary long inputs into a fixed length output: In general this hash is much smaller than the data that was put into the function. Because the hash is a smaller thing that represents a larger thing, it sometimes referred to as a digest, and the hash function as a message digest function.

Is one-way :The hash function should be easy to compute, but given the hash of some data it should be very hard to recover the original data from the hash.

It is hard to find two inputs with the same output : It should be hard to find two different inputs (of any length) that when fed into the hash function result in the same hash (collision free). Note that it is impossible for a hash function not to have collisions. If arbitrarily large inputs are all being reduced to a fixed length hash then there will be lots of collisions. (For example - it is impossible to give each of 60 million people a different 4 digit PIN.) The point is that these collisions should be hard to find.

4. What kind of applications that Hash function can be applied to? (4 marks)

Digital signatures with appendix: hash-functions are used to bind data together and make the signature process more efficient.

Password storage: hash-functions are sometimes used to store highly confidential data such as passwords.

Cryptographic protocols: hash-functions are often used within cryptographic protocols (including entity authentication protocols) to bind different data items together.

Hash-functions can be used as components from which to construct other cryptographic primitives

5. Describe four well known Hash Functions (4 marks)

MD2 (Message Digest Algorithm RDA-MD2) & MD4

Designed for computers with 8-bit processor, and today hardly used. They know there are many attacks on partial versions of MD2. The MD4 demonstrated to be slower and enables the existence of collisions.

MD5 (Message Digest Algorithm RDA-MD5)

It is an improved version of MD4. At the moment it is considered safe.

The algorithm is designed to be fast, simple and secure. Your details are public and free, and have been analyzed by the cryptographic community. It was discovered a weakness, but so far it has not affected the overall security of the algorithm.

SHA-1 (Secure Hash Algorithm)

It is very similar in its mode of operation, with MD5. This algorithm is slightly slower than MD5, but the greater length of the message hash, makes it safer forward looking collision.

SHA-2 (Secure Hash Algorithm)

This is very similar to SHA-1, in its mode of operation. This algorithm is slightly faster than the SHA-1, but the greater length of this algorithm is to use two similar hash functions, different sizes, one different block of 256 bits and 512 other bits.

6. What are the limitations of Using Hash Functions for Authentication? (2 marks)

   Require an authentic channel to transmit the hash of a message: Without such a channel, it is insecure, because anyone can compute the hash value of any message, as the hash function is public. Such a channel may not always exist

7. What do you understand by digital signatures? (2 marks)

   A digital signature is a specific type of MAC (Message Authentication Code) that results from asymmetric encryption systems. To sign a message, a Message Digest function (MD) is used to process the document, producing a small piece of data called a hash

8. Provide the security requirements for digital signatures (4 marks)

   Data origin authentication of the signer : A digital signature validates the message in the sense that assurance is provided about the integrity of the message and of the identity of the entity that signed the message.

   Non-repudiation : A digital signature can be stored by anyone who receives the signed message as evidence that the message was sent and of who sent it. This evidence could later be presented to a third party who could use the evidence to resolve any dispute that relates to the contents and/or origin of the message

Unit Readings and Other Resources

The readings in this unit are to be found at course level readings and other resources.

- GARFINKEL, Simson. PGP: Pretty Good Privacy. O'Reilly & Associates. 1995.
- KHANNA, Raman. Distributed Computing Implementation and Management Strategies. Prentice Hall, 1993.
- Gradient Technologies White Paper – Encryption Security in the Enterprise. URL: http://www.gradient.com/Products/NetCrusader/WhitePaper/wp_pbkey.htm
- White paper on the impact of the Public Key technology and Digital Signatures on CAD. URL: http://www.datakey.com/SignaSURE-EDM_white_paper.htm.

Unit 3. Network security and Security Tools

Unit Introduction

Each day more and more people are accessing computer networks. Undoubtedly the best known network is the Internet. With it you can put information on your machine and available for everyone.

The security-related network problems and ways to solve is the purpose of this unit. Initially, the security will be addressed in computer networks, the techniques available for better reliability (in terms of safety) and all forms of employment, either for encryption or through firewalls. It will be presented some examples of encryption techniques and their use in establishing reliable connections.

On the back of security mechanisms and tools are the standards and protocols that enable communication between stakeholders on well-defined rules. These security protocols ensure the confidentiality of information and the identities of communication involved, both in physical communication as logic (wireless).

In short, this unit will cover the security of computer networks, good practices, main protocols and applications used in this area.

Unit Objectives

Upon completion of this unit you should be able to:

- Identify the protocols and safety standards on the Internet;
- Apply the forms of security in wireless networks;
- Identify key authentication applications on the Internet;
- Apply the good security practices;
- Create the safest forms of electronic transactions;
- Apply the forms of remote authentication (RADIUS serve).

Key Terms

Authentication: is the ability to ensure that someone, or some equipment access, within a defined context.

Remote Access: Access to computer networks from a remote location. Remote access connections can originate from within the company network or from a remote location outside the corporate network.

Protocols: Protocol is the set of rules on how it will communication between the parties involved in the communication.

Vulnerability: failure or weakness that, if exploited, could result in intentional or unintentional compromise of the system.

IP (Internet Protocol): network layer protocol containing address information and some control information that enables packets / data to be targeted and delivered from the source host to the destination host. IP is the primary network layer protocol in the suite of Internet protocols.

Learning Activities

Activity 1 - Protocols and safety standards on the Internet

Introduction

We say that a house is safe when the vulnerabilities it were minimized. But. according to ISO (International Standardization Organization - International Organization for Standardization) in the context of computing, vulnerability is any weakness that could be exploited to violate a system or the information.

Initially the devices were connected to Internet network via dial-up (modem and a telephone line), today, the connection ceased to be exclusive to these computational slide the corporate network, it has also accessed by mobile devices, TVs and even appliance . The network access possibility widened while the vulnerabilities also widened, for this reason it is important that we study ways to protect information both the organization and staff.

Activity Details

The term security is used to mean to minimize the vulnerability of goods (anything of value) and resources. Vulnerability is any weakness that could be exploited to violate a system or the information it contains. Security is related to the need for protection against unauthorized access or manipulation, intentional or not, of confidential information by unauthorized elements, and the unauthorized use of the computer or its peripheral devices. The need for protection should be defined in terms of possible threats and risks and objectives of an organization, formalized in terms of security policy. (SOARES; LEMOS and Colcher 1995, p.448):

Network security starts with the existence of the organization's security policy. This policy should be defined forms of access to the organization's information. There are different forms and levels of security to protect information sent over the network.

The most basic form is the authentication and authorization of the user or device where it identifies itself to the network and the remote location through a username and password, which are checked before the device can enter the system. This security process can be enhanced with data encryption to prevent others from using or reading the data, use the firewall.

Security protocols

As we saw in the previous activities, cryptographic algorithms can be combined to implement different t cryptographic mechanisms such as; the digital signature and hash, etc. These mechanisms are components of cryptographic protocols, embedded in the security architecture of the products for electronic communication, so these protocols come from the services associated with encryption that enable communication on the global network.

Some of these protocols that use cryptographic system include: SSL (Secure Sockets Layer), TLS (Transport Layer Security), PGP (Pretty Good Privacy), Kerberos, SSH, IPSec, S / MIME, SET and other. We will discuss more on these examples later in this unit

Safety standards

Currently for the study of information security, we are referred aso study of standardization rules. However, this information security standard ISO / IEC 17799: 2005, influenced by the standard English (British Standard) BS 7799. The series of ISO / IEC 27000 has been set aside to deal with safety standards of information, including complementation the original work of the English standard.

So for the study of basic attributes of safety standards, they must follow the international standard established by the ISO (International Organization for Standardization), which we quote some standards according to ISO / IEC 27001 stress that this rule is universal for all types of organizations and is designed to specify the requirements for the establishment, implementation, operation, monitoring, reviewing, maintaining and improving an ISMS within the business risks of an organization context.

For assigning a safety certificate according to ISO / IEC 27001 standard involves some audit palaces, which consists of linear review of the information system documentation, the organization's security policy and risk treatment plan.

The 27001 has some requirements that suggest some procedures for a good Security Information Management, which indicated the following:

- Setting the context;
- Risk identification;
- Risk assessment;
- Risk treatment;
- Risk Communication;
- Monitoring and critical risk analysis.

After the process of analysis and risk assessment, there are several options for treatment:

- Apply security measures: choose the most appropriate measures to reduce the cost;
- Accept the risk: to know and consciously accept the risk, knowing that this attentive to the organization's security policy;
- Avoid the risk: Do not allow actions which may cause the occurrence of risks;
- Transfer the risk: transferring the associated risks to other parties, eg insurers or suppliers.

In this regard, it is noted that the safety standards can be useful to meet security requirements of an information system by reusing successful practice for information security, which may be associated with the reference models and used to implement a process management of information security risks.

Within the 27000 series can also be noted that there are other standards, including: 27002 (Code of Practice), 27003 (Implementation Guide), 27004 (Metrics and Measurement), 27005 (Risk Management Guidelines) and 27006 (Service Guidelines Disaster recovery).

Conclusion

We arrived at the end of the lesson which addressed the concept of security in computer networks. We also saw that network security begins with the existence of the organization's security policy, this policy should be set by the higher of the organization in coordination with technical team. We approach information security protocols in computares network, where we assume they work with encryption techniques already studied in previous lessons.

In the end, we address safety standards in organizations and we saw that this must follow the rules established it ISSO (International Organization for Standardization) body that sets standards and certifies the safety mechanisms adopted by organizations.

Assessment

1. List at least three security protocols used in an cryptographic system

Activity 2 - Wireless Network Security

Introduction

The security of remote data transmitted this long with the physical connections still can not believe that it is effective, but with wireless networks many still doubt that their data is not being accessed by unauthorized persons. An encryption without doubt plays an important role.

Today, wireless networks are gaining capo, widely being adopted by organizations due to mobility and cost savings in physical communication materials, although there are still quite expensive equipment.

In this lesson we will discuss security in wireless devices, the main protocols used in this communication.

Activity Details

Wireless networks, translation from English Wireless Network, is any connection between communication devices for transmitting information without the use of wires or cables. Thus, there is no communication without the existence of a wire or cable characterized by a wireless connection. We can cite several ways to use wireless as the connection between the Television and the remote control, between the phone and the towers of the operators and to the police radio to operating plants, other example.

The operation of a wireless network is fairly simple, you only need to use a device called Access Point (Access Point), so it transforms the network data into radio waves or infrared and transmits through antennas.

There are two types of topologies of wireless networks: calls WLAN applications (Wireless Local Area Network) or indoor and WWAN (Wireless Wide Area Network) or outdoor.

Wireless network standards

There are 4 major standards for wireless networks: 802.11b, 802.11a and 802.11g.
The 802.11 standard was developed by the IEEE (Institute of Electrical and Electronics Engineers) for wireless networks. The 802.11 standard can be compared to the local network standards wired 802.3 and 802.5 for Ethernet and Token-Ring. With these patterns you can work with multiple devices from different manufacturers and with great efficiency.

802.11a: Operates in 5Ghz frequency, which offers high reliability, being a frequency less used. It provides a faster speed than the standard 802.11b (up to 54Mbps), but with a lower range.

802.11b: This is the most popular type of wireless network, with frequency is 2.4Ghz and maximum speed of 11 Mbps and maximum operating range of 100 meters indoors and 180 meters in open area.

802.11g: is a product line of wireless networking manufacturers that combines concepts of 802.11a and 802.11b, known as "G" technology provides speed 802.11a, but is fully compatible with existing 802.11b networks. It is cheaper than 802.11a, but still uses a frequency of 2.4 Ghz.

802.11n: 802.11n introduced the possibility to use channels that permitim duplication of channel transfer rates. The available transfer rates ranging from 65 Mbps to 300 Mbps. Transmission Method: MIMO-OFDM and frequency range: 2.4 GHz and / or 5 GHz.

Wireless network security protocols

There are several security protocols in wireless networks, the following are the most used in the security of wireless networks:

WEP (Wired Equivalent Privacy): It was the first encryption protocol released for wireless networks (the oldest). WEP is an encryption system adopted by the IEEE 802.11 standard. It uses a shared password to encrypt the data and functions statically for this reason is considered the weakest in terms of safety.

WPA (Wi-Fi Protected Access): The WPA encrypts the information and ensures that the network security key has been changed. There are two types of WPA authentication: WPA and WPA2. WPA is designed to work with all wireless network adapters. WPA2 is more secure than WPA, but it will not work with some older network adapters. WPA is designed to be used with an 802.1X authentication server, which distributes different keys to each user. This is known as WPA-Enterprise or WPA2-Enterprise. It can also be used in the pre-shared key mode, this is known as WPA-Personal or WPA2-Personal.

802.1x Authentication: 802.1X authentication can help enhance security for 802.11 wireless networks and wired Ethernet networks. 802.1X uses an authentication server to validate users and provide network access. On wireless networks, 802.1X can work with WPA, WPA2 or WEP keys. This type of authentication is typically used when connecting to a local network work.

Wireless network security protocols

There are several security protocols in wireless networks, the following are the most used in the security of wireless networks:

WEP (Wired Equivalent Privacy): It was the first encryption protocol released for wireless networks (the oldest). WEP is an encryption system adopted by the IEEE 802.11 standard. It uses a shared password to encrypt the data and functions statically for this reason is considered the weakest in terms of safety.

WPA (Wi-Fi Protected Access): The WPA encrypts the information and ensures that the network security key has been changed. There are two types of WPA authentication: WPA and WPA2. WPA is designed to work with all wireless network adapters. WPA2 is more secure than WPA, but it will not work with some older network adapters. WPA is designed to be used with an 802.1X authentication server, which distributes different keys to each user. This is known as WPA-Enterprise or WPA2-Enterprise. It can also be used in the pre-shared key mode, this is known as WPA-Personal or WPA2-Personal.

802.1x Authentication: 802.1X authentication can help enhance security for 802.11 wireless networks and wired Ethernet networks. 802.1X uses an authentication server to validate users and provide network access. On wireless networks, 802.1X can work with WPA, WPA2 or WEP keys. This type of authentication is typically used when connecting to a local network work.

Conclusion

Security is a weak point of wireless networks as the signal propagates through the air in all directions and can be received at distances of hundreds of meters by users with data invasion of intent, which makes it inherently vulnerable wireless networks the interception. The choice of a more modern equipment in wireless networks can help implement more sophisticated security mechanism.

Assessment

1. What is the importance of security planning in the organization?
2. What are the detailed items that make up a security plan document ?
3. What does the acronym PDCA mean in full?

Activity 3 - Internet Authentication Applications

Introduction

When a client on the network connects to the Remote Desktop, no need to verify that it is connecting to the remote computer or correct server. This security measure helps prevent it from being connected to a different computer or server required. This process is resorted to authentication applications.

The shape of the verification required to connect is determined by your system security policy, which is defined by the system administrator. In this lesson we will cover some services used for remote authentication.

Activity Details

The Internet is an unsafe place. Some protocols used on the Internet do not provide security. Tools to intercept user passwords for networks are commonly used by malicious users. Thus, applications that send text mode data over the network, such as FTP and Telnet, are extremely vulnerable. The Firewall is one of the security mechanisms widely used today, this is responsible for the control of data transferred to and from your computer over the internet, as well as prevent personal or confidential information is transmitted from your computer to the Internet and prevent the invasion of the machine for malicious software.

It is important to note that before selecting and configuring an authentication service, learn how these services work and how to configure. In addition to authentication, each of the supported services provides the ability to configure authorization rules that define how user privileges are assigned to a particular remote user. Make sure that the function or the appropriate user privilege is assigned.

Kerberos

The Kerberos protocol is designed to solve such problems by providing a reliable authentication over open and insecure networks in which communication between computers can be intercepted. It provides strong authentication for client / server applications by the secret key cryptography so that a client proves its identity to a server (and vice versa) by using such networks.

In 1983, researchers at the MIT started Project Athena to develop a leading-edge model of security for their academic environment. This model was called Kerberos, after the three-headed dog that guarded the entrance to Hades in Greek mythology.

The three heads of Kerberos

1. Key Distribution Center (KDC),
2. The client user
3. The server with the desired services to access

Kerberos Authentication

Provides authentication and encryption through standard clients and servers (It is a network authentication protocol). It is based on the concept of a trusted third party. It Uses a Key Distribution Center (KDC) to issue tickets to those who want access to resources. It performs same function as a Certification authority (CA) Used internally on Windows 2000/XP

Advantages Kerberos include:

- Passwords are not stored on the system
- Widely used in UNIX environment; enables authentication across operating systems

Kerberos builds on symmetric key cryptography and requires a trusted third party. Each computer has a secret key (code) used in encryption. It Requires that you know which computers will be talking to each other so you can install the key on each one. The code provides the key to decoding the message

SSL & TLS

Secure Sockets Layer (SSL): SSL is a protocol that allows the transmission of information via the internet in encrypted form. SSL ensures that the information is sent, unchanged and exclusively for the server to which you want to send.

It was originally developed by Netscape in 1995 to provide secure and authenticated connections between browsers and servers. It Provides transport layer security. Transport Layer Security (TLS) Version 1 is essentially SSLv3.1

SSL Architecture

SSL uses TCP to provide a reliable and secure end-to-end service. It is not a single protocol but two layers of protocols. The Hypertext Transfer Protocol (HTTP) used for server/client interaction on the Internet can operate on top of the SSL Record Protocol

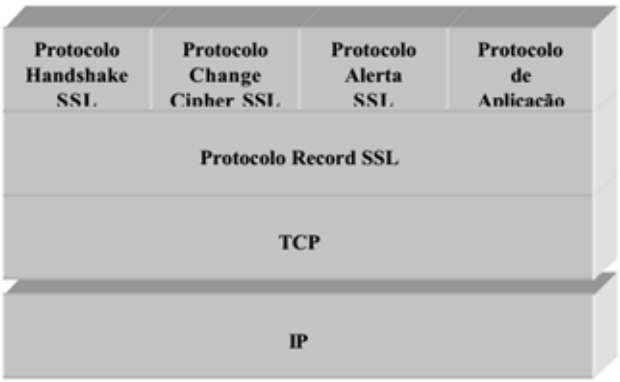


Fig 10: the SSL state and its layers

SSL Connections

A connection is a transport that provides a suitable service. SSL connections are peer-to-peer relationships. These SSL connections are transient. They only last for a certain length of time. Each connection is associated with a session

SSL Sessions

A session in SSL is an association between a client and a server. Such sessions are created by the SSL Handshake Protocol. A session defines the security parameters. A session may be shared by multiple connections. Allows the same settings to be used by many connections without the need for repeatedly sending the security parameters

Transport Layer Security (TLS): TLS was created as the successor to SSL security protocol is through encryption, interoperability, extensibility and efficiency. This means that this protocol is able to establish a secure connection between two entities and to ensure that two applications can communicate or exchange parameters regardless of how they were built.

To deepen more on the SSL & TLS security protocols see: http://www.gta.ufrj.br/grad/11_1/tls/

Radius (remote authentication and dial-in user service): This is used for System authentication and accounting. It checks if information such as the user name and password, which pass through the RADIUS server are correct; if so, it authorizes access to the system. This authentication method can be used with a token, smart card, etc., to provide two-factor authentication.

Secure Electronic Transaction

We have seen how secure protocols are used to ensure the privacy and integrity of communications on the network and these are also replicated to applications running on the network. However, transactions are more complicated than simple relationships between client and server.

The main objective of secure protocols is to ensure data transactions; in particular, purchases with a credit card. SSL and S-HTTP can be used to secure the transaction between buyer and seller. But there are other parties involved in the transaction, as the provider of credit card and the buyer's bank

IP Security (IPSec)

IPSec Provides security services at the IP layer for other TCP/IP protocols and applications to use. It also provides the tools that devices on a TCP/IP network need in order to communicate securely. When two devices wish to securely communicate, they create a secure path between themselves that may traverse across many insecure intermediate systems.

Steps for an IPSec Connection

1. Agree on a set of security protocols to use so that data is in a format both parties can understand.
2. Decide on an encryption algorithm to use in encoding data.
3. Exchange the keys that are used to decrypt the cryptographically encoded data.
4. Use the protocols, methods and keys agreed upon to encode data and send it across the network

IPSec Core Protocols

IPSec Authentication Header (AH): It Provides authentication services, This protocols also Verifies the originator of a message, it Verifies that the data has not been changed on routeand finally it Provides protection against replay attacks

Encapsulating Security Payload (ESP): Since AH ensures integrity but not privacy, IPSec ensures that the datagram can be further protected using ESP, it encrypts the payload of the IP datagram

IPSec Applications

- Securing a company's Virtual Private network (VPN) over the Internet
- Securing remote access over the Internet
- Establishing connections with partners via an extranet
- Enhancing eCommerce security by adding to the security mechanism in the application layer

IPSec Advantages

- Can be applied to a firewall or router and apply to all traffic across that boundary
- It is transparent to applications.
- It is transparent to end users.
- It can provide security for individual users if required.

Vulnerability scanning programs

Today the data is the most active organizations and these circular Internet. The attacker also travels across the Internet and is becoming more sophisticated bias. Often administrators can not identify the vulnerabilities of the system due to lack of means.

However, due to the high cost of proprietary software solutions for vulnerability scanning and creating reports automatically.

In this section we discuss some examples of software that can be used to test and system vulnerability:

1. **Nessus:** is a tool for vulnerability scanning, in some cases for their use equipment may be inoperable or slow due to the large number of tests (through ports) that this application performs.

   According to wikipedia Nessus (https://pt.wikipedia.org/wiki/Nessus), it is a fault verification program / security vulnerabilities (ports, vulnerabilities, exploits). It consists of a client and server, and the scan itself is done by the server (Nessus server). Nessus helps identify and resolve vulnerabilities some problems. The Server part executes the tests while the client part allows configuration and reporting. Nessus is distributed under the terms of the GNU General Public License.

2. **Skipfish:** A tool for security test fully automated sites and is very light and very fast (can run 2,000 requests per second). As well as other security tools, it has several types of safety tests, including Blind SQL Injection. (The program works on Windows, Linux and Mac OS X).

3. **Web securify**: is an open source tool very easy to use that automatically identifies web application vulnerabilities. It can create simple reports (which can be exported in various formats). The tool supports multiple languages and is extensible, with support for plugins. (The program works on Windows, Linux and Mac OS X).

4. **Wireshark:** (formerly known as Ethereal) is a program that analyzes network traffic and organizes for protocols. The features of Wireshark are similar to tcpdump but with a GUI interface, with more information and the possibility of using filters.

It is then possible to control the traffic of a network and know everything that goes in and out of the computer, in different protocols, or network to which the computer is connected (**https://pt.wikipedia.org/wiki/Wireshark**).

For verification programs for security vulnerabilities visit:

http://sectools.org/tag/sniffers/

http://webresourcesdepot.com/10-free-web-application-security-testing-tools/

http://insecure.org/tools/tools-pt.html

Packet Sniffers

A packet sniffer is a wire-tap devices or software that plugs into computer networks and eavesdrops on the network traffic. It basically allows you to listen to other peoples conversations. This is done using a sniffing program.

The packet sniffer can intercept and log traffic passing over a digital network or part of a network. When data streams moves with networks, the sniffer captures each packet and eventually decoded and analyzes it's content according with any specifications. There would be issues since most of computer conversations consist of apparently random binary data. Due to this, most network wiretap programs also come with feature known as protocol analysis. This feature allows the packet sniffers to decode the computer traffic and make sense of it.

How a packet sniffer works

Ethernet was built around a principle known as a shared principle where all machines on a local network share the same medium like same wire This means that all machines can see and hear all the traffic that is transmitted over the same medium like same wire. To avoid this issue, the Ethernet hardware is built with a filter that ignores all traffic that does not belong to it.

This is done by avoiding all frames whose MAC address doesn't match. So in order for a sniffer program to operate in these circumstances, it turns off this filter from the Ethernet hardware. By turning the filter off, it puts the Ethernet hardware into a mode known as promiscuous mode. This makes all the traffic visible from all machines that are sharing the same medium.

The uses of a packet sniffer

Packet Sniffer programs have been existing for such a long time and can be used in two forms:

Commercial packet sniffers: These can be used to help maintain networks

Underground Packet sniffers: These are used to break into computers

This nature of packet sniffers means it can be used to do different things like:

- Analysing network problems
- Detecting network intrusion attempts
- Gaining information for effecting a network intrusion
- Gather and report network statistics
- Filter suspect content from network traffic
- Debug client/server communication

As we have seen, it can also be used for malicious acts:

- Spy on other network users and collect sensitive information such as passwords (depending on any content encryption methods which may be in use)
- Reverse engineering protocols used over the network

Components of a Packet sniffer

The components of a packet sniffer include:

The hardware: Most products work from the standard network hardware adapters, even though some require special hardware. The reason for special hardware is that they have the capability to analyze hardware faults like CRC errors, voltage problems, cable programs, jitter, etc

Capture Driver: This is the most important part. It captures the network traffic from the medium like the wire, filters it for the particular traffic you want, then stores it in a buffer

Buffer: Once the frames are captured from the network, they are stored in a buffer

Decode: This displays the contents of the network traffic with descriptive text so that an analysis can figure out what is going on.

Packet editing/transmission: Some products contain features that allow you to edit your own network packets and transmit them onto the network.

Vulnerability Scanners

Introduction

A vulnerability scanner is software application that assesses security vulnerabilities in networks or host systems and produces a set of scan results. However, because both administrators and attackers can use the same tool for fixing or exploiting a system, administrators need to conduct a scan and fix problems before an attacker can do the same scan and exploit any vulnerabilities found.

A vulnerability scanner can assess a variety of vulnerabilities across information systems (including computers, network systems, operating systems, and software applications) that may have originated from a vendor, system administration activities, or general day to-day user activities:

Vendor-originated: this includes software bugs, missing operating system patches, vulnerable services, insecure default configurations, and web application vulnerabilities.

System administration-originated: this includes incorrect or unauthorized system configuration changes, lack of password protection policies, and so on.

User-originated: this includes sharing directories to unauthorized parties, failure to run virus scanning software, and malicious activities, such as deliberately introducing system backdoors.

The Benefits of Vulnerability Scanners

Firstly, a vulnerability scanner allows early detection and handling of known security problems. By employing ongoing security assessments using vulnerability scanners, it is easy to identify security vulnerabilities that may be present in the network, from both the internal and external perspective.

Secondly, a new device or even a new system may be connected to the network without authorisation. A vulnerability scanner can help identify rogue machines, which might endanger overall system and network security.

Thirdly, a vulnerability scanner helps to verify the inventory of all devices on the network. The inventory includes the device type, operating system version and patch level, hardware configurations and other relevant system information. This information is useful in security management and tracking.

The Limitations of Vulnerability Scanners

The drawbacks of vulnerability scanners are:

1. **Snapshot only:** a vulnerability scanner can only assess a "snapshot of time" in terms of a system or network's security status. Therefore, scanning needs to be conducted regularly, as new vulnerabilities can emerge, or system configuration changes can introduce new security holes.
2. **Human judgment is needed**: Vulnerability scanners can only report vulnerabilities according to the plug-ins installed in the scan database. They cannot determine whether the response is a false negative or a false positive. Human judgment is always needed in analyzing the data after the scanning process.
3. **Others**: a vulnerability scanner is designed to discover known vulnerabilities only. It cannot identify other security threats, such as those related to physical, operational or procedural issues.

In addition, many vulnerability scanners rely on "plug-ins" to determine potential vulnerabilities. Plug-ins are part of the knowledge database (or scan database) of the vulnerabilities that the scanner is capable of detecting.

These databases may be named differently (such as "Scanning Profile") in different scanner products, but the term "plugins" will be used in this article. The finite number of plug-ins can be another drawback with vulnerability scanners.

A scanner can only check for those vulnerabilities that it "knows", by cross checking with the presence of its corresponding installed plug-in set. It cannot identify those vulnerabilities that don't have a plug-in. Not all scanners need plug-ins. For example, port scanners do not need any plug-ins as they just scan a target range of ports.

Architecture of Vulnerability Scanners

In general, a vulnerability scanner is made up of four main modules, namely, a Scan Engine, a Scan Database, a Report Module and a User Interface.

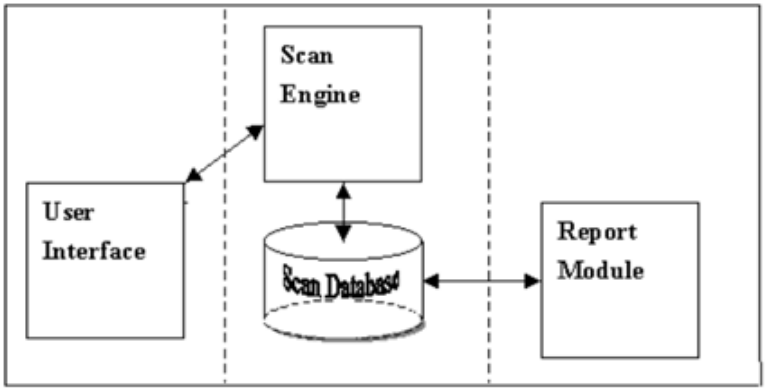


Fig 11: Components of a scanner

1. The Scan Engine executes security checks according to its installed plug-ins, identifying system information and vulnerabilities. It can scan more than one host at a time and compares the results against known vulnerabilities.
2. The Scan Database stores vulnerability information, scan results, and other data used by scanner. The number of available plug-ins, and the updating frequency of plug-ins will vary depending on the corresponding vendor. Each plug-in might contain not only the test case itself, but also a vulnerability description, a Common Vulnerabilities and Exposures (CVE) identifier; and even fixing instructions for a detected vulnerability. Scanners with an "auto-update" feature can download and install the latest set of plug-ins to the database automatically.

3. The Report Module provides different levels of reports on the scan results, such as detailed technical reports with suggested remedies for system administrators, summary reports for security managers, and high-level graph and trend reports for executives.

4. The User Interface allows the administrator to operate the scanner. It may be either a Graphical User Interface (GUI), or just a command line interface.

Most vulnerability scanners are characterized by their modular structure as explained above. However, there are also primitive scanners that are basically sets of scripts or Code exploits producing simple plain-text files as scanning results. Updates to these primitive scanners are infrequent and require manual intervention.

On the other hand, there are now a number of Distributed Network Scanners with more complex architecture. When enterprise networks are widely distributed, Distributed Network Scanners are used. They are composed of remote scanning agents, a plug-in update mechanism for those agents, and a centralized management point. Such scanners are capable of assessing vulnerabilities across multiple, geographically dispersed networks from one centralized management console, which can then distribute updates to scanning agents, modify settings in all scan engines, and schedule testing activities across the whole enterprise. Scan results are in turn collected from all remote scanning agents into the central database for analysis and reporting.

Types of Vulnerability Scanners

Vulnerability scanners can be divided broadly into two groups: network-based scanners that run over the network, and host-based scanners that run on the target host itself.

Network-Based Scanners

A network-based scanner is usually installed on a single machine that scans a number of other hosts on the network. It helps detect critical vulnerabilities such as mis-configured firewalls, vulnerable web servers, risks associated with vendor-supplied software, and risks associated with network and systems administration.

Different types of network-based scanners include:

1. Port Scanners that determine the list of open network ports in remote systems;
2. Web Server Scanners that assess the possible vulnerabilities (e.g. potentially dangerous files or CGIs) in remote web servers;
3. Web Application Scanners that assess the security aspects of web applications (such as cross site scripting and SQL injection) running on web servers. It should be noted that web application scanners cannot provide comprehensive security checks on every aspect of a target web application. Additional manual checking (such as whether a login account is locked after a number of invalid login attempts) might be needed in order to supplement the testing of web applications.

Host-Based Scanners

A host-based scanner is installed in the host to be scanned, and has direct access to low level data, such as specific services and configuration details of the host's operating system. It can therefore provide insight into risky user activities such as using easily guessed passwords or even no password.

It can also detect signs that an attacker has already compromised a system, including looking for suspicious file names, unexpected new system files or device files, and unexpected privileged programs. Host-based scanners can also perform baseline (or file system) checks. Network-based scanners cannot perform this level of security check because they do not have direct access to the file system on the target host.

A database scanner is an example of a host-based vulnerability scanner. It performs detailed security analysis of the authorisation, authentication, and integrity of database systems, and can identify any potential security exposures in database systems, ranging from weak passwords and security mis-configurations to Trojan horses.

Conclusion

In this lesson we covered some services used for remote authentication. Many of the services are implemented in some software that we can find in the market. These software implementan security protocols for remote authentication, Kerberos, SSL & TLS, Radius and others. Unix environment, many network administrators configure remote access via nessus, for this to be simple and indicate the detected vulnerabilities and the steps that must be taken to eliminate.

Assessment

1. List three elements/heads of Kebros
2. What is an SSL sesion ?
3. Describe steps needed to set up an IPSEC connection
4. Provide advantages of IPSEC

Unit Summary

We reached the end of the drive where addressed the concept of security in computer networks. We also saw that network security begins with the existence of the organization's security policy, this policy should be set by the higher of the organization in coordination with technical team. We approach information security protocols in computares network, where we assume they work with encryption techniques already studied in previous lessons.

We address the safety standards in organizations and we saw that this must follow the rules established it ISSO (International Organization for Standardization) body that sets standards and certifies the safety mechanisms adopted by organizations.

Security was the highlight of this unit, which discussed its importance in wireless networks and The choice of a more modern equipment in wireless networks can help implement more sophisticated security mechanism.

In the last lesson we covered some services used for remote authentication and affirmers that many of the services are implemented in some software that we can find in the market. This software implements the security protocols for remote authentication such as the case of Kerberos, SSL & TLS, Radius and others.

Unit Evaluation

To verify that understands the issues discussed in this unit, answer the following questions:

Instructions

In case of doubt read the corresponding content or query again on the Internet.

Unit Assessment

Check your understanding

1. What is a security protocol?
2. List at least three security protocols used in an cryptographic system
3. What are wireless networks?
4. What are the major standards of wireless networks?
5. What are the security protocols of wireless networks?
6. List three elements/heads of Kebros
7. What is an SSL sesion ?
8. Describe steps needed to set up an IPSEC connection
9. Provide advantages and dis-advantages of IPSEC

Assessment Criteria

For the examination setting and marking the AVU generic marking criteria will be used.

For the assignment, criteria will be drawn up appropriate to the skills assessed , based on the AVU generic marking criteria

Grading Scheme

Refer to the course assessment Table above

Activity 3.1: 7 marks

Activity 3.2: 11 marks

Activity 3.3: 13 marks

Answers

1. 1.List seven security protocols used in an cryptographic system (7 marks)

   TLS (Transport Layer Security), PGP (Pretty Good Privacy), Kerberos, SSH, IPSec, S / MIME, SET

2. What are wireless networks? (2marks)

   Wireless Network, is any connection between communication devices for transmitting information without the use of wires or cables

3. What are the major standards of wireless networks? (3 marks)

   802.11b, 802.11a and 802.11g

4. What are the security protocols of wireless networks? (6 marks)

   WEP (Wired Equivalent Privacy): It was the first encryption protocol released for wireless networks (the oldest). WEP is an encryption system adopted by the IEEE 802.11 standard. It uses a shared password to encrypt the data and functions statically for this reason is considered the weakest in terms of safety.

   WPA (Wi-Fi Protected Access): The WPA encrypts the information and ensures that the network security key has been changed. There are two types of WPA authentication: WPA and WPA2. WPA is designed to work with all wireless network adapters. WPA2 is more secure than WPA, but it will not work with some older network adapters. WPA is designed to be used with an 802.1X authentication server, which distributes different keys to each user. This is known as WPA-Enterprise or WPA2-Enterprise. It can also be used in the pre-shared key mode, this is known as WPA-Personal or WPA2-Personal.

   802.1x Authentication: 802.1X authentication can help enhance security for 802.11 wireless networks and wired Ethernet networks. 802.1X uses an authentication server to validate users and provide network access. On wireless networks, 802.1X can work with WPA, WPA2 or WEP keys. This type of authentication is typically used when connecting to a local network work

5. List three elements/heads of Kebros (3 marks)

   - Key Distribution Center (KDC),
   - The client user
   - The server with the desired services to access

6. What is an SSL sesion ? (2 marks)

   A session in SSL is an association between a client and a server

7. Describe steps needed to set up an IPSEC connection (4 marks)

   - Agree on a set of security protocols to use so that data is in a format both parties can understand.
   - Decide on an encryption algorithm to use in encoding data.
   - Exchange the keys that are used to decrypt the cryptographically encoded data.
   - Use the protocols, methods and keys agreed upon to encode data and send it across the network

8. Provide advantages of IPSEC (4 marks)

   IPSec Advantages

   Can be applied to a firewall or router and apply to all traffic across that boundary

   It is transparent to applications.

   It is transparent to end users.

   It can provide security for individual users if required.

Unit Readings and Other Resources

Readings and other features of this unit are in the Reading List and Other Travel Resources

- SOARES, Luiz Fernando Gomes; LEMOS, Guido; Colcher Sergio. computer networks LANs, MANs and WANs to ATM networks. 2.ed. Rio de Janeiro :, 2015.
- Kurose, James; ROSS, Keith. Computer network and the Internet: Umaabordagem top-down. 3.ed. Sao Paulo: Pearson Addison Wesley, 2006 ..
- McCumber, John. Assessing and Managing Security Risk in IT Systems: A Structured Methodology. 1.ed. Auerbach, 2005.
- Andrew S. Tanenbaum, Computer Networks Campus, 4th Edition, 2003.
- James F. Kurose, Keith W. Ross, Computer Networking and the Internet: A Top-Down Approach, 3rd Edition, 2006.
- Luiz Fernando Soares, Guido Lemos, Sérgio Colcher, Computer Networks, LANs, MANs, WANs to Networks and ATM, 2nd edition, 1995.
- Osborne, McGraw-Hill, Networks Security, The complete reference, 2004.
- http://cartilha.cert.br/redes/

Unit 4. Web Security

Unit Introduction

The Web was originally designed without much concern for safety or no. The main objective was to provide information in a more friendly way that the resources available at the time. With the rapid growth of the Web and the diversification of use, security has become a crucial point, especially for those who have the Web as a major source of income or trade.

The unit this will address some safety aspects to be taken into account on a Web server, the security of the machine, the Web client, data in transit, as well as some recommendations to make it more secure Web server.

Unit Objectives

Upon completion of this unit you should be able to:

- Indentify the main web security protocols.
- To evaluate the forms of security on the web.
- Analyze the main forms of attack.
- Apply good security practices on the web.

Key Terms

Authentication: Identity verification process of an individual, device or process. Authentication typically occurs through the use of one or more authentication factors. Threat Condition or activity that may cause information or information processing resources to be intentionally or accidentally lost, modified, exposed, destroyed or otherwise affected to the detriment of the organization.

Protocol: Communication method accepted and used within networks. Specification describing rules and procedures that computers must follow to perform activities on a network.

Port: logical connection points (virtual) associated with a particular communication protocol to facilitate communication between networks.

Firewall: The firewall is an important entry barrier between the private network and the Internet. It should be used to restrict the ports available on the network, the packet types that can pass through the network, allowed protocols, etc.

Learning Activities

Activity 1 - Protocols and safety standards on the Internet

Introduction

Build secure Web Services involves understanding the threats that services are exposed and have set what level of security should be achieved. The most effective way to implement security in web applications is to be in line with the principles, standards and practices. The negative impact of a security breach can compromise confidential data or give unauthorized access and even compromise the reputation and reliability of the organization. In this lesson we will address some security issues, major threats, traffic safety techniques on the web.

Activity Details

The World Wide Web (WWW) is fundamentally a client / served working on the Internet and intranets TCP / IP. Thus, security tools and techniques explained in this module are relevant to web security.

Threats on the Web

Currently, the Web faces different forms of threat that emerged throughout its evolution. The Internet works for the Web as its transport mechanism and therefore inherits its security vulnerabilities. Because of the rush to build new functionality in any environment, designers have not considered the impact on safety that this new technology would cause, failed to see important points of possible attacks and vulnerabilities. The when the Web walked to the commercial world, threats have become more serious researchers started looking to defend their attacks given.

The following are the main forms of threats on the web:

Integrity: integrity against attacks consist of malicious data changes, programs, messages and even information from memory. This type of attack is devastating. On most systems, this type of attack allows the attacker to read / modify / remove any files, send messages, etc.

Confidentiality: This attack attempts to reveal confidential information to third parties. An attacker can try to get this information on the user's machine or server. For example, the "browsers" normally keeps local caches of visits made by users to Web servers that can reveal some "habits" this user.

Denial of Service: This is one of the most serious threats on the Web and the most difficult to prevent. This type of attack is to divert malicious actions that access to a particular service that is available. A typical example of this type of attack, requests made to a particular Web server are diverted to another server, usually a clone.

Authentication: In this case, the attacker impersonates another, getting the user's password by any method whatsoever, such as filtering packets on the network and capturing unencrypted passwords.

Security on the Web Server

In a client / server environment attention is usually directed to the server where the information resides and therefore focus threats. Security on the Web server is generally at a critical point in relation to some organizations that have the Web as their main source of income.

Security matters treated here are directed to the Apache server on Unix environment to be the most used on the Internet. But most of the recommendations, topics, suggestions, etc. It is valid for other Web servers.

Basic Settings: One of the biggest security problems on the web, as well as network services, is the mis-configuration and this can lead to. a disaster. If you do not have a good setting it is difficult to employ a satisfactory security policy.

Directory structure: Separation of Root directories and documents. The server root: server has control information, such as configuration files, additional applications, etc. Document root (the server Web space): contains the "public" content (information available via HTTP connections). Usually this is a server root directory sub-directory.

Server-Side Include (SSI): SSI is an HTML code that "injects" the output of a command or a file within the page when sent by the server to the browser. The HTML formatting is a static content, SSI is a dynamic content. The SSI's are very useful, but they may also end with the portability and can open serious security holes.

Authentication: In general, Web services are very dependent on name servers. If a name server is attacked, dependent on Web servers of this service may be compromised authentication.

CGI Scripts: It is a platform independent mechanism provided by the Web servers that enable you to run programs / scripts from a URL. These scripts are usually written in Perl, Shell, Tcl, Java, Python or C (mostly written in interpreted language).

Conclusion

We arrived at the end of this activity, which covered the services of the main threats forms of Wed and prevent further mechanisms these threats through Web security mechanisms.9

Assessment

1. What is Web Services?
2. Indicate the main forms of web threats.
3. What are the important spectra to take into account the safety of the web server?

Activity 2 - Major Web Protocols

Introduction

In this lesson we will learn the main TCP / IP (also known as Internet protocols) and its main features. This protocol forms the group of communications protocols that implement the protocol stack on which the Internet carries and most commercial networks run. They are called TCP / IP protocol because the TCP (Transfer Control Protocol) and IP (Internet Protocol) were the first to be defined.

Activity Details

The communication on the Internet is made up using various protocols, of which we quote:
HTTP (Hyper Text Transfer Protocol): This is the protocol used to control communication between the Internet server and the browser. When you open a Web page, see text, images, links or other services associated with the Internet or an intranet. HTTP is responsible for redirecting the services when selecting any of the web page options.

HTTPS (Hyper Text Transfer Protocol Over Secure Socket Layer): HTTP Protocol Version insurance, which provides authentication and encrypted communication on the World Wide Web made for communications that need to be safe, such as authentication Web.

SMTP (Simple Mail Transfer Protocol): This protocol is to make the transfer of e-mail between servers. The mail server uses POP or IMAP to send email messages to users.

FTP (File Transfer Protocol): This protocol allows transfer of data or files between computers, even with different operating systems such as Linux and Windows. FTP is also a command that allows connection of a client to an FTP server to transfer data via the Internet or Intranet.

SET (Secure Electronic Transaction): SET is a protocol developed by a consortium of companies formed by Visa, MasterCard, Netscape, IBM, Microsoft, GTE, and SAIC, to ensure the safe transmission of personal and financial information on public networks. This security is ensured with the use of encryption schemes for the authorization of activities, identification and authentication of electronic purchase and sale.

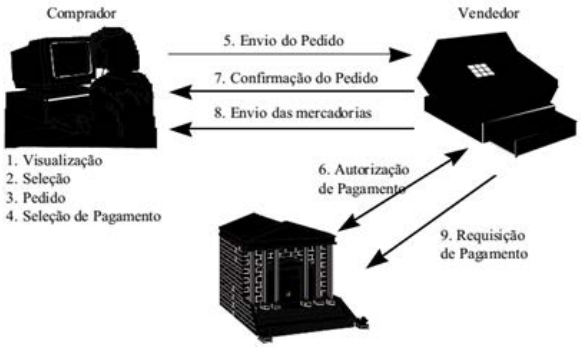


Fig 12 purchase process using the STP

IPSec: IPSec protocol implement a way of tunneling at the network layer (IP) and is part of the IPV6 protocol stack specifications. It provides authentication at the network level, the verification of data integrity and transmission with encryption and strong 128-bit keys. Implements a high degree of security in the transmission of information.

The IPSec difficult permanently any attempted attack coming from the "hacker", making it very difficult to make a staple in communication lines and get any useful information from the network traffic.

Transport Layer Security (TLS): & SSL (Secure Sockets Layer): Protocols already described in the previous unit, but not fail to address due to its importance in web security. These protocol allows client / server applications can exchange information safely, protecting the integrity and veracity of the content that travels over the Internet. The SSL protocol was originally developed by Netscape for use in their browser's transmission of sensitive data.

Conclusion

In this lesson we saw the main protocols used on the Web, its main features.

We have seen the SSL Protocol, TLS now offers a security layer for two communicating applications (client and server). Interestingly this protocol and is not restricted to a single type of application, on the contrary, it is open to thus be used with any type of application where the client and server want to exchange data. For this TLS whether it's symmetric encryption, asymmetric encryption and calculation of a message authentication code (MAC).

However, we can assume that the SET protocol has been shown to be a strong communication standard candidate in e-commerce although there are still many Cyrillic on the various entities involved.

Assessment

1. Briefly describe the major web protocols that are used in communication

Activity 3 - Virtual Private Network (VN)

Introduction

In recent times of computer networks in the world of computer networks has often used the term private or public. The VPN concept has been much discussed and used, reason has become one of the technologies commonly used today.

In this lesson we will address the VPNs, its technology, used protocols; types of VPNs and development.

Activity Details

Virtual Private Network or Virtual Private Network (VPN) is the implementation of a private communication network over a public network such as the Internet. In general, data is transmitted over the public network using standard protocols and communication is via tunnels (with or without encryption) between authorized points, thus providing the necessary confidentiality and security.

By definition, Virtual Private Network (VPN) is a private communications network built on a public communications network. This implementation can be made with aid of software, such. SoftEther, OpenVPN, Cisco VPN, UltraVPN, CyberGhost;,Hamachi; Loki VPN Client; WinGate VPN among others.

As the Internet is a public network, you must create some security mechanisms so that the information exchanged between computers in a VPN can not be read by others. The most widely used protection is encryption, as this ensures that the data transmitted by a network computer is the same as the other machines will receive. Once encrypted, the data is then encapsulated and transmitted over the Internet, using the tunneling protocol

Types of VPNs

There are basically three types of VPNs, the Seguer presented:

Access VPN: Provides remote access to intranet or extranet over an infrastructure that shares the same private network policies. Through the VPN users gain a means to secure access to corporate resources wherever you are and when required.

VPN for intranet: The links connect and integrate the headquarters of the network, remote and branch offices over a shared infrastructure. Businesses use the same private network policy as well as security, quality of service, management and reliability.

VPN for Extranet: Performs interaction through the Internet network profiles with a compatible infrastructure using dedicated connections: chain between customers and suppliers, and business partners, communities of common

Tunneling

The virtual private networks based on the tunneling protocol. The use of tunneling in the VPN incorporates a new component to this technique, before encapsulating the packet, it is encrypted.

This tunneling protocol encapsulates the packet with an additional header that contains routing information.The so-called tunnel is the logical path taken by the package along the intermediate network.

However, the process involves tunneling encapsulation, transmission, along the intermediate network and uncoating of the package. The transport information are made co help of the following communication protocols:

- IPSec - Internet Protocol Security
- L2TP - Layer 2 Tunneling Protocol
- L2F - Layer 2 Forwarding
- PPTP - Point-to-Pont Tunneling Protocol

Tunnels can be created in two different ways, either voluntarily or compulsorily.

Tunneling volunteer

The client issues a VPN request to configure and create a voluntary tunnel. In this case, the user computer operates as an end of the tunnel, and also as tunnel client.

Tunneling compulsory

A dial-up VPN access server configures and creates a compulsory tunnel. In this case, the client computer does not function as the tunnel endpoint. Another device, the remote access server, located between the user's computer and the tunnel server functions as one end and acts as the tunnel client.

Conclusion

In this lesson we approach the concept Virtual Private Network (VPN), I fear that became well-known at present poles administrators corporate networks. Security in a VPN is an important factor that should be handled carefully because the data are going in a public environment. Among the main tools segurançatemos in VPN's point the firewall, encryption, digital certificates, RADIUS, and IPSec.

Finally we saw the tunneling mechanism of Virtual Networks runs private (VPN).

Assessment

1. What is a VPN?
2. What are the main types of VPN?
3. What is tunneling?
4. What are the main types of VPNs through the Network Layer?

Unit Summary

We arrived at the end of this unit, which addressed the services of the main threats forms of Wed and prevent further mechanisms these threats through Web security mechanisms.

In the second lesson we saw the SSL Protocol, TLS now offers a security layer for two communicating applications (client and server). Interestingly this protocol and is not restricted to a single type of application, on the contrary, it is open to thus be used with any type of application where the client and server want to exchange data. For this TLS whether it's symmetric encryption, asymmetric encryption and calculation of a message authentication code (MAC).

In the last lesson of the unit approached the concept Virtual Private Network (VPN), which discussed security on a VPN network, your engine runs for tunneling, where we address the main security tools in VPN's, such as Firewall, Encryption, Certificates digital, RADIUS, and IPSec.

Unit Evaluation

Now check your learning by solving the following exercises:

Instructions

In case of doubt about some of the issues again read the lessons that address content in doubt.

Unit Assessment

Check your understanding

1. What is Web Services?
2. Indicate the main forms of web threats.
3. What are the important spectra to take into account the safety of the web server?
4. What is web security protocols?
5. What is the web security protocol that is considered to be more fragile?
6. Which web protocol that is responsible for forwarding files and documents
7. What is a VPN?
8. What are the main types of VPN?
9. What is tunneling?
10. What are the main types of VPNs through the Network Layer?

Grading Scheme

Refer to the course assessment Table above

Activity 4.1: 12 marks

Activity 4.2: 6 marks

Activity 4.3: 10 marks

Answers

1. A Web service is a solution used in systems integration and communication between different applications. (2 marks)
2. The main forms of web threats are: Integrity, Confidentiality, Service, Authentication Denial of service (5 marks)
3. Important spectra to be taken into account in the web server security are (5 marks)

   Basic settings , directory structure, Server-Side Include; Authentication of names; CGI Scripts.

4. Web security protocols are concrete communication that performs a safety function and application of encryption methods. (2 marks)
5. The web protocol is considered the most fragile security is HTPP. (2 marks)
6. The web protocol responsible for forwarding of files and documents is FTP. (2 marks)
7. A VPN (Virtual Private Network) is the implementation of a private communication network over a public network such as the Internet. (2marks)
8. The main types of VPN are: VPN access, VPN, Intranet, Extranet VPN (3 marks)
9. The tunneling is a technique which consists in encapsulating one protocol inside another. (2 marks)
10. The main VPN protocols are: PPTP, L2TP and IPSec. (3 marks)

Mini Assessment

Instructions

Attempt all questions

1. Set the Security Concept within IT? (5 marks)
2. Name two modes of IPsec operation (5 marks)
3. What are some VPN software. (5 marks)
4. Name umavantagem and one disadvantage of using a VPN (5 marks)

Grading Scheme

Mini-Test = 20%

Answers

1. Safety is the process of protecting information from misuse, both accidental and intentional internal or external people the organization, including employees, consultants and hackers.
2. IPSec works in the modes: mode of transport and tunneling mode. In the first, only the message is encrypted and ocabeçalho IP is not modified.

   In the second, IP opacote is encrypted completely, and so énecessário encapsulating a new IP packet paradistribuí it.
3. SoftEther; OpenVPN; Cisco VPN; UltraVPN
4. An advantage is the low cost of a VPN, as it works through a public network. One drawback is the lack of control over the quality of service of the public network, since it is difficult to guarantee speed, stampede allocation, among others

Final Assessment

Instructions

Attempt all questions

1. What is a security Policy?
2. Briefly describe the four steps of a security Policy
3. Differentiate Symmetric Cryptography Asymmetric.
4. Differentiate Block ciphers from stream ciphers
5. Describe four well known Hash Functions
6. Describe steps needed to set up an IPSEC connection
7. Provide advantages of IPSEC

Grading Scheme

Final Exam= 30%

Answers

1. What is a security Policy?

   A security policy is a formal statement of the rules by which people who are given access to an organization's technology and information assets must abide

2. Briefly describe the four steps of a security Policy

   Network security is a continuous process built around a security policy it involves four steps which are:

   - **Step 1: Secure**
   - **Step 2: Monitor**
   - **Step 3: Test**
   - **Step 4: Improve**

Step 1: Secure the Network

Implement security solutions to stop or prevent unauthorized access or activities , and to protect information. It involves the following processes

- Authentication
- Encryption
- Firewalls
- Vulnerability patching

Step 2: Monitor Security

This step detects violations to the security policy. It involves system auditing and real-time intrusion detection. It validates the security implementation in Step 1

Step 3: Test Security

This step validates the effectiveness of the security policy through system auditing and vulnerability scanning

Step 4: Improve Security

This step uses information from the monitor and test phases to make improvements to the security implementation. It adjusts the security policy as security vulnerabilities and risks are identified

3. Differentiate Symmetric Cryptography Asymmetric.

symmetrical encryption secret or private key encryption, uses the same key both to encode and to decode information, that is, the password is used both by the sender to encode the message and the recipient to decrypt it

In asymmetric encryption also known as public key encryption uses two separate keys: a public, which can be freely disseminated, and one private, which must be kept secret by its owner. When information is encrypted with one key, only the other pair of the key can decode it. It is with the private key that the recipient can decrypt a message that was encrypted.

4. Differentiate Block ciphers from stream ciphers

Block ciphers use algorithms to encrypt and decrypt a fixed-size block of plaintext and ciphertext, respectively, usually a multiple of 64 bits where as Stream ciphers continuously encrypt any amount of data as it is presented, usually by mathematically combining the data with a keystream, an infinitely long key sequence that is generated based on a finite key starting value

5. Describe four well known Hash Functions

MD2 (Message Digest Algorithm RDA-MD2) & MD4

Designed for computers with 8-bit processor, and today hardly used. They know there are many attacks on partial versions of MD2. The MD4 demonstrated to be slower and enables the existence of collisions.

MD5 (Message Digest Algorithm RDA-MD5)

It is an improved version of MD4. At the moment it is considered safe. The algorithm is designed to be fast, simple and secure. Your details are public and free, and have been analyzed by the cryptographic community. It was discovered a weakness, but so far it has not affected the overall security of the algorithm.

SHA-1 (Secure Hash Algorithm)

It is very similar in its mode of operation, with MD5. This algorithm is slightly slower than MD5, but the greater length of the message hash, makes it safer forward looking collision.

SHA-2 (Secure Hash Algorithm)

This is very similar to SHA-1, in its mode of operation. This algorithm is slightly faster than the SHA-1, but the greater length of this algorithm is to use two similar hash functions, different sizes, one different block of 256 bits and 512 other bits.

6. Describe steps needed to set up an IPSEC connection

    1. Agree on a set of security protocols to use so that data is in a format both parties can understand.
    2. Decide on an encryption algorithm to use in encoding data.
    3. Exchange the keys that are used to decrypt the cryptographically encoded data.
    4. Use the protocols, methods and keys agreed upon to encode data and send it across the network

7. Provide advantages of IPSEC

IPSec Advantages

Can be applied to a firewall or router and apply to all traffic across that boundary

It is transparent to applications.

It is transparent to end users.

It can provide security for individual users if required.

[LAB]

Instructions

Do all the labs

Grading Scheme

Lab= 10%Download the Nessus or Skipfish software depending on your operating system and do a vulnerability test on your machine. Study the results and possible solutions to minimize vulnerabilities.

Unit Readings and Other Resources

- Readings and other features of this unit are in Readings and Other Travel Resources list.
- A. D. Rubin, D. Geer, and M. J. Ranum, Web Security Sourcebook, John Wiley & Sons, New York, 1997.
- A. D. Rubin, D. Geer, A Survey of Web Security, Computer, September 1998, pp 34-41.
- Laurie B. and P. Laurie, Apache: The Definite Guide, 2nd Edition, O'Reilly, 1999.
- http://www.gta.ufrj.br/grad/04_1/vpn/Script/RDIIntroducao.html
- Scott, Charlie; Wolfe, Paul; Erwin, Mike.Virtual Private Networks, Second Edition. O'Reilly, 1999
- Brian Browne, "Best Practices For VPNImplementation," Business Communication Review, March2001.
- Hanks, S., Editor, "Generic RoutingEncapsulation over IPv4", RFC 1702, October 1994.

- A. D. Rubin, D. Geer, and M. J. Ranum, Web Security Sourcebook, John Wiley & Sons, New York, 1997.
- A. D. Rubin, D. Geer, A Survey of Web Security, Computer, September 1998, pp 34-41.
- Laurie B. and P. Laurie, Apache: The Definite Guide, 2nd Edition, O'Reilly, 1999.
- http://www.gta.ufrj.br/grad/04_1/vpn/Script/RDIIntroducao.html
- Scott, Charlie; Wolfe, Paul; Erwin, Mike.Virtual Private Networks, Second Edition. O'Reilly, 1999
- Brian Browne, "Best Practices For VPNImplementation," Business Communication Review, March2001.
- Hanks, S., Editor, "Generic RoutingEncapsulation over IPv4", RFC 1702, October 1994.

Unit 5. Advanced Computer Security Labs

Unit Introduction

The module you just study provides a set of tools for implementing advanced methods of data encryption and detention of vulnerabilities in servers. He focused on advanced aspects of computer security , such as encryption , security practices , system security , security for authentication on the Web and password management techniques.

The main module is to provide management skills of IT infrastructure to students , focusing on information security to ensure the integrity of data and the normal operation of the various systems : computer networks, servers and personal computers in the organization . The Security Advanced Computing Module that this or just study requires practice, for this reason it has the laboratory to consolidate the theory to practice

Unit Objective

After completion you , must be able to :

- Understand the methods and computer security tools Nessus ;
- Be able to interpret the results of the vulnerability scan ;
- Taking responsibility to install, configure and manage network security .

Necessary resources for installation of Nessus will need the following :

- Computer with internet access and Linux operating system preference or windows instead

Time

- 1 hour;

Activity Details

In order to verify that there are some existing security vulnerabilities on your local machine, install the Nessus software. Point out that the same settings should be made on the server. Although the version Nessus Software may vary with time, the settings here demonstrates those of version 5.2 for Windows and then Linux environment.

First go to the website: www.tenable.com/ or www.nessus.org

Note: First of all we need to register on the website to receive the activation code. After register on the site you will receive an email from the code for download and activation of Nessus Vulnerability Scanner to your email.

For installation of Nessus via Linux console, follow these steps:

- Install nessus using the following command as superuser or use sudo Sudo apt-get install nessus nessusd
- In the next step install client (nessus) and server (nessusd) Nessus. Next we will install the plugins and register plication through the rebido code by email.

#Nessus-fetch --register XXXX- sudo XXXX - XXXX - XXXX – XXXX

- Next step we will add the Nessus user, as follows:

Sudo nessus-adduser

Login: <user that will be used to acessoar the server>

Authentication (pass / cert) [pass]: <enter the authentication type, we will use pass>

Login password: <enter the password>

Login password (again): <enter the password again

user rules <Will be displayed on the screen a set of information about the rules for added user, fill out only the username and password, then accepted by pressing CTRL + D>

- After these procedures the server and client Nessus were installed and registered a user to access. If you have been enabled encryption libraries during the setup, you must create a certificate for encryption of traffic using the command: # nessus-mkcert
- The next step is to boot the server, even as superuser (root), using the command:

Nessusd D or # nessusd start

- Next step is to perform machine vulnerabilities tests, this is done by applying the seuinte command:

Nessus 127.0.0.1 3001 root alvo.txt result.txt

Where: Nessus Server Port Login Targets Result

Server - IP or host is where running nessusd.

Port - the port where the nessusd is listen (default 3001)

Login - user to login.

Targets - file with IP or name of the machines to be scanned.

Results - file where the results will be stored.

In case the previous command line line, Nessus does a scan on the local machine using the default port, root username. In this file alvo.txt saved only the ip of the local host 127.0.0.1, if you want to scan many machines must separate by comma (,).

NOTE: If you want INSTALLING manually, download the following files on the site (www.tenable.com/products/nessus/select-your-operating-system):

- nessus-libraries-1.x.x.tar.gz;
- nessus-core-1.x.x.tar.gz;
- libnasl-1.x.x.tar.gz;
- nessus-plugins-1.x.x.tar.gz;

After downloading these files must be decompressed into the / usr / directory in Linux terminal (using administrative privileges), with the following command:

tar -xvzf [filename], for example:

tar -xvzf nessus-libraries-1.x.x.tar.gz

Activity Summary

Nessus is a werent tool used to test and find security holes (ports, vulnerabilities, exploits) of one or more machines.

When installed, the Nessus uses a client-server system, when the module server is started, you can run the client on any machine on the network. Nessus offers discovery of security vulnerabilities, is a software under GPL license.

However, we hope you have been able to install and configure Nessus on your computer and obtained some results . If you have any questions on this subject, visit the links below for more tips and details.

Unit Readings and Other Resources

Readings and other resources of this lab exercises are in the following list:

- http://wiki.ubuntu-br.org/Nessus
- https://www.vivaolinux.com.br/artigo/Detectando-vulnerabilidades-com-o-Nessus?pagina=1
- http://www.hardware.com.br/livros/redes/usando-nessus.html
- http://www.dicas-l.com.br/arquivo/introducao_ao_nessus.php

Lab 1 Title: Configuring an intrusion Prevention System (IPS) Using the CLI

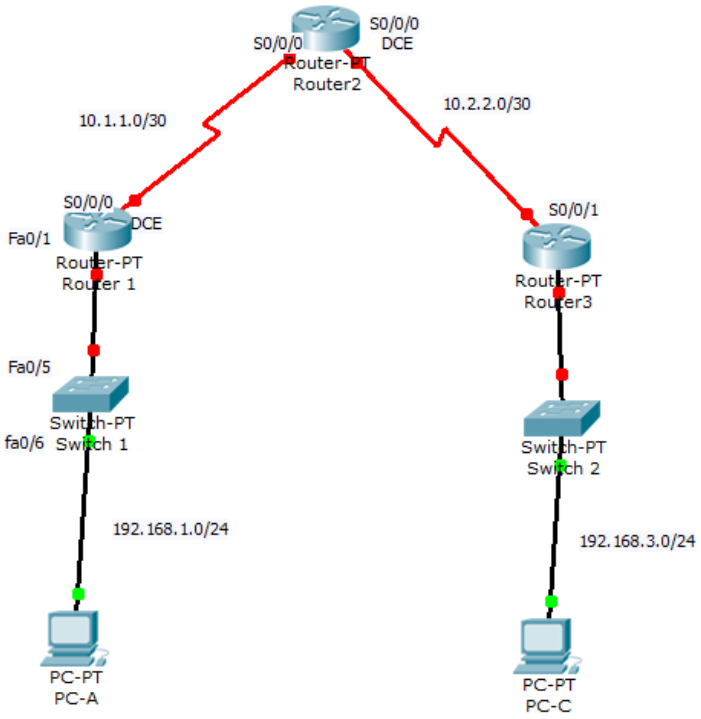


Fig 13: Lab 2 Topology

Objectives:

In the first part of this lab, we will configure hostname, interface IP addresses and access passwords. We will also configure the static routing.

In the second part of this lab, we will use CLI to configure an IOS Intrusion Prevention System (IPS), Configure IOS IPS using CLI.

Background

In this lab, you configure the Intrusion Prevention System (IPS), which is part of the Firewall feature set. IPS examines certain attack patterns and alerts or mitigates when those patterns occur. IPS alone is not enough to make a router into a secure Internet firewall, but in addition to other security features, it can be a powerful defense. You will configure IPS using the CLI on one route. You will load the IPS Signature package from a TFTP server and configure the public crypto key using CLI

Required Resources

- 3 routers
- 2 switches
- PC-A: Windows XP, Vista or Windows 7 with syslog and TFTP servers
- PC-C: Windows XP, Vista or Windows 7 with Java 6 Standard Edition,
- Serial and Ethernet cables as shown in the topology
- Rollover cables to configure the routers via the console
- IPS Signature package and public crypto key files on PC-A and PC-C (provided by instructor or downloaded)

Part 1: Basic Router Configuration

In Part 1 of this lab, you set up the network topology and configure basic settings such as host names, interface IP addresses, static routing, device access, and passwords.

- Note: Refer to Lab 1

Part 2: Configuring IPS Using the CLI

In Part 2 of this lab, you configure IPS on R1 using the CLI. You then review and test the resulting configuration.

Task 1: Verify Access to the R1 LAN from R2

In this task, you verify that without IPS configured, the external router R2 can ping the R1 S0/0/0 interface and PC-A on the R1 internal LAN. Ping from R2 to R1 and Ping from R2 to PC-A on the R1 LAN.

If the pings are not successful, troubleshoot the basic device configurations before continuing.

Task 2: Prepare the Router and TFTP Server

Step 1: Verify the availability of Cisco IOS IPS files.

To configure IPS 5.x, the IOS IPS Signature package file and public crypto key file must be available on PC-A. These files can be downloaded from Cisco.com with a valid user account that has proper authorization.

- Verify that the IOS-Sxxx-CLI.pkg file is in a TFTP folder. This is the signature package. The xxx is the version number and varies depending on which file was downloaded.
- Verify that the realm-cisco.pub.key.txt file is available and note its location on PC-A. This is the public crypto key used by IOS IPS.

Step 2: Verify or create the IPS directory in router flash on R1.

In this step, you verify the existence of, or create a directory in, the router flash memory where the required signature files and configurations will be stored. Alternatively, you can use a USB flash drive connected to the router USB port to store the signature files and configurations. The USB flash drive needs to remain connected to the router USB port if it is used as the IOS IPS configuration directory location.

- From the R1 CLI, display the contents of flash memory using the show flash command and check for the ipsdir directory. R1# show flash
- If the ipsdir directory is not listed, create it in privileged EXEC mode.R1# mkdir ipsdir
- Create directory filename [ipsdir]? Press Enter Created dir flash:ipsdir
- From the R1 CLI, verify that the directory is present using the dir flash: or dir flash:ipsdir command. R1# dir flash:

Task 3: Configuring the IPS Crypto Key

The crypto key verifies the digital signature for the master signature file (sigdef-default.xml)..

Step 1: Locate and open the crypto key file.

On PC-A, locate the crypto key file named realm-cisco.pub.key.txt and open it using Notepad or another

text editor. The contents should look similar to the following:

crypto key pubkey-chain rsa

named-key realm-cisco.pub signature key-string

30820122 300D0609 2A864886 F70D0101 01050003 82010F00 3082010A 02820101

00C19E93 A8AF124A D6CC7A24 5097A975 206BE3A2 06FBA13F 6F12CB5B 4E441F16

17E630D5 C02AC252 912BE27F 37FDD9C8 11FC7AF7 DCDD81D9 43CDABC3 6007D128

B199ABCB D34ED0F9 085FADC1 359C189E F30AF10A C0EFB624 7E0764BF 3E53053E

5B2146A9 D7A5EDE3 0298AF03 DED7A5B8 9479039D 20F30663 9AC64B93 C0112A35

FE3F0C87 89BCB7BB 994AE74C FA9E481D F65875D6 85EAF974 6D9CC8E3 F0B08B85

50437722 FFBE85B9 5E4189FF CC189CB9 69C46F9C A84DFBA5 7A0AF99E AD768C36

006CF498 079F88F8 A3B3FB1F 9FB7B3CB 5539E1D1 9693CCBB 551F78D2 892356AE

2F56D826 8918EF3C 80CA4F4D 87BFCA3B BFF668E9 689782A5 CF31CB6E B4B094D3

F3020301 0001

quit

Step 2: Copy the contents of the text file.

- From the Notepad menu bar, choose Edit > Select All. Choose Edit > Copy (or press Ctrl+C)Step 3: Apply the contents of the text file to the router.
- At the R1 privileged EXEC prompt, enter global config mode using the config t command, With the cursor at the R1(config)# prompt, paste the text file contents from HyperTerminal by right clicking and selecting Paste to Host from the context menu.

Task 4: Configure IPS

Step 1: Create an IPS rule.

- On R1, create an IPS rule name using the ip ips name name command in global configuration mode. Name the IPS rule iosips. This will be used later on an interface to enable IPS. R1(config)# ip ips name iosips
- You can specify an optional extended or standard access control list (ACL) to filter the traffic that will be scanned by this rule name. All traffic that is permitted by the ACL is subject to inspection by the IPS. Traffic that is denied by the ACL is not inspected by the IPS.
- To see the options available for specifying an ACL with the rule name, use the ip ips name command and the CLI help function (?).

R1(config)# ip ips name ips list ?

<1-199> Numbered access list

WORD Named access list

Step 2: Configure the IPS Signature storage location in router flash memory.

The IPS files will be stored in the ipsdir directory that was created in Task 2, Step 2. Configure the location using the ip ips config location command.

R1(config)# ip ips config location flash:ipsdir

Step 3: Enable IPS SDEE event notification.

R1(config)# ip ips notify sdee

Step 4: Enable IPS syslog support.

- IOS IPS also supports the use of syslog to send event notification. SDEE and syslog can be used independently or enabled at the same time to send IOS IPS event notification. Syslog notification is enabled by default. R1(config)# ip ips notify log
- Use the show clock command to verify the current time and date for the router. Use the clock set command from privileged EXEC mode to reset the clock if necessary. The following is an example of how to set the clock. R1# clock set 01:20:00 3 march 2016
- Verify that the timestamp service for logging is enabled on the router using the show run command. Enable the timestamp service if it is not enabled.
- R1(config)# service timestamps log datetime msec
- To send log messages to the syslog server on PC-A, use the following command: R1(config)# logging 192.168.1.3
- To see the type and level of logging enabled on R1, use the show logging command. R1# show logging

Step 5: Configure IOS IPS to use one of the pre-defined signature categories.

R1(config)# ip ips signature-category

R1(config-ips-category)# category all

R1(config-ips-category-action)# retired true

R1(config-ips-category-action)# exit

R1(config-ips-category)# category ios_ips basic

R1(config-ips-category-action)# retired false

R1(config-ips-category-action)# exit

R1(config-ips-category)# exit

Do you want to accept these changes? [confirm] <Enter>

Step 6: Apply the IPS rule to an interface.

Apply the IPS rule to an interface with the ip ips name direction command in interface configuration mode. Apply the rule you just created inbound on the S0/0/0 interface. After you enable IPS, some log messages will be sent to the console line indicating that the IPS engines are being initialized. The direction in means that IPS inspects only traffic going into the interface. Similarly, out means only traffic going out the interface. To enable IPS to inspect both in and out traffic, enter the IPS rule name for in and out separately on the same interface.

R1(config)# interface serial0/0/0

R1(config-if)# ip ips iosips in

Although the R1 Fa0/1 interface is an internal interface, it might be desirable to configure it with IPS to respond to internal attacks. Apply the IPS rule to the R1 Fa0/1 interface in the inbound direction.

R1(config)# interface fa0/1

R1(config-if)# ip ips iosips in

Step 7: Save the running configuration.

R1# copy run start

Lab 2 Title: Exploring Methods

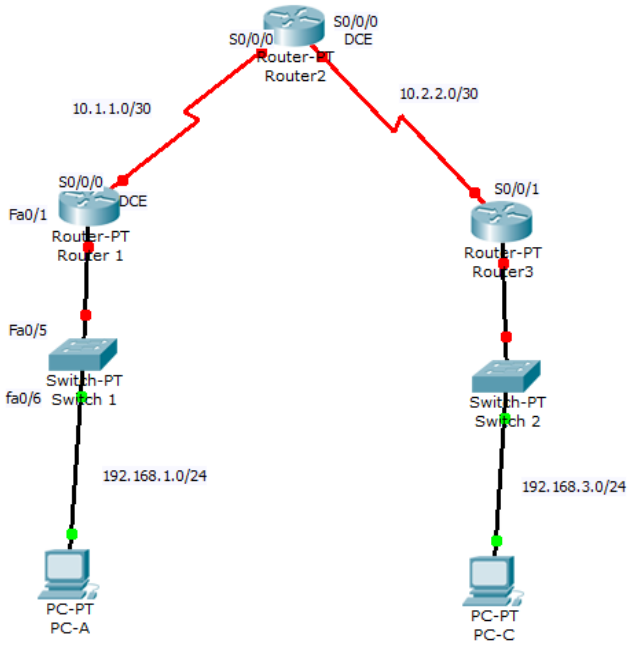


Fig 14: Lab 3 Topology

Objectives

In the first part of this lab, we will Decipher a Pre-encrypted Message Using the Vigenere Cipher,given an encrypted message, a cipher key, and the Vigenere cipher square, decipher the message.

In the second part of this lab, we will Create a Vigenere Cipher Encrypted Message and Decrypt It, Work with a lab partner and agree on a secret password, Create a secret message using the Vigenere cipher and the key, Exchange messages and decipher them using the pre-shared key and Use an interactive Vigenere decoding tool to verify decryption.

In the final part of this lab we will, use Steganography to Embed a Secret Message in a Graphic, Create a secret message and save it as a .txt file, Use S-Tools to embed the secret text message into a .bmp graphic and Send the graphic to a lab partner to reveal the embedded message.

Background

Most of Password encryption service algorithms are based on the Vigenere cipher. Vigenere is an example of a common type of cipher mechanism called polyalphabetic substitution. Although not a strong encryption technique, Vigenere serves to illustrate a commonly used encryption and decryption process.

Note: Students can work in teams of two for this lab.

Required Resources

2 switches

PC-A (Windows XP or Vista)

PC-B (Windows XP or Vista)

Ethernet cables as necessary

Activity 1: Decipher a Pre-encrypted Message Using the Vigenere Cipher

In this activity we are going to analyze an encrypted message and decrypt it using a cipher key and the Vigenere cipher square.

Step 1: **Review the encrypted message.**

The following message has been encrypted using the Vigenere cipher.

VECIHXEJZXMA

Can you tell what the message says? _____

Step 2: Review the cipher keyword.

The cipher keyword TCPIP was used to encrypt the message. The same keyword will be used to decrypt or decipher the message.

Step 3: Review the structure of the Vigenere square.

A standard Vigenere square or table is used with the keyword to decipher

Step 4: Decrypt the message using the keyword and Vigenere square.

- Use the table below to help you decrypt the message. Start by entering the letters of the encrypted message in the second row of cells, from left to right.
- Enter the keyword TCPIP in the top row, repeating the letters until there is a keyword letter for each letter of the encrypted message, even if the keyword letters at the end do not represent the complete keyword.
- Refer to the Vigenere square or table shown in Step 3 and find the horizontal row that starts with the first letter of the keyword (the letter T). Scan across that row and locate the first letter of the encrypted message in the row (the letter V). The letter at the top of the column where the encrypted message letter appears is the first letter of the decrypted message (the letter C).
- Continue this process until you have decrypted the entire message and enter it in the following table.

Cipher Keyword												
Encrypted Message												
Decrypted Message												

Activity 2: Create a Vigenere Cipher Encrypted Message and Decrypt It

In this activity, you work with a lab partner and agree on a secret password, referred to as the preshared key. Each lab partner creates a secret message using the Vigenere cipher and the key. Partners exchange messages and decipher them using their pre-shared key.

Note: If you do not have a partner, you can perform the steps by yourself.

Step 1: Determine the cipher keyword.

With your partner, establish a cipher keyword and enter it here._____

Step 2: Create a plain text message and encrypt it (both partners).

- Create a plain text (decrypted) message to be encrypted by your partner.
  _____
- You can use the following table to help you encrypt the message. You can enter the unencrypted message and cipher keyword here, but do not let your partner see it.
- In the Vigenere table, locate the row that starts with the first letter of the cipher keyword. Next locate the first letter to be encrypted at the top of the column in the table. The point (cell) at which the table row (key letter) and column (message letter) intersect is the first letter of the encrypted message. Continue this process until you have encrypted the entire message.

Note: This table is limited to messages of 12 characters. You can create longer messages if desired. Message encryption and decryption is not case sensitive.

Cipher Keyword												
Encrypted Message												
Decrypted Message												

Step 3: Decrypt the message from your partner.

- You can use the following table to help you decrypt your partner's encrypted message. Enter the encrypted message from your partner and the cipher keyword. Use the same procedure described in Part 2, Step 4.

Cipher Keyword											
Encrypted Message											
Decrypted Message											

Activity 3: Use Steganography to Embed a Secret Message in a Graphic

In this activity, you create a secret message for your partner, embed it into a graphic file, and then give it to your partner to retrieve it. You embed the message in a graphic file using S-Tools. S-Tools is a steganography tool that hides files in BMP, GIF, and WAV files. You start by opening S-Tools and then drag graphics and sounds into the blank window. To hide files, you drag them into open graphics or sound windows. Data is compressed before being encrypted and then hidden.

Note: The following steps should be performed by both partners, one at PC-A and the other at PC-B. If you do not have a partner, you can perform the steps by yourself.

Step 1: (Optional) Download and install S-Tools.

If the S-Tools application is not installed on the PC, download it from

http://www.spychecker.com/program/stools.html or another site and unzip the files to a folder.

Step 2: Create a secret message text file (both partners).

- On PC-A or PC-B, open the Windows Notepad application and create a message.
- Save the message in a folder on the desktop and name it secret.txt.
- Close the Notepad application.

Step 3: Create a simple .bmp graphics file.

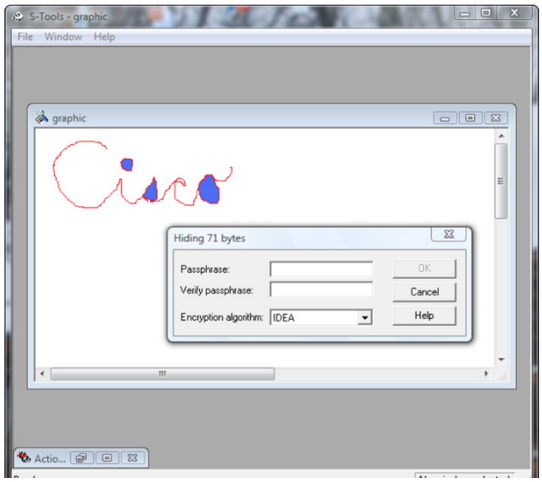
- Open the Windows Paint application and create a simple graphic. For example, you can write your first name using the pencil tool or text tool and apply some color using the spray can or fill tool.
- Save the graphic as a .bmp file in a folder on the desktop and name it graphic.bmp.
- Close the Paint application.

Step 4: Create a secret password using the Vigenere cipher.

- Choose a passphrase to be encrypted using the Vigenere cipher and record it here. _____ Do not share the passphrase with your partner. This passphrase will be used later to protect the text file when it is embedded in the graphics file.
- Choose a cipher keyword to be used when encrypting and decrypting the passphrase and record it here. _____
- Encrypt the passphrase using the cipher keyword and the procedure described in Part 3, Step 2. Record the encrypted passphrase here. _____

Step 5: Embed the message into a graphic image file.

- Open the S-Tools.exe application.
- Locate the file named graphic.bmp, which you saved previously. Determine its size by right-clicking the file and selecting Properties. Record the file size, for example 2,359,350 bytes._____
- Drag the graphic.bmp file into the S-Tools window.
- Drag the file secret.txt, which you created in Step 2, and place it inside the graphic.bmp window. The image should still be displayed. A dialog box is displayed showing the number of bytes being hidden. You can enter a passphrase and select the encryption algorithm to be used. The default algorithm is IDEA.



Step 6: Use the unencrypted passphrase to protect the embedded text file.

- Enter the unencrypted passphrase from Step 4 in the Passphrase and Verify passphrase fields.
- Choose Triple DES from the Encryption Algorithm field and click OK. This creates a second image with the name "hidden data".
- Right-click the hidden data graphic image and choose Save As from the menu. Name the file graphic2 and save it as a bmp file.
- Close the S-Tools application.

Step 7: Provide the graphic2.bmp file to your partner.

- Provide a copy of your graphic2.bmp file to your partner. You can also copy the file onto a removable drive (flash drive or floppy disk), or send it as an email attachment if you are performing the lab remotely.
- Provide your partner with the Vigenere-encrypted passphrase from Step 4 and the cipher keyword that you used to create it.

Step 8: Decrypt the Vigenere password from your partner.

- Decrypt your partner's passphrase using the procedure described in Part 1, Step 4. This is done so that you can use it with S-Tools to reveal the hidden message embedded in your partner's graphic.

Step 9: Reveal the embedded message from your partner.

- Open the S-Tools application.
- Locate the graphic2.bmp file from your partner, and determine how large it is using the same method as in Step 5. Record the file size here. _____ _____
- Has the file size changed? _____
- Drag the file into the S-Tools window. The image should be displayed. Can you tell that there is a secret message embedded in the graphic image? _____
- Right-click the image and choose Reveal from the menu.
- Enter the Vigenere passphrase decrypted in Step 8 into the Passphrase field.
- Choose Triple DES from the Encryption Algorithm field and click OK. This displays a revealed archive.
- Right-click the hidden message file and choose Save As from the menu. Name the file secret2.txt.
- Close the S-Tools application.

Open the secret2.txt file from your partner to reveal the hidden message and write it here.____

_____

Lab 3 Title: Configuring a Ssit-to-Site VPN

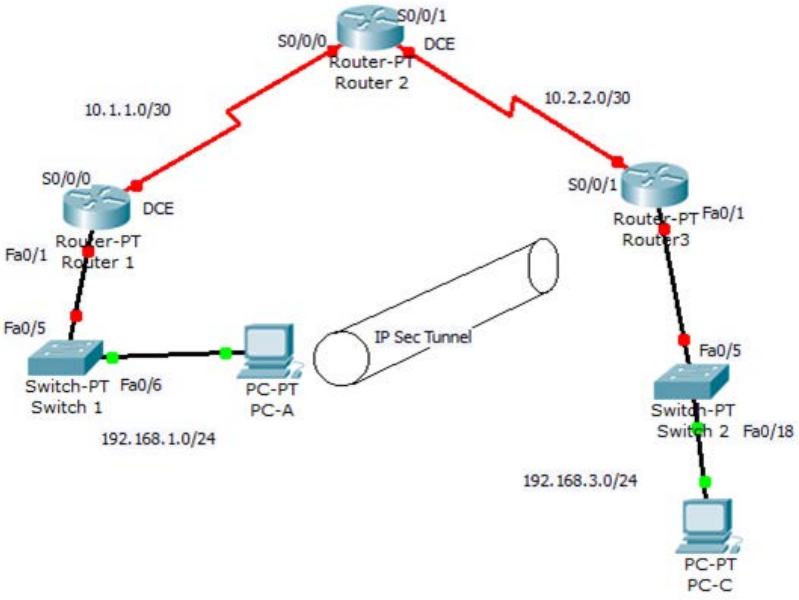


Fig 15: Lab 4 Topology

Objectives

In the first part of this lab you will configure some Basic Router Configuration such as; Configure host names, interface IP addresses, and access passwords. You will also learn how to configure the EIGRP dynamic routing protocol.

In the second part of this lab, you will learn how to configure a Site-to-Site VPN where we configure IPsec VPN settings on R1 and R3, verify site-to-site IPsec VPN configuration.and finally test IPsec VPN operation.

Background

VPNs can provide a secure method of transmitting data over a public network, such as the Internet. VPN connections can help reduce the costs associated with leased lines. Site-to-Site VPNs typically provide asecure (IPsec or other) tunnel between a branch office and a central office. Another common implementation that uses VPN technology is remote access to a corporate office from a telecommuter location such as a small office or home office.

In this lab you will build and configure a multi-router network, and then configure a site-to-site IPsec VPN and then test it. The IPsec VPN tunnel is from router R1 to router R3 via R2. R2 acts as a pass-through and has no knowledge of the VPN. IPsec provides secure transmission of sensitive information over unprotected networks such as the Internet. IPsec acts at the network layer, protecting and authenticating IP packets between participating IPsec devices (peers).

Required Resources

- 3 routers
- 2 switches
- PC-A: Windows XP, Vista, or Windows 7
- PC-C: Windows XP, Vista, or Windows 7
- Serial and Ethernet cables as shown in the topology
- Rollover cables to configure the routers via the console

Part 1: Basic Router Configuration

In Part 1 of this lab, you set up the network topology and configure basic settings, such as the interface IP addresses, dynamic routing, device access, and passwords. All tasks should be performed on routers R1, R2, and R3. Here we are providing examples of router 1

Step 1: Cable the network as shown in the topology. Attach the devices shown in the topology diagram, and cable as necessary.

Step 2: Configure basic settings for each router such as, ip addresses, hostnames,clockrate on DCE interface (you can also refer to previous labs).

R1(config)# interface S0/0/0

R1(config-if)# clock rate 64000

Step 3: Disable DNS lookup.

To prevent the router from attempting to translate incorrectly entered commands, disable DNS lookup.

R1(config)# no ip domain-lookup

Step 4: Configure the EIGRP routing protocol on R1, R2, and R3.

Router 1:

R1(config)# router eigrp 101

R1(config-router)# network 192.168.1.0 0.0.0.255

R1(config-router)# network 10.1.1.0 0.0.0.3

R1(config-router)# no auto-summary

Router 2:

R2(config)# router eigrp 101

R2(config-router)# network 10.1.1.0 0.0.0.3

R2(config-router)# network 10.2.2.0 0.0.0.3

R2(config-router)# no auto-summary

Router 3

R3(config)# router eigrp 101

R3(config-router)# network 192.168.3.0 0.0.0.255

R3(config-router)# network 10.2.2.0 0.0.0.3

R3(config-router)# no auto-summary

Step 5: Configure PC host IP settings.

Refer to previous labs

Step 6: Verify basic network connectivity.

Use Ping command to verify connectivity within the network, If the pings are not successful, troubleshoot the basic device configurations before continuing.

Step 7: Configure a minimum password length.

R1(config)# security passwords min-length 10

Step 8: Configure the basic console and vty lines.

R1(config)# line console 0

R1(config-line)# password ciscoconpass

R1(config-line)# exec-timeout 5 0

R1(config-line)# login

R1(config-line)# logging synchronous

Configure the password on the vty lines for router R1.

R1(config)# line vty 0 4

R1(config-line)# password ciscovtypass

R1(config-line)# exec-timeout 5 0

R1(config-line)# login

You have to repeat these configurations on both R2 and R3.

Step 9: Encrypt clear text passwords.

R1(config)# service password-encryption

You have to repeat these configurations on both R2 and R3.

Step 10: Save the basic running configuration for all three routers.

R1# copy running-config startup-config

Activity 2: Configure a Site-to-Site VPN with Cisco IOS

In this activity, we will configure an IPsec VPN tunnel between R1 and R3 that passes through R2

Task 1: **Configure IPsec VPN Settings on R1 and R3**

Step 1: Verify connectivity from the R1 LAN to the R3 LAN.

Use ping command to test connectivity, If the pings are not successful, troubleshoot the basic device configurations before continuing.

Step 2: Enable IKE policies on R1 and R3.

IPsec is an open framework that allows the exchange of security protocols as new technologies, such as encryption algorithms, are developed. There are two central configuration elements to the implementation of an IPsec VPN:

1. Implement Internet Key Exchange (IKE) parameters
2. Implement IPsec parameters

Verify that IKE is supported and enabled.

R1(config)# crypto isakmp enable

R3(config)# crypto isakmp enable

Establish an Internet Security Association and Key Management Protocol (ISAKMP) policy and view the available options. To allow IKE Phase 1 negotiation, you must create an ISAKMP policy and configure a peer association involving that ISAKMP policy. An ISAKMP policy defines the authentication and encryption algorithms and hash function used to send control traffic between the two VPN endpoints. When an ISAKMP security association has been accepted by the IKE peers, IKE Phase 1 has been completed. IKE Phase 2 parameters will be configured later. Issue the crypto isakmp policy number configuration command on R1 for policy 10.

R1(config)# crypto isakmp policy 10

Step 3: Configure ISAKMP policy parameters on R1 and R3.

Configure an authentication type of pre-shared keys. Use AES 256 encryption, SHA as your hash algorithm, and Diffie-Hellman group 5 key exchange for this IKE policy

Give the policy a life time of 3600 seconds (one hour). Configure the same policy on R3.

R1(config)# crypto isakmp policy 10

R1(config-isakmp)# authentication pre-share

R1(config-isakmp)# encryption aes 256

R1(config-isakmp)# hash sha

R1(config-isakmp)# group 5

R1(config-isakmp)# lifetime 3600

R1(config-isakmp)# end

R3(config)# crypto isakmp policy 10

R3(config-isakmp)# authentication pre-share

R3(config-isakmp)# encryption aes 256

R3(config-isakmp)# hash sha

R3(config-isakmp)# group 5

R3(config-isakmp)# lifetime 3600

R3(config-isakmp)# end

Verify the IKE policy with the show crypto isakmp policy command.

R1# show crypto isakmp policy

Step 4: Configure pre-shared keys.

R1(config)# crypto isakmp key xxx address 10.2.2.1

The command for R3 points to the R1 S0/0/0 IP address. Configure the pre-shared key on router R1 using the following command.

R3(config)# crypto isakmp key xxx address 10.1.1.1

Step 5: Configure the IPsec transform set and life times.

The IPsec transform set is another crypto configuration parameter that routers negotiate to form a security association. On R1 and R3, create a transform set with tag 50 and use an Encapsulating Security Protocol (ESP) transform with an AES 256 cipher with ESP and the SHA hash function. The transform sets must match.

R1(config)# crypto ipsec transform-set 50 esp-aes 256 esp-sha-hmac

R3(cfg-crypto-trans)#exit

You can also change the IPsec security association life times from the default of 3600 seconds or 4,608,000 kilobytes, whichever comes first. On R1 and R3, set the IPsec security association life time to 30 minutes, or 1800 seconds.

R1(config)# crypto ipsec security-association lifetime seconds 1800

R3(config)# crypto ipsec security-association lifetime seconds 1800

Step 6: Define interesting traffic.

In our topology, the traffic you want to encrypt is traffic going from R1's Ethernet LAN to R3's Ethernet LAN, or vice versa. These access lists are used outbound on the VPN endpoint interfaces and must mirror each other.

Configure the IPsec VPN interesting traffic ACL on R1.

R1(config)# access-list 101 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255

Configure the IPsec VPN interesting traffic ACL on R3.

R3(config)# access-list 101 permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255

Step 7: Create and apply a crypto map.

Create the crypto map on R1, name it CMAP, and use 10 as the sequence number. A message will display after the command is issued.

R1(config)# crypto map CMAP 10 ipsec-isakmp

Use the match address access-list command to specify which access list defines which traffic to encrypt.

R1(config-crypto-map)# match address 101

Setting a peer IP or host name is required, so set it to R3's remote VPN endpoint interface using the following command.

R1(config-crypto-map)# set peer 10.2.2.1

Hard code the transform set to be used with this peer, using the set transform-set tag

command. Set the perfect forwarding secrecy type using the set pfs type command, and also modify the default IPsec security association life time with the set security-association lifetime seconds seconds command.

R1(config-crypto-map)# set pfs group5

R1(config-crypto-map)# set transform-set 50

R1(config-crypto-map)# set security-association lifetime seconds 900

R1(config-crypto-map)# exit

Create a mirrored matching crypto map on R3.

R3(config)# crypto map CMAP 10 ipsec-isakmp

R3(config-crypto-map)# match address 101

R3(config-crypto-map)# set peer 10.1.1.1

R3(config-crypto-map)# set pfs group5

R3(config-crypto-map)# set transform-set 50

R3(config-crypto-map)# set security-association lifetime seconds 900

R3(config-crypto-map)# exit

Apply the crypto maps to the appropriate interfaces on R1 and R3.

R1(config)# interface S0/0/0

R1(config-if)# crypto map CMAP

R1(config)# end

R3(config)# interface S0/0/1

R3(config-if)# crypto map CMAP

R3(config)# end

Task 2: Verify Site-to-Site IPsec VPN Configuration

Step 1: Verify the IPsec configuration on R1 and R3.

R1# show crypto ipsec transform-set

R1# show crypto map

R3# show crypto map

Task 3: Verify IPsec VPN Operation

Step 1: Display isakmp security associations..

R1# show crypto isakmp sa

Step 2: Display IPsec security associations.

R1# show crypto ipsec sa

The African Virtual University Headquarters

Cape Office Park

Ring Road Kilimani

PO Box 25405-00603

Nairobi, Kenya

Tel: +254 20 25283333

contact@avu.org

oer@avu.org

The African Virtual University Regional Office in Dakar

Université Virtuelle Africaine

Bureau Régional de l'Afrique de l'Ouest

Sicap Liberté VI Extension

Villa No.8 VDN

B.P. 50609 Dakar, Sénégal

Tel: +221 338670324

bureauregional@avu.org