M2 CyberSecurity
Security Architecture: network, system, key management, cybersecurity of industrial system.

Systems and Network Security

Florent Autréau - florent.autreau@imag.fr
2016 /2017

Objectives / Organization

- Basics of unix systems administration, basics of network security
  - Linux installation/administration
  - Network Security
  - System hardening and tools configuration
- Florent Autréau – florent.autreau@imag.fr - available on appointment – F314
- Grégory Mounié - Gregory.Mounie@imag.fr -

Lectures

- Introduction / Concepts / Threat Landscape
- Network Architecture - Theats/Protection Layer 1 to 7
- Communication Security
  - Firewall / proxying
  - VPN : ipsec, ssh, ssl
  - Wireless Security
  - IPv6 security

Lectures (cont.)

- Services / Application Security
  - DNS / DNSSec
  - E-mail
  - Web
- PKI : integration with application, operation
- OS Security hardening
  - SeLinux, AppArmor, GRSec
  - HIDS

Tutoring / Exercices

- Presentation : technical description of a threat/attack and recommendation
- Attack Tree
- Presentation : technical description of a protection mechanism

Practical Works

- TP1 Installation and environment setup (VM running web server)
- TP2 Tools / Iptables
- TP3 Network filtering / Network Attacks
- TP4 ssh / ssl
- TP5 HA – Hardening
- TP6 SDN (1/9/17 – to be confirmed)

Evaluation : *show me that it works*

Practical Works

- **Goal :** Set-up a secure minimal infrastructure
  - Installation and configuration of web server running in a VM
  - The web service will have to be hardened, secured and will benefit from HA mechanisms
  - OS hardening
  - Application setup and hardening
  - Network setup and security
  - Attack / Defense

Evaluation

- Evaluation for this class will be based on:
  - 0.75 - Individual reports from the Hand-on Labs (M2CySecAudit-TP<num>-<name>.pdf)

    Practical evaluation (“show me that it works and how”)
  - 1.25 - Final Exam

Références - Bibliographie

- 'TCP/IP Illustrated Volume 1,2 and 3', W.Richard Stevens and al.
- 'Practical Unix and Internet Security', Simon Garfinkel and Gene Spafford

Network Security - Part 1

- Introduction
-

Definitions

Confidentiality : Make sure that IT services and resources are ONLY available to accredited entities.

garantie que seules les entités autorisées ont accès aux éléments considérés.

Intégrité : Make sure that information as well as information processing is exact, reliable, trusted and eventually provable.

garantie que les éléments considérés sont exacts et complets.

Definitions

Availability : Make sure that IT services and resources are available for accredited users (employees, customers, partners, contractors).

garantie que ces éléments considérés sont accessibles au moment voulu par les personnes autorisées.

Traceability (“Auditability”) : *garantie que les accès et tentatives d'accès aux éléments considérés sont tracés et que ces traces sont conservées et exploitables.*

Non-repudiation / *irréfutabilité*

Authorization

Authentication/Identification

- Authentication : process of verifiying the identity of an entity (user, service, …), to allow acces to ressources (system, network, application). Authentification determines if the given entity is who/what she claims to be.
- Identification : process of determining the identity of an entity. It is the act of finding out who someone is or what something is.
- Identification is the act of finding out the identity of an entity. Authentication is the verification of the identity.

Authentification/Identification

- Authentification : la procédure qui consiste, pour un système informatique, à vérifier l'identité d'une entité (personne, ordinateur...), afin d'autoriser l'accès de cette entité à des ressources (systèmes, réseaux, applications...). L'authentification permet donc de valider l'authenticité de l'entité en question.
- Identification : action permettant de connaître l'identité d'une entité, souvent à l'aide d'un identifiant tel qu'un nom d'utilisateur
- L'identification permet donc de connaître l'identité d'une entité alors que l'authentification permet de vérifier cette identité.

Authentification (1)

L’authentification permet de vérifier l'identité d'un utilisateur sur une des bases suivantes :

- Un élément d'information que l'utilisateur connaît (mot de passe, passphrase, etc.) - *ce qu'il sait*
- Un élément que l'utilisateur possède (carte à puce, clé de stockage, certificat) – *ce qu'il a*
- Une caractéristique physique propre à l'utilisateur, on parle alors de biométrie (photo, fond de rétine, empreinte digitale, ADN, etc.) - *ce qu'il est*
- Un élément que l'utilisateur réalise (signature, geste) – *ce qu'il fait*

Authentification (2)

Authentification simple : l'authentification ne repose que sur un seul élément ou « facteur » (exemple : l'utilisateur indique son mot de passe).

Authentification forte : l'authentification repose sur deux facteurs ou plus[1].

Authentification unique : (Single Sign-On ou SSO) méthode permettant à un utilisateur de ne procéder qu'à une seule authentification pour accéder à plusieurs applications informatiques (ou sites internet sécurisés).

Authentification (3)

L'authentification intervient à différents niveaux dans les couches de protocoles du modèle internet :

* Au niveau applicatif : HTTP, FTP
* Au niveau transport : SSL, SSH
* Au niveau réseau : IPSEC
* Au niveau transmission : PAP, CHAP

Authentification (4)

Exemples de protocoles d'authentification :

- SSL (qui peut également fournir du chiffrement)
- NTLM (utilisé dans les réseaux de Microsoft Windows)
- Kerberos (standard développé au MIT et notamment utilisé par Windows et bien d'autres systèmes)
- Central Authentication Service (CAS) Mécanisme d'authentification et de SSO, libre et gratuit développé par l'Université Yale
- 802.1x mécanisme standard de contrôle de port et d'authentification.
- ...

Network Security - Part 1

- Introduction
- Threats landscape
-

Risk Analysis - Terminology

- **Threat** :
  - what from you want protect valuable assets
  - anything (man made or act of nature) that has the potential to cause harm (a.k.a Menace)
- **Vulnerability** :
  - Failure or Deviation of the Information System
  - weakness that could be used to endanger or cause harm to an informational asset
- **Risk** :
  - when Threat exploits Vulnerability against Valuable Asset
  - Probability that event will happen with a negative impact to an informational asset

Vulnerability

Failure or operational weakness of IS

- Eventually known and documented;
- Can eventually be exploited.

Main reasons :

- Design/inception;
- Implementation;
- Operation.

Sources / enumeration:

- cwe.mitre.org – Common Weakness Enumeration
- owasp.org

Vulnerabilities Impact Classification

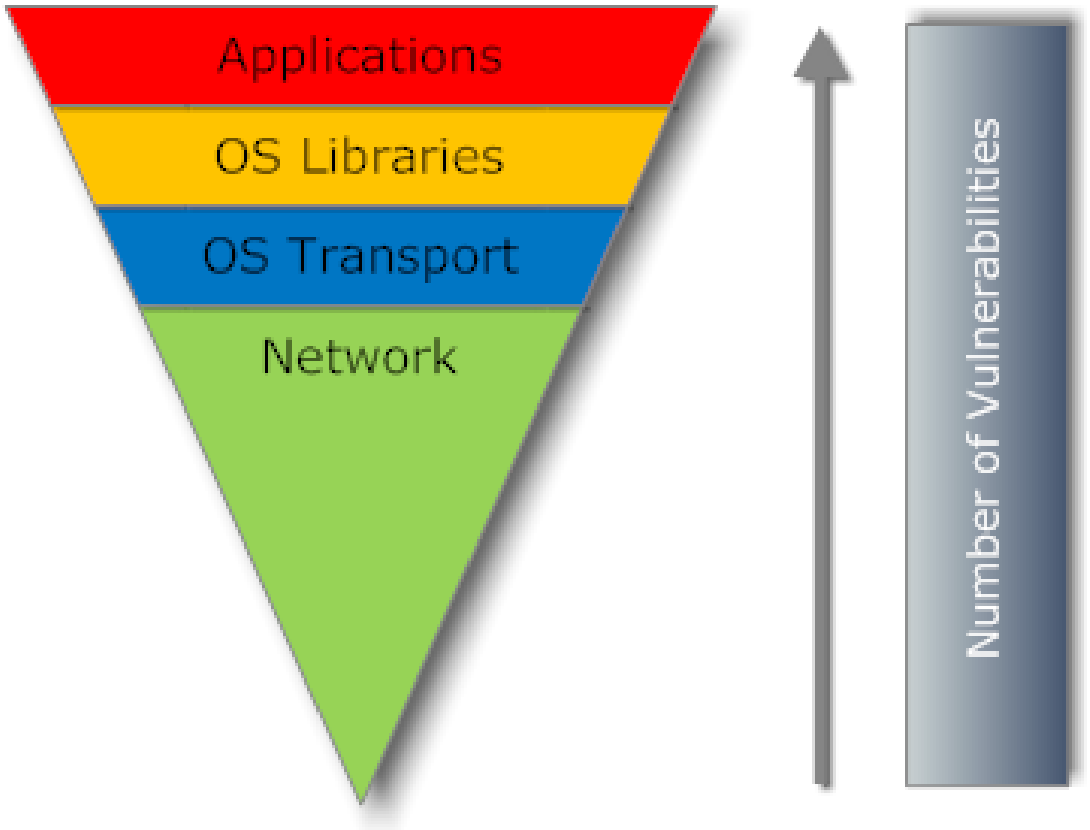
From Microsoft STRIDE threat model

- **spoofing**: usurpation of a legitimate user credential
- **tampering**: alteration (modification or destruction) of data or system
- **repudiation**: unability to prove that an action has been performed
- **information disclosure**: leak of information (data, or system configuration)
- **denial of service**: inability of the system to serve legitimate users
- **elevation of privilege**: gain of additional rights allowing the attacker to perform additional actions

The good questions

- What are the assets ?
- What are the threats ?
- What are the vulnerabilities ?
- What could be the impact/cost ?
- What are the strategies to handle the risk ?

Vulnerability - trends



Top 10 – owasp.org (1)

- **A1 – Injections Flaws Injection flaws, such as SQL, OS, and LDAP** injection, are common in web applications. Injection occurs when user-supplied data is sent to an interpreter as part of a command or query. The attacker's hostile data tricks the interpreter into executing unintended commands or changing data.
- **A2 - Cross Site Scripting (XSS)** XSS flaws occur whenever an application takes user supplied data and sends it to a web browser without first validating or encoding that content. XSS allows attackers to execute script in the victim's browser which can hijack user sessions, deface web sites, possibly introduce worms, etc.
- **A3 - Broken Authentication and Session Management**

  Application functions related to authentication and session management are often notimplemented correctly, allowing attackers to compromise passwords, keys, session tokens, or exploit other implementation flaws to assume other users’ identities.

Top 10 – owasp.org (2)

- **A4 - Insecure Direct Object Reference** A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, database record, or key, as a URL or form parameter. Attackers can manipulate those references to access other objects without authorization.
- **A5 - Cross Site Request Forgery (CSRF)** A CSRF attack forces a logged-on victim's browser to send a pre-authenticated request to a vulnerable web application, which then forces the victim's browser to perform a hostile action to the benefit of the attacker. CSRF can be as powerful as the web application that it attacks.
- **A6 – Security Misconfiguration**

  Good security requires having a secure configuration defined and deployed for the application, frameworks, application server, web server, database server, and platform.

Top 10 – owasp.org (3)

- **A7: Insecure Cryptographic Storage** Many web applications do not properly protect sensitive data, such as credit cards, SSNs, and authentication credentials, with appropriate encryption or hashing.
- **A8: Failure to Restrict URL** Access Many web applications check URL access rights before rendering protected links and buttons.
- **A9: Insufficient Transport Layer Protection** Applications frequently fail to authenticate, encrypt, and protect the confidentiality and integrity of sensitive network traffic.
- **A10: Unvalidated Redirects and Forwards** Web applications frequently redirect and forward users to other pages and websites, and use untrusted data to determine the destination page

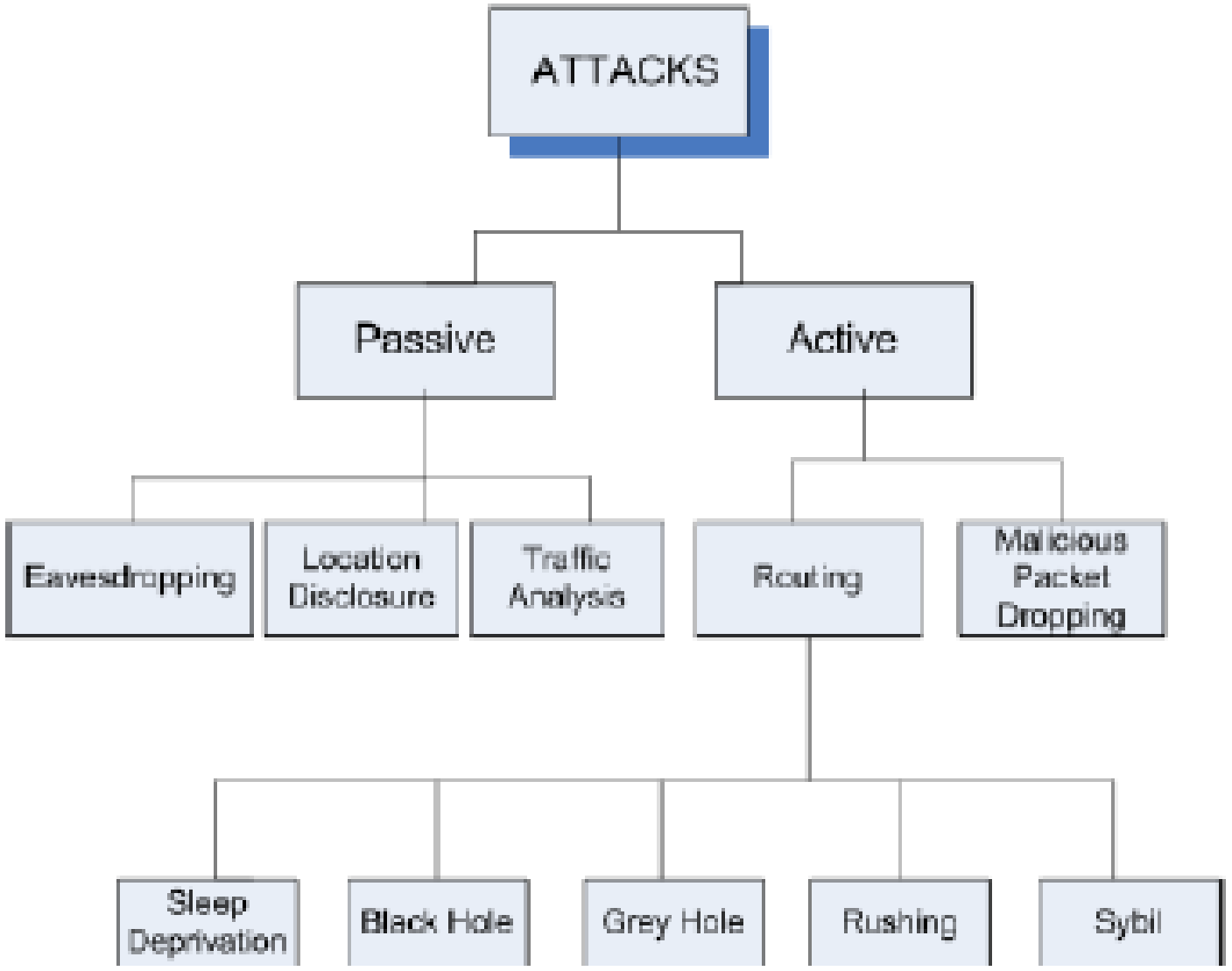
Taxonomy of Threats

- Interruption (ex Denial of Service) – compromises availability
- Interception (ex MiM) – compromises confidentiality
- Modification – compromises integrity
- Forging – compromises authenticity

Exercise 1

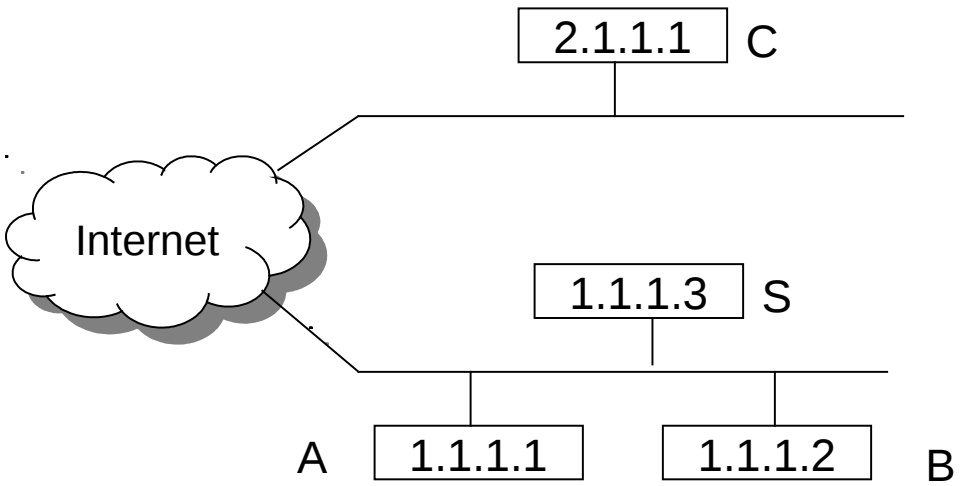
Complete and present the classification of network attacks (based on different Layers for ex.) :

- IP Attacks
- ICMP Attacks
- Routing Attacks
- TCP Attacks
- Application Layer Attacks...


ATTACKS
Passive
Active
Eavesdropping
Location Disclosure
Traffic Analysis
Routing
Malicious Packet Dropping
Sleep Deprivation
Black Hole
Grey Hole
Rushing
Sybil

Security Flaws in IP

- The IP addresses are filled in by the originating host
  - Address spoofing
- Using source address for authentication
  - r-utilities (rlogin, rsh, rhosts etc..)



•Can A claim it is B to the server S?

•ARP Spoofing

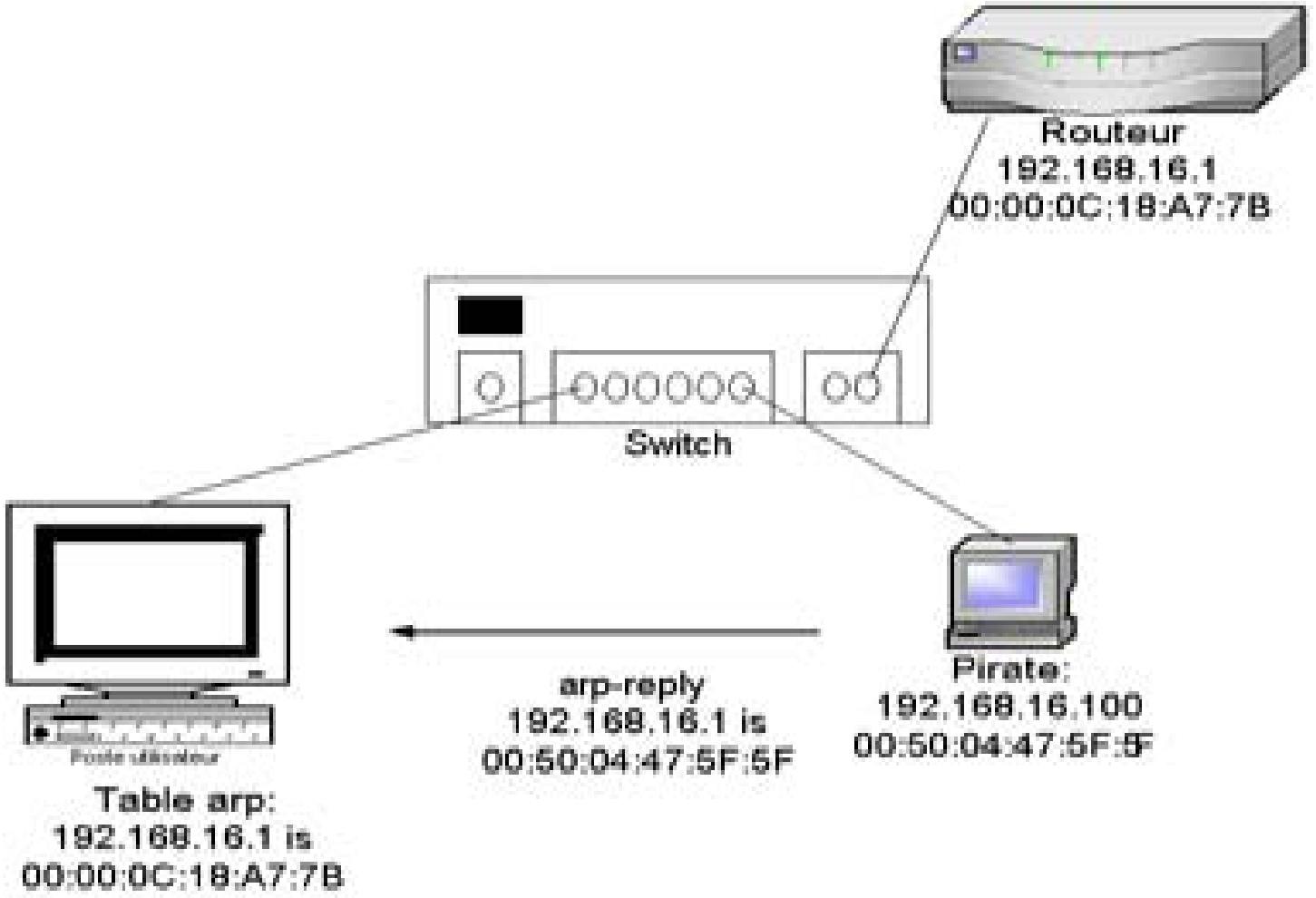
•Can C claim it is B to the server S?

•Source Routing

Security Flaws in IP

- IP fragmentation attack
  - End hosts need to keep the fragments till all the fragments arrive
- Traffic amplification attack
  - IP allows broadcast destination
  - Problems?

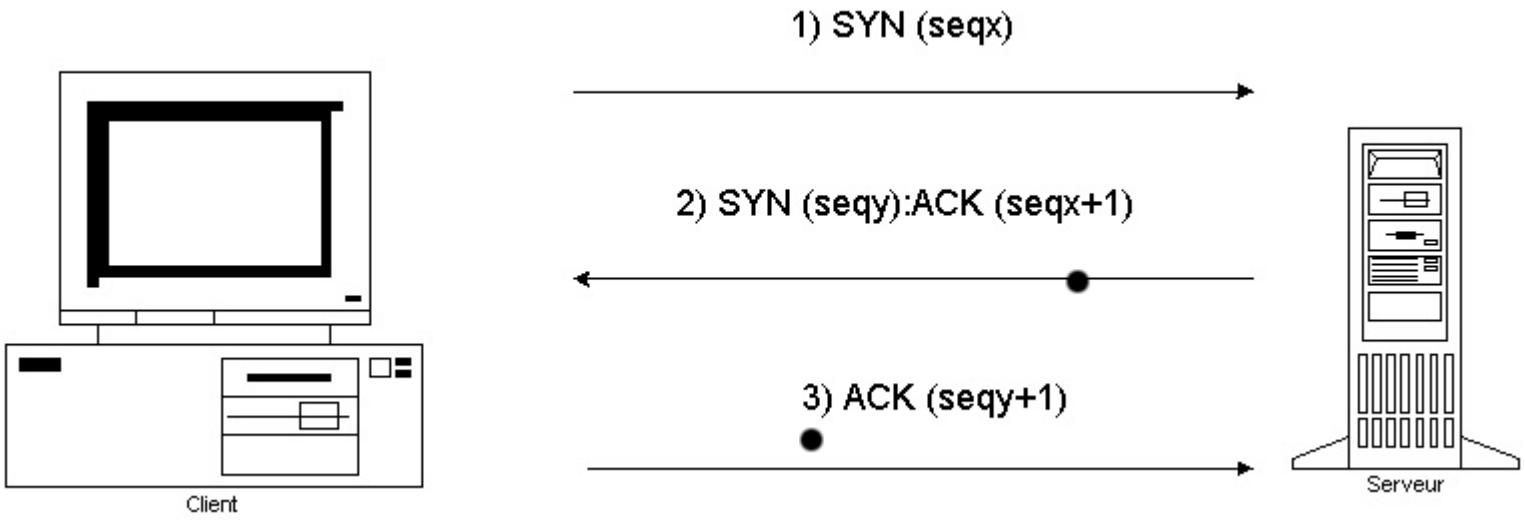
ARP Spoofing



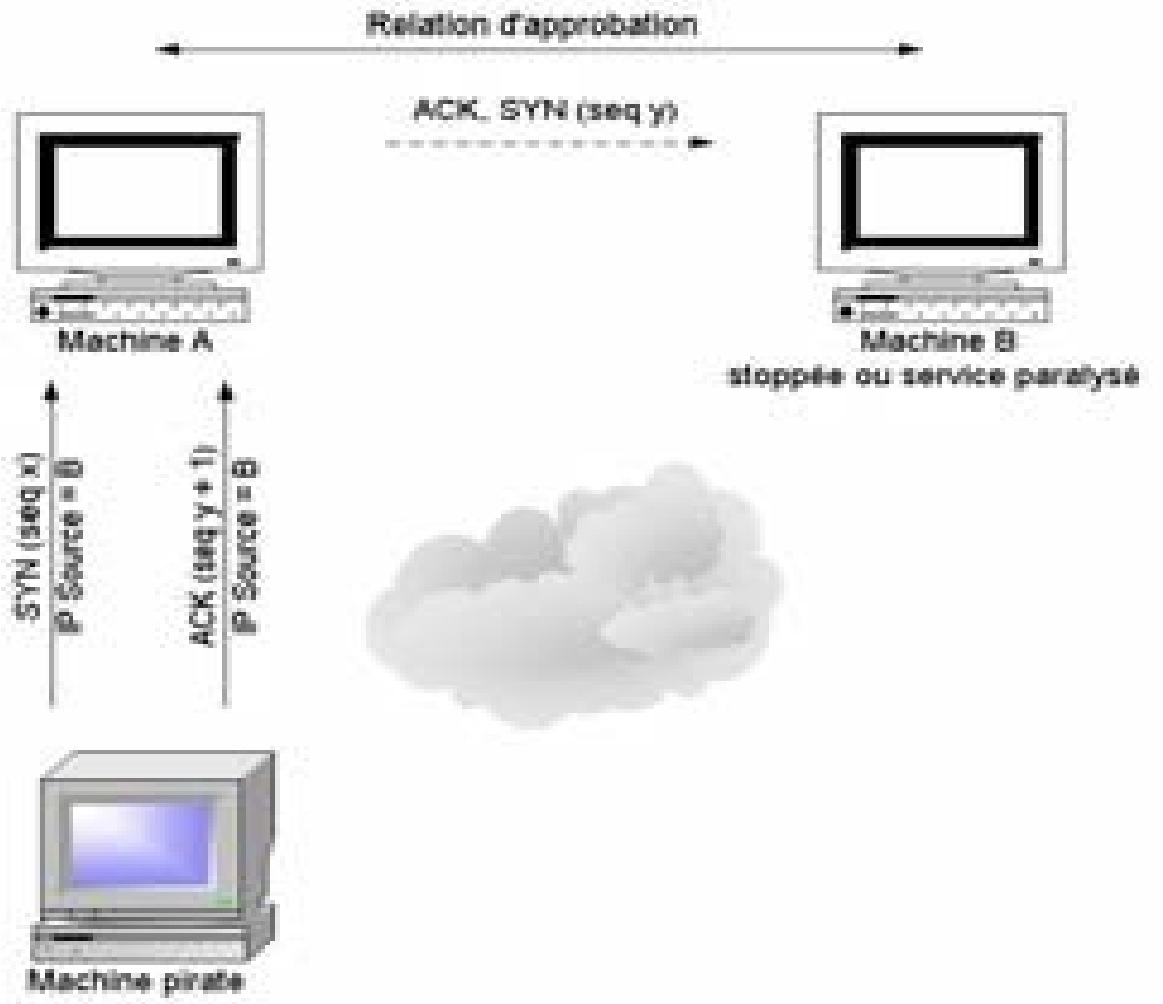
IP Spoofing

- Méthode d'attaque qui parodie l'adresse IP d'un autre ordinateur (usurpation).
- Permet de brouiller les pistes ou d'obtenir un accès à des systèmes sur lesquels l'authentification est fondée sur l'adresse IP (rlogin, rsh sur les machines à numéro de séquence TCP prévisible).

IP Spoofing (2)



IP Spoofing (3)



TCP Layer Attacks

- TCP SYN Flooding
  - Exploit state allocated at server after initial SYN packet
  - Send a SYN and don’t reply with ACK
  - Server will wait for 511 seconds for ACK
  - Finite queue size for incomplete connections (1024)
  - Once the queue is full it doesn’t accept requests

TCP Layer Attacks

- TCP Session Hijack
  - When is a TCP packet valid?
    - Address/Port/Sequence Number in window
  - How to get sequence number?
    - Sniff traffic
    - Guess it
      - Many earlier systems had predictable ISN
  - Inject arbitrary data to the connection

TCP Layer Attacks

- TCP Session Poisoning
  - Send RST packet
    - Will tear down connection
  - Do you have to guess the exact sequence number?
    - Anywhere in window is fine
    - For 64k window it takes 64k packets to reset
    - About 15 seconds for a T1

Application Layer Attacks

- Applications don’t authenticate properly
- Authentication information in clear
  - FTP, Telnet, POP
- DNS insecurity
  - DNS poisoning
  - DNS zone transfer

ICMP Attacks

- No authentication
- ICMP redirect message
  - Can cause the host to switch gateways
  - Benefit of doing this?
    - Man in the middle attack, sniffing
- ICMP destination unreachable
  - Can cause the host to drop connection
- ICMP echo request/reply
- Many more…
  - http://www.sans.org/rr/whitepapers/threats/477.php

Routing Attacks

- Distance Vector Routing
  - Announce 0 distance to all other nodes
    - Blackhole traffic
    - Eavesdrop
- Link State Routing
  - Can drop links randomly
  - Can claim direct link to any other routers
  - A bit harder to attack than DV
- BGP
  - ASes can announce arbitrary prefix
  - ASes can alter path

DOS – Denial of Service

- Déni de service (DOS)
- Attaque destinée à empêcher l 'utilisation d 'une machine ou d 'un service.
- Type d'attaque utilisée par frustration, par rancune, par nécessité, ...
- Ce type d 'attaque peut engendrer des pertes très importantes pour une entreprise : perte d'exploitation ou atteinte à la réputation.
- Attaque relativement simple à mettre en oeuvre (outils faciles a trouver).

DOS – Denial of Service

- Objective → make a service unusable, usually by overloading the server or network
- Consume host resources
  - TCP SYN floods
  - ICMP ECHO (ping) floods
- Consume bandwidth
  - UDP floods
  - ICMP floods

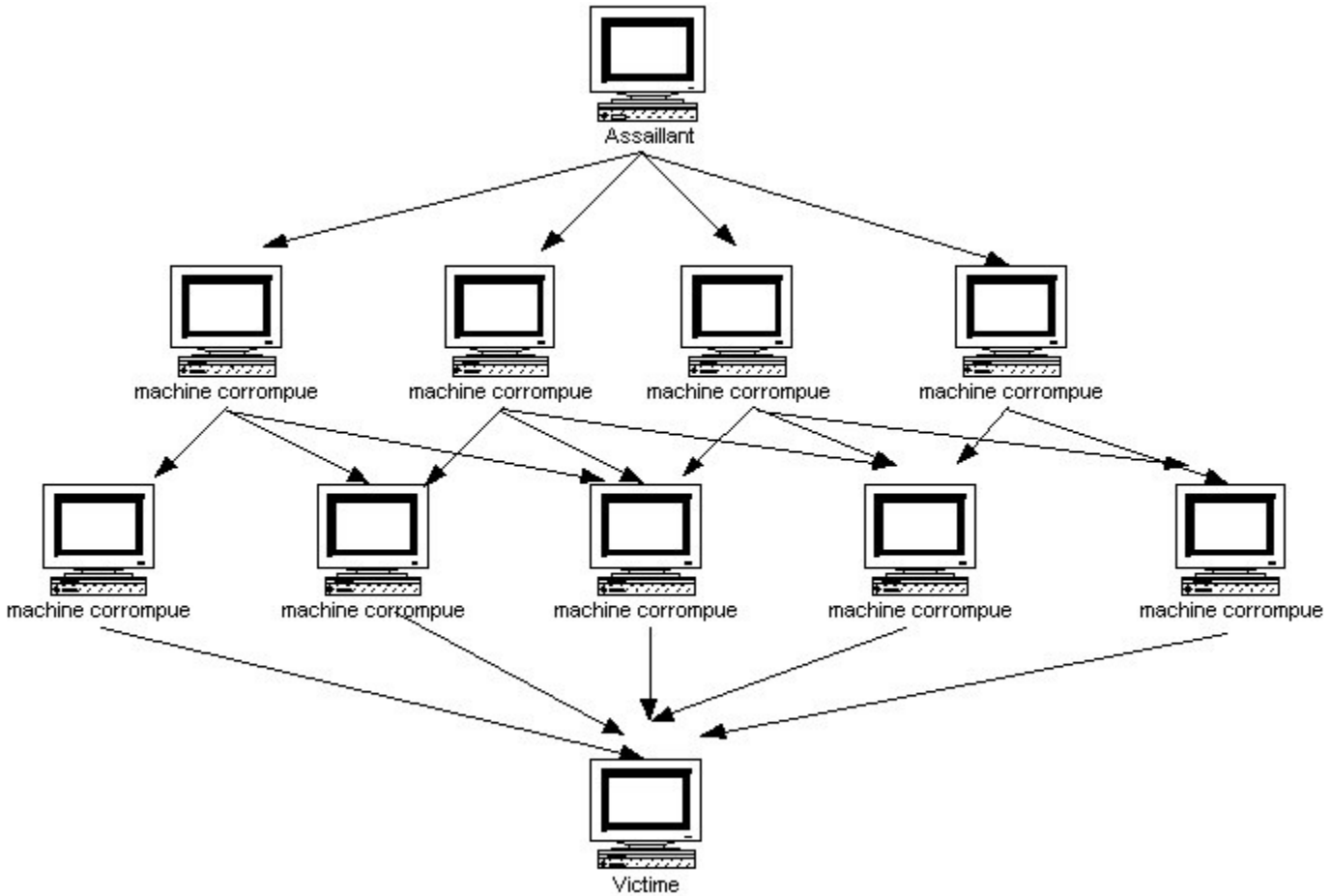
Denial of Service

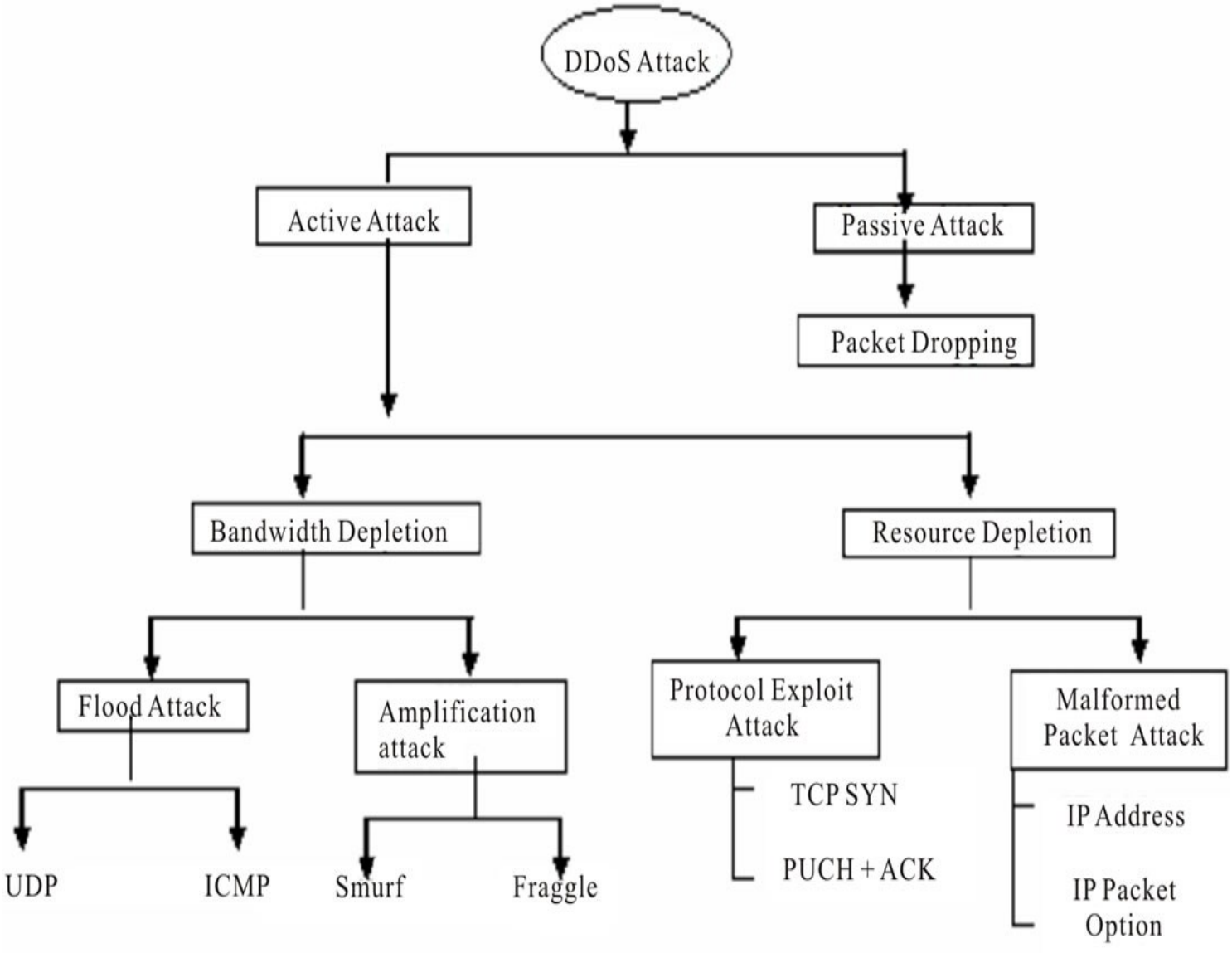
- Crashing the victim
  - Ping-of-Death
  - TCP options (unused, or used incorrectly)
- Forcing more computation
  - Taking long path in processing of packets

DOS – Denial of Service

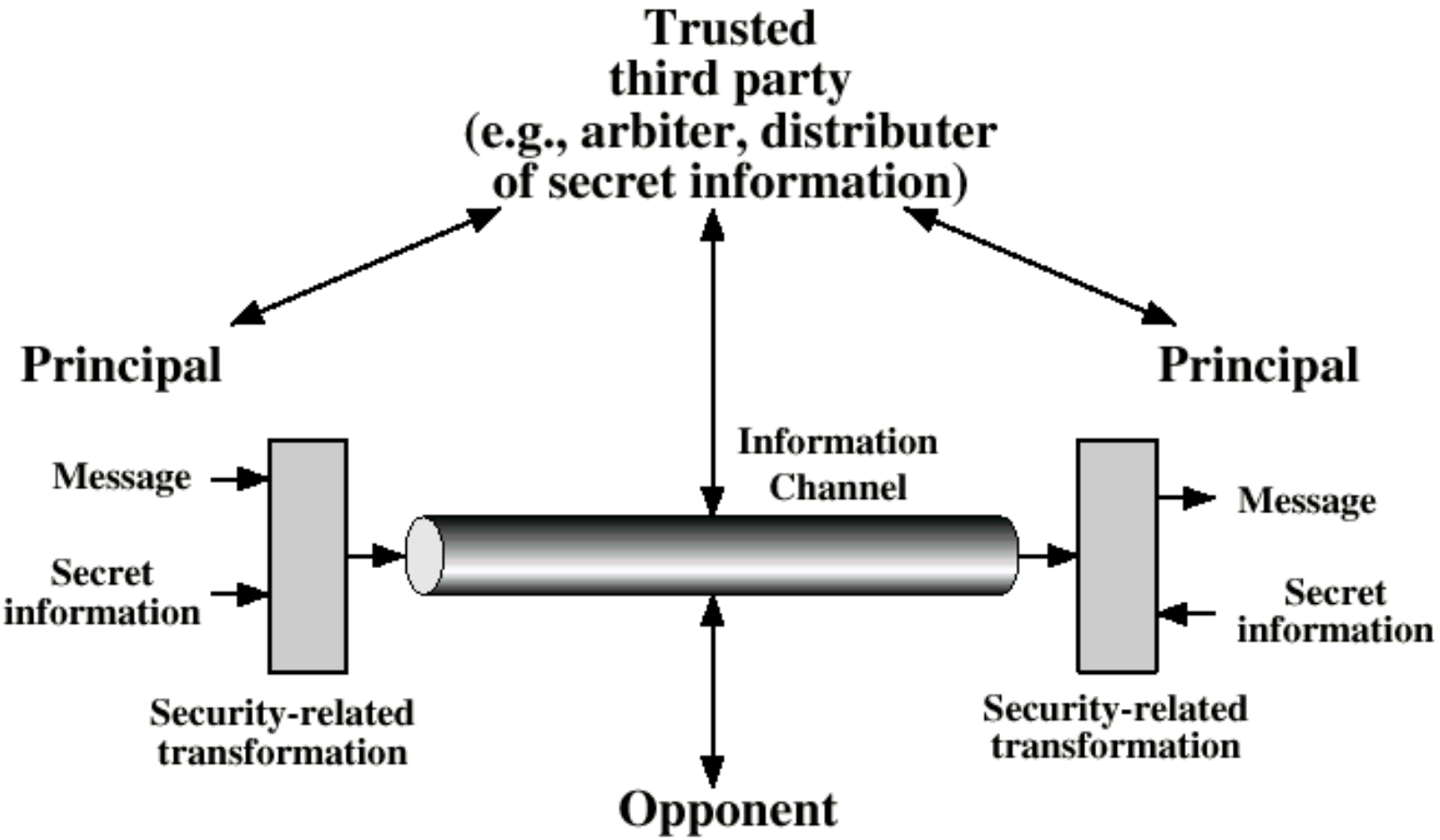
- DOS local (épuisement des ressources du système)
  - Saturation de l'espace disque, cpu, swap,
  - répertoires récursifs
  - boucle infinie
  - ...
- DOS par le réseau (consommation de bande passante)
  - Réassemblage de fragments (Ex: teardrop, ping of death)
  - Flags TCP illégaux
  - SYN flood

Distributed Denial of Service




DDoS Attack
Active Attack
Passive Attack
Packet Dropping
Bandwidth Depletion
Resource Depletion
Flood Attack
Amplification attack
Protocol Exploit Attack
Malformed Packet Attack
UDP
ICMP
Smurf
Fraggle
TCP SYN
PUCH + ACK
IP Address
IP Packet Option

Model for network security



Opponent – security threads and possible attacks

[Stallings'01]

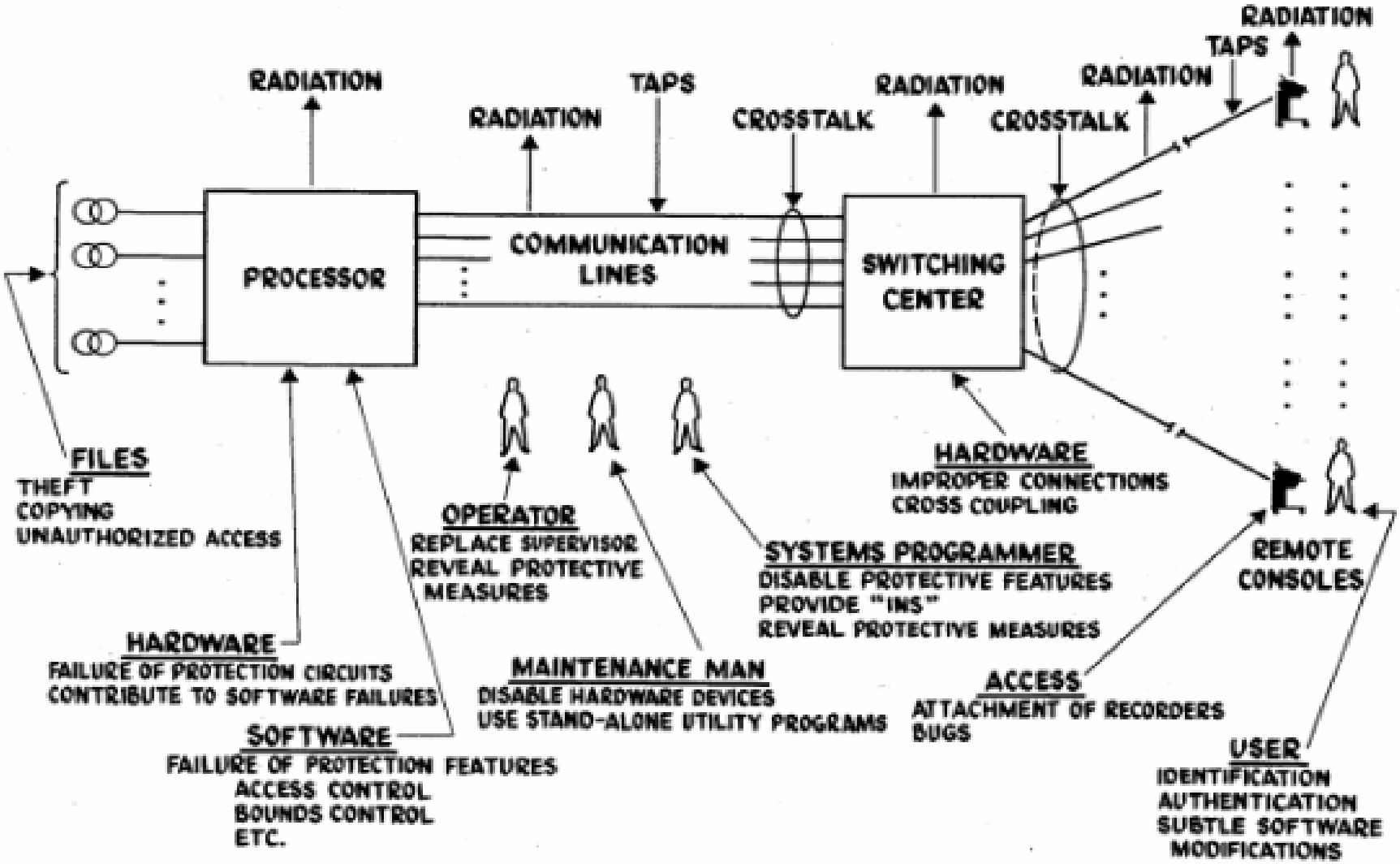

COMPUTER NETWORK VULNERABILITIES
RADIATION
RADIATION
TAPS
CROSSTALK
RADIATION
CROSSTALK
RADIATION
TAPS
RADIATION
PROCESSOR
COMMUNICATION LINES
SWITCHING CENTER
FILES
THEFT
COPYING
UNAUTHORIZED ACCESS
OPERATOR
REPLACE SUPERVISOR
REVEAL PROTECTIVE MEASURES
HARDWARE
IMPROPER CONNECTIONS
CROSS COUPLING
SYSTEMS PROGRAMMER
DISABLE PROTECTIVE FEATURES
PROVIDE "INS"
REVEAL PROTECTIVE MEASURES
REMOTE CONSOLES
HARDWARE
FAILURE OF PROTECTION CIRCUITS
CONTRIBUTE TO SOFTWARE FAILURES
MAINTENANCE MAN
DISABLE HARDWARE DEVICES
USE STAND-ALONE UTILITY PROGRAMS
ACCESS
ATTACHMENT OF RECORDERS
BUGS
SOFTWARE
FAILURE OF PROTECTION FEATURES
ACCESS CONTROL
BOUNDS CONTROL
ETC.
USER
IDENTIFICATION
AUTHENTICATION
SUBTLE SOFTWARE MODIFICATIONS

Figure 3

Exercise 2

- Investigate and present an existing attack amongst the following categories
  - Side Channel
  - Interception, observation,
  - Spoofing,
  - DynDos, …
- Recommend and describe protection/mitigation mechanisms