DI-FCT-UNL
Segurança de Redes e Sistemas de Computadores
Network and Computer Systems Security

Mestrado Integrado em Engenharia Informática
MSc Course: Informatics Engineering

1º Sem, 2019/2020

1. Introduction (Part I)

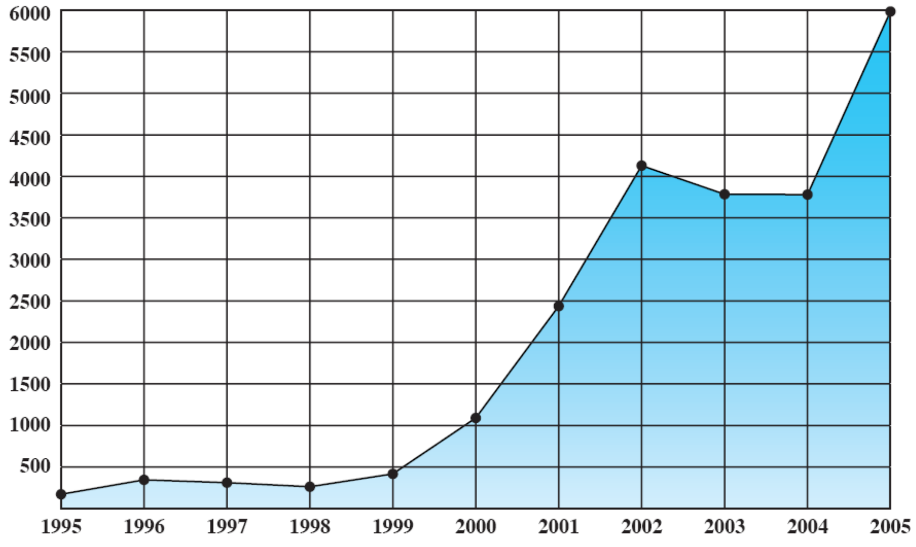
Concepts, Terminology
Frameworks

A Preliminary Background: Security Concerns and Complexity Issues

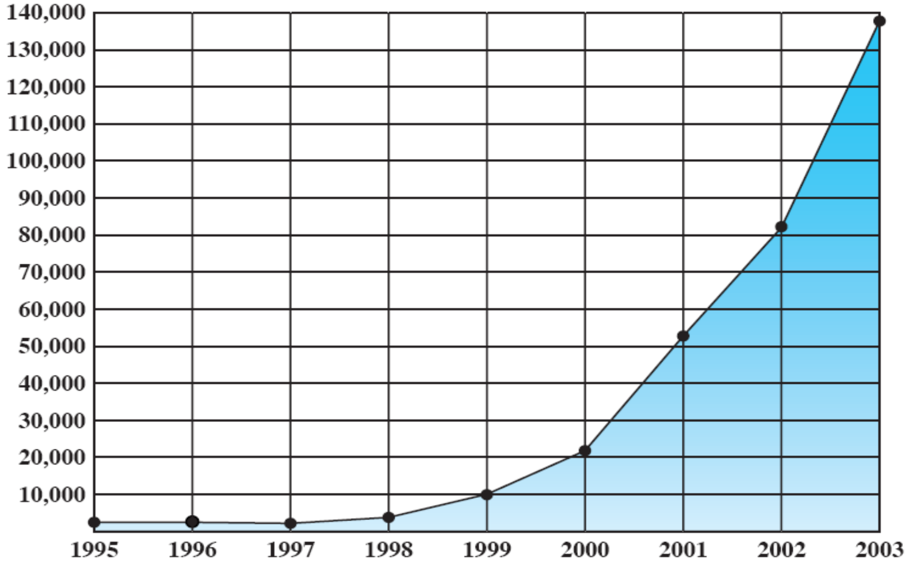
Internet, Scale, Complexity
Vulnerabilities, Threats and Incidents

Vulnerabilities
(Cycles / Growing)

Incidents
(Growing)

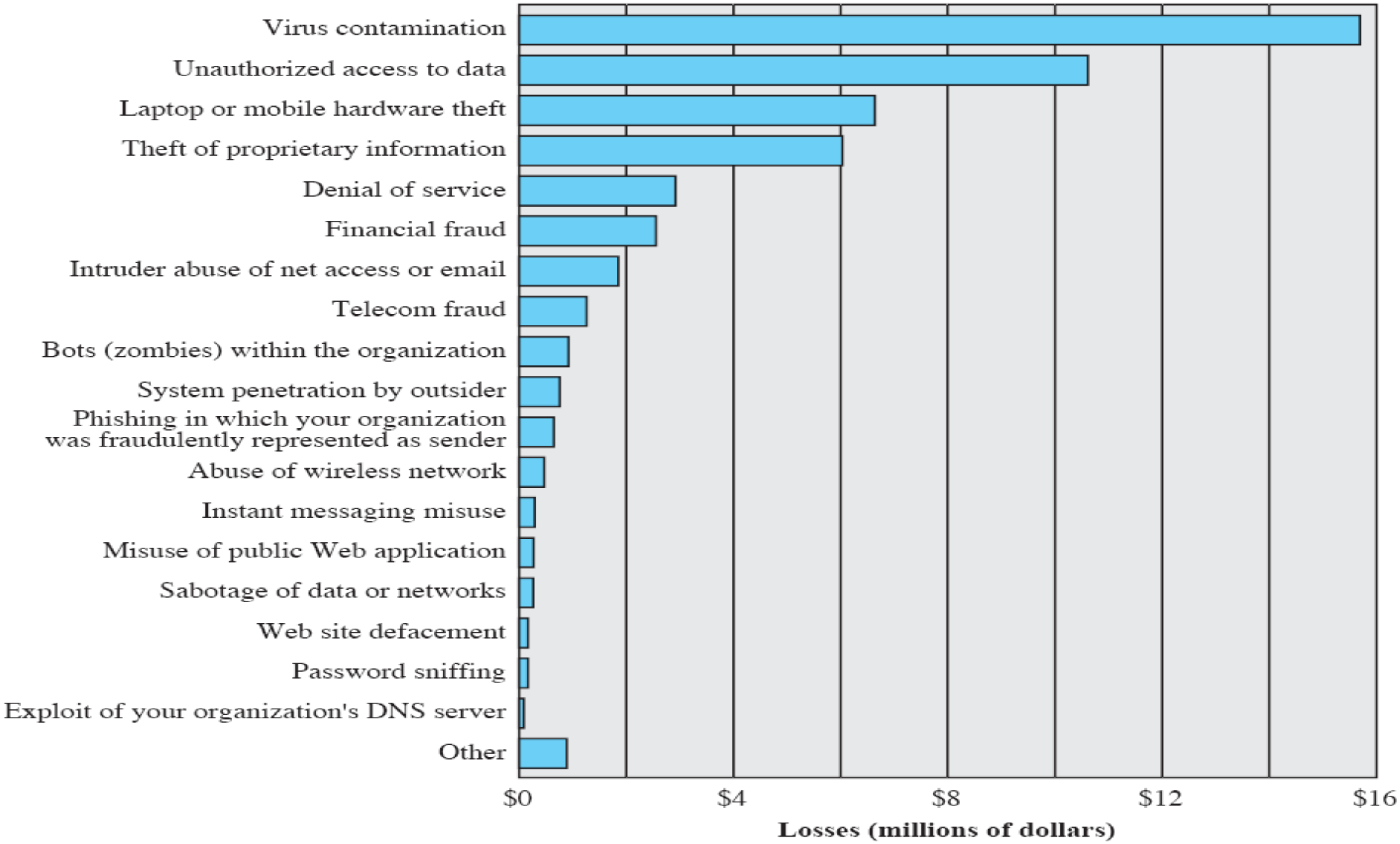


(a) Vulnerabilities reported



(b) Incidents reported

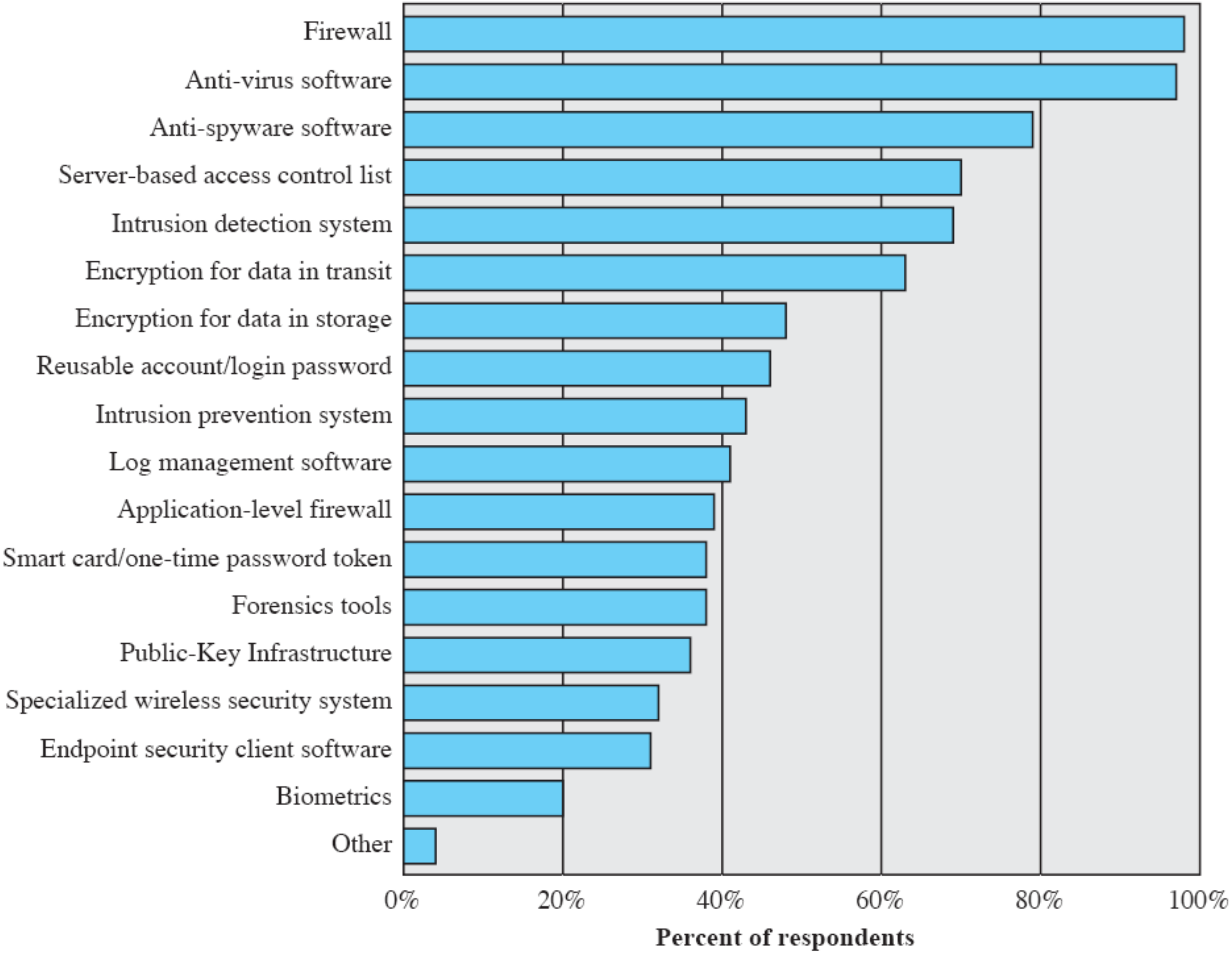
Security Concerns, Costs of Insecurity



Source: Computer Security Institute/FBI 2006 Computer Crime and Security Survey

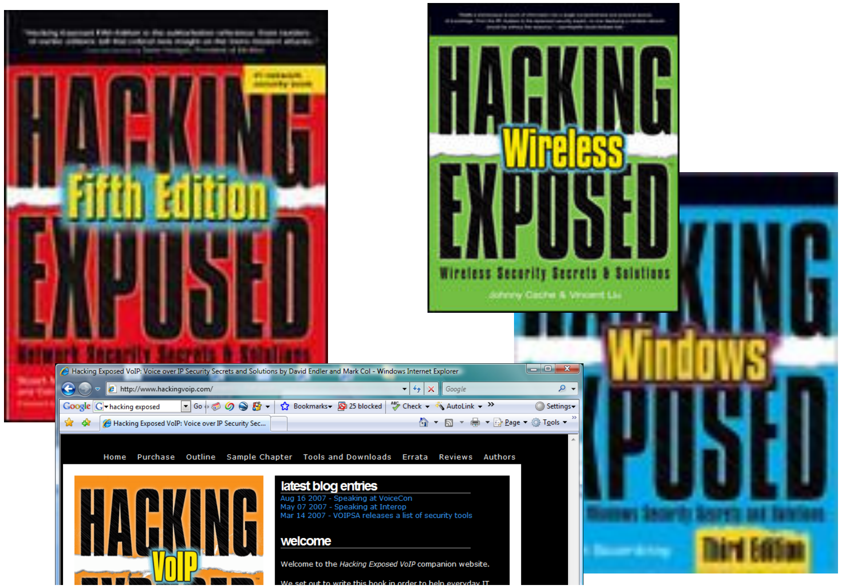
Figure 1.7 Dollar Amount Losses by Type

Security Technologies / Security *mismatches* ?



Hacking exposed, Vast Bibliography, Many Information on Vulnerabilities, Many Attack Tools …

Hacking for dummies !!! (But not only ⋯)


HACKING Fifth Edition EXPOSED
Network Security Secrets & Solutions
HACKING Wireless EXPOSED
Wireless Security Secrets & Solutions
Johnny Cache & Vincent Liu
HACKING Windows EXPOSED
Windows Security Secrets and Solutions
Third Edition
HACKING VoIP

Hacking Exposed VoIP: Voice over IP Security Secrets and Solutions by David Endler and Mark Col - Windows Internet Explorer

http://www.hackingvoip.com/

Google hacking exposed Go Bookmarks 25 blocked Check AutoLink Settings

Hacking Exposed VoIP: Voice over IP Security Sec... Page Tools

Home Purchase Outline Sample Chapter Tools and Downloads Errata Reviews Authors

latest blog entries

Aug 16 2007 - Speaking at VoiceCon
May 07 2007 - Speaking at Interop
Mar 14 2007 - VOIPSA releases a list of security tools

welcome

Welcome to the *Hacking Exposed VoIP* companion website.

We set out to write this book in order to help everyday IT

SECOND EDITION
HACKING Web Applications EXPOSED
HACKING Cisco Networ EXPOSED
HACKING Linux Second Edition

Tools for Attackers (Opponents, Adversaries, Malicious Users), Hackers (Black, Red, White, Ethical)

Outsider vs. Insider Attackers

Non-Educated/Non-Ethical/Unconscious Users or System Administrators (errors, distractions, poor preparation, abuse of privilege, incorrect use of systems)

Origins from Attacks
(… w/ possible related crimes)…

- Tools used by Attackers (Opponents, Adversaries, Malicious Users)
- Hackers (w/ different Hats: Black, Gray, Red, White)
- Ethical Hackers, CEHs,
- Outsider vs. Insider Attackers
- Also vulnerabilities exploited by … or incidents caused by:
  - Unaware / Not-Educated Users
    - Include Errors, Distractions, Naïve-Operation, Poor-Preparation, Incorrect Use / Unknown Consequences
  - Non-Educated/Non-Ethical Users or System Administrators
    - Conscious Malicious Actions, Abuse of Privileges, Incorrect Use w/ Known Consequences

Past, Present ! … and Next ?

- **Mobile and Ubiquitous computing**
  - Problems/Vulnerabilities exposed by Mobile Devices, Mobile OSes and Mobile SW/Apps
    - The "user" as the "superuser", Usability vs. Simplicity
  - Cloud Computing / Cloud Storage Services
    - *aaS …. Security "as a service" too ! Challenges in Outsourced Security and Trust !
- **IoT Security** Challenges: 30, 50 Billion Devices ? ... The way for the "Internet of Everything"
  - Unsecure Devices, Cheap Devices, Resource Constrains, Untrusted/Non-Patcheable Devices
- **Digitalization of more and more critical systems/services**
- From the personal computing to **collective/aggregated/large-scale(intelligent/autonomous computing and information sharing**
  - Big Data Analytics
  - Value of Digital Economy, Digital Politics, Digital Power
  - Privacy breaks / The High-Value of Privacy

Current concerns on "Internet Security"

- Guided Tour
  - See the ref. provided reference(s) in class
- Ex. "The current "kids in town":
  - Web Attacks / Formjack Attacks / Top Ten (recurrent) Vulnerabilities / On-Line Attack Tolkits and Tools
  - Cryptojacking, Overall Ransomware (now in more scale and mobiles)
  - Supply Chain Attacks
  - Malicious Email and Social Networks / Malware, Spamming, Scamming, Physhing and Social Engineering Attacks
  - Mobile "unsecurity": Mobile OSes and IoT Devices
  - Privacy Breaks
  - Cloud Security Issues: Privacy and Trust Breaks (…. Drawbacks grom Outsourced Security and Trust)
  - "Underground" digital economy breaks, disruptions and takedowns (Dark Web Tools,

Complexity Issues

Initial Challenges and Complexity (1) …

- **Requirements in "one-word" labels, but** … specific/specialized meanings and mechanisms beyond quite complex, involving subtle reasoning and maturity

- **Mismatches** between targeted protections/defenses and the proper/real adversarial conditions

- Use of **old-adversary models** not fitting the usage/exposition of provided systems

- **Counterintuitive issues**: Security procedures and usage models are many times often counterintuitive

Initial Challenges and Complexity (2) …

- **Security management procedures** and functions, as well as, **complex human factors** are beyond the properties of security services and mechanisms (ex., A user can be "the adversary")
  - Ex., Management, distributions and use of Passwords, User and Management Interfaces, Cryptographic Keys, Unsecure Computer devices and SW (ex., OS), etc …

- **Security as a process**
  - Security By Design (Good) vs. Security Monitoring and Auditing in systems' life cycle of operation
  - "A dance" between attackers and defenders …
  - Regular and continuous battle … With possible advantages on the adversary side !
  - Difficulty to manage security vs. Availability Operation Tradeoffs (in useful time)

Initial Challenges and Complexity (3) …

- **Perception of Security** relevance, requirements and investment: only when bad things (security incidents) occur
- **Danger of security by patching** and by the **adoption of inappropriate adversary models and not correctly defined attack surfaces**
- **Security is hard under High Scale Conditions** … (ex., Mobile Computing/Devices, IoT, … User as the SysAdmin)
- **Risks of Outsourced Security Control** (ex., Clouds, Outsourced System Administration, etc)
- **Security vs. Usability Tradeoffs:** "Big/Complex Challenge
- Remember also that sometimes … Security Mechanisms and Tools, known and used as Powerful Attack Guns !
  - … **Possible advantages of the Attacker !**

Starting Points

Interesting starting points …

Complexity

> *The combination of space, time, and strength that must be considered as the basic elements of this theory of defense makes this a fairly complicated matter. Consequently, it is not easy to find a fixed point of departure.*
>
> — *On War*, Carl Von Clausewitz

On the Relevance of Adversary Models

> *The art of war teaches us to rely not on the likelihood of the enemy's not coming, but on our own readiness to receive him; not on the chance of his not attacking, but rather on the fact that we have made our position unassailable.*
>
> — *The Art of War,* Sun Tzu

A Good Starting Point …

Relevance of concepts, definitions, correct terminology, security frameworks and standards

Bien sûr. Bien sûr. Mais je dis: tout est bien qui finit bien!...
Ah oui, votre salle de marine?...Très bien, en effet!...
Merci. Mais je disais simplement que nos aventures s'étaient bien terminées, qu'elles avaient heureusement pris fin!...
Non, merci... Jamais entre les repas....
Mais non, mille sabords!... Tout est bien qui finit bien!... TOUT EST BIEN QUI FINIT BIEN!...
Sans aucun doute...

.. Making these words to make a clear sense …

DAC, MAC, RBAC

Deception

DAC, MAC, RBAC

Principal

Security Surface

X509v3

Crypto Padding

Intrusion

Perimeter Defence

Replaying Attacks

Integrity

Replaying Attacks

Digital Signature

Spoofing

Message Forgery

SQLi

DoS, DDoS, DRADoS, …

Security Surface

IPSec

MAC, HMAC, CMAC…

Asymmetric Crypto

Trust Computing Base

Adversary Model

Message Tampering

Sniffing

XSS

PKI

TLS

Hearbleed

Symmetric Crypto

.. Making these words to make a clear sense ...

AES

NIDS

Blowfish

HTTPS

SSH

Subject

DHID

S/MIME

Crypto Provider

RSA

Honeynets

Firewalls

HIDS

Honeypots

OS Hardening

Virtualization Security

PKCS#5, PKCS#7, OAEP

Multi-Factor Authentication

MAC, DAC, RBAC, ABAC

802.1x

ECB, CBC, CTR, OFB, CFB

Java JCA/JCE

Biometric Authentication

X.800, FIPS/PUB

Message Tampering

IP Spoofing

DSA

DH Key Exchange

PGP

ISO 27001

S/MIME

Introductory questions …

- **What is a secure system** ? Can we expect that secure systems exist? How to define a secure system ?
- **What is an "adversary model"** for a secure system? How to define the adversary model?
- **How to approach a common attack taxonomy and anatomy** and how to address a typology of threats and attacks using well-known concepts, notions and terminology ?
- **What means "attack surface", "attack tree" or "security surface" ?**
- **What is a "Trust Computing Base"?** How to define it?
- **What is a "security framework"** and related standards ?
- **How to address the different dimensions of computer systems and networks security ?** (Distributed Systems Security?
- **How to have an initial "structural" vision of security services for Distributed Computing Systems?**

What is a Secure System ?
Can we expect that secure systems exist ?
How to Define a Secure System ?

How to define a "Secure System" ?

Possible definition :

A system that never revealed vulnerabilities or a system that has never been subject to any attack

Intrinsically or paradoxically, this definition says that …

TEHERE ARE NO SECURE SYSTEMS !
IMPOSSIBILITY !

☹ Why ?
☹ Ok ... this doesn't help !

How to define a "Secure System" ?

Secure System (in the context of the CSNS Course):

A System designed with secure objectives addressed as verifiable security properties implemented by security services built from security mechanisms, afforded to attain the applicable objectives of preserving authentication, confidentiality, integrity, availability and access-control protecting principals, information and computation assets, including HW, SW, FW, Data and Communications.

In a Secure System the security services are designed and implemented as countermeasures against attack vectors (or attack typology), to avoid vulnerabilities and to minimize risk, …

… giving to a well-defined threat or adversary model and with security mechanisms established by well-identified, verifiable and minimized trust computing base (TCB) assumptions

How to define a "Secure System" ?

Secure System (in the context of the CSNS Course):

A System designed with secure objectives addressed as verifiable security properties implemented by security services built from security mechanisms, afforded to attain the applicable objectives of preserving authentication, confidentiality, integrity, availability and access-control protecting principals, information and computation assets, including HW, SW, FW, Data and Communications.

In a Secure System the security services are designed and implemented as countermeasures against attack vectors (or attack typology), to avoid vulnerabilities and to minimize risk, …

... giving a well-defined threat or adversary model and with security mechanisms established by well-identified, verifiable and minimized trust computing base (TCB) assumptions

Security and Risk Mitigation

Thinking on RISK:
Security as the Minimization (or Mitigation) of Risks

ATTACKS are manifestations (concretization) of THREATS (attacks as security incidents)

RISK = VULNERABILITIES x THREAT-Potential

RISK (t) = VULNERABILITIES(t) x THREAT-Potential (t)

Computer Systems Security Dimensions

Ex., NIST FIPS PUB 800-12, Oct/2005
(NIST Computer Security Handbook,
NISTIR – Glossary 7298
https://www.nist.gov

Security Properties (as objetives)

The protection afforded to an automated information system in order to attain the applicable objectives of preserving confidentiality, integrity and availability of information resources, including HW, SW, FW, data and information being processed, stored and communicated

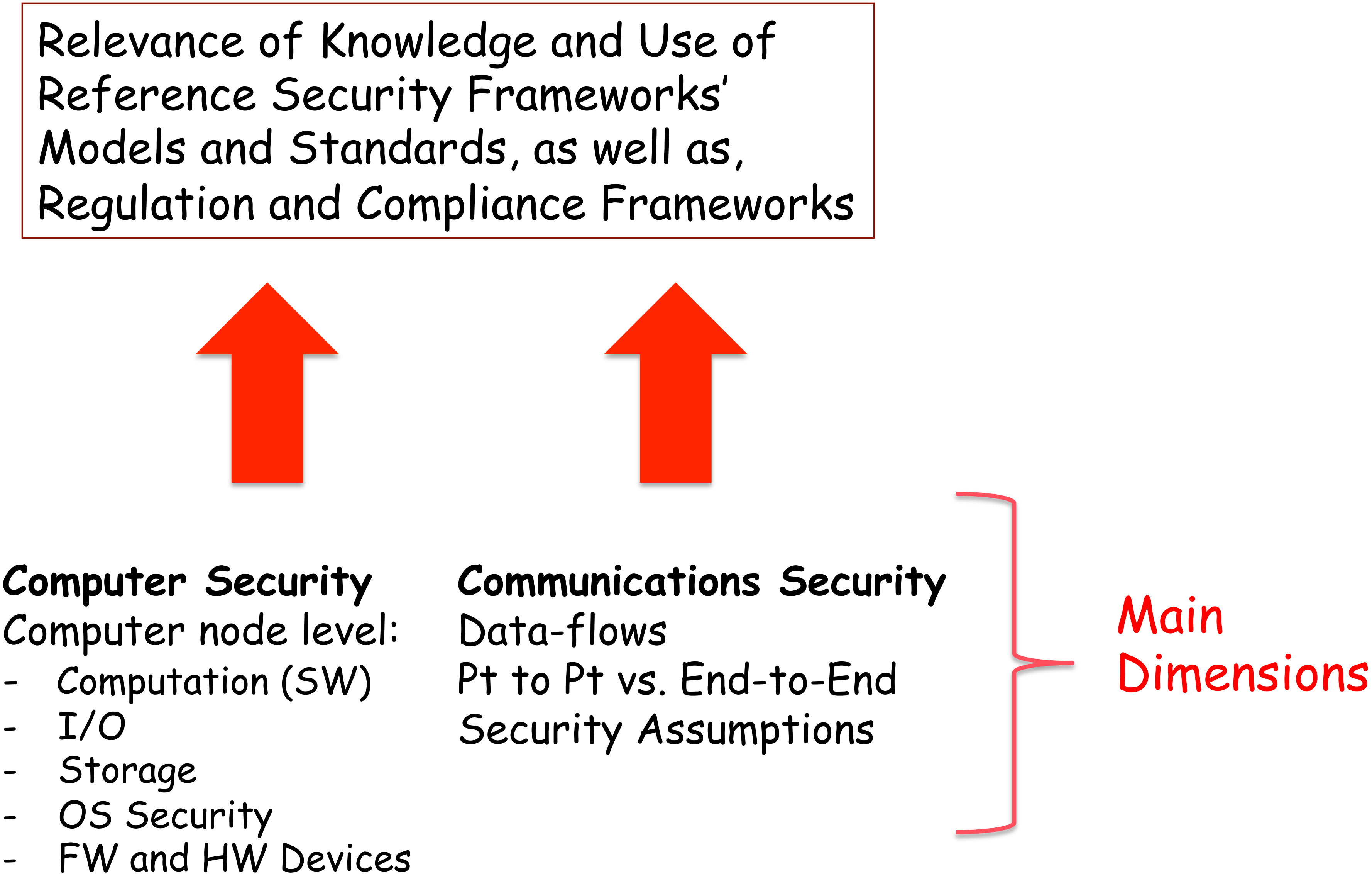
Resources as Protected Assets

Computer Security
Computer node level:

- Computation (SW)
- I/O
- Storage
- OS Security
- FW and HW Devices

Communications Security
Data-flows
Pt to Pt vs. End-to-End
Security Assumptions

Revising Computer Systems' Security Dimensions. How to address ?



Relevance of Knowledge and Use of Reference Security Frameworks' Models and Standards, as well as, Regulation and Compliance Frameworks

Computer Security

Computer node level:

- Computation (SW)
- I/O
- Storage
- OS Security
- FW and HW Devices

Communications Security

Data-flows

Pt to Pt vs. End-to-End

Security Assumptions

Main Dimensions

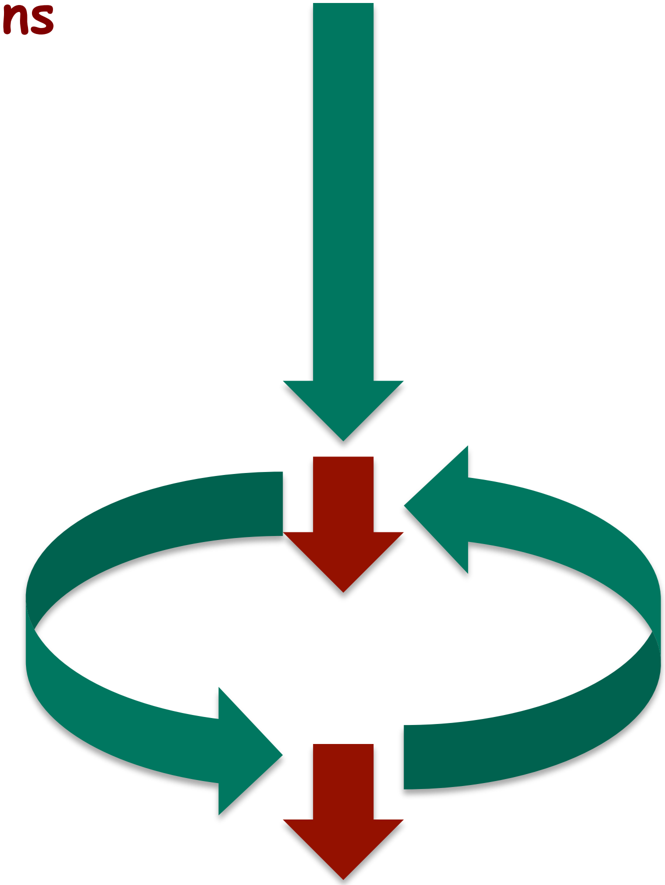
How to approach a security framework ?

Two approaches:

Design Time and Development Foundations

Operational Security

(Runtime, Security as a Process)



End of Operation Life Cycle

How to approach a security framework ?

Two approaches:

Design Time and Development (Security By Design)

- SW/FW/HW Design, Development Methods and Tools
  - White-Box Approach (ex., SW Security, Static Analysis
  - Minimization of TCBs and Trusted Execution Environments (ex., HW-Shielded foundations

Operational Security (Runtime, Security as a Process)

- Verification and maintenance of correct operation in the op. lifecycle
  - Detection/correction of errors and defects, hardening & patching,
- Security Auditing and Dynamic Analysis (runtime): Inspection Methods and Verification/Auditing Tools
- Mix of White-Box, Gray-Box, Black Box Approaches
- Ex. PEN Testing and Evaluation; "The defender" leaning and performing as an adversary"
- (Continuous) Identification of Potential Vulnerabilities and revision of Adversary Model Assumptions

Security Frameworks:

- Information security frameworks
- Standard Security Frameworks
- Regulation and Compliance Frameworks

Relevant frameworks

(Computer Systems and Networks Engineering)

- NISTIR / FIPS Pub 180
- IETF Standards / IETF RFC 4848
- OSI X.800

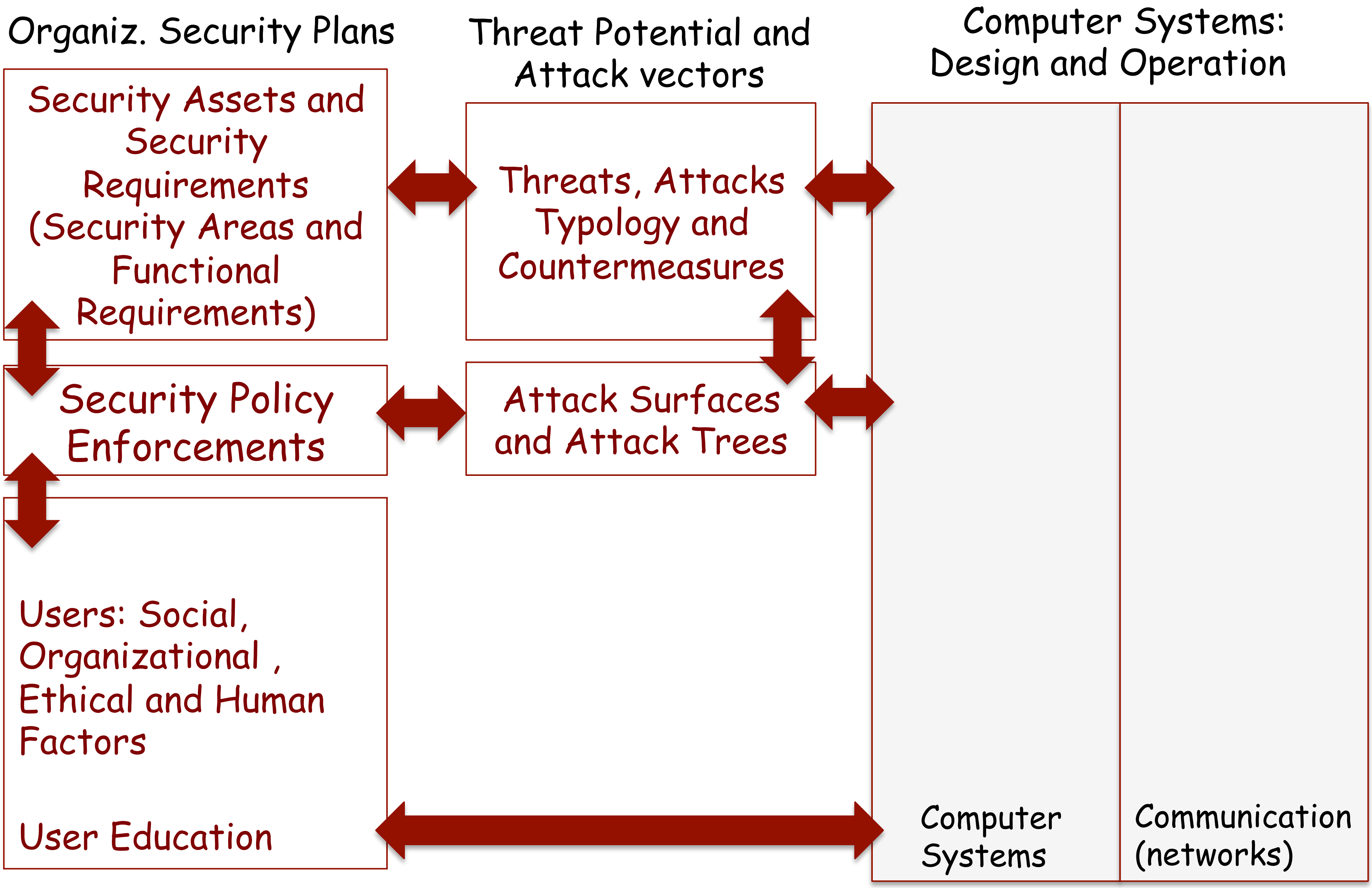
What is a Security Framework ?

- Information **security framework:**
  - **Series of documented processes, terminology, concepts, definitions, good-practices and related standards** (including security applications, services, protocols, mechanisms) that are **used to define policies and procedures around the implementation and operation of security controls**

- **Regulation and Compliance Frameworks**: Law, Regulation and Compliance, Ethical
  - Can be more generic or more specific (ex., vertical sectors)

- **Standard Security Frameworks:** related to Organizational or Technical Security Standards for:
  - **Organizational Security Policies and Requirements**
  - **Systems and SW Security Design**
  - **Operational Security and Systems' Security Management**

Generic Conceptual Security Framework



Organiz. Security Plans

Threat Potential and Attack vectors

Computer Systems: Design and Operation

Security Assets and Security Requirements (Security Areas and Functional Requirements)

Threats, Attacks Typology and Countermeasures

Security Policy Enforcements

Attack Surfaces and Attack Trees

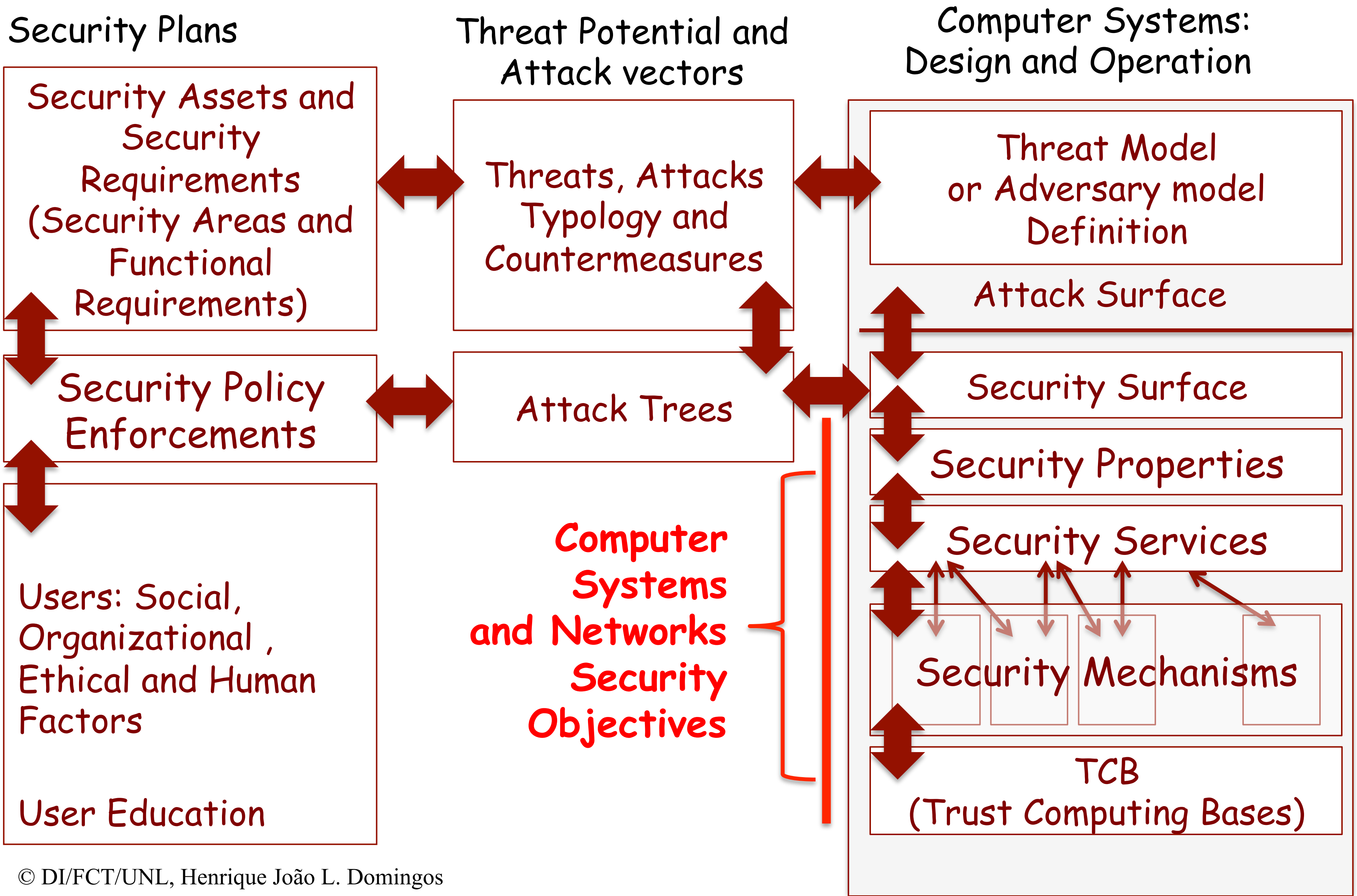
Users: Social, Organizational , Ethical and Human Factors

User Education

Computer Systems

Communication (networks)

Generic Conceptual Security Framework



Security Plans

Security Assets and Security Requirements (Security Areas and Functional Requirements)

Security Policy Enforcements

Users: Social, Organizational , Ethical and Human Factors

User Education

Threat Potential and Attack vectors

Threats, Attacks Typology and Countermeasures

Attack Trees

Computer Systems and Networks Security Objectives

Computer Systems: Design and Operation

Threat Model or Adversary model Definition

Attack Surface

Security Surface

Security Properties

Security Services

Security Mechanisms

TCB (Trust Computing Bases)

Generic Conceptual Security Framework

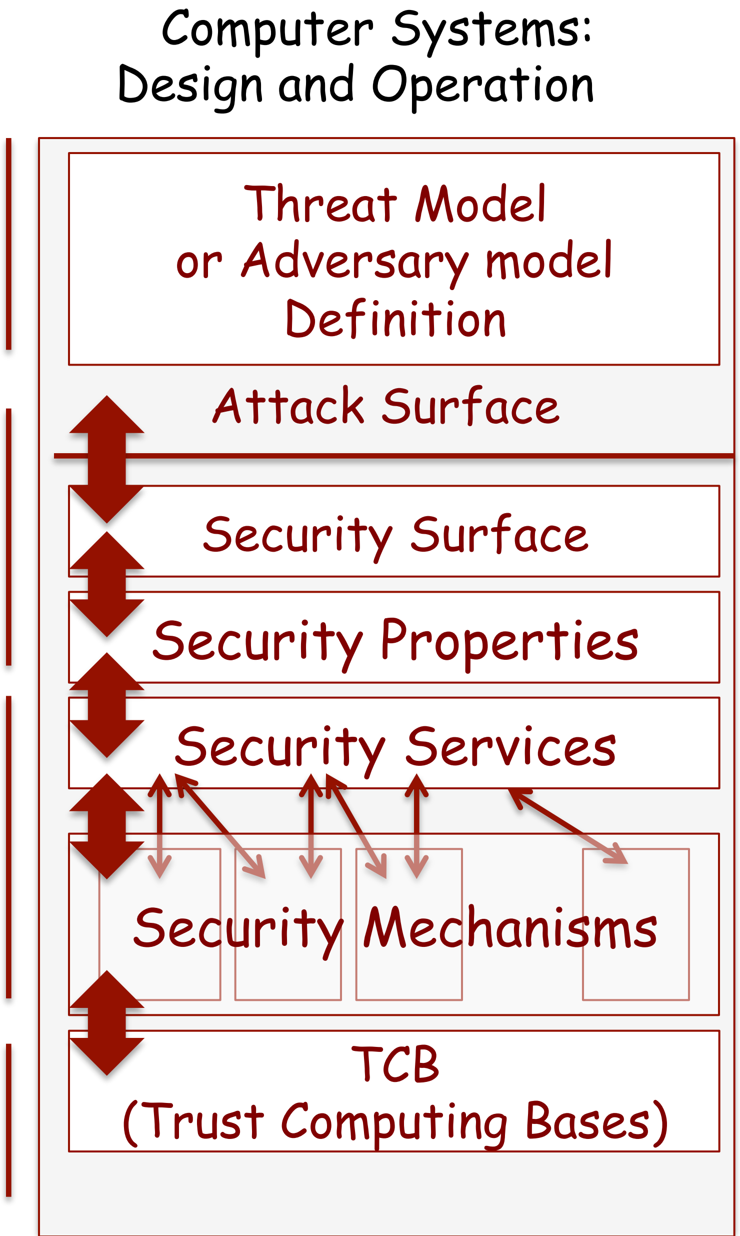
Need to define correctly
the Adversary Model

Need to Establish the Security Surface
(including perimeter defence) and
define the supported security properties

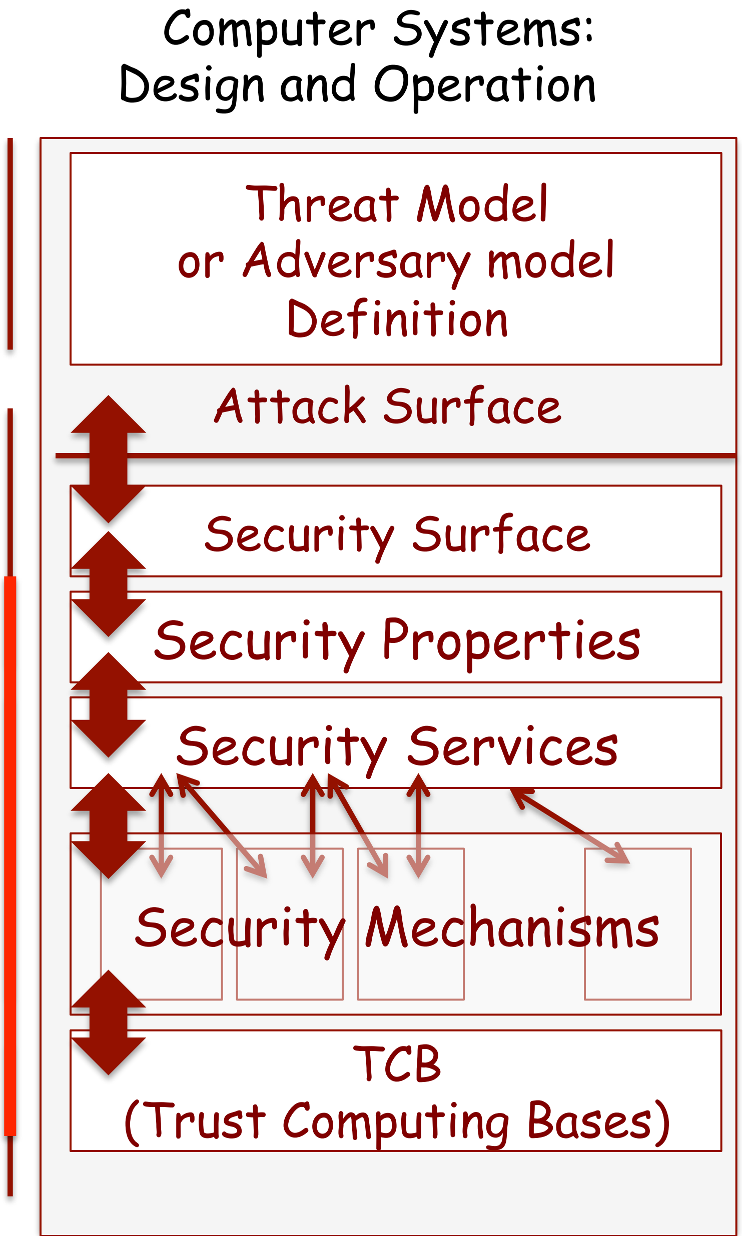
Need to Design, Build, Develop and Operate
The Security Services that must be based on
proper security mechanisms

- Security Foundations
- Specific vs. Pervasive Mechanisms
- Can include SW, FW and HW Devices
  (ex., Dedicated Security HW devices)

Need to identify and minimize the
Trust Computing Bas



Generic Conceptual Security Framework



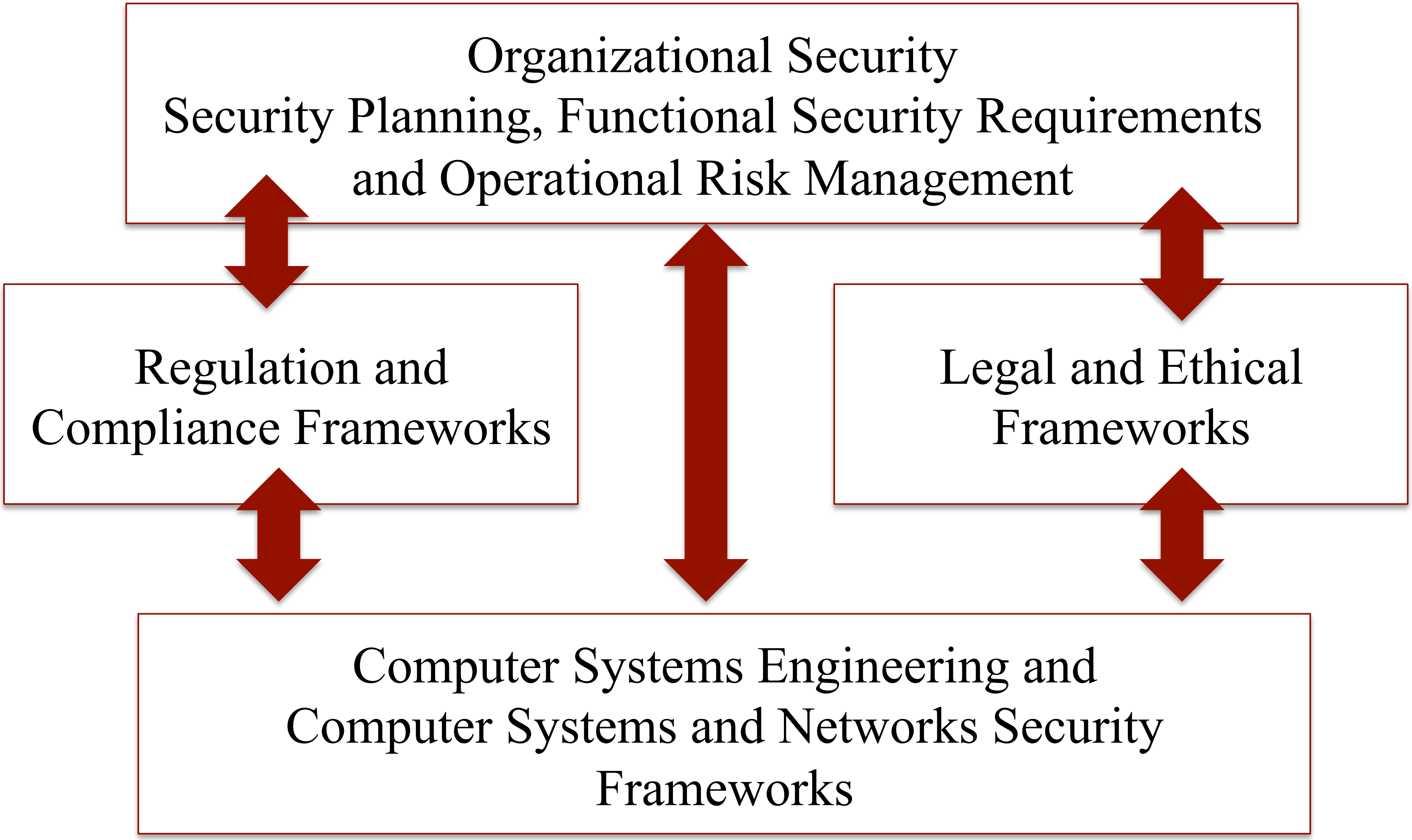
Design and Implementation Options
Following "FUNDAMENTAL SECURITY DESIGN PRINCIPLES

Readings (!!!) …See Bibliography

- Model Assumptions for Computer Security
- Assets, Threats, Attacks, Incidents
  - Typology; Relationships between those concepts and notions
- Attack Surfaces and Attack Trees
  - Examples, Categories and Representation Guidelines
- Relevance of the Adversary Model Definition
- Typical Attack Anatomies (and related tools)
- Fundamental Security Design Principles
- Computer Security Strategy Issues
- TCB or Trust Computing Model Assumptions
  - Identification, Delimitation, Minimization, and Isolation
- Remarks on Security Complexity Issues

[CS] W. Stallings, L. Brown, Computer Systems – Principles and Practice, 1 – Overview
[NSE] W. Stallings, Network Security Essentials, 1 – Introduction

Mappings Involved (Summary)



Organizational Security
Security Planning, Functional Security Requirements
and Operational Risk Management

Regulation and
Compliance Frameworks

Legal and Ethical
Frameworks

Computer Systems Engineering and
Computer Systems and Networks Security
Frameworks

Typology of Security Services and Mechanisms

Assets > Risk-Management > Organizational Security > Threats and Vulnerability Assessment

- **Organizational Security Plan**

Correct Mappings:

Information Systems Security Patterns

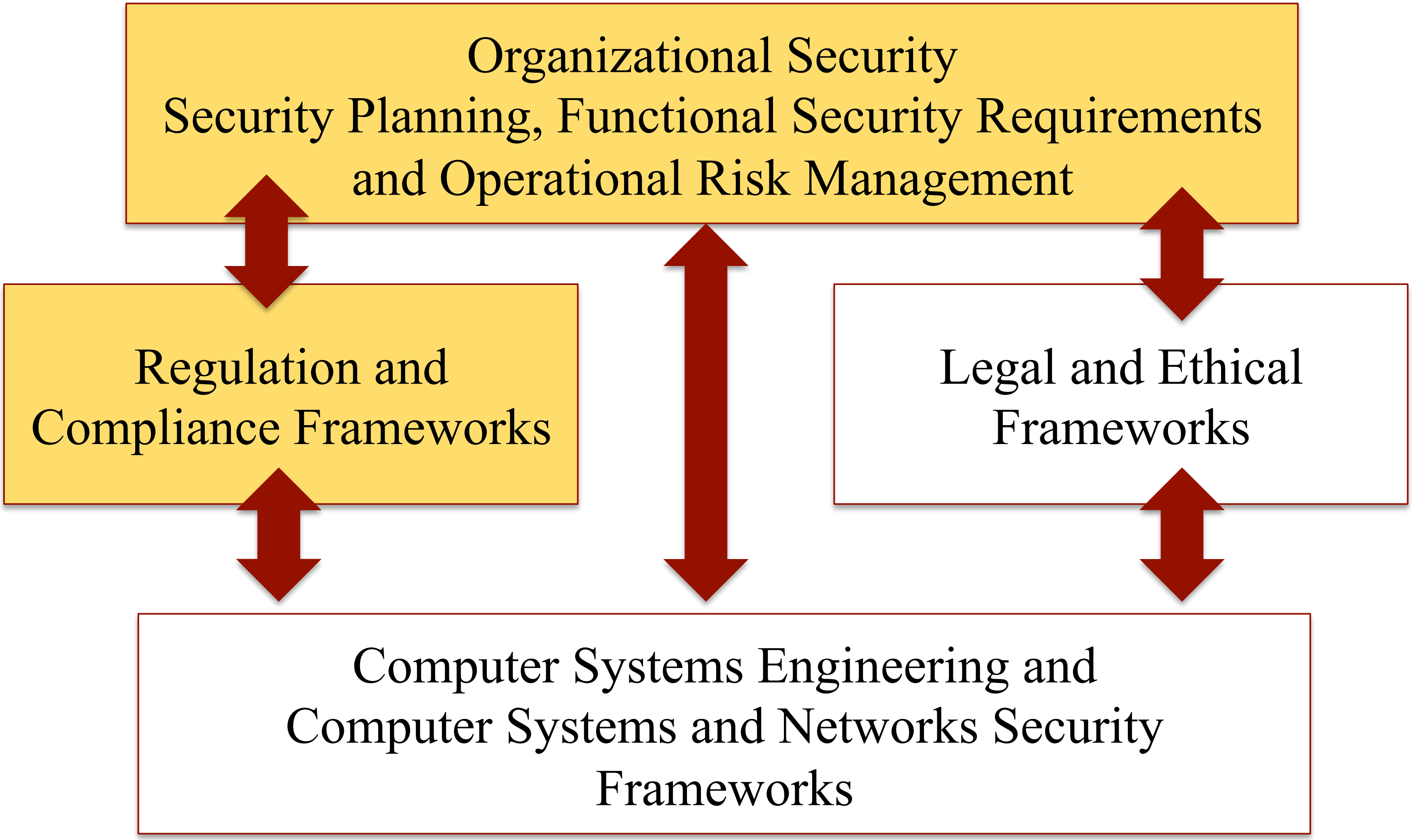
- **Threat Model**: Attacks typology, Security Properties and Required Security Services
- **Security Services require Security mechanisms** (different types):
  - Different typology of defenses
  - Technical vulnerability and risk factors
  - Perimeter vs. "in deep" defenses
  - Security policy enforcements of related security mechanisms
  - Point to Point vs End-to-End Security Arguments
  - Security services for computer Systems and communications (Networks, Data-Centers, SW Development and Operational Management Processes)

Organizational Security Challenges

- Risk-Management, Organizational Security, Threats and Vulnerability Assessment
- Organizational Security Plan

How to organize such mappings in different approach levels ?

Mappings Involved (Summary)



Organizational Security
Security Planning, Functional Security Requirements
and Operational Risk Management

Regulation and
Compliance Frameworks

Legal and Ethical
Frameworks

Computer Systems Engineering and
Computer Systems and Networks Security
Frameworks

Instruments (Regulation and Compliance)

- Risk-Management, Organizational Security, Threats and Vulnerability Assessment

- Organizational Security Plan

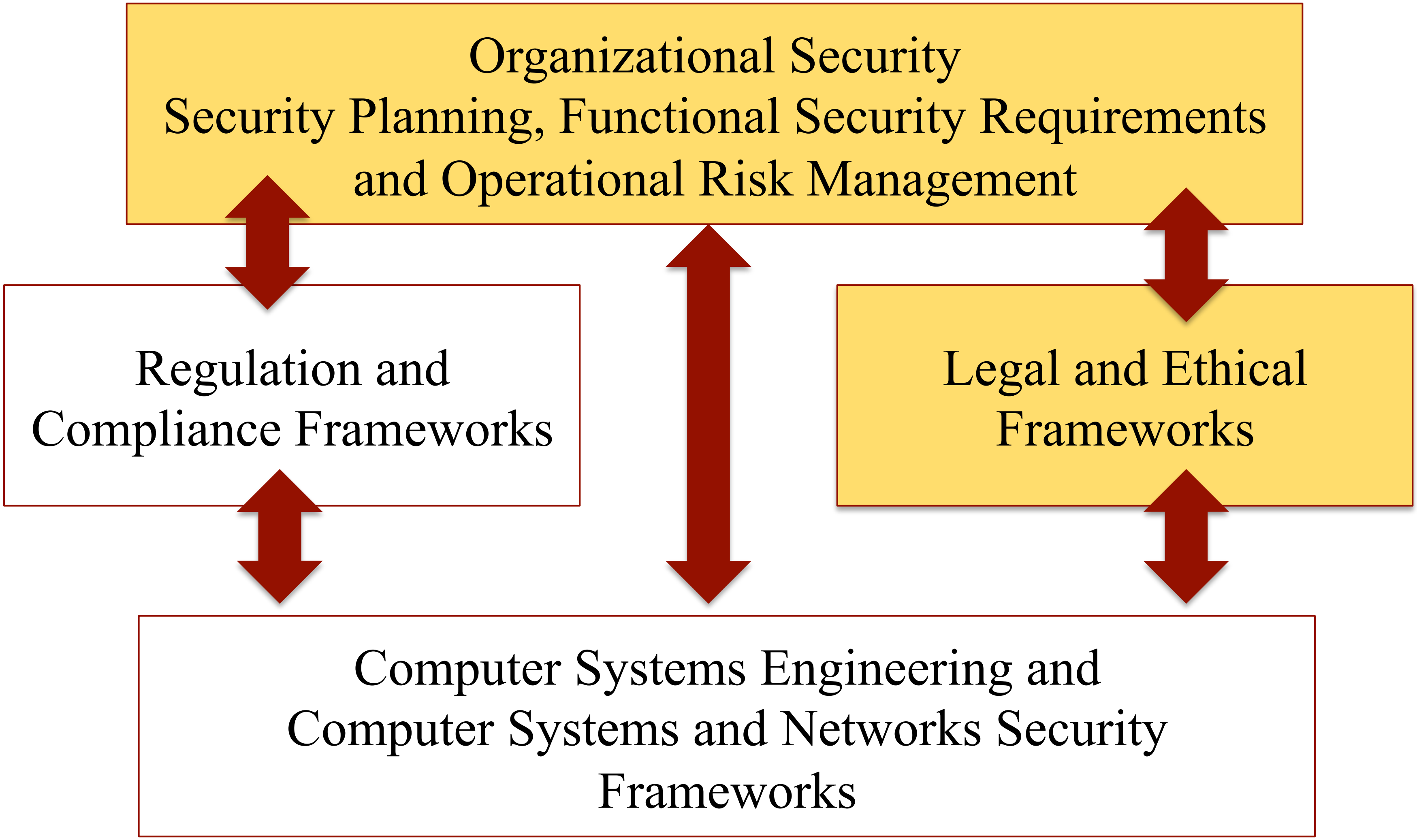
How to establish a correct mapping:

Implementation of regulations and related technical recommendations on generic and specific sectorial security frameworks, at governmental or institutional levels, in national, or international regulation levels

(Some) Examples:

GDPR	HIPAA (usa)	HIMSS.eu	NIST (Security and Privacy in Public Cloud Computing)	EU Banking and Finance
Data Privacy	Healthcare	Healthcare		

Mappings Involved (Summary)



Organizational Security
Security Planning, Functional Security Requirements
and Operational Risk Management

Regulation and
Compliance Frameworks

Legal and Ethical
Frameworks

Computer Systems Engineering and
Computer Systems and Networks Security
Frameworks

Instruments (Legal Instruments)

- Risk-Management, Organizational Security, Threats and Vulnerability Assessment
- Organizational Security Plan

How to establish a correct mapping:

Compliance with Legal Frameworks

Some **Examples** (Portuese Law Frameworks and Transpositions)

Proteção de Dados Pessoais	Criminalidade Informática	Regime Jurídico de Documentos Eletrónicos e Assinaturas Digitais		Defesa do Consumidor	Comunicações de Emergência e Segurança
Art 35º Constituição sobre utilização de Informática, UE L119/2016,	Lei 199/2009	DL 290-D/99, 62/2003 25/2004, 165/2004, 116-A/2006, 88/2009	DL 116-A/2006, 88/2009	DL 102/2017, 74/2017, 58/2016, Lei 14/2019	DL 14/2019, 2/2019, Lei 46/2018, …

Instruments (Regulation and Compliance)

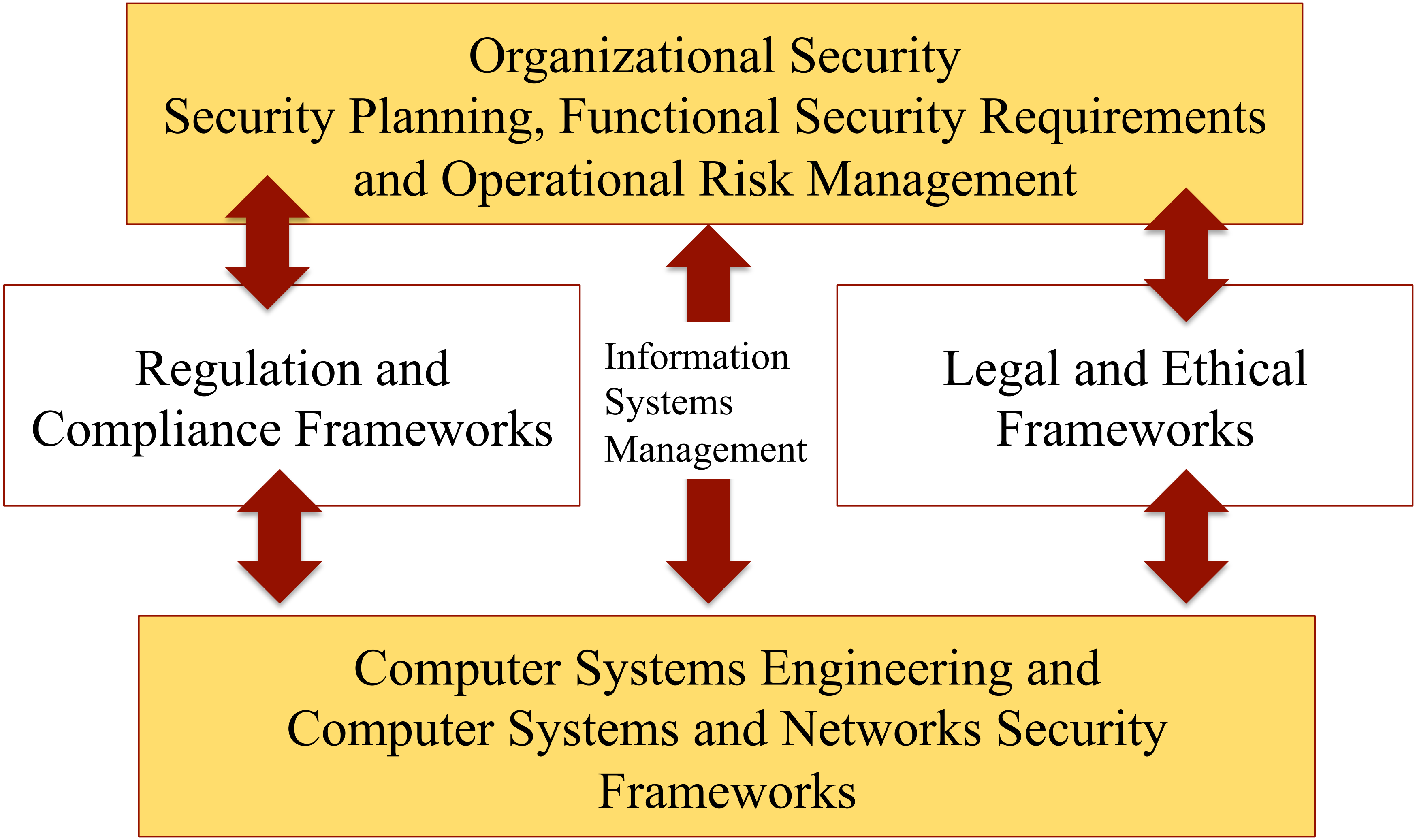
- Risk-Management, Organizational Security, Threats and Vulnerability Assessment
- Organizational Security Plan

How to establish a correct mapping:

Legal and Regulatory Frameworks (examples):

- https://www.cnpd.pt/bin/legis/leis_nacional.htm
- https://www.cnpd.pt/bin/legis/leis_internacional.htm
- https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en
- “PT GDPR Transposition – RGPD: Prop. LEI 120/XIII, CM 28/3/2018
- RGPD – Administração Pública: Resolução CM 41/2018
- https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=OJ:L:2016:119:FULL&from=EN
- https://protecao-dados.pt/o-regulamento/

Mappings Involved (Summary)



Organizational Security
Security Planning, Functional Security Requirements and Operational Risk Management

Regulation and Compliance Frameworks

Information Systems Management

Legal and Ethical Frameworks

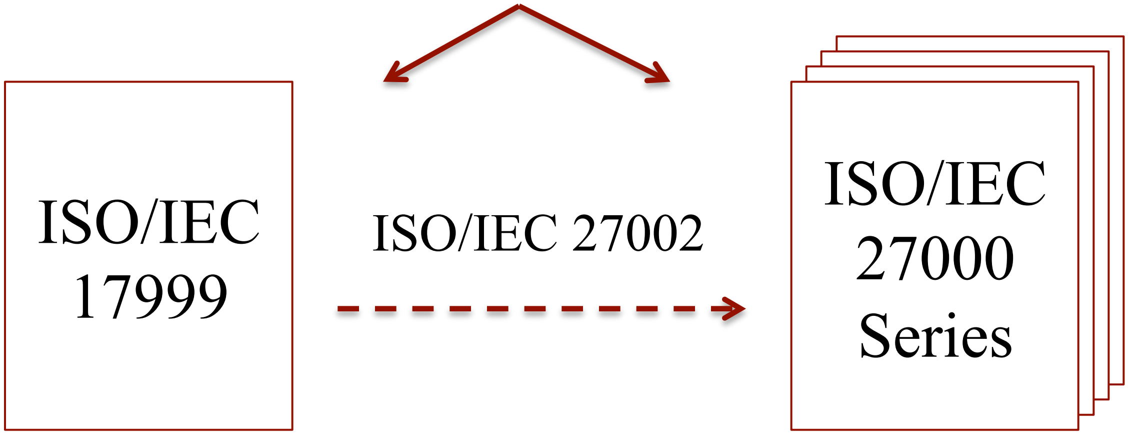
Computer Systems Engineering and Computer Systems and Networks Security Frameworks

Frameworks:
Organizational vs. information Systems Security Management

- Risk-Management, Organizational Security, Threats and Vulnerability Assessment
- Organizational Security Plan

How to establish a correct mapping:

Definition and Implementation of Security Principles, Good Practices, Recommendations inspired by Standardized Frameworks for ISMS (Information Security Management Systems)



ISO/IEC 27001

ISO/IEC 27002

ISO/IEC 27050

ISO/IEC 27799

☹ ~50 Pub. Standards

https://www.iso.org/standard/39612.html

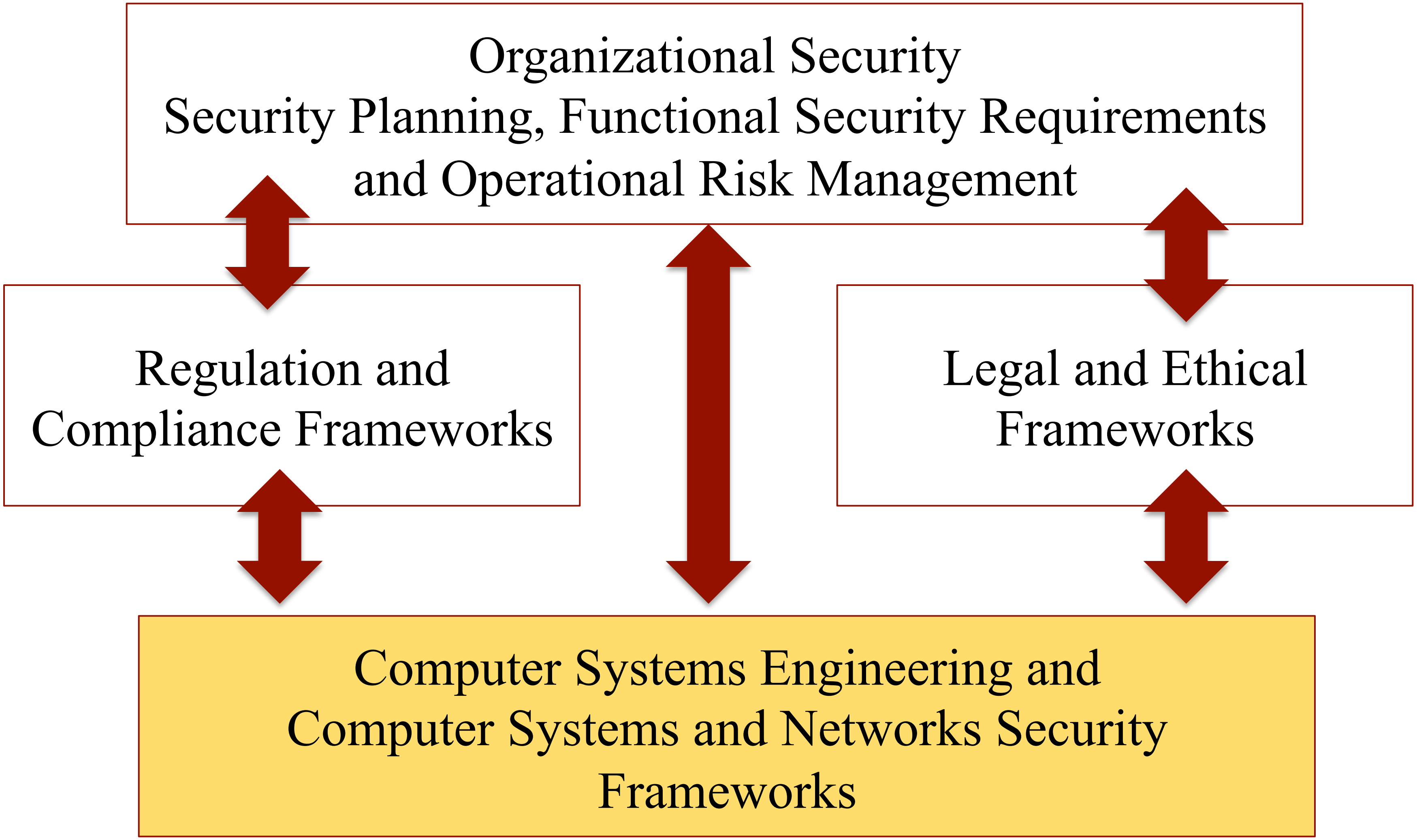
Principles in ISO/IEC 17001 and 27000 Patterns

- Criteria for **Information Security Management Systems**
  - Business continuity planning
  - Systems access control
  - Systems development and maintenance processes
  - Physical and environmental security criteria
  - Govern, Regulation and Compliance (GRC) criteria
  - Personnel security management
  - Organizational information security criteria
  - Computer systems and network management criteria and technical guarantees)
  - Asset classification and control
  - Organization Security Strategy

ISO/IEC 27000 Series/Family & ISO/IEC 17999 (Code of Practice)

- https://www.iso.org/isoiec-27001-information-security.html
- https://www.iso.org/standard/39612.html

Mappings Involved (Summary)



Organizational Security
Security Planning, Functional Security Requirements
and Operational Risk Management

Regulation and
Compliance Frameworks

Legal and Ethical
Frameworks

Computer Systems Engineering and
Computer Systems and Networks Security
Frameworks

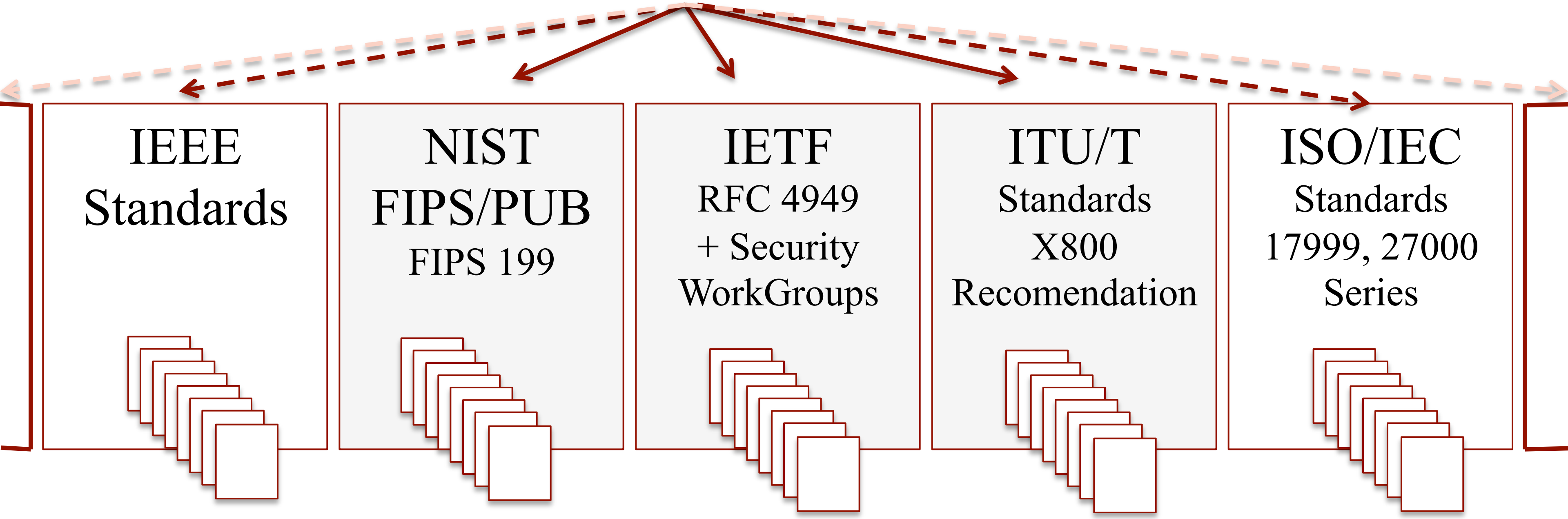
Frameworks (Technology and Engineering)

Regulation & Compliance
Law and Ethics

Organizational Security
Information Systems Security
Management

Engineering mappings:

Technical Security Standard Frameworks
(Relevance as Engineering Frameworks)



IEEE
Standards

NIST
FIPS/PUB
FIPS 199

IETF
RFC 4949
+ Security
WorkGroups

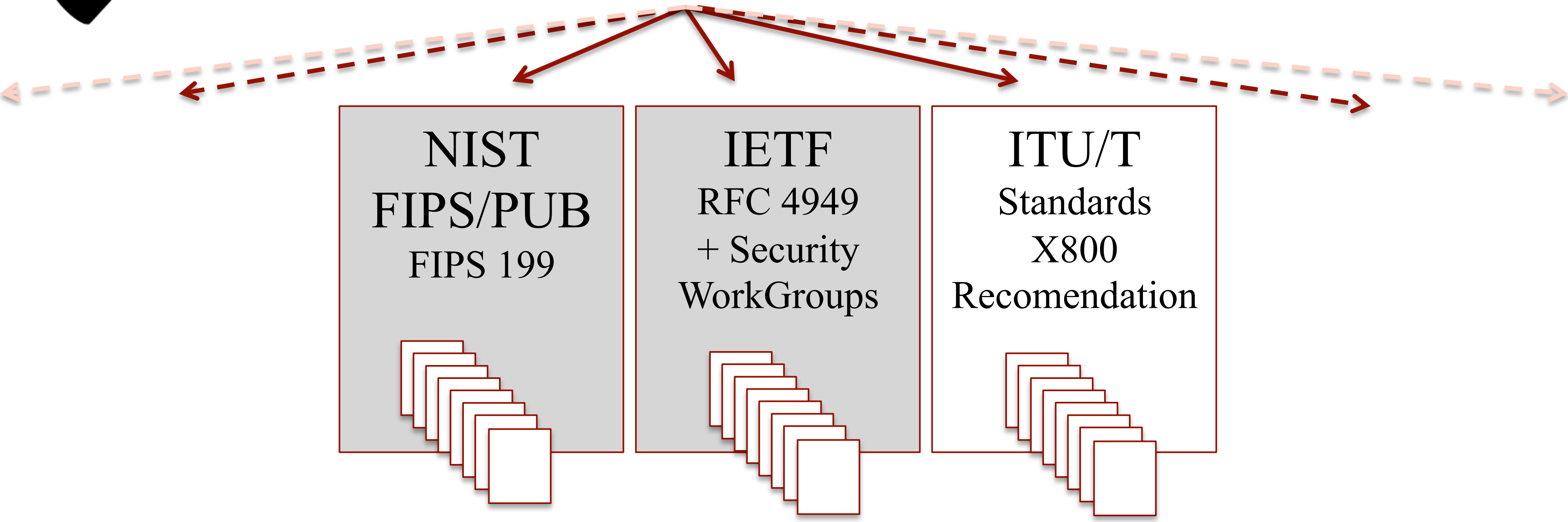
ITU/T
Standards
X800
Recomendation

ISO/IEC
Standards
17999, 27000
Series

Computer Security Objectives

Systems Engineering Focus

Technical Security Standardization Frameworks



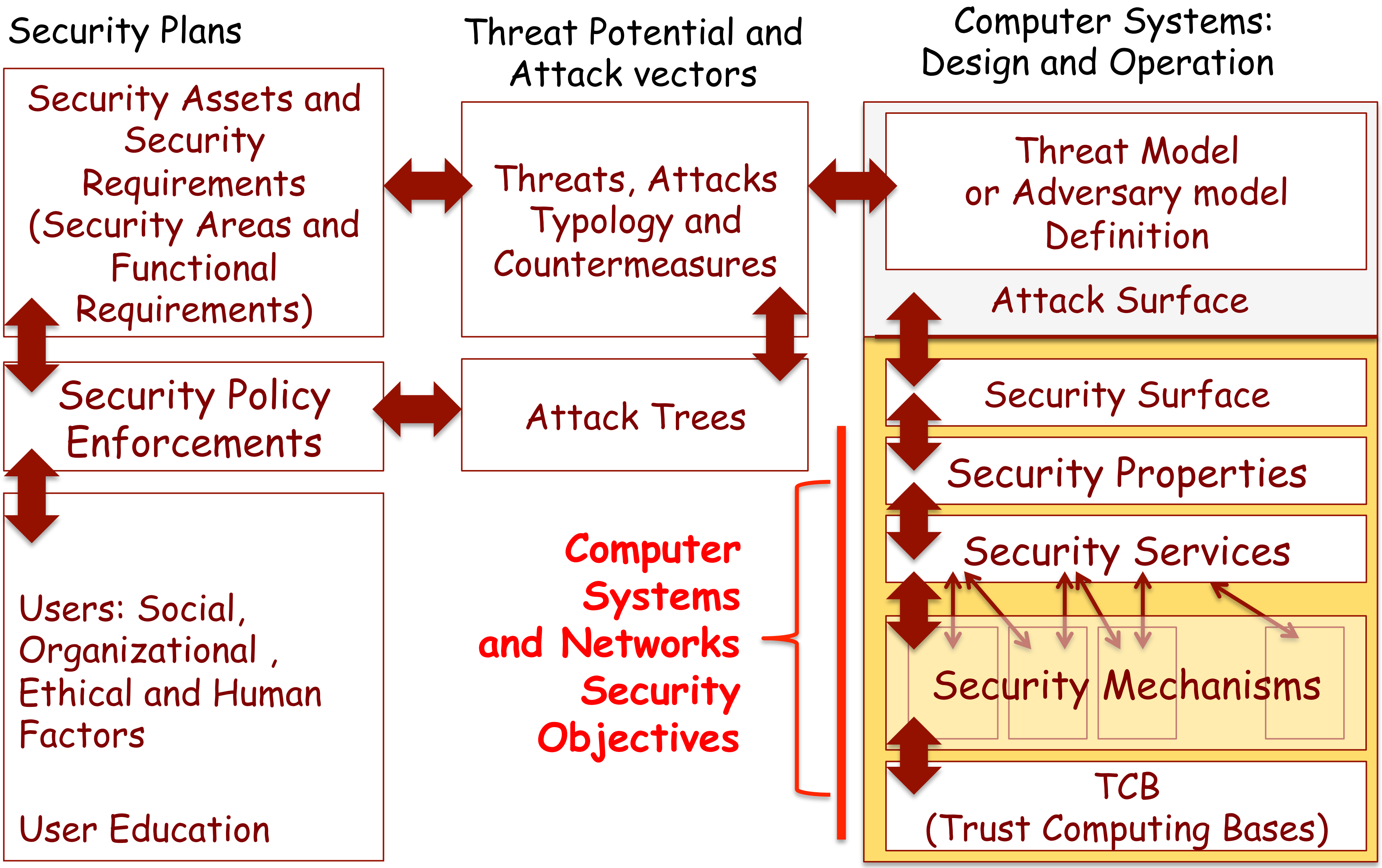
NIST
FIPS/PUB
FIPS 199

IETF
RFC 4949
+ Security
WorkGroups

ITU/T
Standards
X800
Recomendation

CIA Triad (NIST - NISTIR) FIPS Pub 199 Series

Remembering our conceptual framework



Security Plans

Security Assets and Security Requirements (Security Areas and Functional Requirements)

Security Policy Enforcements

Users: Social, Organizational , Ethical and Human Factors

User Education

Threat Potential and Attack vectors

Threats, Attacks Typology and Countermeasures

Attack Trees

Computer Systems and Networks Security Objectives

Computer Systems: Design and Operation

Threat Model or Adversary model Definition

Attack Surface

Security Surface

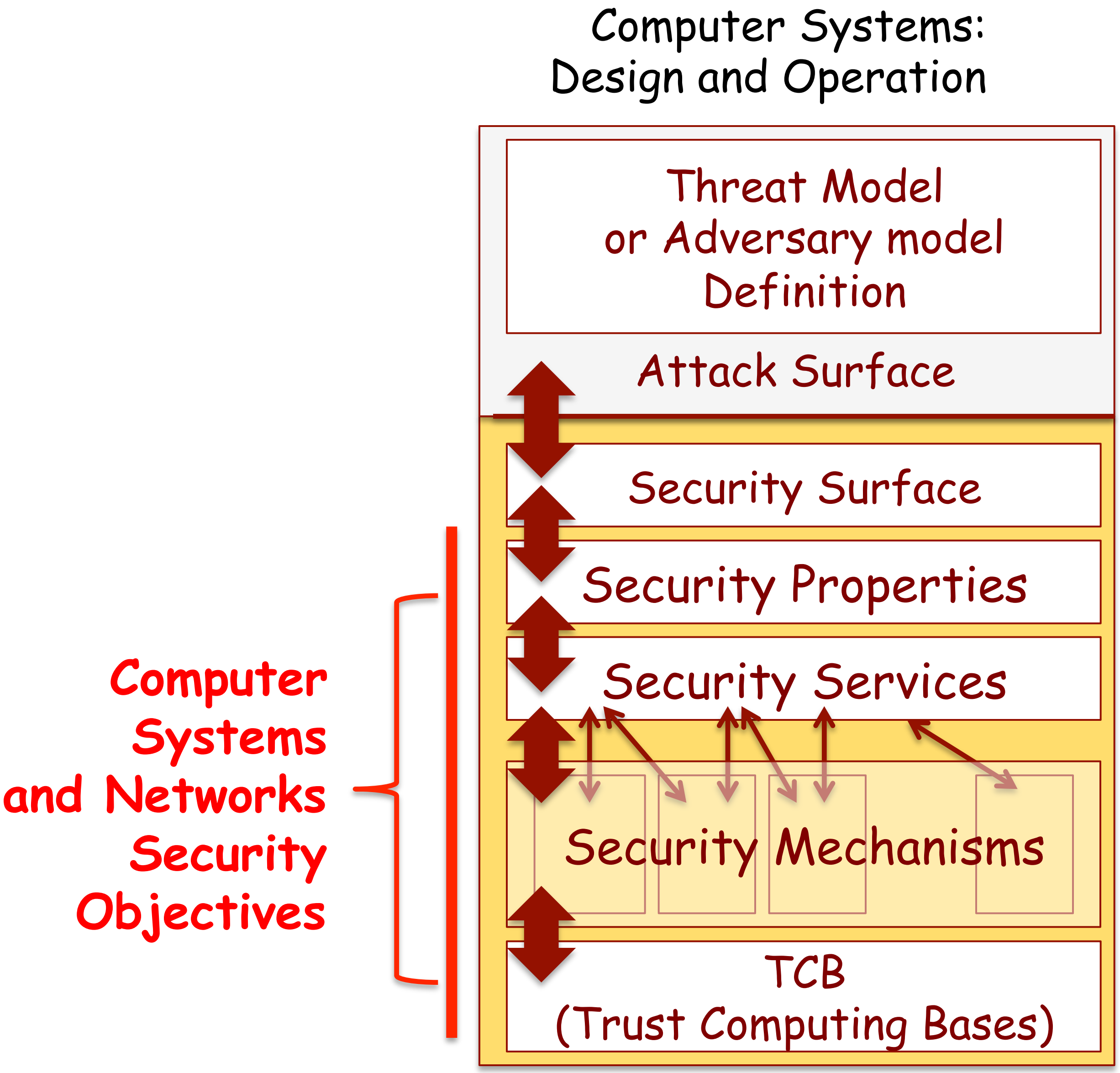
Security Properties

Security Services

Security Mechanisms

TCB (Trust Computing Bases)

Remembering our conceptual framework



CIA Triad, NIST, NISTIR 7298

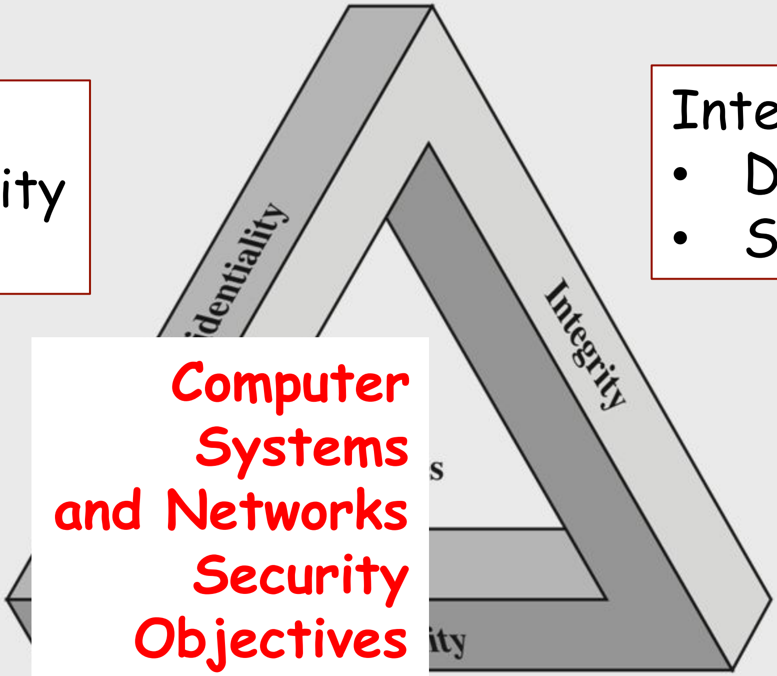
- Glossary of Key Information Security Terms, May 2013

Security Objectives

CIA Triad

Confidentiality:
- Data Confidentiality
- Privacy Control

Integrity
- Data Integrity
- Systems Integrity



Computer Systems and Networks Security Objectives

Availability: Correct Operation for Authorized Users

Security Objectives (FIPS PUB 199)

Standards for Security Categorization of Federal Information and Information Systems, Feb 2004

- **Confidentiality:**
  - Preservation of Authorization Restrictions on Information Access and Disclosure, including means for privacy and propriety protection
    - Avoidance of unauthorized disclosure of info and data
- **Integrity**
  - Prevention against improper info modification or destruction, including ensuring info non-repudiation and authenticity
    - avoids: loss of unauthorized modification or info destruction
- **Availability**
  - Ensures timely and reliable access to and use of info
    - avoids: disruption of access to or use of info or info systems

Complementary Objectives

Authenticity

- Property of being genuine, able to be verified and trusted
  - Principals, Message Origin, Messages, Info Sources, Data
  - Principals are who they say they are
  - Authenticity of digital identities and designations

Access Control

- Authorization control to available resources and assets

Accountability

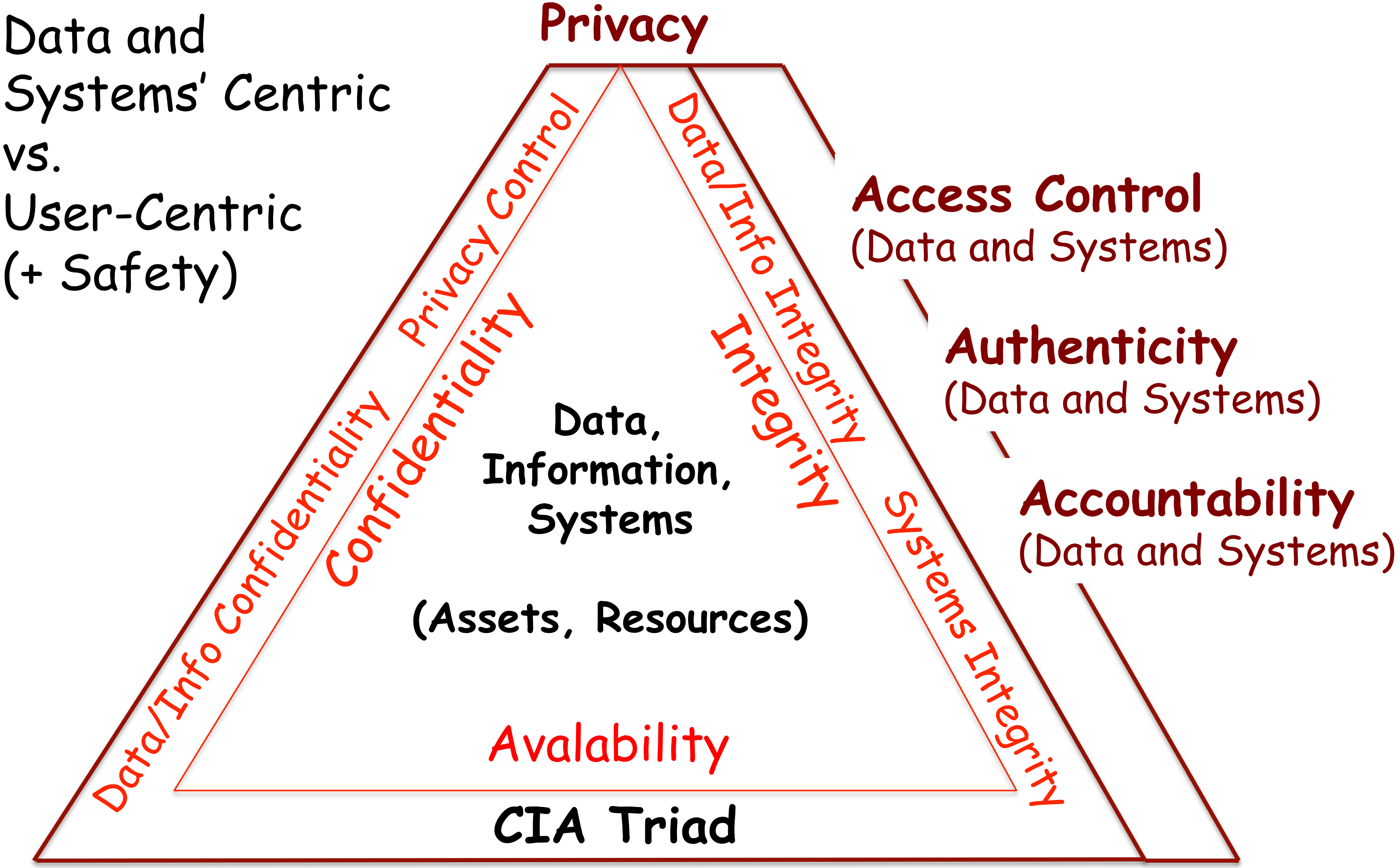
- Ensures Traceability (logging/auditing), non-repudiation, deterrence, fault isolation, intrusion detection and prevention, after-action recovery, including forensics analysis and legal action

Privacy

- Focused enforcement on access control, authorization conditions, permission and consent from owners, relatively to owned assets and resources

Computer Security Objectives

Data and
Systems' Centric
vs.
User-Centric
(+ Safety)



Readings (!!!) ...See Bibliography

- Model Assumptions for Computer Security
- Assets, Threats, Attacks, Incidents
  - Typology; Relationships between those concepts and notions
- Attack Surfaces and Attack Trees
  - Examples, Categories and Representation Guidelines
- Relevance of the Adversary Model Definition
- Typical Attack Anatomies (and related tools)
- Fundamental Security Design Principles
- Computer Security Strategy Issues
- TCB or Trust Computing Model Assumptions
  - Identification, Delimitation, Minimization, and Isolation
- Remarks on Security Complexity Issues

[CS] W. Stallings, L. Brown, Computer Systems – Principles and Practice, 1 – Overview

[NSE] W. Stallings, Network Security Essentials, 1 – Introduction

Concepts and Terminology: Assets, Threats, Attacks, Incidents

See [CS], Chap.1, section 1.1, 1.2, 1.3

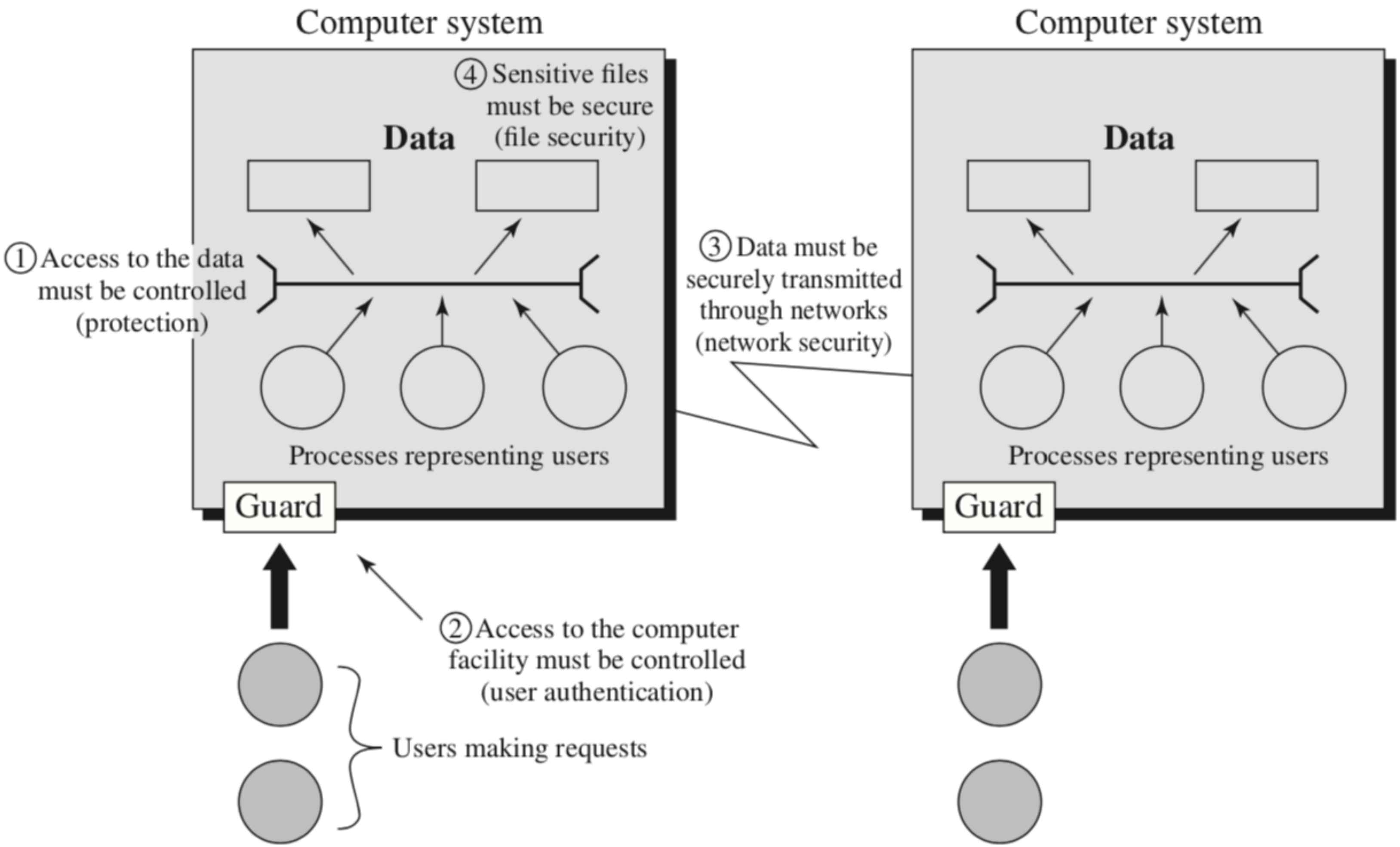
Model for Computer Security

Correct entities: Principals, Subjects, Correct Principals …
Notion of Adversary, Opponent, Attackers

Assets:

- HW
  - Computer Systems and Data Processing, Storage and Communication Devices
- SW
  - OS, System Utilities , Runtime Libraries, Applications
- Data
  - Information, Files, Databases, Key-Value-Stores
- Communication Facilities and Networks
  - LANs, WANs, Communication Links, Bridges, Routers, …

Scope of Computer Security


Computer system
④ Sensitive files must be secure (file security)
Data
① Access to the data must be controlled (protection)
Processes representing users
Guard
③ Data must be securely transmitted through networks (network security)
Computer system
Data
Processes representing users
Guard
② Access to the computer facility must be controlled (user authentication)
Users making requests

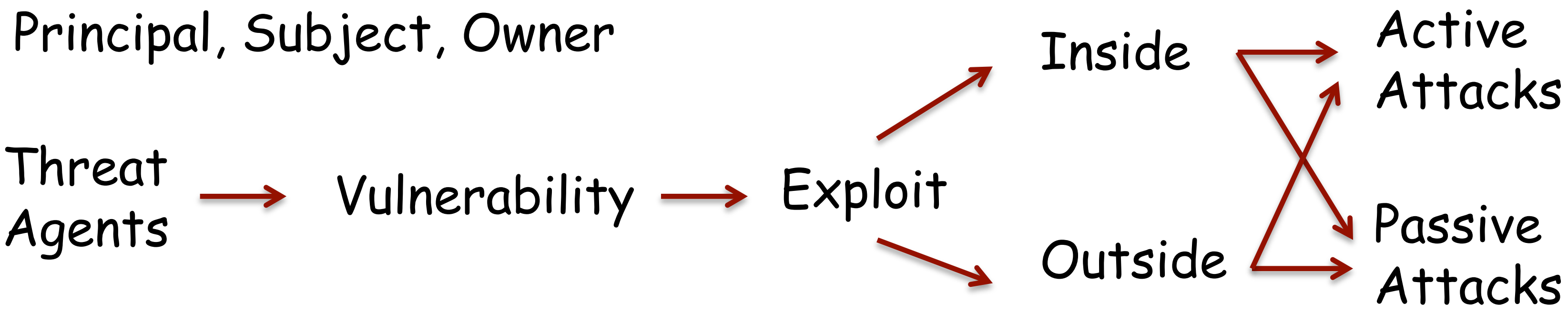
Threats, Attacks, Assets (IETF RFC 4949)

- Disclosure
  - Exposure
  - Interception
  - Inference
  - Intrusion
- Deception
  - Masquerade
  - Falsification
  - Repudiation
- Disruption
  - Incapacitation
  - Corruption
  - Obstruction
- Usurpation
  - Misappropriation
  - Misuse

Threats, Assets, Attacks, Incidents

- Adversary, Opponent, Attacker, Threat Agents
- Threats
- Attacks: Passive Attacks vs. Active Attacks
- Attacks as manifestations (actions) of threats
- Security Properties as Countermeasures
- Risk
- Security Policy
- System Resources / Assets
- Vulnerability
  - Corruption, Leaky, Unavailability
- Principal, Subject, Owner

Attack Origin
Attack Vectors



Inside

Active Attacks

Threat Agents

Vulnerability

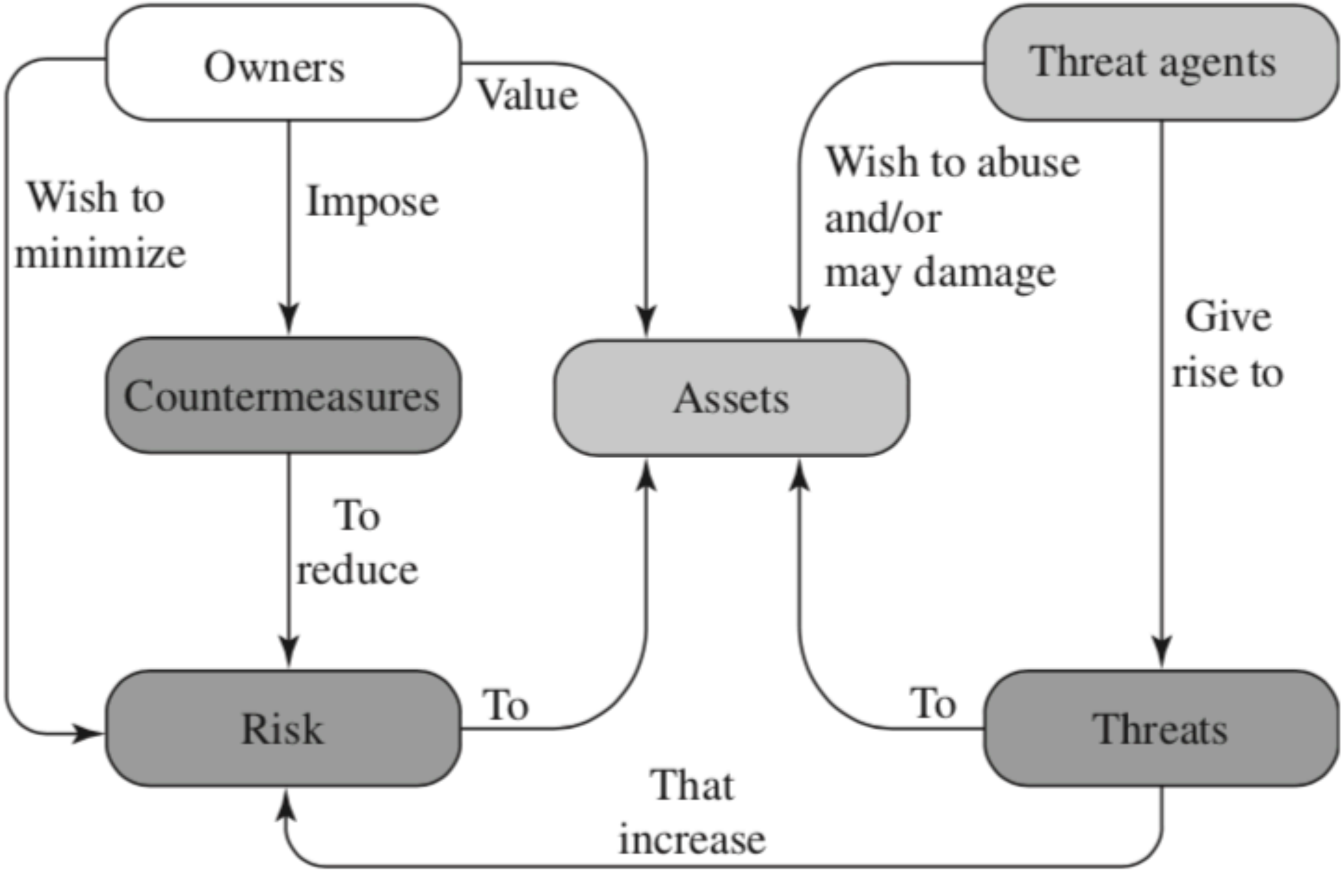
Exploit

Outside

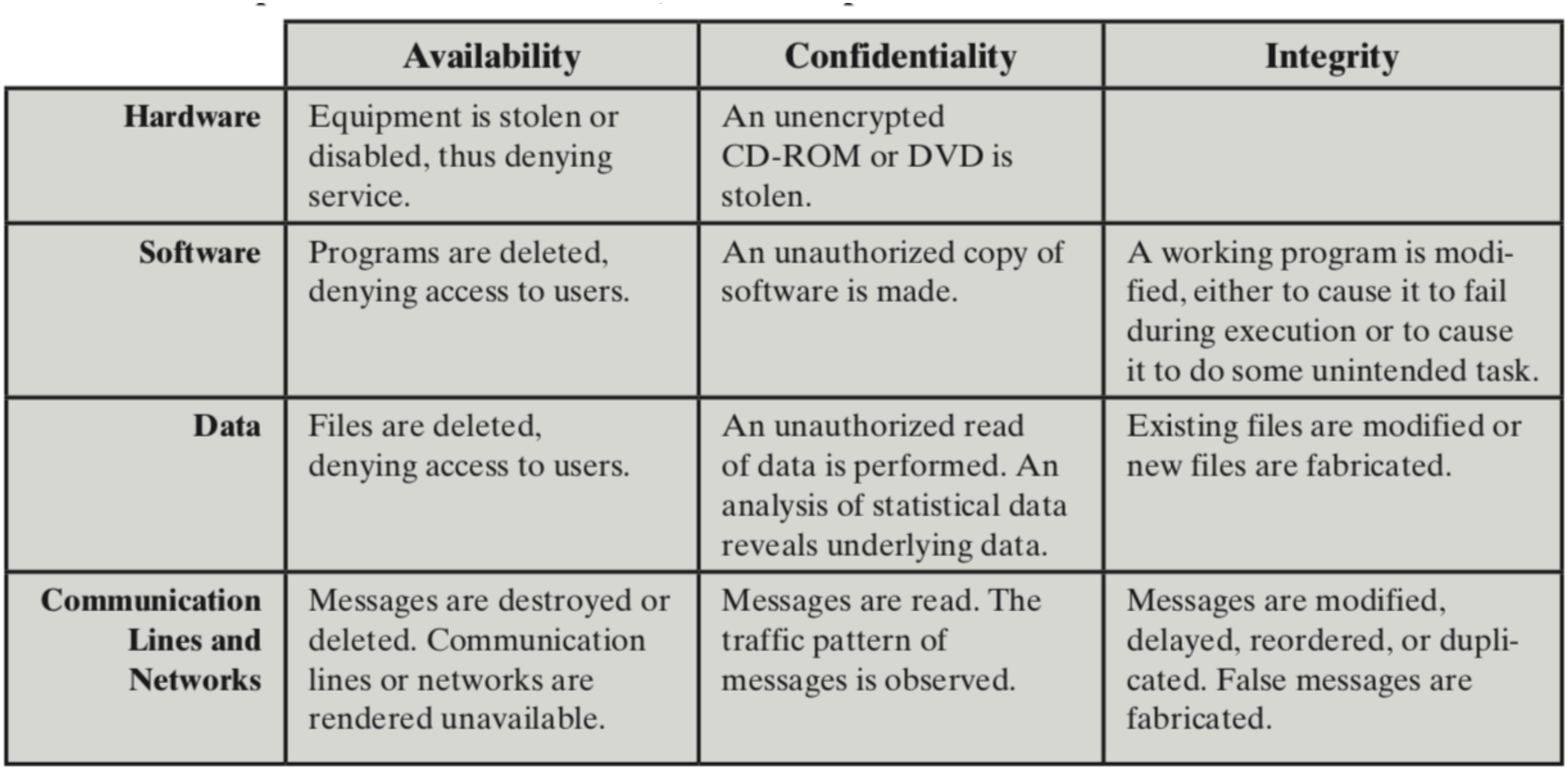
Passive Attacks

Terminology and Relationships

Ref. IETF RFC 4949, Internet Security Glossary



Computer Security: Assets vs. Threats



	Availability	Confidentiality	Integrity
Hardware	Equipment is stolen or disabled, thus denying service.	An unencrypted CD-ROM or DVD is stolen.	
Software	Programs are deleted, denying access to users.	An unauthorized copy of software is made.	A working program is modified, either to cause it to fail during execution or to cause it to do some unintended task.
Data	Files are deleted, denying access to users.	An unauthorized read of data is performed. An analysis of statistical data reveals underlying data.	Existing files are modified or new files are fabricated.
Communication Lines and Networks	Messages are destroyed or deleted. Communication lines or networks are rendered unavailable.	Messages are read. The traffic pattern of messages is observed.	Messages are modified, delayed, reordered, or duplicated. False messages are fabricated.

Fundamental Security Design Principles

See [CS], Chap.1, section 1.4

Security Design Principles

See [CS], Chap.1, section 1.4

- Economy of Mechanism
- Fail-Safe Defaults
- Complete Mediation
- Open Design (no security by obscurity)
- Separation of Privileges
- Least Privilege
- Least common security mechanism
- Psychological acceptability (usable security)
- Isolation
- Encapsulation
- Modularity
- Layering
- Least Astonishment

Attack Surfaces and Attack Trees

See [CS], Chap.1, section 1.5

Attack Surfaces and Attack Trees

- **Attack Surfaces**
  - defined as all the reachable and exploitable vulnerabilities in system exposed endpoints
  - Can be classified in taxonomies of risk levels, including guidance on setting priorities, testing, strengthening security measures, reconfigurations or new setups

- **Attack Trees**
  - Branching, hierarchical data structures (as a structural representation with related information) representing a set of potential techniques for exploiting security vulnerabilities (that can be used in attack surfaces)
    - Structured Information on Threats and Attack Patterns

Examples of Attack Surfaces

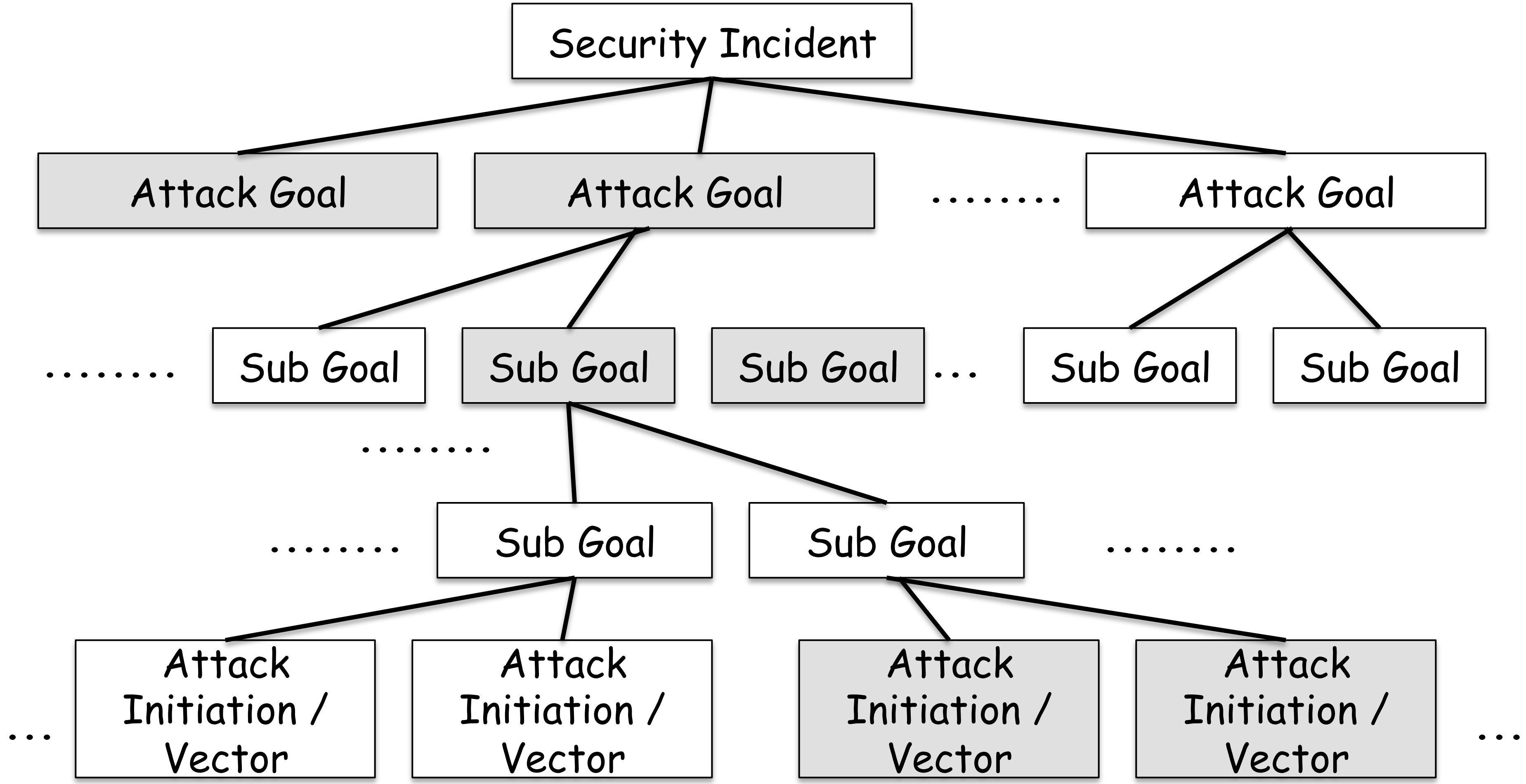
- Open Ports (TCP/IP Ports)
- Services (ex., supporting management functions or parameterizations) inside IPS, Firewalls, Intrusion Detection Systems
- Remote Procedure Call endpoints
- Code processing incoming data (ex., EMAIL messages, XML, REST/JSON messages, Documents, or specific Data and File Formats
- Interfaces or APIs, ex., SQL Interfaces, Web Forms, etc
- Human Factors, ex., vulnerabilities induced by Social Engineering Attacks, Social Network Scams, etc …

Categories of Attack Surfaces

Attack Surfaces can be categorized (and subcategorized) , ex:

- **Network Attack Surface**
  - LANs, WLANs, Internet
  - Exploitable Vulnerabilities in Network Protocols
- **Software Attack Surface**
  - Vulnerabilities in SW, Applications (ex., Web Applications and Services), Utilities
  - Operating System Code
- **Human Attack Surface**
  - Vulnerabilities created by users (errors/mistakes or malicious actions)
  - Also related to Social Engineering Attacks, Bad-Operation, Abuse of Authority or incorrect/malicious actions from trusted insiders or outsourcing personel

Representation of Attack Trees



See in [CS] the example for a possible Attacjk Tree for Internet Banking Authentication

Adversary Model Definition

“A defender must think as her/his adversary or opponent

Adversary Model Definition and Relevance …

The art of war teaches us to rely not on the likelihood of the enemy's not coming, but on our own readiness to receive him; not on the chance of his not attacking, but rather on the fact that we have made our position unassailable.

—*The Art of War*, Sun Tzu

Adversary Model is Critical Issue

> *A system without an adversary definition cannot possibly be insecure; it can only be astonishing…*

> *… astonishment is a much underrated security vice.*
> (Principle of Least Astonishment)

Virgil Gligor, MIT, On the Evolution of Adversary Models

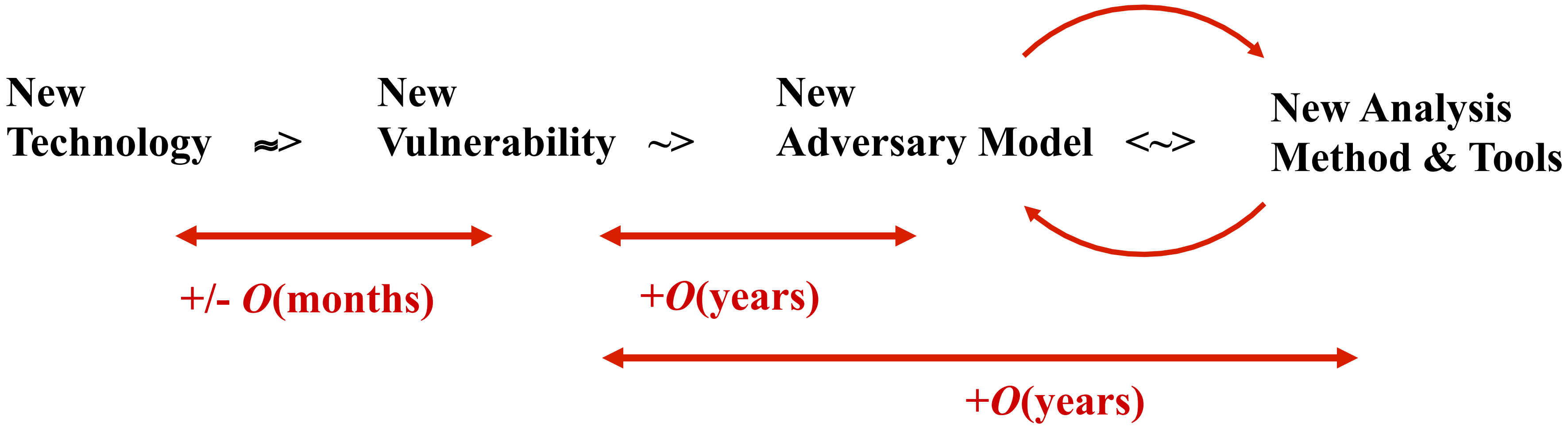
1. New Technologies often require a New Adversary Model Definition. What if you use old/mismatched ones ?
2. Continuous Vulnerability State: use old Adversary Models for New Technologies
3. **Challenge: Define (New Adversary Models and Security Protocols to Handle New Threats in a Timely Manner**
   Redefine the Adv. Model => New Security Design …
   Is it possible ? Realistic ?

Why an Adv. Def. is a fundamental concern ?

1. New Technology	≈> Vulnerability ~>	Adversary	<~> Methods & Tools
-sharing user-mode programs& data; - computing utility (early – mid 1960s)	confidentiality and integrity breaches; system penetration;	untrusted user-mode programs & subsystems	sys. vs. user mode ('62->) rings, sec. kernel ('65, '72) FHM ('75) theory/tool ('91)* access. policy models ('71)
- shared *stateful* Services, e.g, DBMS, net. protocols dyn. resource alloc. (early - mid 1970s)	DoS instances	untrusted user processes; concurrent, coord. attacks	DoS = a diff. prob.(83-'85)* formal spec. & verif. ('88)* DoS models ('92 ->)
- PCs, LANs; public-domain Crypto (mid 1970s)	read, modify, block, replay, forge messages	"man in the middle" active, adaptive network adversary	informal: NS, DS ('78–81) semi-formal: DY ('83) Byzantine ('82 –>) crypto attk models ('84->) auth. prot. analysis (87->)
- internetworking (mid – late 1980s)	large-scale effects: worms, viruses, DDoS (e.g., flooding)	geo. distributed, coordinated attacks	virus scans, tracebacks intrusion detection (mid '90s ->)

2. Technology Cost -> 0, Security Concerns persist

The "Continuous State of Vulnerability"



New Technology ≈> New Vulnerability ~> New Adversary Model <~> New Analysis Method & Tools

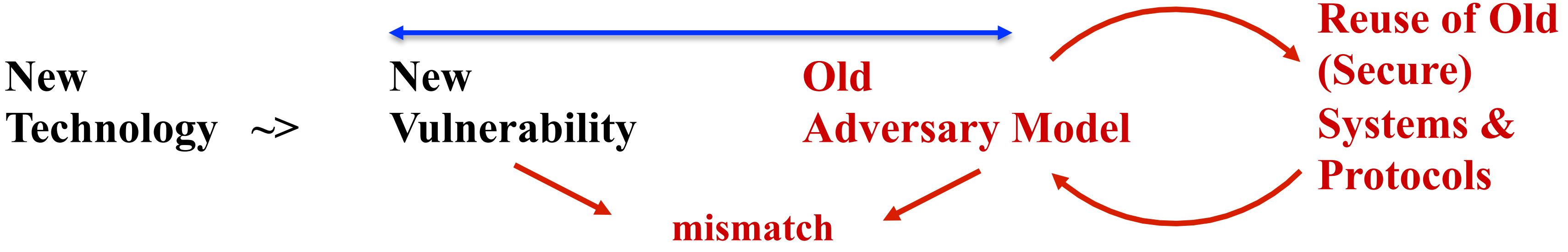
+/- *O*(months)

+*O*(years)

+*O*(years)

… a perennial challenge ("fighting old wars")

This is why you must also audit and patch ☹ !



New Technology ~> New Vulnerability

Old Adversary Model

Reuse of Old (Secure) Systems & Protocols

mismatch

Approaching the adversary model

- You must “know” about your possible attacker ! And you must learn to know the same she/he knows !!!
- Be paranoid !
  - You must recognize her/his potential advantages !
    - What advantages ?
  - You must know her/his tools, methods, …
  - You must antecipate and characterize her/his attack-typology
  - You must anticipate her/his potential targets
  - You must know and avoid your potential vulnerabilities (before her/him)
  - Remember that the user is a possible “adversary”
    - Your must know implications of incorrect use
  - …
  - Evaluation of computer systems security as “adversaries”
    - Know / Discover vulnerabilities as the adversary does

Typical Attack Anatomy
(… also valid for Pen-Testing Strategies)

Anatomy of attacks

1. Enumeration / Information Gathering

   Scanning, Enumeration Tools

2. Vulnerability Analysis

   Vulnerability Inspection Tools, Vulnerability Checkers

   Specific "In-Deep" SW Vulnerability Tools (ex., Web)

3. Exploit

   Network Attack Tools

   Vulnerability Exploiters (outside exploiting attacks)

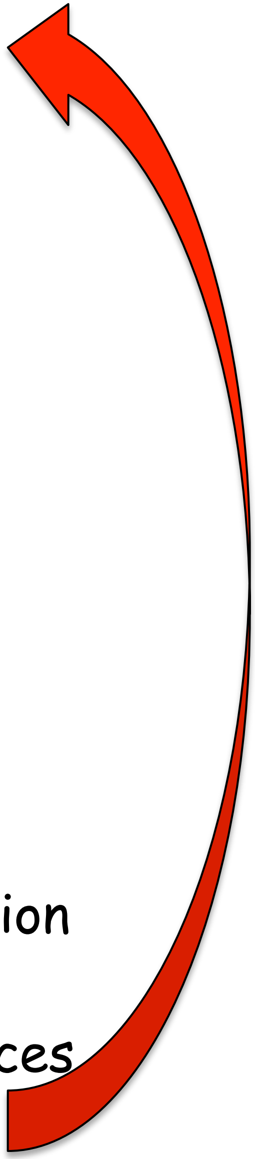
   Stress tools

4. Penetration / Intrusion

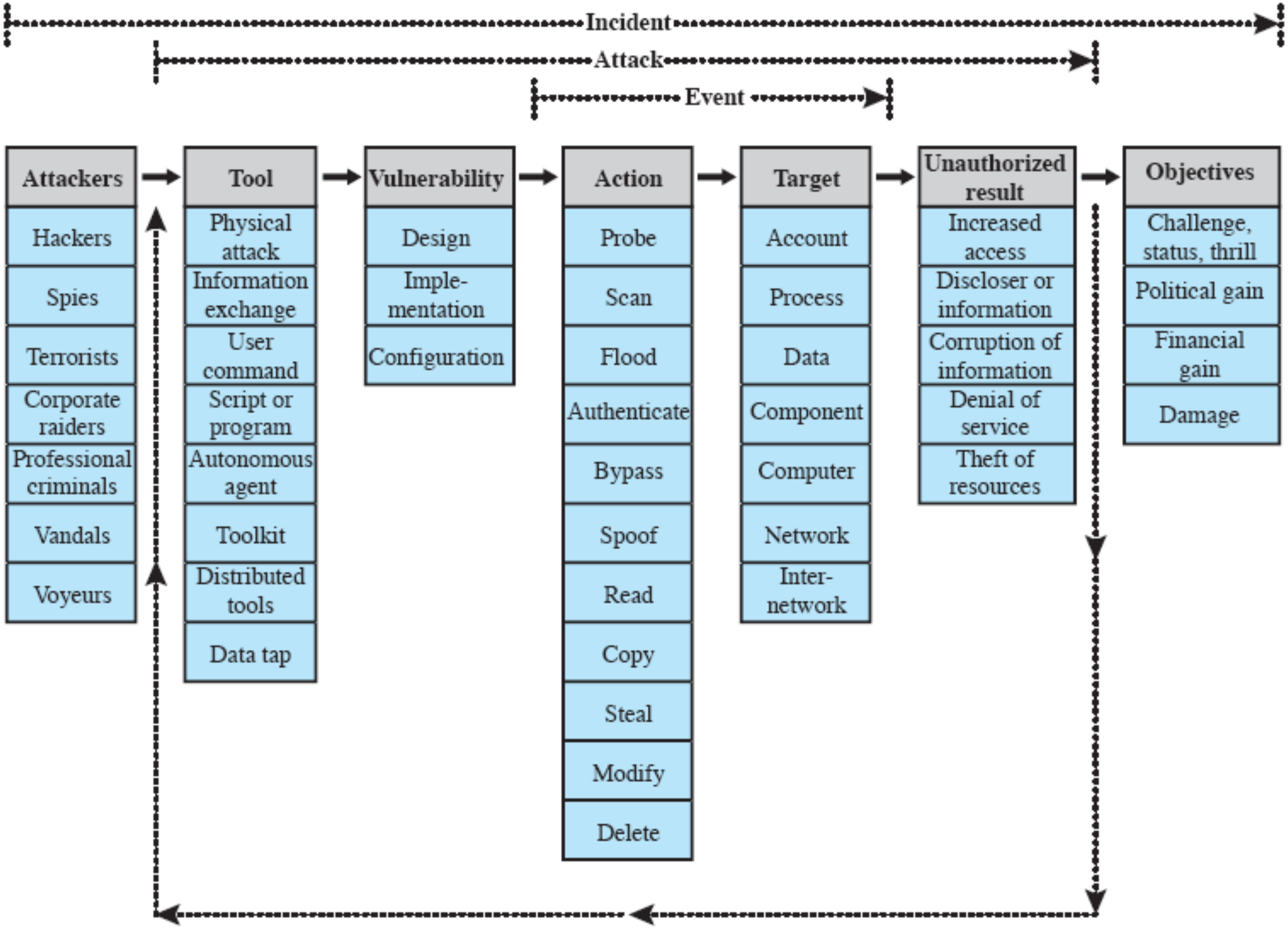
   Insider (In-deep) exploiting attack

   Exploit Tools, Pen-Testing/Exploit, Forensics Tools

5. Data leakage/corruption and/or Malicious Code Injection (Active vs. Passive Attacks)
6. Maintenance of intrusion/illicit control, Delete Evidences
7. Base for new launching attacks



Taxonomy



Attackers	Tool	Vulnerability	Action	Target	Unauthorized result	Objectives
Hackers	Physical attack	Design	Probe	Account	Increased access	Challenge, status, thrill
Spies	Information exchange	Implementation	Scan	Process	Discloser or information	Political gain
Terrorists	User command	Configuration	Flood	Data	Corruption of information	Financial gain
Corporate raiders	Script or program		Authenticate	Component	Denial of service	Damage
Professional criminals	Autonomous agent		Bypass	Computer	Theft of resources	
Vandals	Toolkit		Spoof	Network		
Voyeurs	Distributed tools		Read	Internetwork		
	Data tap		Copy			
			Steal			
			Modify			
			Delete			

Many well-known "guns"

- Wirshark, tcpdump, ethertool (*packet / frame sniffers*)
- Ettercap (Comprimising with ARP, DNS Spoofing…)
- Password Cracker http://www.openwall.com/john/, http://sectools.org/crackers.html
- Air Snort (Wlan key-recovering / hacking or test tool)
- Port Scanners (ex., http://sectools.org/port-scanners.html)
- Snort IDS, Tripwire (IDS / Auditing tools)
- Teardrop (www.rat.pp.se), jolt (www.jakubie.com), newtar (itrac.bourg.net) (ICMP DoS – ataques por inundação)
- SynFlooder (www.hackersclub.com), LAND (www.jakubie.com) (TCP SYN Flooding DoS)
- Arnudp100 (DoS em serviços de implementação vulnerável por masquerading do endereço IP origem)
- puke (www.jakubie.com), pong (www.ludat.tlh.se) (ICMP DoS com masquerading do IP origem e/ou unreachable IP addresses)
- Satan (www.fish.com/satan) ferramenta potente e integrada de auditoria e teste de vulerabilidades a sistemas
- Nessus (Vulnerability Scanner) : http://www.nessus.org/nessus/

Lots of Tools (Guns) for good and bad guys

- https://www.kali.org/
- https://tools.kali.org/tools-listing
- https://itsfoss.com/linux-hacking-penetration-testing/
- https://sectools.org/
- https://www.owasp.org/index.php/OWASP_Hacking_Lab
- https://www.owasp.org/index.php/OWASP_Testing_Guide_v4_Table_of_Contents
- https://www.owasp.org/index.php/Appendix_A:_Testing_Tools
- https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf
- … etc

Computer Security Strategy

See [CS], Chap.1, section 1.6

Components of the security strategy

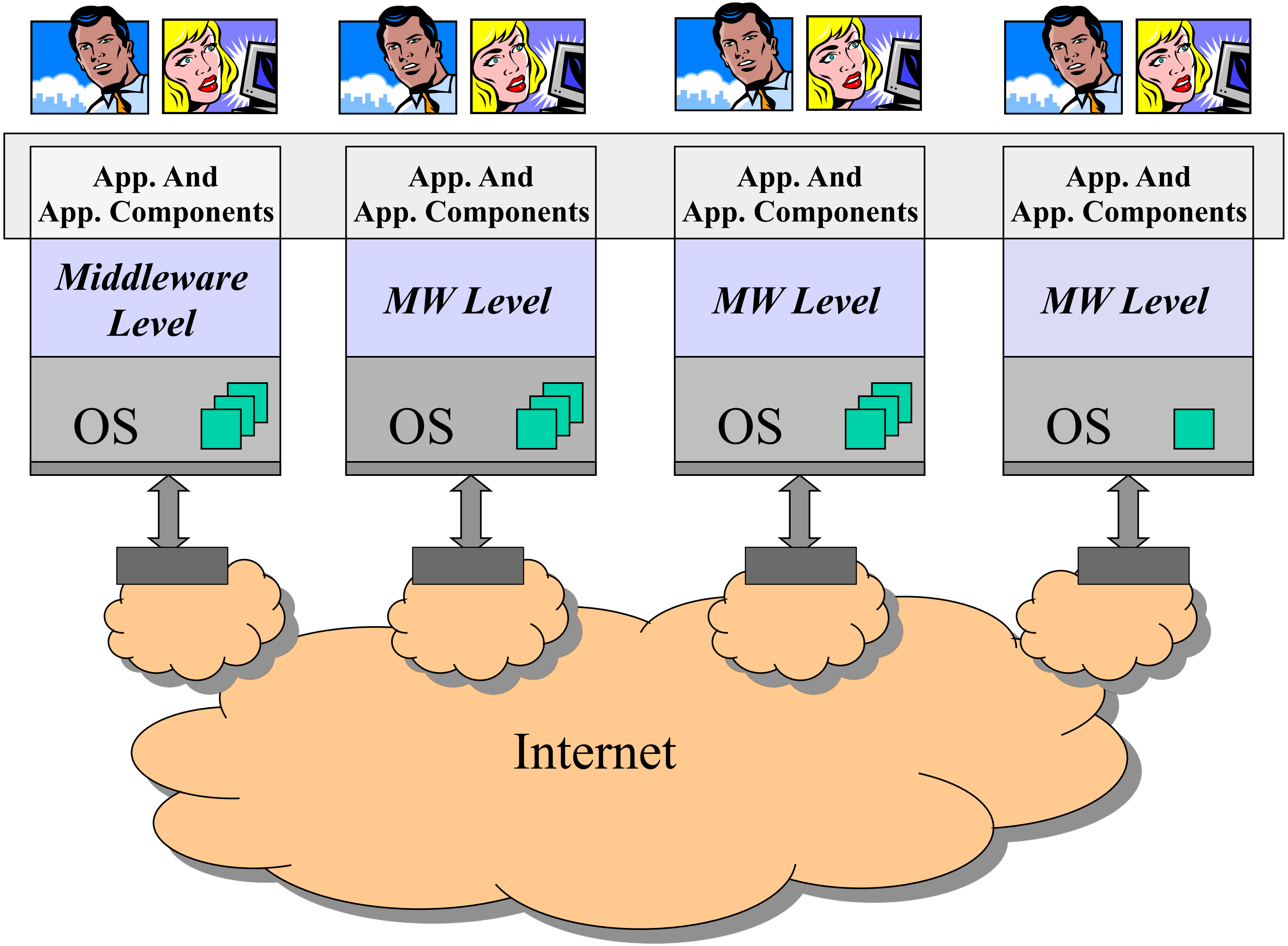
- Security specifications and policy or policy enforcements
- Implementation
  - Key-Fundamental security design principles
  - Implementation of services from mechanisms
    - Complementary courses of approach
      - Prevention
      - Detection
      - Response
      - Recovery
        - » Reactive Recovery
        - » Pro-active Recovery
        - » Fault/Intrusion Tolerance Guarantees
- Assurance and Evaluation
    - Foundations, Confidence, Auditing Criteria, Testing
    - Possible use of formal proofs, analytics or mathematical proofs

TCB - Trust Computing Base

Trust Computing Base

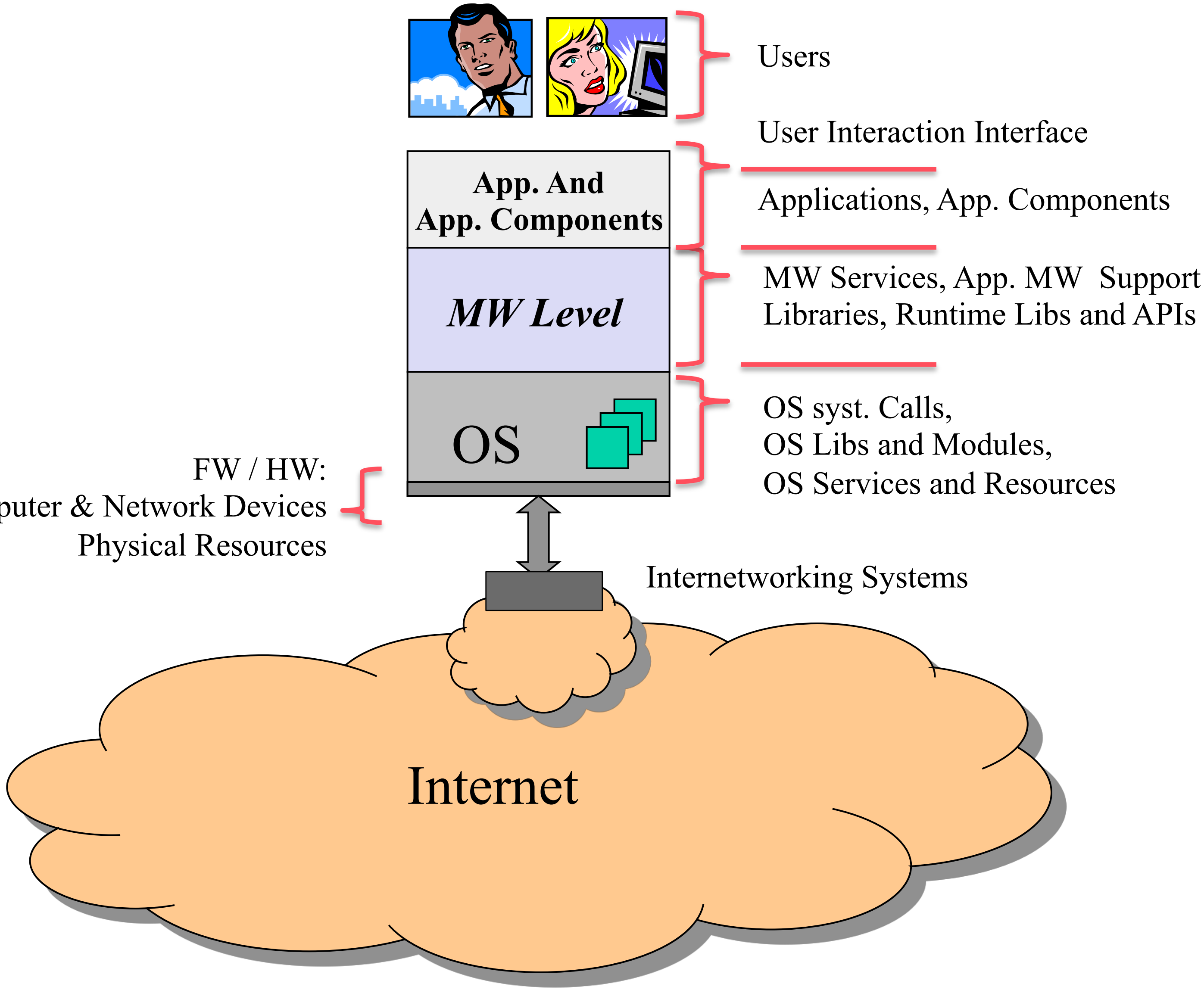
- The trusted base and foundations beyond the security mechanisms and services
  - Proven abstractions and foundations
  - Trusted "essential" components
- For Security (Security Mechanisms and Services) we always depend on a TCB !
  - Why ?
- The better is that it must be Dependable, Delimited, Identifiable, Auditable, Verifiable, Minimal, Simple ...
  - Is it easy to address such criteria ?
  - "What means" minimal (abstraction level) ?
  - Think on the current Large-Scale Distributed Systems

Identification and delimitation of TCB

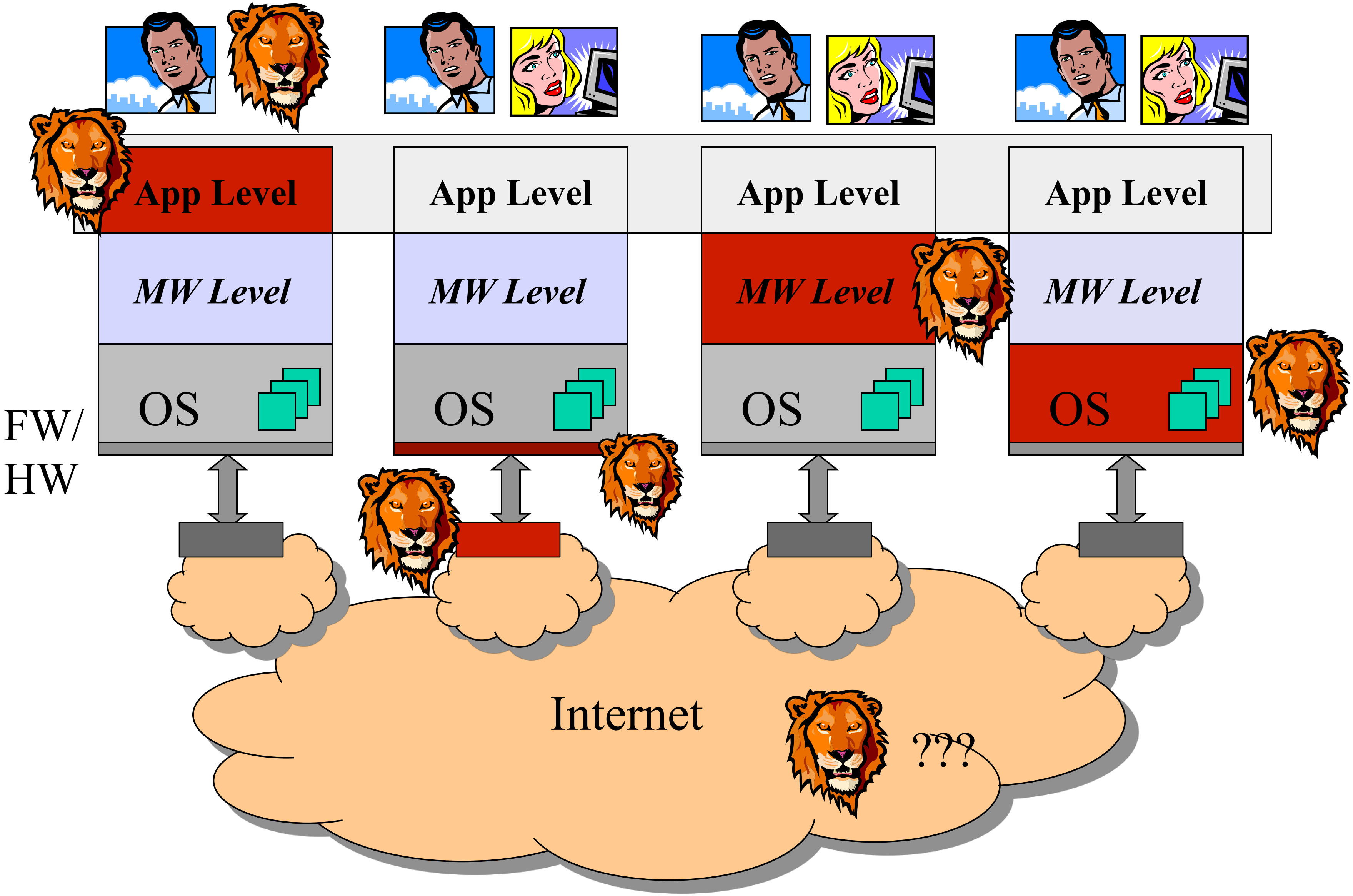


Users and
Distributed
Applications

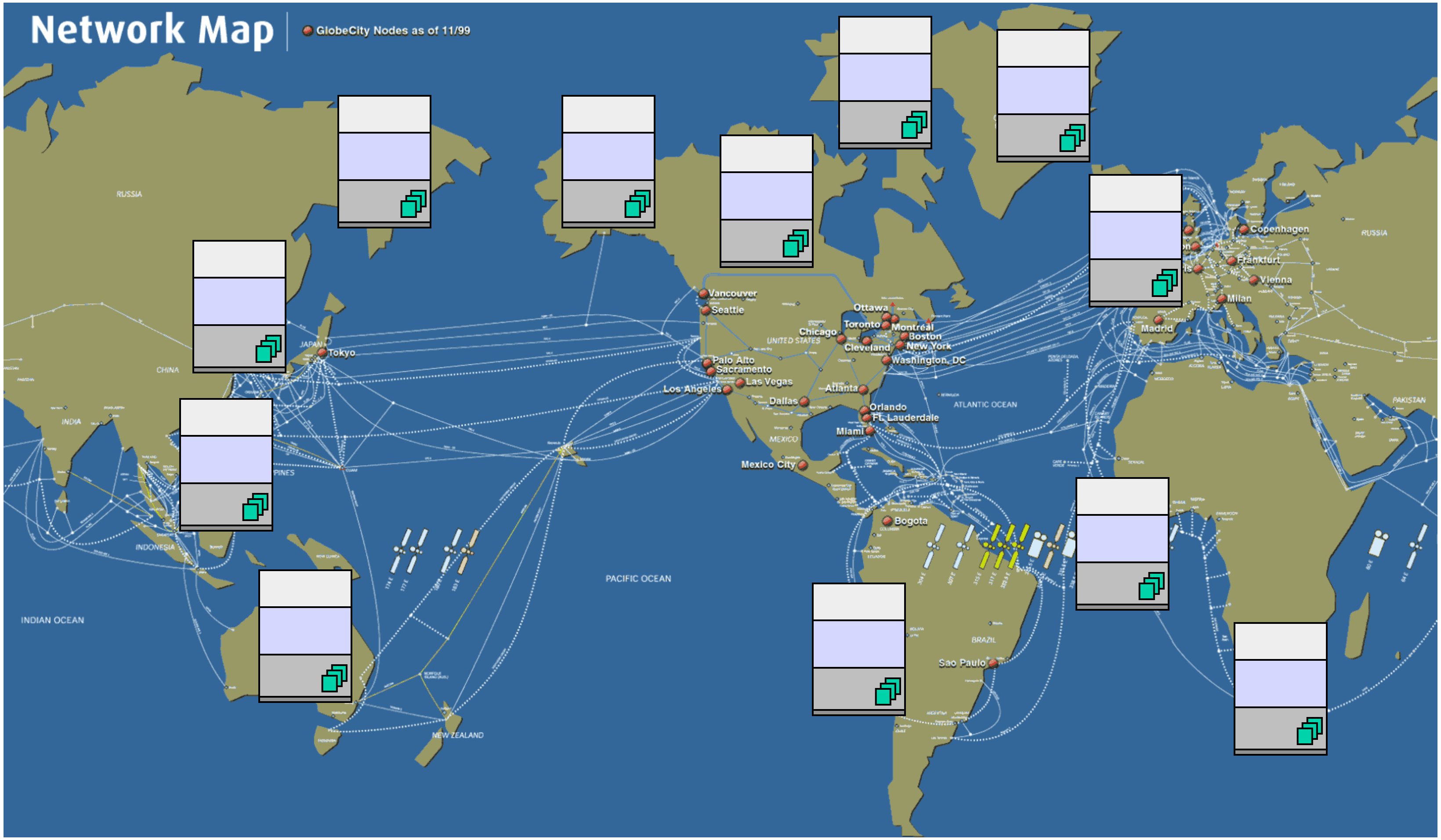
Identification and delimitation of TCB


Users
User Interaction Interface
Applications, App. Components
MW Services, App. MW Support
Libraries, Runtime Libs and APIs
OS syst. Calls,
OS Libs and Modules,
OS Services and Resources
App. And
App. Components
MW Level
OS
FW / HW:
Computer & Network Devices
Physical Resources
Internetworking Systems
Internet

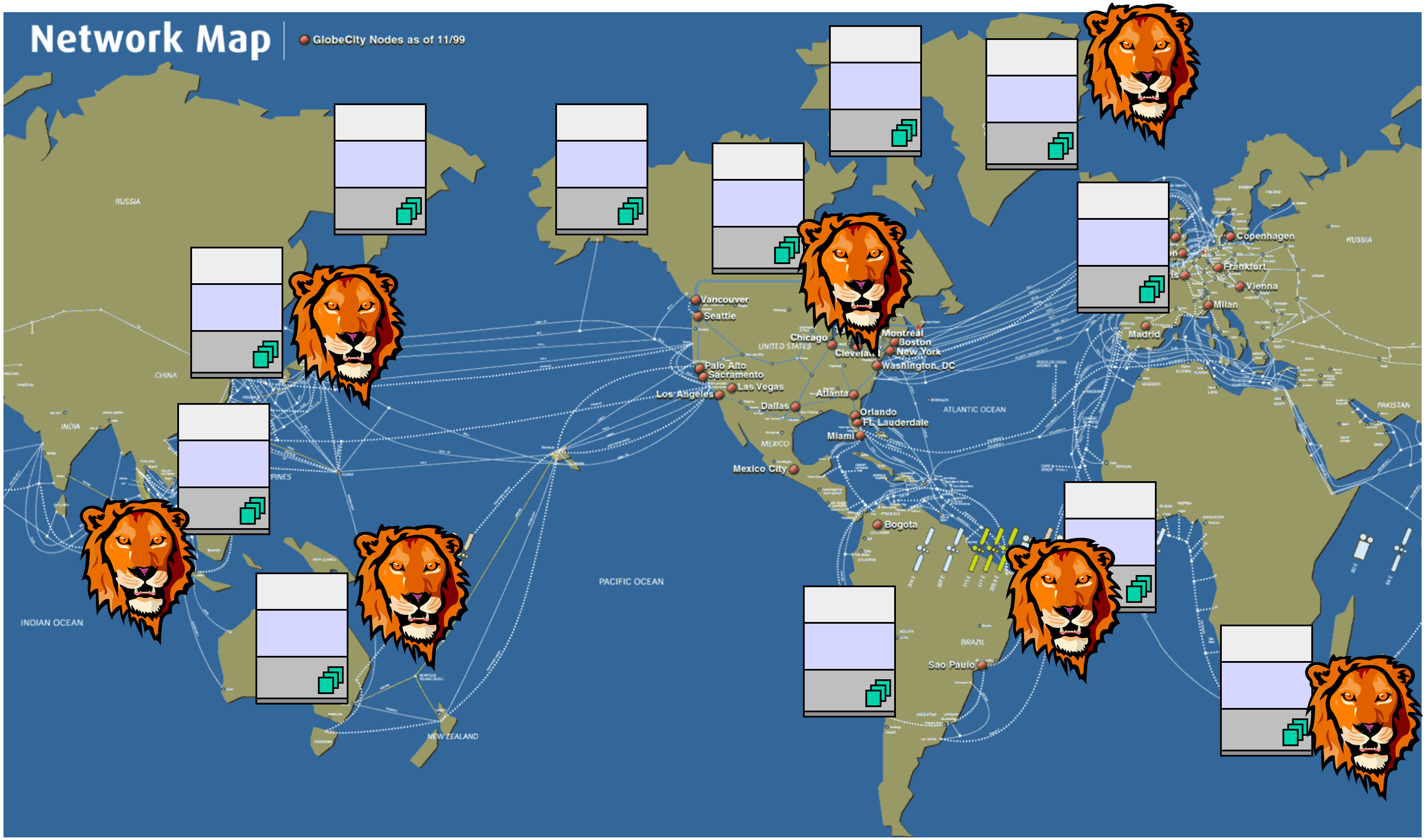
Approach level and reduction of TCBs



Distribution of TCBs



How to address a TCB in a Large Scale Distributed System ?



Secure Systems:
Complexity and Challenges

Security challenges: fascinating and complex

- **Different and many concerns, viewpoints, dimensions ...**

  . . . holistic approaches …

- **Base security mechanisms are complex**

- **Security services** operate at different levels of implementation
  - "End-to-End Security Arguments in Systems' Design

- Procedures and mechanisms **sometimes (often) counterintuitive**

- **Human factors … (security vs. usability treade-offs)**
  - **Is the "user" an "adversary" ?**

Security challenges: fascinating and complex

- Security mechanisms require **specific proofs (ex., Math proofs), but many mechanisms are pervasive**

- **Verifiable properties and trustability assumptions** must be established by correct and valid **TCB components**
  - **TCB: Trust Computing Base**

- **The identification, reduction and verification of TCBs is a very complex problem** (think on large scale, pervasive and heterogeneous systems as we are faced today)

- **To design a secure system we need to define its threat model (or adversary model)**
  - **The correct definition of threat models** and risk-management tradeoffs is very complex … and it is a moving target

Organizational Security Challenges

Organizational security and cybersecurity knowledgement domains

Security as a discipline in Informatics Engineering and Computer Science: it is a pillar in a **multidisciplinary field**

Requires an extensive and broad comprehension of many involved dimensions and interdependencies: organization culture, business models, business & risk management factors, operational-processes, persons, type of assets, classification of information and resources, regulation and law, ethical factors, … etc.

⇒ Factors: Organizational, Economical, Sociological, Psychological, Educational, Cultural, Human and Motivational Factors, Defense, Politics …

⇒ Inter-Organizational and Social-Engineering Factors

⇒ **Multidisciplinary approaches: cooperation**

Suggested Readings

- W. Stallings, L. Brown, Computer Security – Principles and Practice, Person, Chap.1
- W. Stallings, Network Security Essentials – Applications and Standards, Chap 1
- A. Zúquete, Segurança em Redes Informáticas, Ed. FCA, Cap 1 – Introdução

  https://www.fca.pt/pt/catalogo/informatica/seguranca-ciberseguranca-protecao-de-dados/seguranca-em-redes-informaticas-2/

Complementary materials:

- See Available Security Reports

  CLIP Course Documentation