Université Grenoble Alpes

http://www.gipsa-lab.grenoble-inp.fr/~jean-marc.thiriet/lpro/cnms_en.html

Course on “security of information systems”
M33-5. Security strategies and policies,
Audits

M33-5. Security strategies and policies - Audits

- 5.1 Security policy, standards
- 5.2 Actors for security
- 5.3 Audit
- 5.4 Synthesis
- 5.5 Conclusions

One of the rules of a security manager

- In security, you should know!
- Be at the good state of the art => to implement « good practices »
- We should prove than we have done/implemented the best regarding the state of the art. => it means that it should be documented

5.1 Security policy, standards

5.1 Introduction

- Establishing a security strategy is an important challenge to protect and make safe a network
  - Need for procedures (documents to be signed by new staff, type of training from them…, password policy, updating some firewalls, saving, during an incident (degraded running, resilience), recovery)
  - Definition of the suitable behaviors
  - Operational and management consensus
  - Measures to be taken in the event of unacceptable behavior (intern within the company, legal action …)
  - **Role and responsibilities** of each group for the security of the company
  - Definition of the necessary tools – expenses dedicated to security

5.1 Definition of the security policy

- Simple and comprehensible (understandable)
- Acceptable by a personnel beforehand sensitized (or maybe trained)
- Easily realizable
- Of easy maintenance
- Verifiable and controllable (periodically)
- Configurable and adaptable to the user needs (according to the profiles of the users, the flows, the context, the localization of the persons)
- Temporal dimension: working days, working hours
- Space dimension: “nomad” users

5.1 ISO certification and security (1/4)

- ISO 17799/27001/27002/… (*Information technology - Security techniques - Code of practice for information security management*),
  - 27005: Information security risk management
    - www.iso.org
- Planning of the continuation of the activity
  - The company must continue to be run normally following a failure or a major incident
- Access control to the system
  - Defines how to control information
  - Defines how to detect the unauthorized activities
- Development and maintenance of the systems
  - Process for the security of the systems, software, data
- Physical and environmental security
  - To protect from any unauthorized access or harmful action

5.1 ISO certification and security (2/4)

- Conformity
  - With the law
  - With the security requirements
- Staff security
  - Risk of human errors
  - Theft (stealing)
  - misuse
- Organization of the security
  - To describe how to maintain and manage it, update it.
- Management of the computers and the operations
  - To describe how to increase security
- Classification and control of the goods
  - To apply and maintain the appropriate degree of protection to the data and information of the company

5.1 ISO certification and security (3/4)

- Adoption of the standard supported by the fact that some insurance companies impose it
- Based on the risk management
- Code of practice for the security management and identification of the requirements for security
- But does not specify the ways of carrying them out
- This standard approaches the organizational, human, legal and technological aspects
- Steps of design, implementation and maintenance of the security
- www.iso.org

5.1 ISO certification and security (4/4)

Fields of security covered by the standards

1. Security policy
2. Organisation of the security
3. Classification and control of the tools
4. Human resources management and security
5. Physical and environmental security
6. Exploitation and management of systems and networks
7. Access control
8. Development and maintenance of the systems
9. Continuity of the service
10. Conformity

5.1 Methods (1/2)

- Methods recommended by the CLUSIF (*Club de la Sécurité de l'Information Français* / French Club for Information security:
  - Marion (*Méthode d'Analyse des Risques Informatiques et Optimisation par Niveau /* Method for the Analysis of the Data-processing Risks and Optimization per Level)
  - Méhari (*Méthode Harmonisée d'Analyse des Risques* / Harmonized Method for Risks Analysis)
- Methods of the DCSSI (*Direction centrale de la sécurité des systèmes d'information /* Central Direction of the information system security:
  - EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité)
  - Melisa (Méthode d'évaluation de la vulnérabilité résiduelle des systèmes d'information)

5.1 Methods (2/2)

- AFAI (*Association Française de l'Audit et du Conseil Informatique /* French Association for the Audit and Data-processing Council), branch of French ISACA (Information Systems Audit and Control Association) => method of governorship and audit of the information systems (CobiT : Control objectives for information and Technology)
- Octave Method (Operationally Critical Threat, Asset, and Vulmnerability Evaluation)
  - Cramm (CCTA Risk Analysis and Management Method)

5.1 Other guides

- CERT (Computer Emergency Readiness Team, www.cert.org) proposes a “Guide to system and network practices”
- NCSA (National Center for Supercomputing Applications, www.ncsa.edu) proposes a “guide to enterprise security”
- Internet Security Alliance (www.isalliance.org) proposes a “Common sense guide for senior manager”
- Information Security Forum (https://www.securityforum.org/) proposes “the standard of good practice for information security”
- The 60 minutes network security guide (first stage towards a secure network environment), SNAC (System and Network Attack Center, USA)

5.2 Actors for security

5.2 Actors for the security (1/4)

- Person in charge of security
  - (director or person in charge of the security mission, administrator…)
  - Function which is more organizational than technical
    - Control of the management and the administration of the means and security measures implemented on the various targets of security
    - Definition of the access privileges to the resources for each category of users
    - Regular revaluation of the access privileges
    - Elaboration and maintenance of the documents for the administrators and the general users
    - To make sure that the targets of security are under monitoring, to take part in the analysis of possible incidents and to decide, with the actors concerned, of the actions necessary to cure the noted failures

5.2 Actors for the security (2/4)

- Person in charge for human resources
  - To carry out controls necessary before the engagement of new collaborators
  - To sensitize the new collaborators towards their responsibility concerning security (directives of security, ethical behavior, charter of use of the resources, clauses of nondisclosure and confidentiality)
  - To make sign the declaration of professional secrecy, non-reproduction of information and their approval of the security policy
  - To coordinate the activities with the person in charge of security when a contract with a collaborator is stopped

5.2 Actors for the security (3/4)

- Heads of department, managing staff
  - To take care that their collaborators or consultants are informed of the security policy so that they respect the regulations
  - To inform the administrators of security concerned of all the modifications having a potential impact on the level of security and its management
  - To analyze, validate and take decisions concerning the requests access to the resources emanating from their collaborators
  - To make a census and recover the significant information held by a collaborator who leaves her/his position in the organization

5.2 Actors for the security (4/4)

- Users (weak link)
  - To comply with the regulations defined by the security policy
  - Not to reveal any confidential information
  - Use of the computer resources of the company only for professional ends
  - Obligation to inform the person in charge of security for any element having a potential impact on security
    - ! Some risks become concrete in a progressive way!

5.2 Measuring user awareness a security policy

- Does your organisation have an information security policy?
- Do you have a copy of that policy?
- Do you refer to that copy frequently?
- Do you know what security awareness means?
- How often doe your organisation conduct security awareness training and refresher sessions?
- Do you feel your security awareness training provides with the necessary knowledge and skills to handle information security incidents?
- Are you aware of what would be considered an information security incident?
- If you think an incident has occurred, what actions would you take?
- To whom would you report an incident?
- Do you feel comfortable in handling an information security incident?

5.3 Audit/security certification

Basic principles of audits

- It is not:
  - Unannounced arrival of controllers who come suddenly to do anything and everything
- It is:
  - Write the operations to be done black and white
  - Informing the people concerned and settling beforehand any difficulty before they become unmanageable
  - ISO 19011 procedures:
    - Describe all the steps of the l'audit
      - From the planification
      - Until the approval of the final report
    - Fundamental principles to be respected by the auditor

Principles of audit

- Ethics (respect for the confidentiality of received information)
- Impartiality: to be factual
- Professional conscience: very precise mission to accomplish in a finite time
- Independence: not to be judge and part
- Evidence-Based Approach: Look for Evidence Proving the Facts

Why an audit?

- Inventory
- Purchase of a subsidiary
- New business application
- Certification
- Customer-supplier relationship (contract)
- Forensic (legal aspects)
- Insurance policies ...

Conduct of an audit (1/3)

1. First contact, analysis of the issues
2. Documentation Review (Concept Audit)
3. Audit plan
4. Opening meeting: explain to the actors what will happen

Conduct of an audit (2/3)

5. Audit activities
   - Analyzes:
   - Architecture
   - Vulnerabilities
   - Applications
   - Components
   - Configurations
   - Penetration tests
   - Risk Analysis / Action Plan

Conduct of an audit (3/3)

6. Closing meeting
7. After the audit
   - Audit report
   - Validation
   - Contest Procedures

Last Homework/Assignment: Deadline ??????

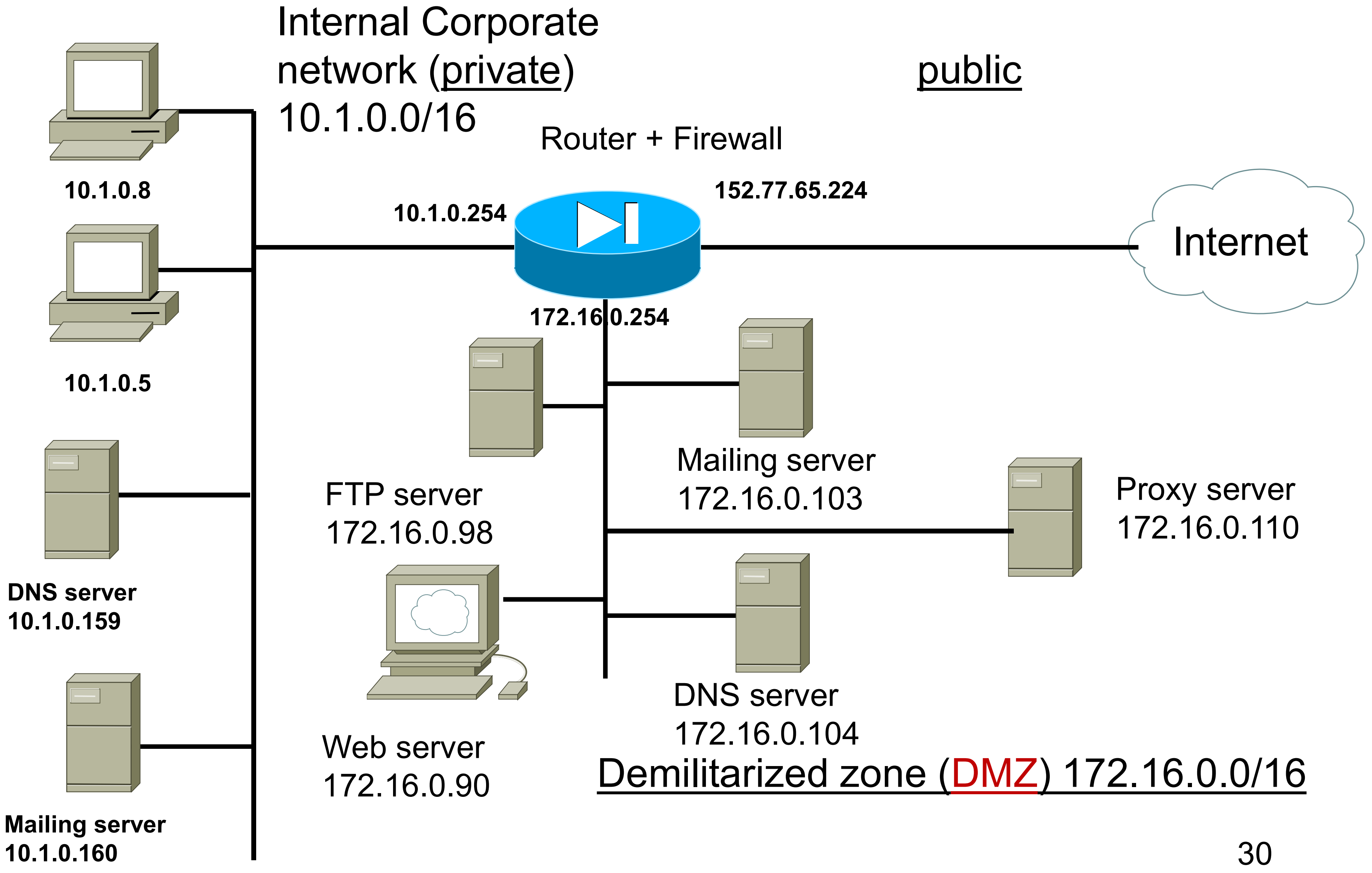
- Based on the document « Master checklist » I gave to you during the first lab
- You are the person in charge of Cyber-security in your company
- You must prepare a summary sheet from this document targeted to the managers of your company.
- It is considered that the company's managers are not specialists in information systems (computers, network).
- Give the elements of this summary sheet.
- The good size of this summary sheet is between 1 and 2 pages.

5.4. Synthesis – Security policy

Guiding principles for the configuration of a firewall => can be applied to security in a general way

- Less privilege: do not grant the users with a higher level of rights that they need; to prohibit for example the peer-to-peer protocol within a company
- Default Prohibition: To prohibit everything by default: everything which is authorized should be explicitely authorized
- In-depth defense: to use the protection means at all the possible levels, for example by analyzing and filtering everything which can be analyzed at the level of the firewall. This principle prevents letting enter the network undesirable communications, even if another method of control is used more in-depth in the network
- Bottleneck: all the communications incoming and outgoing of the network must pass through the firewall. Other paths are strictly forbidden, such as for example unauthorized modems or access points
- Simplicity: the firewall filtering rules must be the simplest and most comprehensible as possible in order to avoid any error on behalf of the administrator or his successors (every rule should be documented and traceable)
- Participation of the users: the users must be involved in the firewall definition. They must indeed express their needs and receive in exchange the reasons and the objectives of the installation of such a device; the constraints related with the firewall will be accepted thus better.

A secure architecture…



Internal Corporate network (private) 10.1.0.0/16

public

Router + Firewall

10.1.0.8

10.1.0.254

152.77.65.224

Internet

10.1.0.5

172.16.0.254

Mailing server
172.16.0.103

FTP server
172.16.0.98

Proxy server
172.16.0.110

DNS server
10.1.0.159

Web server
172.16.0.90

DNS server
172.16.0.104

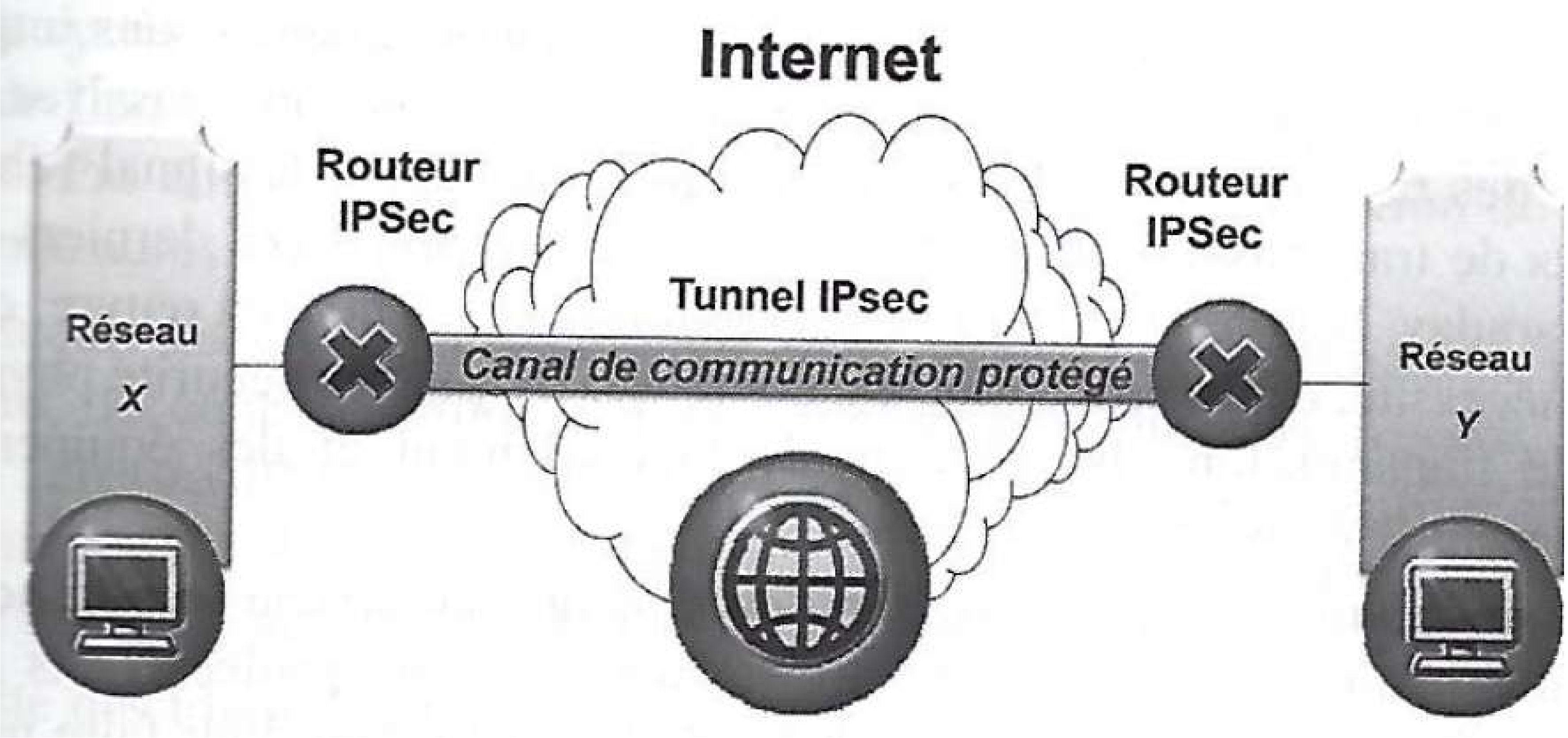
Demilitarized zone (DMZ) 172.16.0.0/16

Mailing server
10.1.0.160

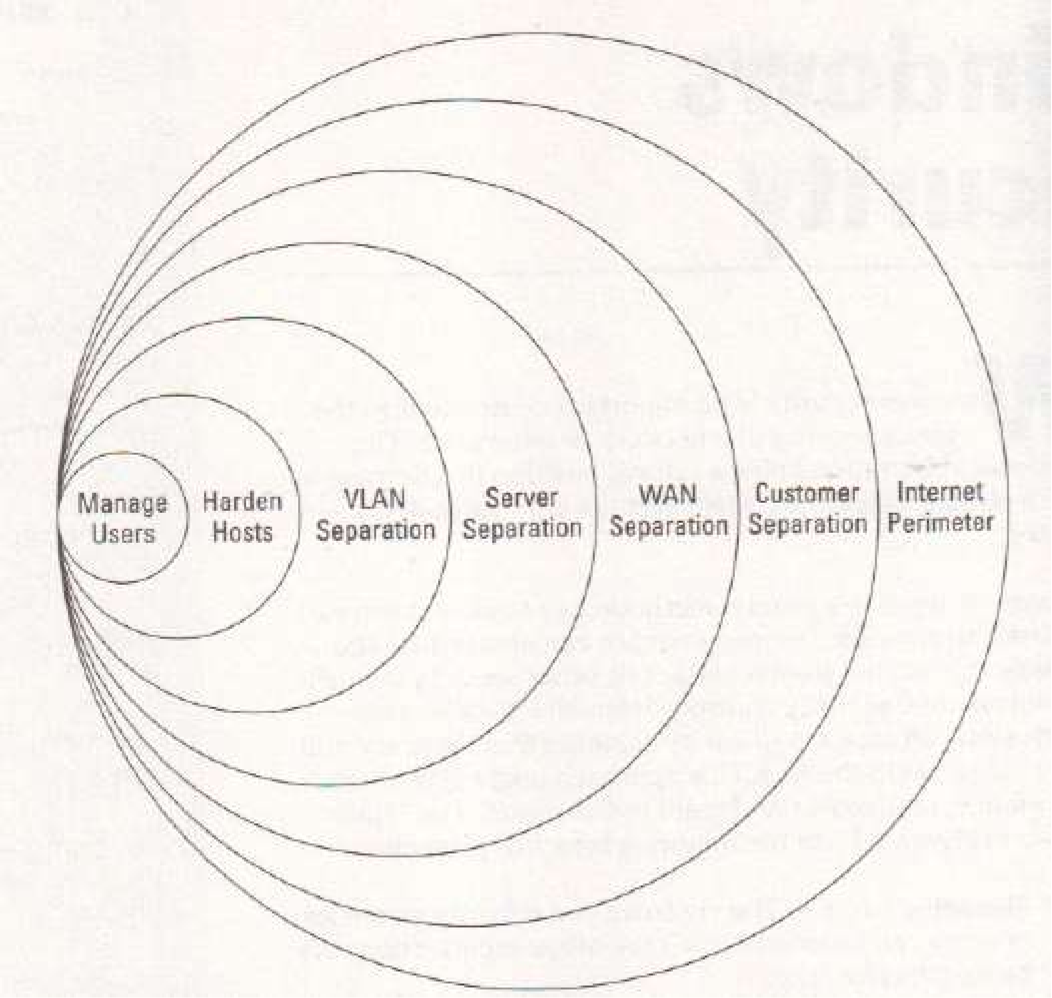
Cryptography applications

- Protecting sensitive data or connections (as a function of the risk analysis)
  - Encryption/enciphering (Confidentiality)
  - Digital signature (integrity, authenticity)
  - Quality of service, real time
  - Trustability, confidence

Security protocols: Ex IPSec tunnel mode



Defense-in-depth methodology



Managing users

The vigilance and security awareness of users can be crucial to all the other security controls to be effective

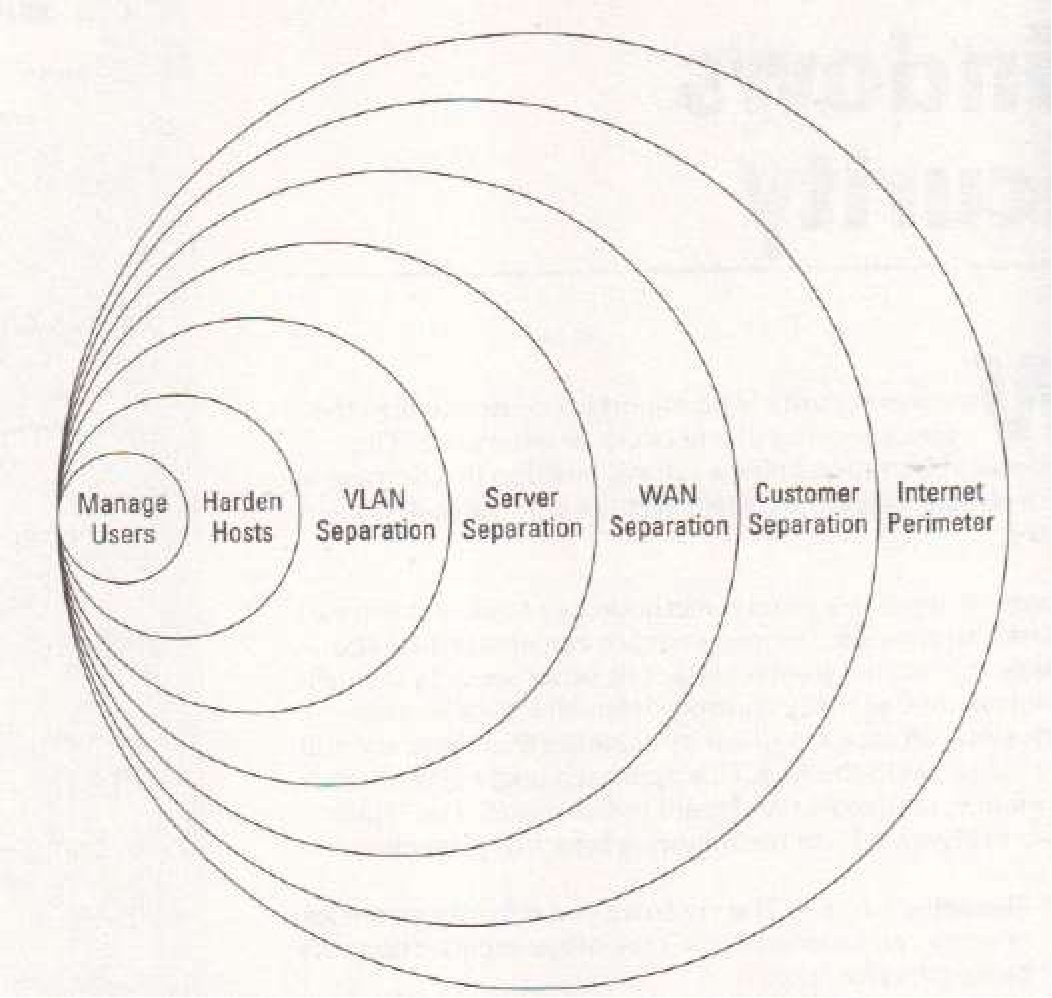
Harden hosts

Defaults features are prime targets for attackers and always make the Top 10 on vulnerability lists

VLAN separation

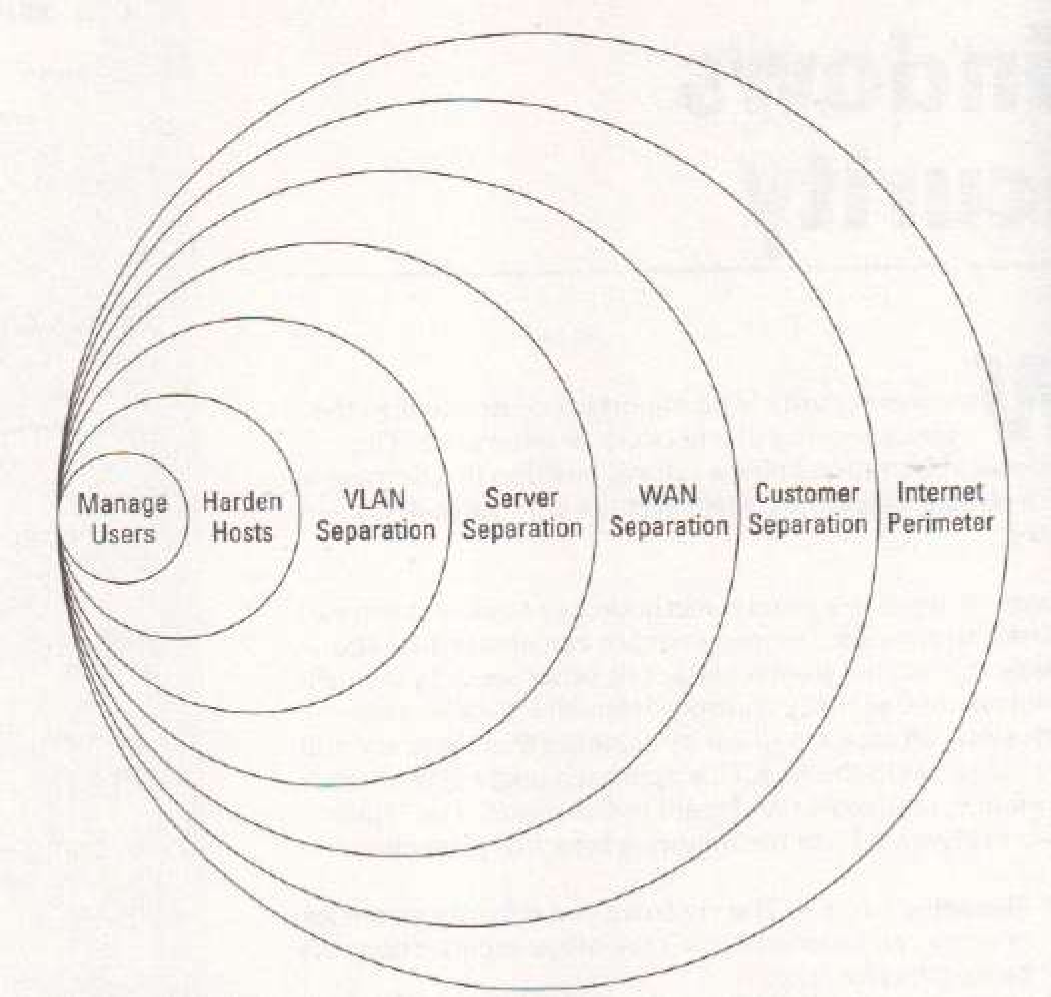
Trust but separate – no one aside specific administrators need to be able to reach strategic servers

Defense-in-depth methodology



- Server separation
  - Provide a place of enhanced security for high-value targets
- WAN separation
  - Establish access criteria between hosts and servers
- Customer separation
  - Assume that any users and hosts outside of an organisation's control are insecure
- Internet perimeter
  - The Internet contains many threads, but most attacks come from inside

Defense-in-depth methodology



Convenient target

Hacker Discouraged, because of the price to « pay » for the attack…

Chosen target

Implement multiple security layers to successfully detect a running advanced attack…

5.5 Conclusion

5.5 It is possible to protect systems and networks

- Multiple protection technics, but each solution gets some weaknesses
  - Problems of configuration
  - Software security holes
- Hacking is more and more easy
  - Hacking a Wi-Fi network with a PDA
- More and more risks
  - Remote working
  - Communicating tools
- Vital/strategic data for companies

5.5 A "good" security

The network administrator should

- know everything about configurations
  - Servers
  - Network devices
  - Client computer
- know about other communicating devices
  - Phones
  - IoT objects with network capabilties
  - WIFI
- Use of probes
- Use of logs
- Good documentation

5.5 What is certain?

- We won’t avoid hacking
  - But we will protect data
    - Saving policy
    - Recoverage plan after an incident
  - We should know when the system is hacked…
    - Log
    - Real-time alarms
- Train the users about
  - Risks
  - Consequences
- Managing security requires to remain curious and open-minded, but not to be paranoiaque

Final exams M25 and M33

- No documents
- Questions about the course or applications of the course
- M33: Questions of a general nature about a security policy, with the same « feeling » as the report / memoir

- Good luck!

Université Grenoble Alpes

References (1/2)

- J.F. Aubry – Cours de Sûreté de Fonctionnement, INPL Lorraine, 2005.
- E. Cole, R. Krutz, JW Conley - Network security bible – Wiley, 2005.
- A. Fernandez-Toro, management de la sécurité de l'information, implémentation ISO 27001 et 27002
- C. Davis, M. Schiller, K. Wheeler – IT auditing : using controls to protect information assets
- J.C. Laprie & al. – Guide de la sûreté de fonctionnement – Cépaduès, 1995.
- A. Villemeur – *Sûreté de fonctionnement des systèmes industriels* – Editions Eyrolles, Paris, 1988.
- S. Ghernaouti-Helie – *Sécurité informatique et réseaux, 4ème édition* – Dunod, 2013.
- Security for industrial communication systems, Dacfey Dzung, Martin Naedele, Thomas P. Von Hoff, Mario Crevatin, pp. 1152-1177, Proceedings of the IEEE, Vol. 93, n° 6 "Industrial Communication Systems", June 2005
- La sécurité des réseaux-First steps, Tom Thomas, Cisco Press, 2005
- Les réseaux, édition 2005, G. Pujolle, Eyrolles 2004
- Course of Jean-Luc Noizette, ESSTIN, Nancy.
- G. Avoine, P. Junod, P. Oechslin – Sécurité informatique, exercices corrigés – Vuibert, Paris, 2006
- Presentation of Eric WIESS
- VPN, mise en œuvre sous Windows Server 2003, P. Mathon, 2004

References (2/2)

- Compression et cryptage des données multimedia, X. Marsault, Hermès, 1995
- SSL VPN, Understanding, evaluating and planning secure, web-based remote access – J. Steinberg & T. Speed, 2005.
- P. H. Oechlin, LASEC/EPFL
- http://sebsauvage.net/comprendre/encryptage/crypto_rsa.html
- F. Halsall – Computer networking and the internet – Addison Welseley, 2005 + additional student support at www.pearsoned.co.uk/halsall
- SSH, le shell sécurisé, D. J. Barrett et R.E. Silverman, O'Reilly, 2001
- Hacking interdit, IIème édition, Micro Applications, 2007
- D. Vergnaud – Exercices et problèmes de cryptographie, Dunod, 2015
- CEH, Certified Ethical Hacker, Matt Walker, McGrawHill, 2017
- L. Bloch & al. – Sécurité informatique pour les DSI, RSSI et administrateurs, Eyrolles, 2016.
- Collectif sous la Direction de Y. Fouratier & L. Petre-Cambacedes – Cybersécurité des installations industrielles – Cepadues, 2015.

- The use of the methods described in this course engages the responsibility of the users!