

DI-FCT-UNL

Segurança de Redes e Sistemas de Computadores
Network and Computer Systems Security

Mestrado Integrado em Engenharia Informática
MSc Course: Informatics Engineering
2º Semestre, 2018/2019

1. Introduction (Part I)

Concepts, Terminology
Frameworks

Interesting starting points ...

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

Complexity, Security as a Process

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

What is a Secure System ?

How to define a "Secure System" ?

Possible definition :

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

Intrinsically or paradoxically, this definition says that

...

**TEHERE ARE NO SECURE SYSTEMS !
IMPOSSIBILITY !**

☹ ... this doesn't help !

More interesting definitions

Ex., NIST FIPS PUB 800-12, Oct/2005
(NIST Computer Security Handbook)

<https://www.nist.gov>

Computer security

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 Telecommunications**

Security
Properties
(as objectives)

Computer Security
Computer node level:
Computation+ I/
O+Storage Resources

**(Tele)Communications
Security**
Data-flows
End-to-End
vs. Pt-to-Pt
(Secure comm. channels)

Resources as
Protected Assets

Security and Risk Mitigation

More interesting

Thinking on RISK

Security as the Minimization (or Mitigation) of Risks

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

$$\text{RISK} = \text{VULNERABILITIES} \times \text{THREAT-Potential}$$
$$\text{RISK}(t) = \text{VULNERABILITIES}(t) \times \text{THREAT-Potential}(t)$$

How to define a "Secure System" ?

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

A System designed with secure objectives addressed by 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, ...

... according 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):

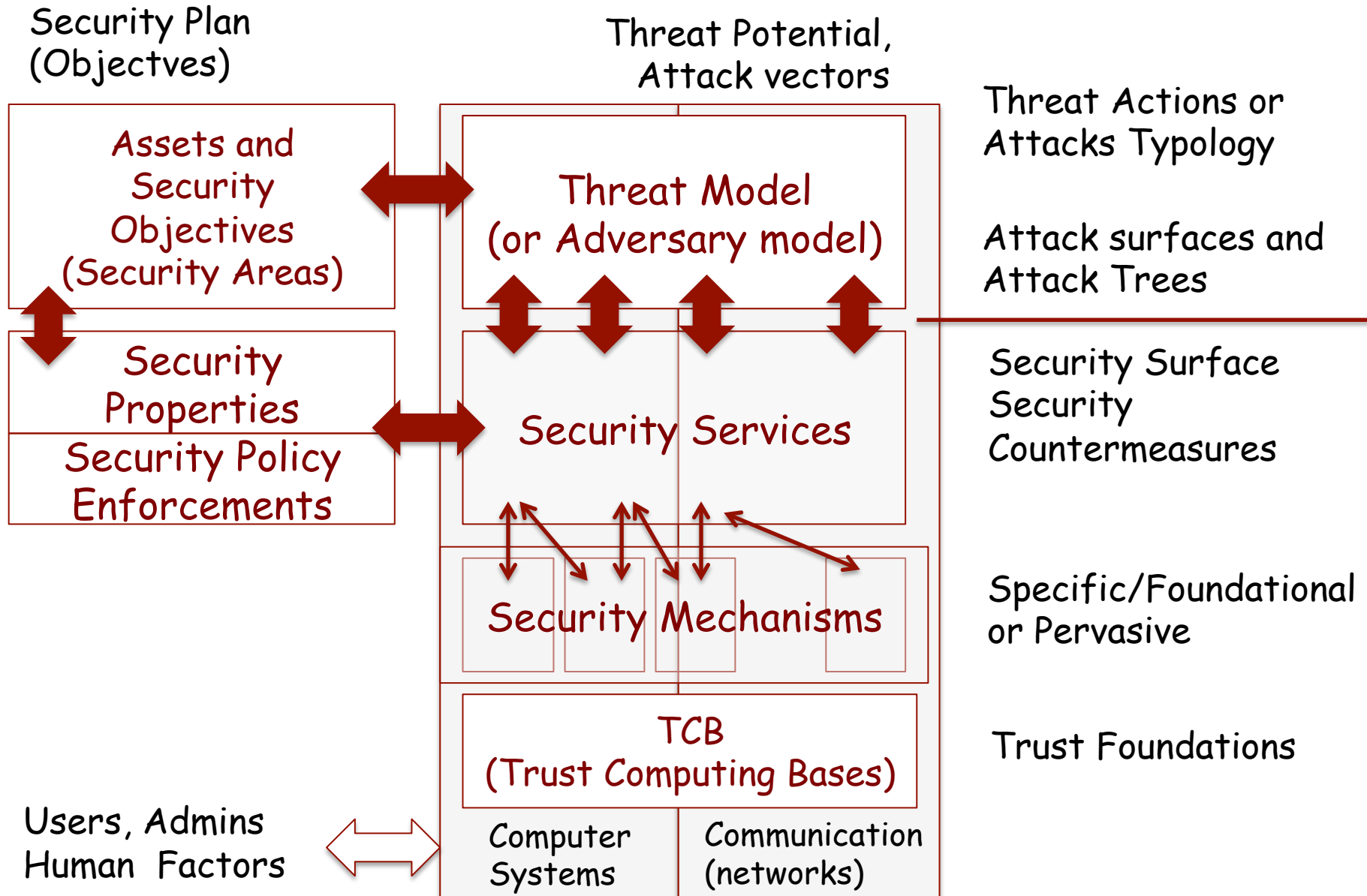
A System designed with **secure objectives** addressed by verifiable **security properties** implemented by **security services** built from **security mechanisms**, afforded to attain the applicable objectives of **preserving authentication, confidentiality, integrity, availability and access-control** 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, ...

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

Generic framework for the previous definition



How to instantiate the proposed framework ?

- How to define Secure Objectives ?
- How to define the Security Properties ?
- How to design Security Services for those Properties ?
- What are the Correct Security Mechanisms to build the Security Services ?
- How to identify principals ? (Different Levels of Approach)
- How to define an Adversary Model
- How to identify the correct TCB components ?
- How to establish the Correct Security Arguments in the Systems Design Options ?
- What can we learn from existent and standardized security solutions and their arguments to have solid System Design Assumptions ?

How to instantiate the proposed framework ?

Considering ...

- Security By Design
 - › Foundations, Design+Dev+Test Life Cycles)
 - White-Box Approach
- Security as a Process
 - › Operation lifecycle
 - Security Auditing
 - White-Box, Gray-Box, BlackBox Approaches

Complexity and Challenges

Security challenges: fascinating and complex

- Different and many concerns, viewpoints, dimensions ...
 - . . . holistic approach ...
- 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 trade-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 knowledge 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**

Relevance of concepts and terminology

Initial Readings

Security Objectives and Challenges



Suggested Readings:

W. Stallings, L. Brown, Computer Security - Principles and Practice, Person, Chap. 1, section 1.1, pp.24-29

W. Stallings, Network Security Essentials - Applications and Standards, Chap 1, section 1.1, 20-24

Computer Systems and Networks Security (Distributed Systems Security Approach)

... Dependability and the notion of "Dependable System"

Computer Systems and Network Security

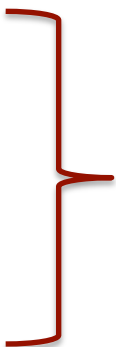
2 dimensions involved

(Distributed System Approach):

- **Computer Systems (Computing Nodes)**
 - Computer Security Services and Mechanisms
- **Network (Communication Security)**
 - Secure Communication Channels
 - End-to-End Security Arguments


Computer Systems and Network Security

Network (or Internetwork) Security Level

- Communications' Protection
 - Private/Dedicated/Shared/Public/Outsourced
 - Wired, Wireless, Supervised, Non-Supervised ...
 - Internet Communication
 - Physical Level
 - Access Level (Data Link)
 - Traffic Flow Level (Net Level)
 - Transport Level
 - Session/Representation Level
 - Application-Protocol Level
- 
- Secure Com. Channels**
PtP vs. End-to-End
Secure Protocols
Secure Endpoints

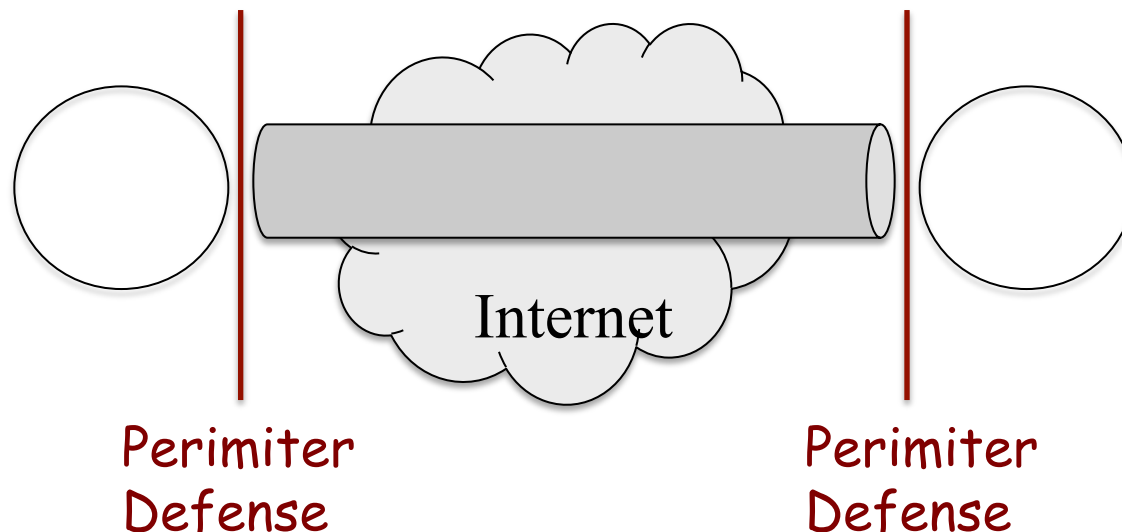
Computer Systems and Network Security

Computer Systems Security Level

- Computer Systems (Computing Nodes)
 - Private/Dedicated/Shared/Public/Outsourced Computing
 - Stationary, Mobile, Supervised, Non-Supervised ...
 - Physical Level
 - HW Level
 - OS Level
 - MW / Runtime Libraries' Level
 - Application-Support Level
- 
- Secure Data Storage
Software Security +
Software Attestation +
Isolation and Containment
Trusted Execution

How to define a Secure Channel ?

- Definition example using a standardized framework (OSI X.800):
 - A channel where traffic flows are protected, being immune to the Attack Typology of MiM attacks, according to the **OSI X.800 attack typology and OSI X.800 defined services and mechanisms**



- **PtP vs. End-to-End Security Arguments**

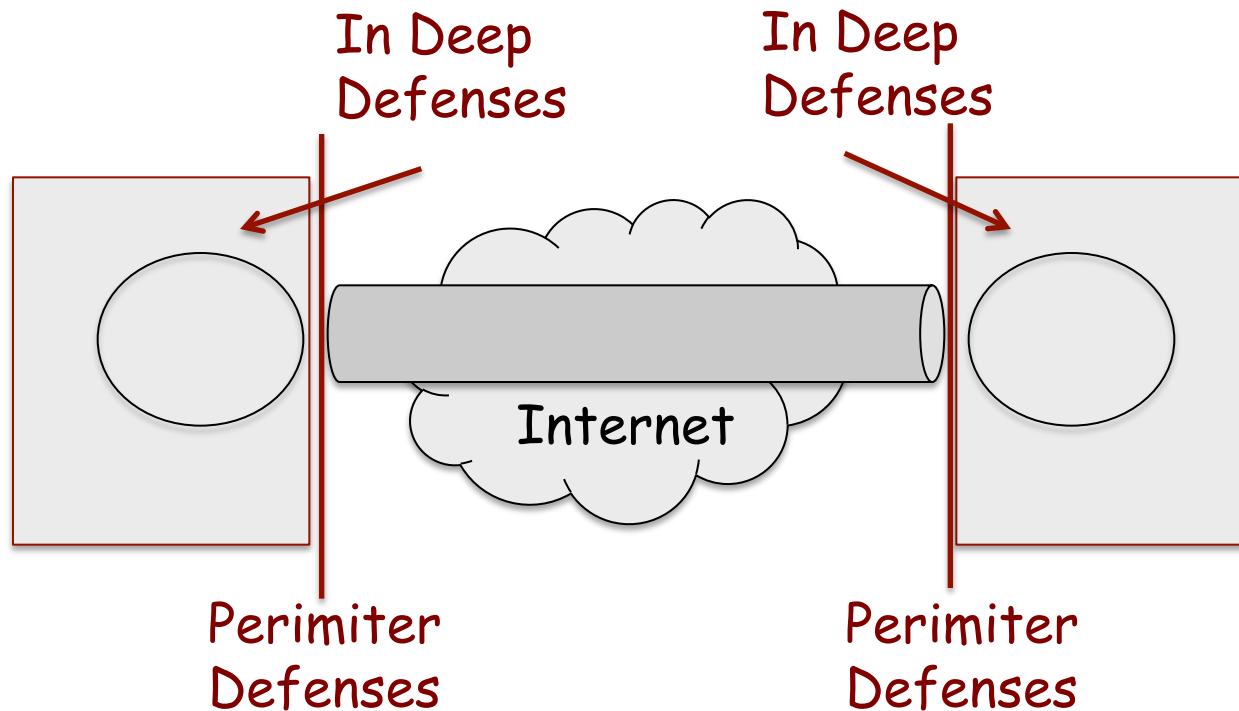
How to define a Secure Channel ?

Security properties: see OSI X.800 (later)

- Authenticated endpoints (principals, mutual authentication)
- Traffic and data flow confidentiality
- Traffic and data flow integrity
- No replaying

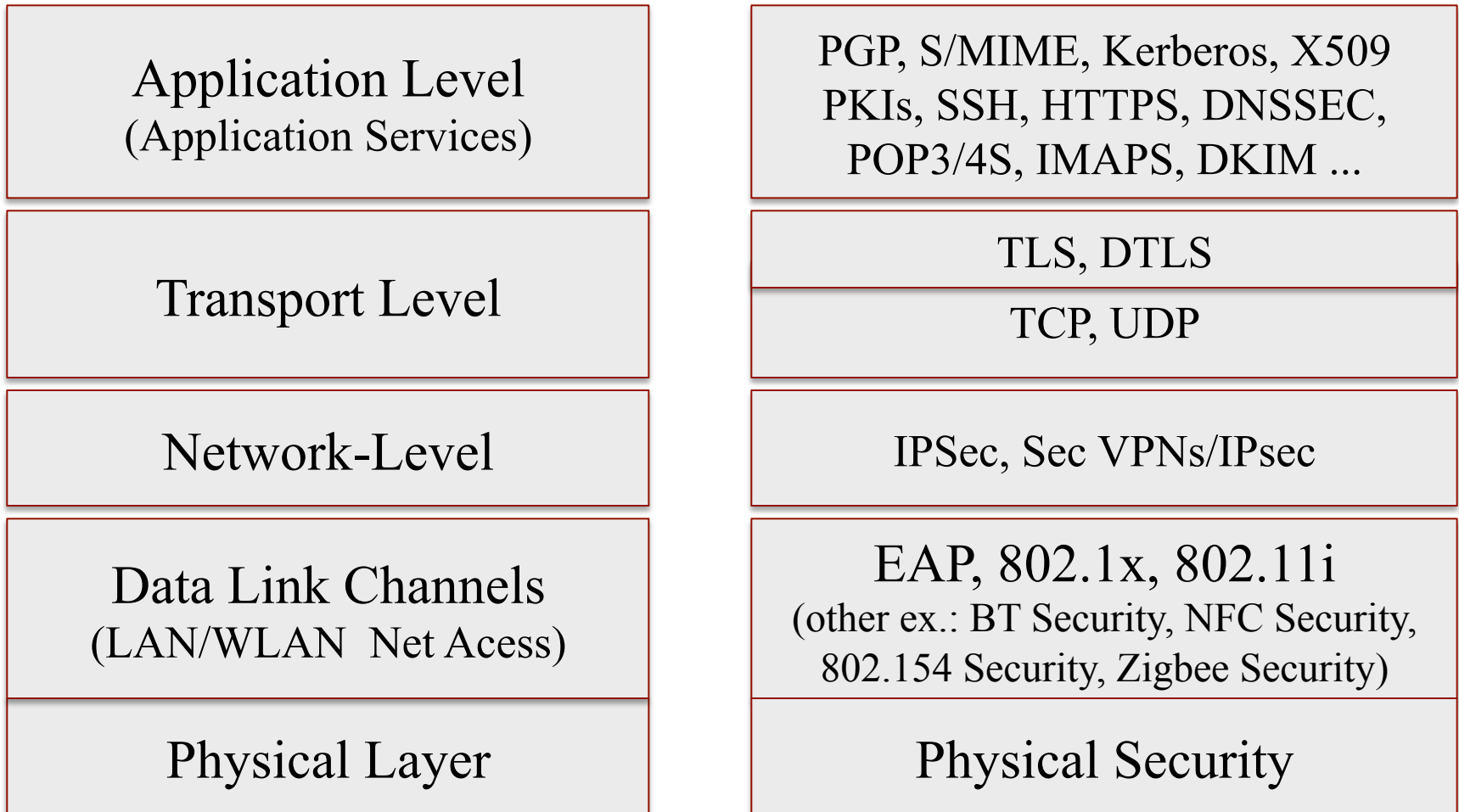
More ?

- No Repudiation
- Routing Control
- Availability
- Connection control
- Reliability
- ...



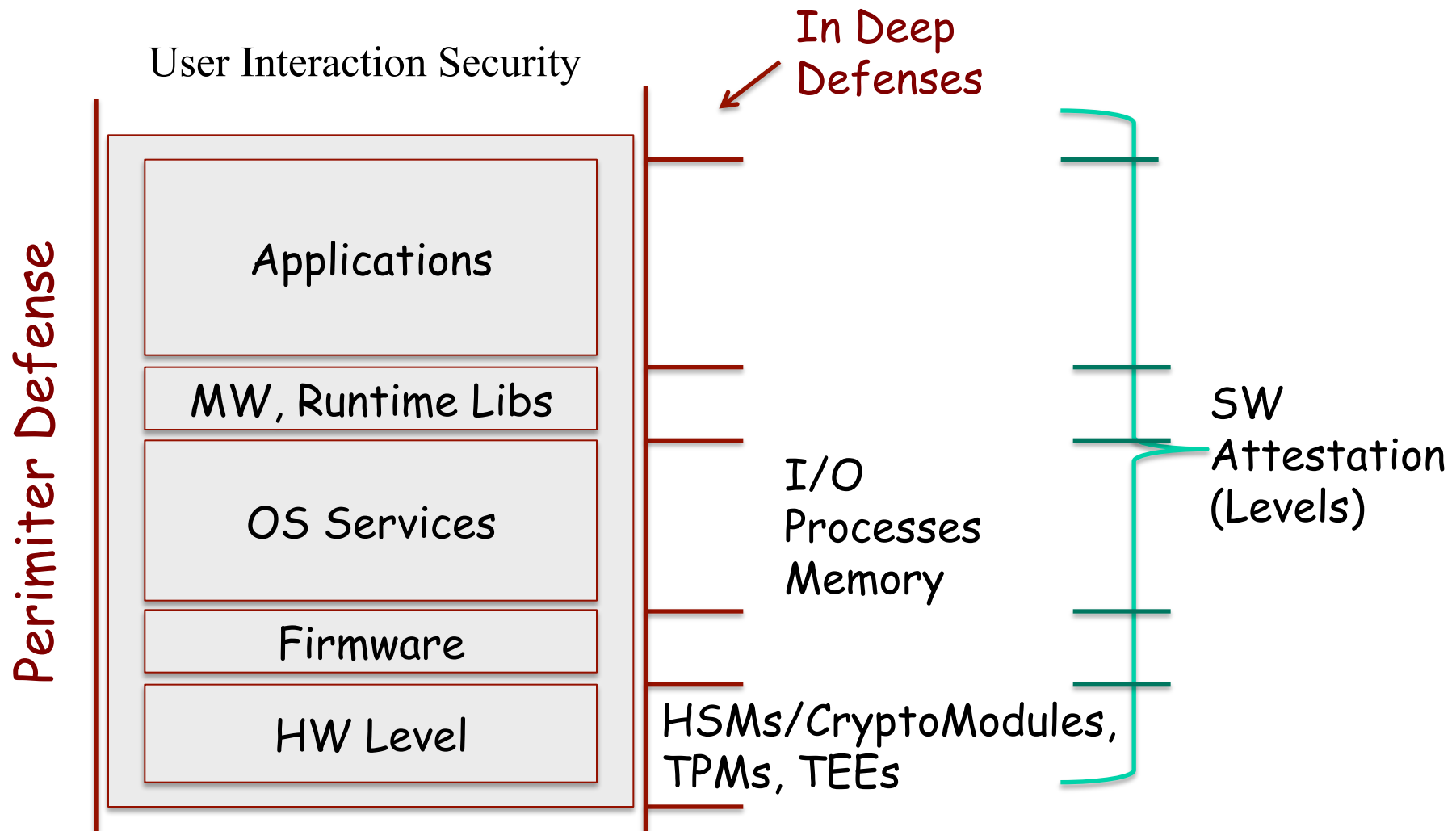
Example: TCP/IP Security Stack

- Discussion: Security Services and Protocols in the TCP/IP Security Stack



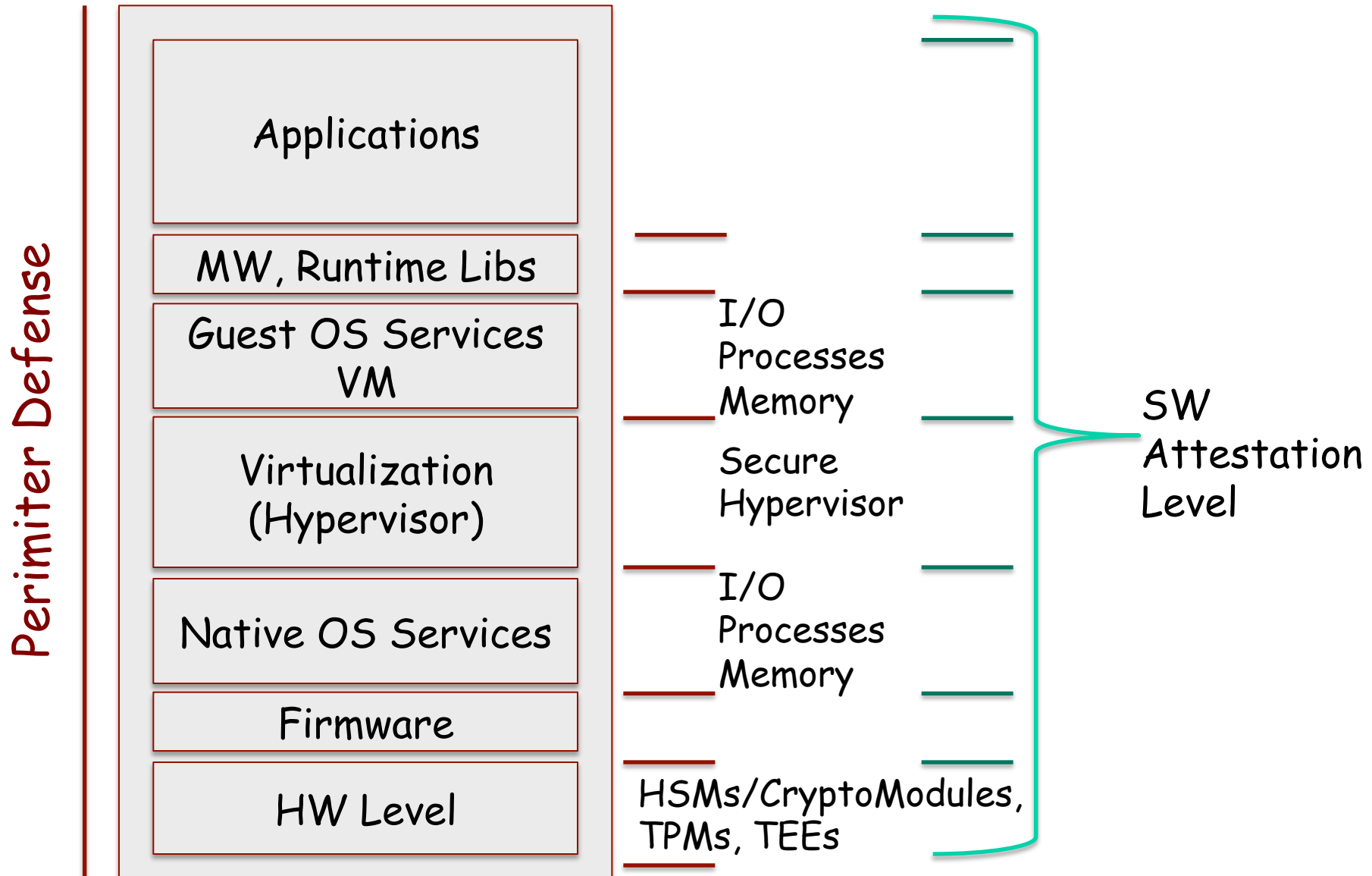
Scope of Computer Security

Isolation and TCB Level



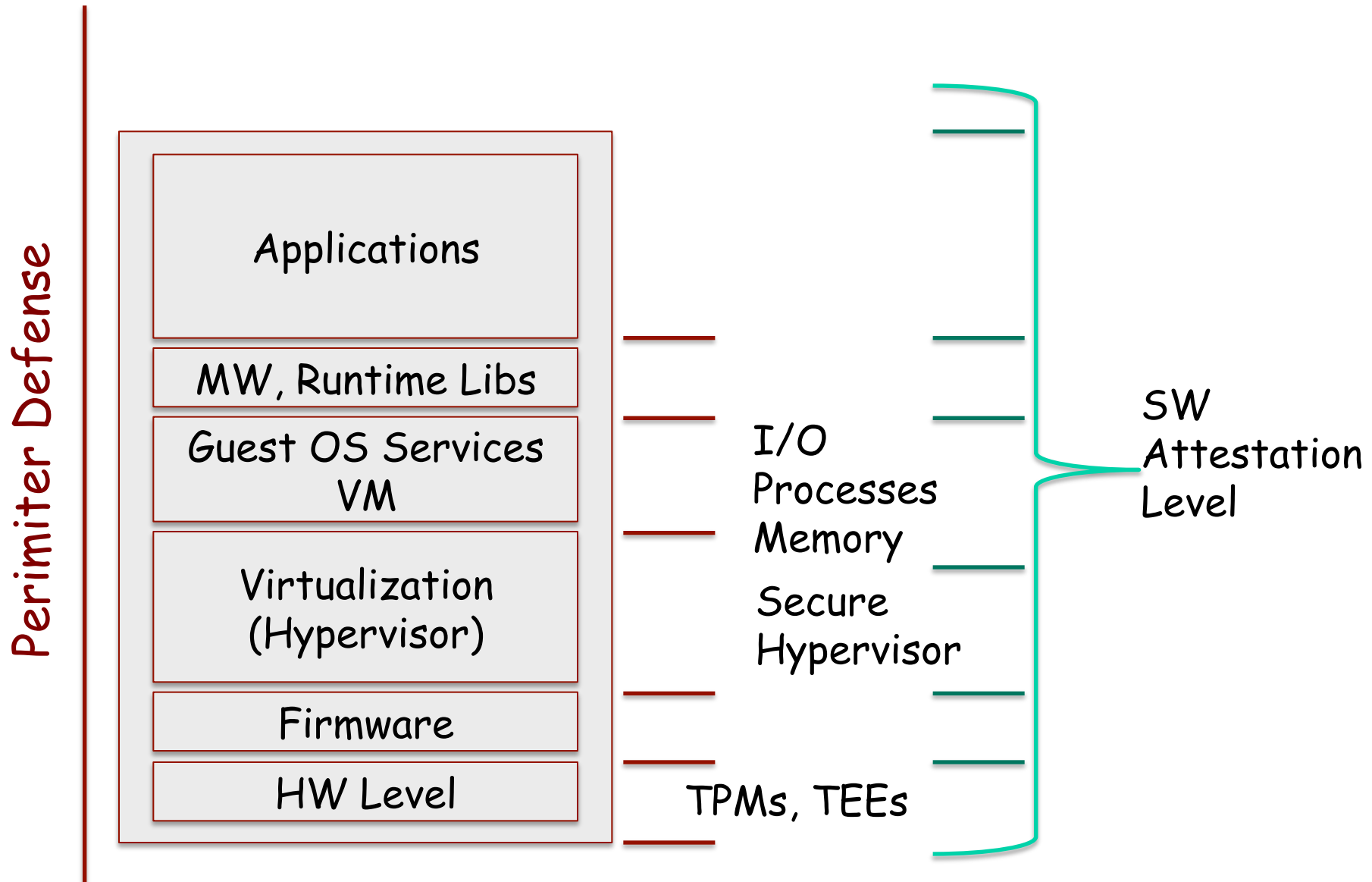
Scope of Computer Security

Isolation and TCB Level



Scope of Computer Security

Isolation and TCB Level



Computer Systems and Network Security

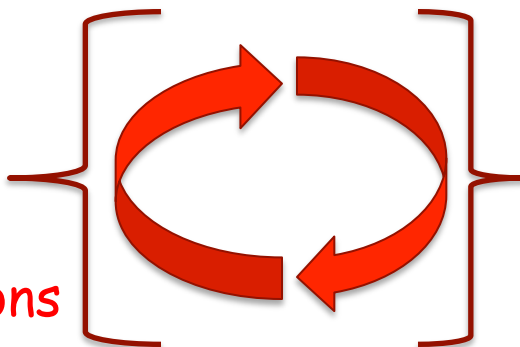
- 
- Computer Systems (Computing Nodes)
 - Network (Communication Security)

Distributed Systems Security
Dependable Distributed Systems

Failure Models and Threat Models
Security, Intrusion Tolerance and Fault Tolerance

Secure Data Storage
Software Security +
Software Attestation +
Trusted Execution +

Dependability Assumptions



Secure Com. Channels
PtP vs. End-to-End
Secure Protocols
Secure Endpoints

Dependability Assumptions

**What/Where/How to Identify
the Trust Computing Model**

Dependability

- In Systems Engineering **dependability** is a measure of a system's **availability, reliability, and its maintainability, and maintenance support performance**, and, in some cases, other more characteristics such as **durability (or availability), safety and security**.
- In Software Engineering, **dependability** is the **ability to provide services that can defensibly be trusted within a time-period (a certain life cycle)**

Those properties may also encompass mechanisms designed to increase and maintain the dependability of a system or software

Dependable System

*A system is dependable
if reliance can justifiably be placed on
the service it delivers.*

Dependability thus includes as special cases such attributes as reliability, availability, safety, security.

Suggested reading

- Targets of Defense
- Vulnerability vs. Risk Management Issues
- Typology of Defenses in CSNS
- Perimeter vs. "in Deep" Defenses
- Security Policy Enforcement
- Types of Security Mechanisms
- Distributed Systems Security Principles and Risks



Suggested Reading (Portuguese Language):

A. Zúquete, *Segurança em Redes Informáticas*, Cap. 1 - Introdução (pp 11-16), FCA, 5ª Ed., 2018

Typology of Defenses in CSNS

- **Physical Defenses: Catastrophes/Disasters**
- **Prevention Defenses against Systems' Faults or Failures**
- **Prevention defenses against non-authorized activities**

Typology of Defenses in CSNS

- **Physical Defenses: Catastrophes/Disasters**
 - Ex., Environmental, Political, Material, Natural/Accidental
- **Prevention Defenses against Systems' Faults or Failures**
 - Energy or Blocking faults causing stop-failures
 - Temporary faults causing intermittent failures in processing and communication (connectivity conditions)
 - Possible arbitrary faults (or byzantine faults)
- **Prevention defenses against non-authorized activities**
 - Information access, abuse of privileges
 - Tampering, fake information forging or illicit modification
 - Unfairness and abusive use of computational resources (ex., abuses in multi-shared resources)
 - Service denial activities

Vulnerabilities in CSNS

- **Complexity Issues**
- **Realistic Approaches**
- **Perimeter Defenses vs. “in deep” Defenses**

Vulnerabilities in CSNS

- Complexity Issues
- Realistic Approaches
- Perimeter Defenses vs. “in deep” Defenses
- Perimeter Defenses (ex., IPS or FWs: NIPS, HIPS; IDS: HIDS, NIDS; Hports and Hnets)
 - Separation (no direct interaction) between:
 - Side where threats are originated or where adversaries (or attackers) act
(regarded as “external attackers” on “external perimeters”)
 - Side of protected resources on “internal perimeters”
 - What if adversaries exist in the protected perimeter ?
 - Protection of security domains / different security levels
 - Possible Fine-grained granularity

Vulnerabilities in CSNS

- **Complexity Issues**
- **Realistic Approaches**
- **Perimeter Defenses vs. “in deep” Defenses**
- **In Deep Defense:**
 - More complex (but can be more effective)
 - Protection of all security levels involved (not only the externalization of systems or interfaces between security domains)

Security Policy Enforcements

- **Define security requirements that must be verified**

Security Policy Enforcements

- **Define security requirements that must be verified**
 - Classified information, confidentiality and access-control (permission/deniable models)
 - Protection of sensitive data: privacy guarantees, backup and recovery guarantees
 - Business or organization services' continuity
 - Trustworthy conditions for systems' operation and compliance
 - Proofs of correction, authenticity, attestation, origin, authoring, ownership in information exchanges
 - Logging and auditing of relevant events or retention of evidences for forensics and analysis of occurred actions
 - Authentication factors and proofs to authenticate roles, users and systems' principals, entities or subjects
 - Authorization rules and privileges for roles, users or principals
 - Monitoring/Auditing processes

Correct choice of security mechanisms: Different types => Different Purposes

Problem: How to choose the right mechanism for the right purpose?

Classification approach of different types of mechanisms:

Correct choice of security mechanisms: Different types => Different Purposes

Problem: How to choose the right mechanism for the right purpose?

Classification approach of different types of mechanisms:

- Containment
- Access-Control
- Privileged Execution
- Filtering
- Registration
- Inspection
- Auditing
- Cryptographic mechanisms
- Secure Channels and Cryptographically Secure Protocols

Correct choice of security mechanisms: Different types => Different Purposes

Problem: How to choose the right mechanism for the right purpose?

Classification approach of different types of mechanisms:

- **Containment** (IPS, Sandboxing, Isolation)
- **Access-Control** (MAC, DAC, RBAC, ABAC, C-ABAC Models)
- **Privileged Execution** (Separation of Rights and Duties)
- **Filtering** (Ex., Filtering Rules, Tainting Analysis and Dynamic Content and Stateful Inspection)
- **Registration** (Event Logging)
- **Inspection** (IDS, Static and Dynamic in Runtime and/or Real-Time Anomalous Detection)
- **Auditing** (Automatic + Semiautomatic Verification and Supervision)
- **Cryptographic mechanisms** (Algs, Construction schemes, Secure Parameterizations, Programming Techniques and Tools)
- **Secure Channels and Cryptographically Secure Protocols**

No Security by Obscurity ...

NO SECURITY BY OBSCURITY !!!!

- We must choose mechanisms ...
 - Well established, well accepted and respectable in the scrutiny of the **scientific and research community and relevant venues**
 - **Published, with information sources (and possibly implementation) allowing for study**
 - **Correctly implemented with public verification and certification acknowledgement from well-reputable entities**
 - **Open (published), considered relevant and interesting as object of broad study by the research, scientific and R&D communities**
 - **From certified standards by relevant entities and organizations (ex., ANSI, NIST, FIPS-PUB, ISO, IEEE, IETF ... IACR,) or Certified Labs (ex., NIST/NVLAP and accredited CMTLs, compliant implementations with valid/updated IETF/RFCs , RSA Labs, ...)**

Relevance of concepts and terminology:

Security Frameworks

Correct terminology and correct concepts



.. 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

Message Forgery

Spoofing

DoS, DDoS, DRADoS, ...

SQLi

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

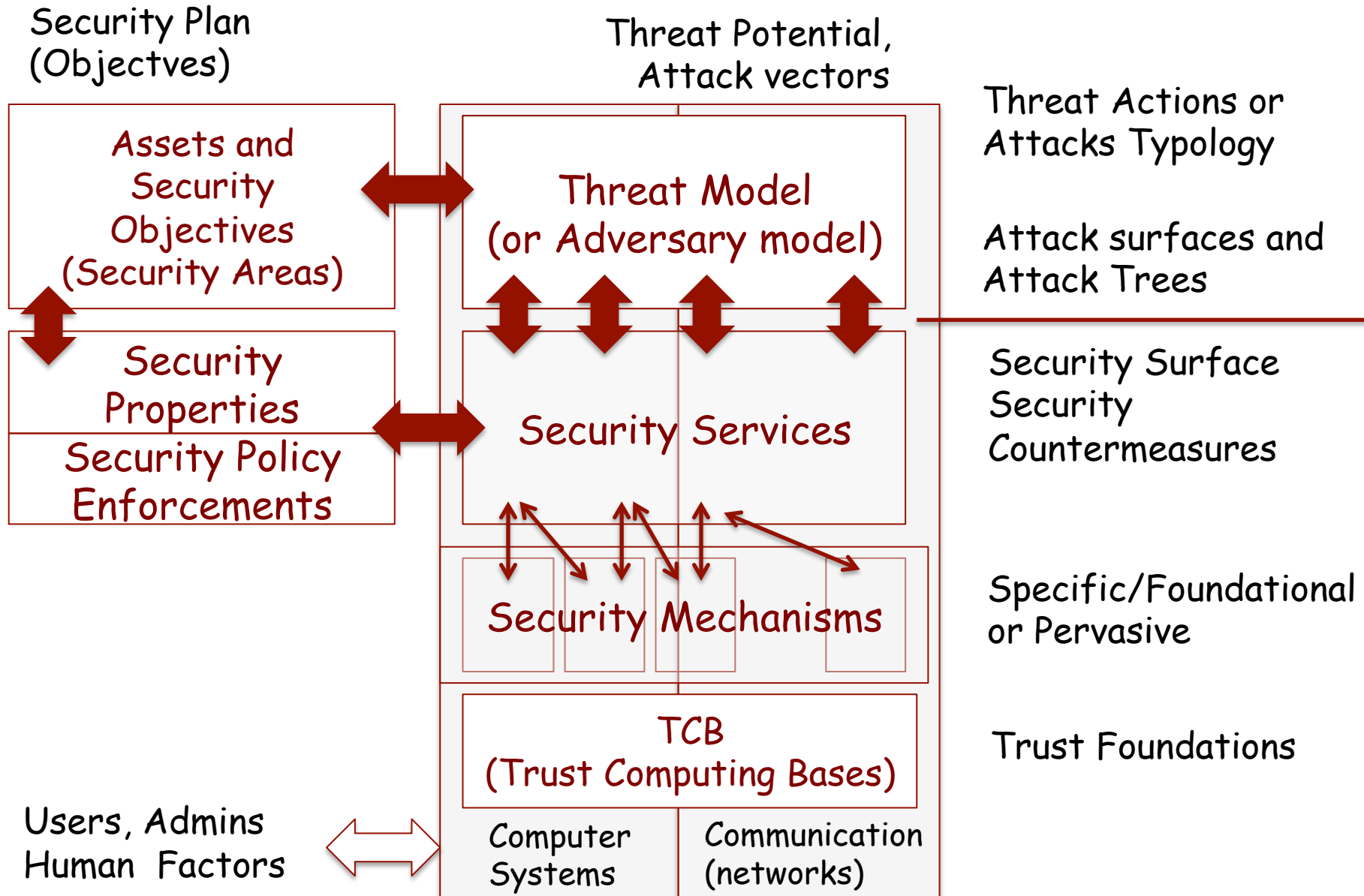
DH Key
Exchange

PGP

ISO 27001

S/MIME

Generic framework for the previous definition: Instantiation w/ Standardized Security Frameworks



What is a Security Framework ?

- An information **security framework** is a series of documented processes, including terminology, concepts and definitions, that are used to define policies and procedures around the implementation of **security** controls
- Frameworks related to Security Standards and Good Practices in:
 - Systems and SW Security Design
 - Operational and Systems' Management Security

Typology of Security Services and Mechanisms

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

- Organizational Security Plan

Correct Mappings:



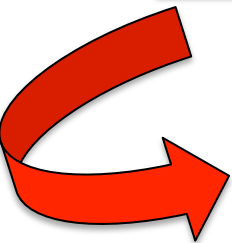
Information Systems Security Patterns

- **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, DataCenters, 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 ?



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:

EU
GDPR

HIPAA

HIMSS.eu

NIST
(Security and
Privacy in
Public Cloud
Computing)

EU
Banking and
Finance

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/>

Instruments (Compliance and 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 102/2017, 74/2017, 58/2016, Lei 14/2019	DL 14/2019, 2/2019, Lei 46/2018, ...

Frameworks:

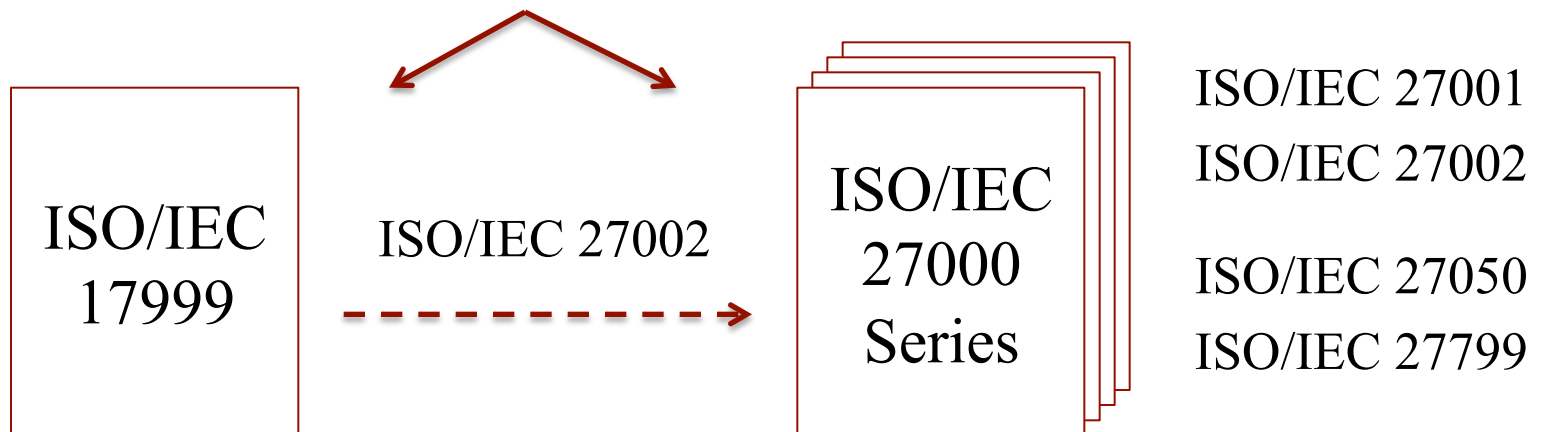
Organizational vs. information Systems Security Management

- 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)



☹ ~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
 - System access control
 - System development and maintenance processes
 - Physical and environmental security criteria
 - Govern, Regulation and Compliance (GRC) criteria
 - Personnel security management criteria
 - Organizational information security criteria at 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>

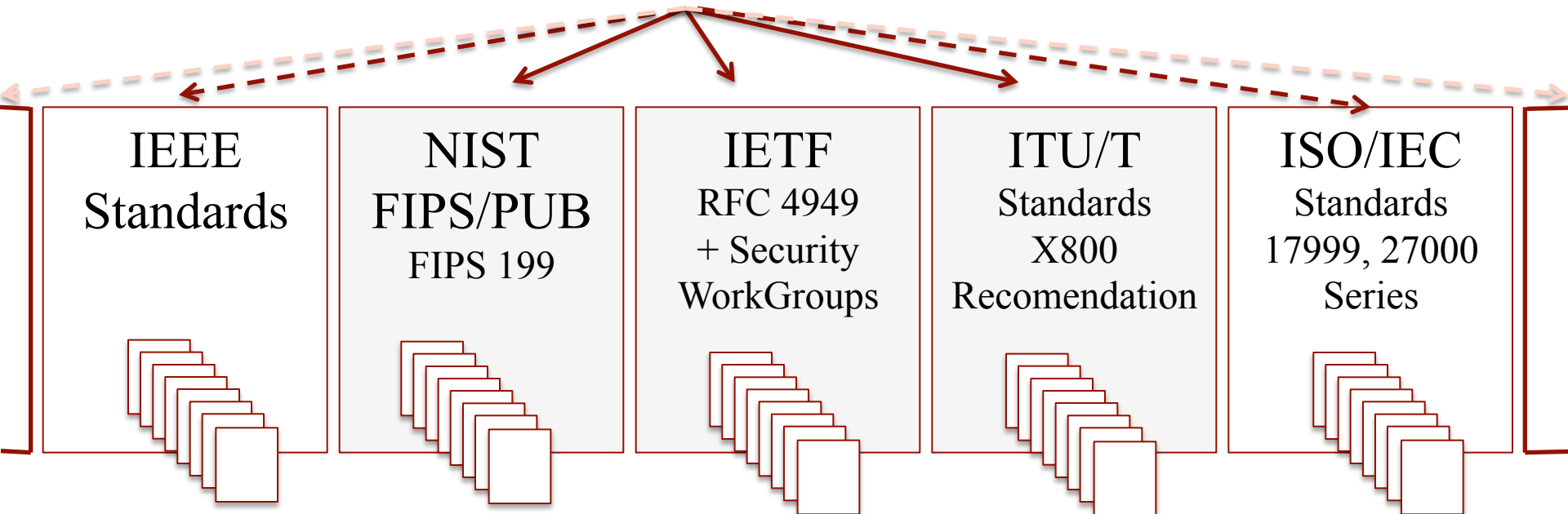
Instruments (Engineering, Technology)

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

How to establish a correct mapping:



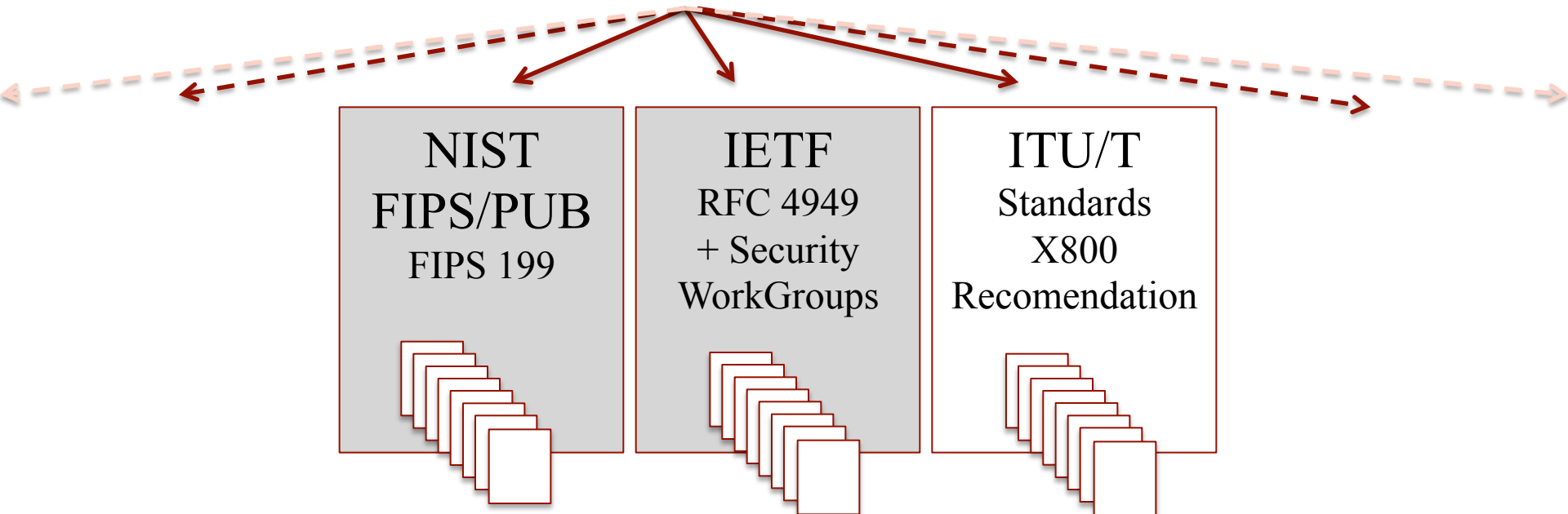
Technical Security Standardization Frameworks
(Relevance as Engineering Security Frameworks)



Computer Security Objectives

Computer Security Objectives

Technical Security Standardization Frameworks



CIA Triad (NIST - NISTIR
FIPS Pub 199 Series,

CIA Triad, NIST, NISTIR 7298

- Glossary of Key Information Security Terms, May 2013

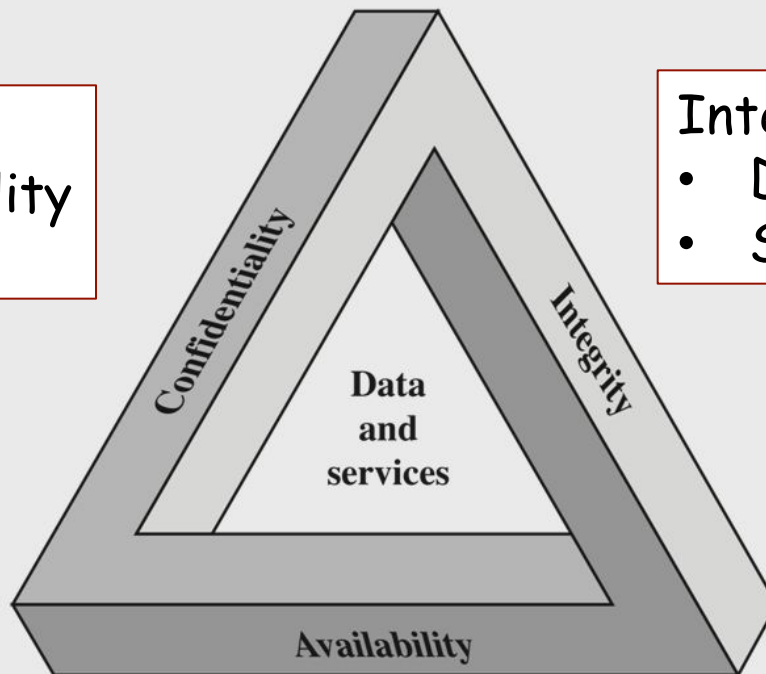
CIA Triad

Confidentiality:

- Data Confidentiality
- Privacy Control

Integrity

- Data Integrity
- Systems Integrity



Availability: Correct Continuity for Authorized Users

Security Objectives (NIST CIA Triad)

NIST (NISTIR 7298 - Glossary of Key Information Security Terms, May 2013)

- **Confidentiality:**

- **Data Confidentiality:** Private or Confidential Information is not made available or disclosed to unauthorized principals
- **Privacy:** Principals control or influence what information related to them may be collected and stored and by whom and to whom the information may be disclosed

- **Integrity**

- **Data Integrity:** Information and Programs are changed only in a well-specified and authorized manner
- **System Integrity:** the system performs the intended function in an unpaired way, free from deliberate or inadvertent unauthorized manipulation

- **Availability:** systems work promptly and its services will not be denied to the 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
 - avoids: unauthorized disclosure of info
- **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

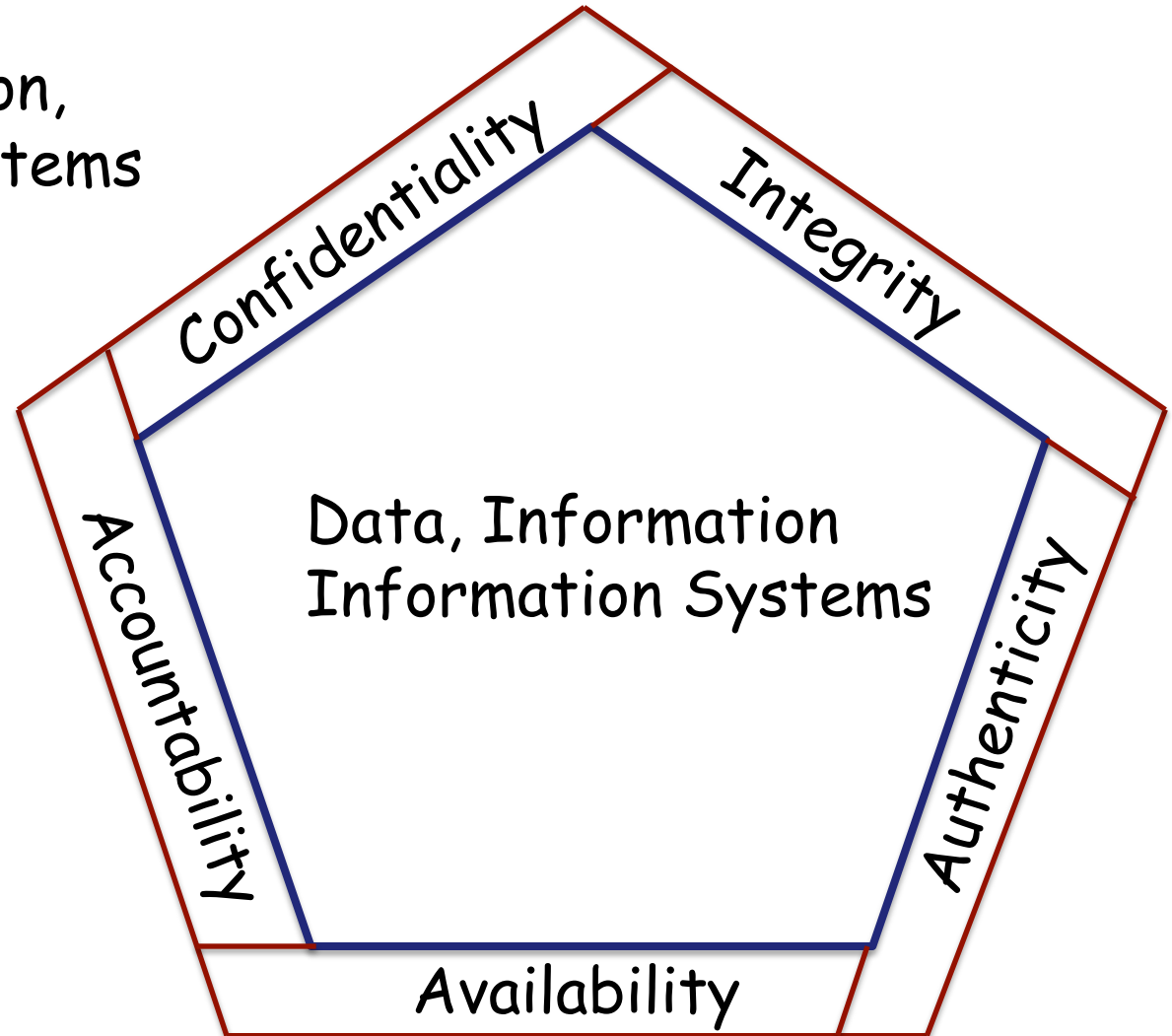
NIST CIA Triad, FIPS PUB

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

- **Accountability**
 - Ensures traceability, non-Repudiation, deterrence, fault isolation, intrusion detection and prevention, after-action recovery, forensics analysis and legal action

Computer Security Objectives

Emphasis:
Data, Information,
Information Systems



Computer Security Concepts and Terminology

Suggested Readings

Security Objectives Challenges

Suggested Readings:

W. Stallings, L. Brown, Computer Security - Principles and Practice, Person, Chap. 1, sections 1.1-1.3

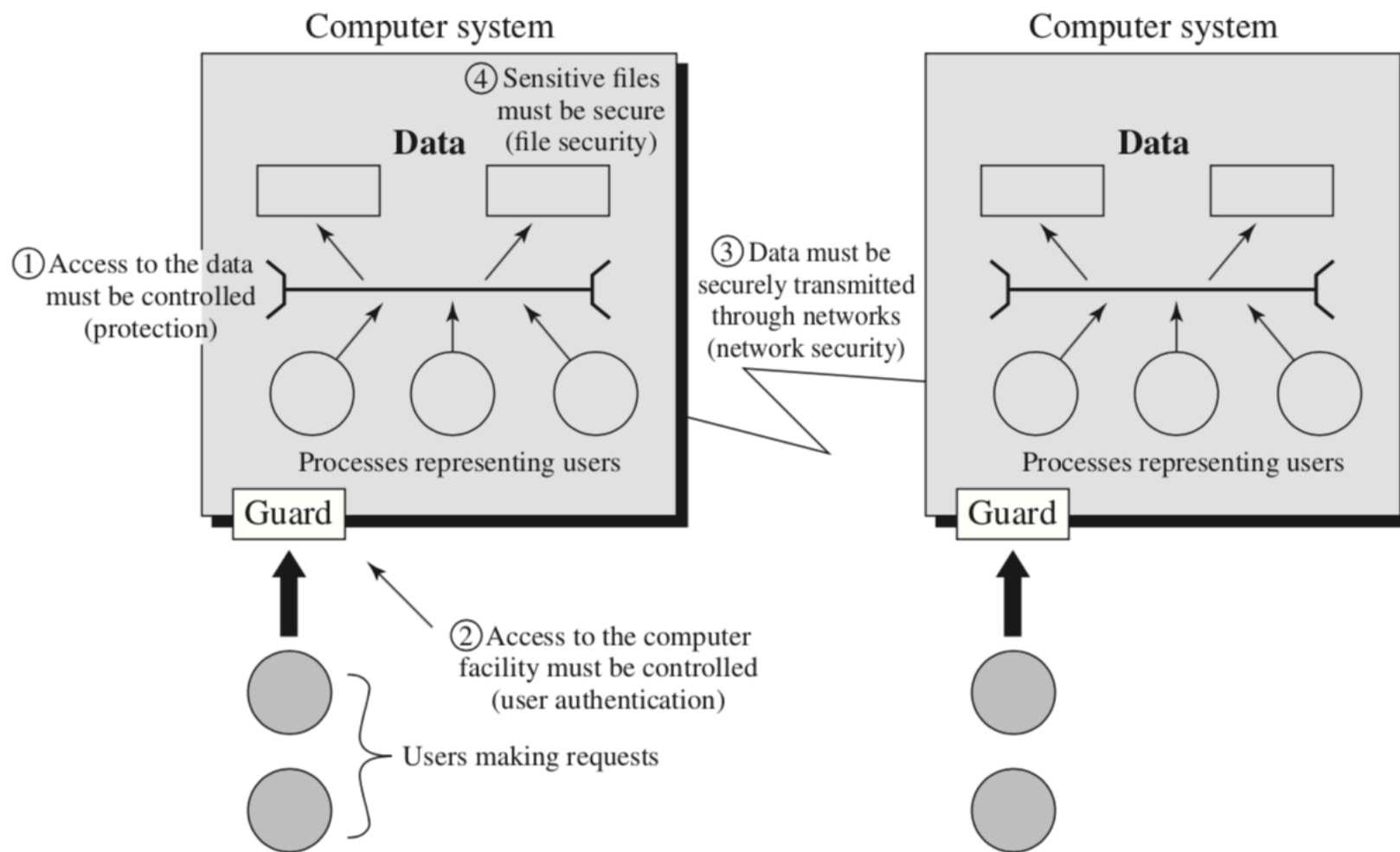


Model for Computer Security

Assets:

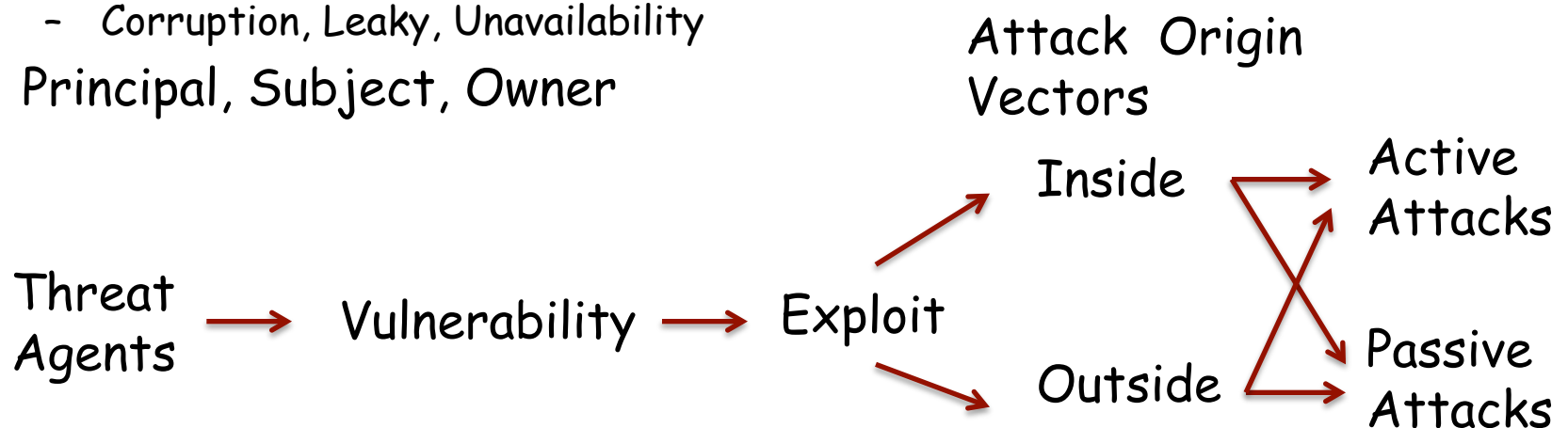
- HW
 - Computer Systems and Data Processing, Storage and Communication Devices
- SW
 - OS, System Utilities , Runtime Libraries, Applications
- Data
 - Files, Databases, Key-Value-Stores
- Communication Facilities and Networks
 - LANs, WANs, Communication Links, Bridges, Routers, ...

Scope of Computer Security



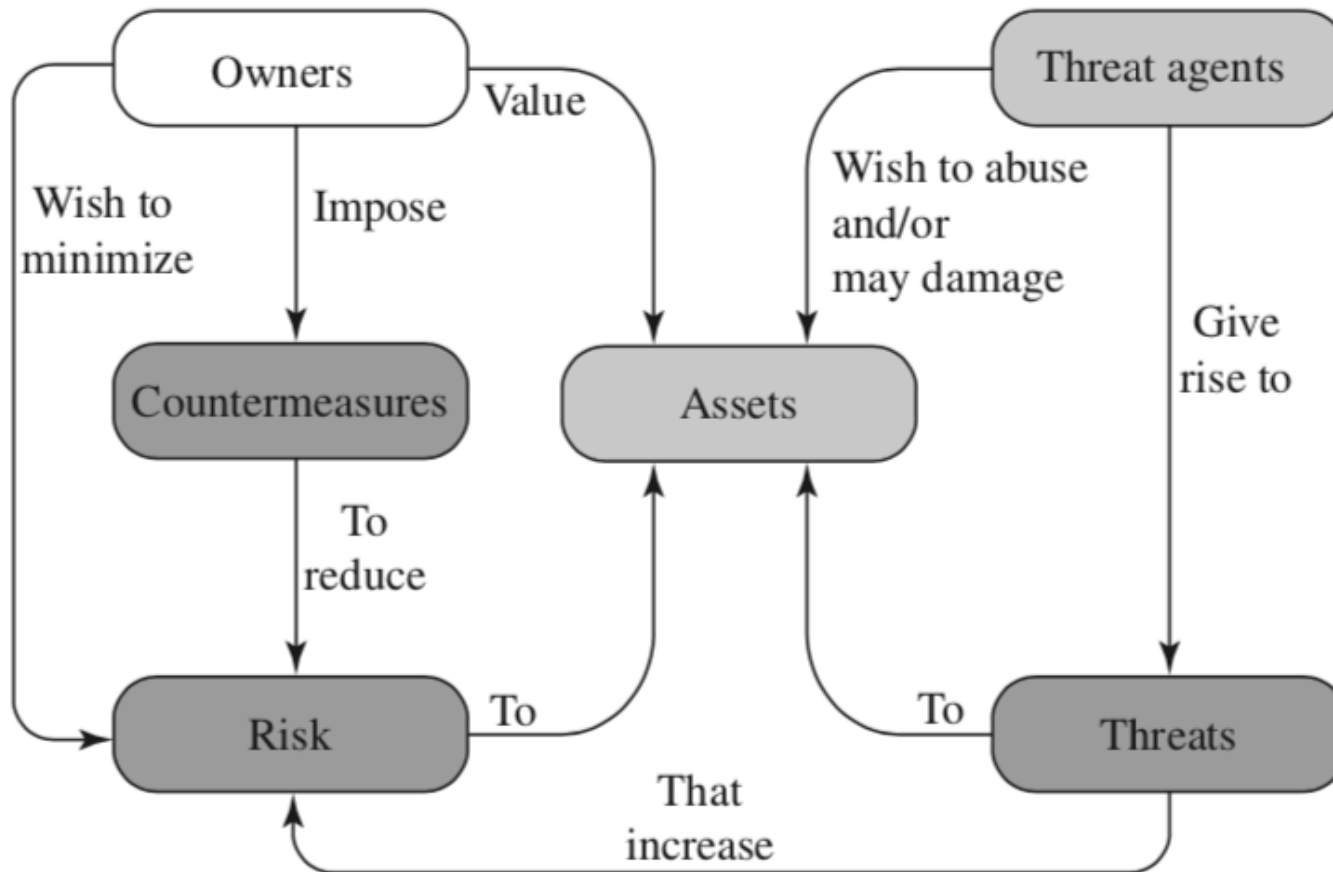
Terminology: Concepts

- Adversary, Opponent, Attacker, Threat Agents
- Attack
- Countermeasure, Security Property,
- Risk
- Security Policy
- System Resources / Assets)
- Threat
- Vulnerability
 - Corruption, Leaky, Unavailability
- Principal, Subject, Owner



Terminology: Concepts and Relationships

Ref. IETF RFC 4949, Internet Security Glossary



Threats, Attacks, Assets (IETF RFC 4949)

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

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.

Computer Security Concepts and Terminology: Other relevant concepts

Other relevant concepts

- Security Design Principles
 - Economy of mechanism • Fail-safe defaults
 - Complete mediation
 - Open design
 - Separation of privilege
 - Least privilege
 - Least common mechanism
 - Psychological acceptability
 - Isolation
 - Encapsulation
 - Modularity
 - Layering
 - Least astonishment

Other relevant concepts

- Modelling Attack Surfaces and Attack Trees
- Trade-offs in Security Policy Enforcements
 - Usability versus security
 - Cost of security versus cost of failure and recovery
- Security Implementation Solutions
 - Prevention
 - Detection
 - Response
 - Recovery

(Reactive vs. Pro-active vs. Fault & Intrusion Tolerance)

Suggested Readings

Security Objectives Challenges

Suggested Readings:

W. Stallings, L. Brown, Computer Security - Principles and Practice, Person, Chap. 1, sections 1.4 to 1.6

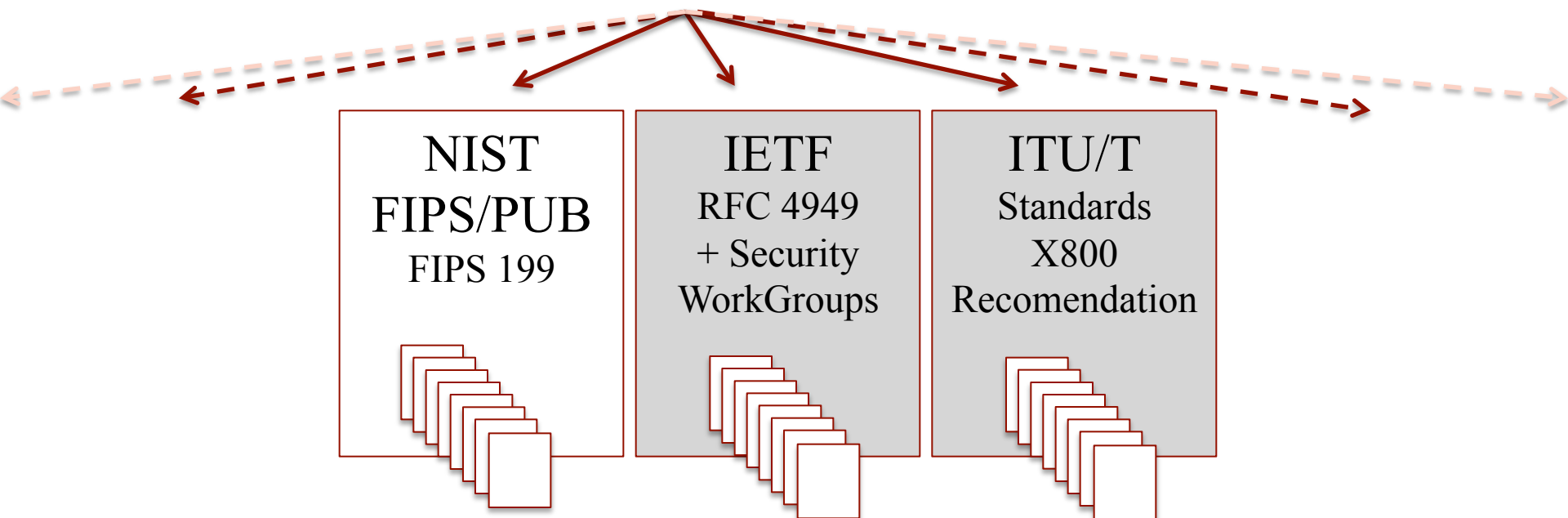


Network Security Concepts and Terminology

OSI X.800 Rec. IETF RFC 4949 + IETF Security Standards (RFC)

Network Security Objectives

Technical Security Standardization Frameworks



OSI Security Architecture

ITU-T OSI X.800 Framework

Threat

A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm. That is, a threat is a possible danger that might exploit a vulnerability.

Attack

An assault on system security that derives from an intelligent threat. That is, an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system.

OSI X.800: Attacks

- **Passive Attacks**

- Release of Message Contents
- Traffic Analysis (Sniffing)

- **Active Attacks**

- Masquerade (Message Forgery)
- Replay
- Modification of Messages (Tampering)
- DoS (Message Discarding, Message Dropping, Saturation)

OSI X.800: Security Services

- **Authentication**
 - Peer-Entity Authentication (or Principal Authentication)
 - Data Origin Authentication
- **Access Control**
 - Prevention of access to unauthorized (nor permissioned) resources
- **Data Confidentiality**
 - Connection-Oriented Confidentiality
 - Connectionless Confidentiality
 - Selective-Field Confidentiality
 - Traffic Flow Confidentiality
- **Data Integrity**
 - Connection-Integrity w/ Recovery
 - Connection-Integrity without recovery
 - Selective-Field Connection Integrity
 - Connectionless Integrity
 - Selective-Field Connectionless Integrity
- **Nonrepudiation**
 - Non-Repudiation of Origin
 - Non-Repudtaion of Destination

OSI X.800: Security Mechanisms

Specific Security Mechanisms

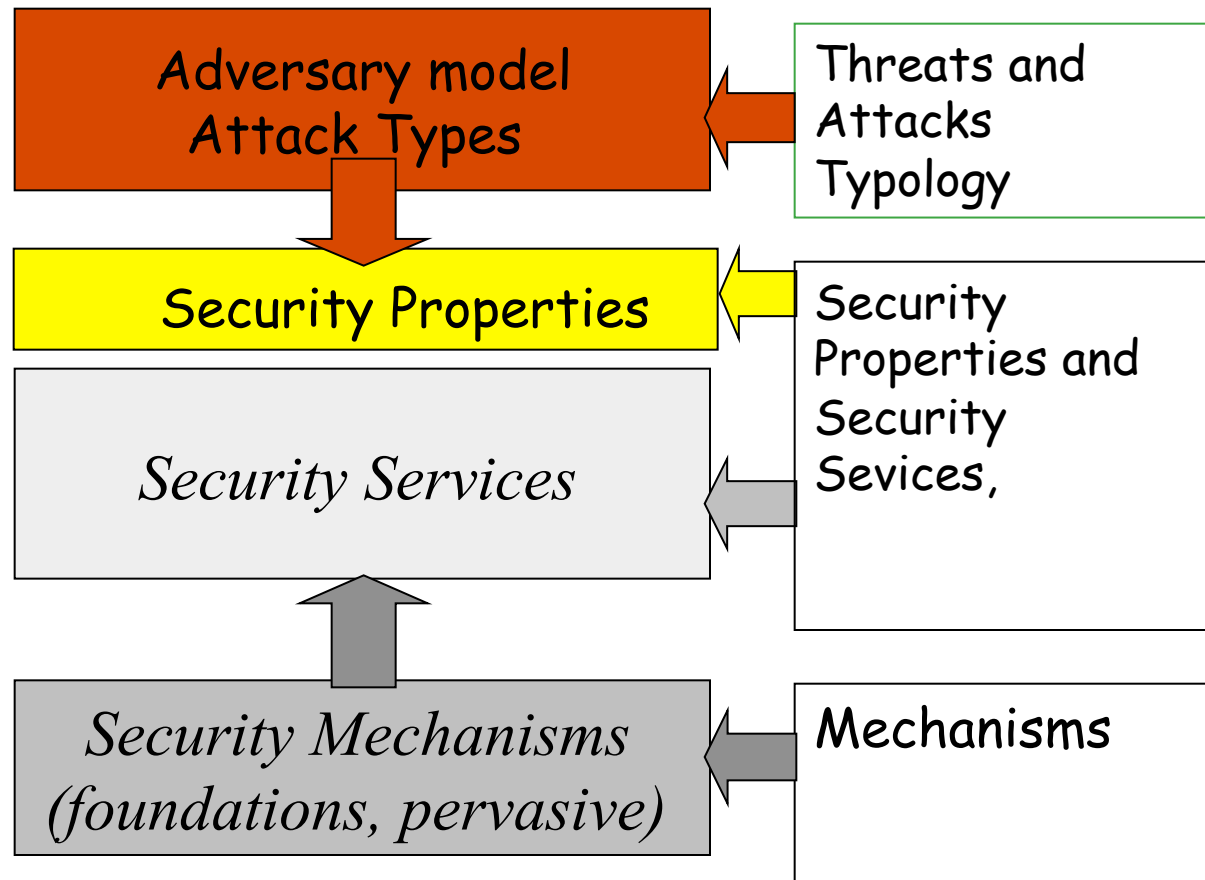
- Encipherment
- Digital Signatures
- Data Integrity
- Authentication Exchanges
- Access Control
- Traffic Padding
- Routing Control
- Notarization

Cryptographic Algorithms,
Methods and Techniques

Pervasive Security Mechanisms

- Trusted Mechanisms imposed by Security Policy Enforcement
- Security Labels for Security Attributes
- Event Detection
- Security Audit Trails
- Security Recovery

OSI X.800 mappings (in a nutshell)



Mapping Attacks vs. Security Services

Attack Typology

Security Services	Release of message contents	Traffic analysis	Masquerade	Replay	Modification of messages	Denial of service
Peer entity authentication			Y			
Data origin authentication			Y			
Access control			Y			
Confidentiality	Y					
Traffic flow confidentiality		Y				
Data integrity				Y	Y	
Non-repudiation			Y			
Availability						Y

Attacks vs. Security Mechanisms

Attack Typology

Security Mechanisms	Release of message contents	Traffic analysis	Masquerade	Replay	Modification of messages	Denial of service
Encipherment	Y					
Digital signature			Y	Y	Y	
Access control	Y	Y	Y	Y		Y
Data integrity				Y	Y	
Authentication exchange	Y		Y	Y		Y
Traffic padding		Y				
Routing control	Y	Y				Y
Notarization			Y	Y	Y	

Security services vs. Security Mechanisms

Security Mechanisms

Security Services	Encipherment	Digital signature	Access control	Data integrity	Authentication exchange	Traffic padding	Routing control	Notarization
Peer entity authentication	Y	Y			Y			
Data origin authentication	Y	Y						
Access control			Y					
Confidentiality	Y						Y	
Traffic flow confidentiality	Y					Y	Y	
Data integrity	Y	Y		Y				
Non-repudiation		Y		Y				Y
Availability				Y	Y			

Cryptographic tools as mechanisms

Authentication and Key Distribution Protocols

Service	Mechanism							
	Enciph- erment	Digital signature	Access control	Data integrity	Authenti- cation exchange	Traffic padding	Routing control	Notari- zation
Peer entity authentication					Y			
Data origin authentication								
Access control			Y					
Confidentiality							Y	
Traffic flow confidentiality						Y	Y	
Data integrity								
Non-repudiation								Y
Availability					Y			

**Symmetric
Crypto
Methods**

**Asymmetric
Crypto
Methods**

**Secure Hash
Funtions,
HMACs
or CMACs**

Big Picture (X.800 framework example)

	Release of message contents	Traffic analysis	Masquerade	Replay	Modification of messages	Denial of service
Peer entity authentication			Y			
Data origin authentication			Y			
Access control			Y			
Confidentiality	Y					
Traffic flow confidentiality		Y				
Data integrity				Y	Y	
Non-repudiation			Y			
Availability						Y

	Release of message contents	Traffic analysis	Masquerade	Replay	Modification of messages	Denial of service
Encipherment	Y					
Digital signature			Y	Y	Y	
Access control	Y	Y	Y	Y		Y
Data integrity				Y	Y	
Authentication exchange	Y		Y	Y		Y
Traffic padding		Y				
Routing control	Y	Y				Y
Notarization			Y	Y	Y	

**Cryptography methods,
Algorithms, models, techniques**

Service	Mechanism							
	Enciph-erment	Digital signature	Access control	Data integrity	Authenti-cation exchange	Traffic padding	Routing control	Notari-zation
Peer entity authentication	Y	Y			Y			
Data origin authentication	Y	Y						
Access control			Y					
Confidentiality	Y						Y	
Traffic flow confidentiality	Y					Y	Y	
Data integrity	Y	Y		Y				
Non-repudiation		Y		Y				Y
Availability				Y	Y			

Big Picture (X.800 mappings)

	Release of message contents	Traffic analysis	Masquerade	Replay	Modification of messages	Denial of service
Peer entity authentication			Y			
Data origin authentication			Y			
Access control			Y			
Confidentiality	Y					
Traffic flow confidentiality		Y				
Data integrity				Y	Y	
Non-repudiation			Y			
Availability						Y

	Release of message contents	Traffic analysis	Masquerade	Replay	Modification of messages	Denial of service
Encipherment	Y					
Digital signature			Y	Y	Y	
Access control	Y	Y	Y	Y		Y
Data integrity				Y	Y	
Authentication exchange	Y		Y	Y		Y
Traffic padding		Y				
Routing control	Y	Y				Y
Notarization			Y	Y	Y	

**Cryptography methods,
Algorithms, models, techniques**

Service	Mechanism							
	Enciph-erment	Digital signature	Access control	Data integrity	Authenti-cation exchange	Traffic padding	Routing control	Notari-zation
Peer entity authentication	Y	Y			Y			
Data origin authentication	Y	Y						
Access control			Y					
Confidentiality	Y						Y	
Traffic flow confidentiality	Y					Y	Y	
Data integrity	Y	Y		Y				
Non-repudiation		Y		Y				Y
Availability				Y	Y			

Suggested Readings

Security Objectives Challenges

Suggested Readings:

W. Stallings, Network Security Essentials - Applications and Standards, Person, Chap. 1, section 1.2-1.5, pp.24-32



Cryptosystems: Algorithms and Methods

- Foundation security mechanisms and building blocks for security services

- Encryption: data blocks, messages

- Symmetric cryptosystems
 - Stream Ciphers vs. Block ciphers

- Some asymmetric crypto systems (not all)

Confidentiality

- Digital signatures: authentication of data blocks, messages

- Asymmetric cryptosystems

Authentication

- Message authentication Codes

- Sometimes called "Lightweight" Signatures
- MACs, HMACs or CMACs

Cryptosystems: Algorithms and Methods

- Foundation security mechanisms and building blocks for security services

- Integrity protection

- Examples:

MICs, CS, CRCs, MICs, EDCs, ECCs, etc...

Weak Integrity Checks ?

- More Secure Methods for Integrity Checks:

- Cryptographic Hash Functions
- Use of Cryptographic Hash Functions in HMACs

Integrity

Big Picture (X.800 framework example)

	Release of message contents	Traffic analysis	Masquerade	Replay	Modification of messages	Denial of service
Peer entity authentication			Y			
Data origin authentication			Y			
Access control			Y			
Confidentiality	Y					
Traffic flow confidentiality		Y				
Data integrity				Y	Y	
Non-repudiation			Y			
Availability						Y

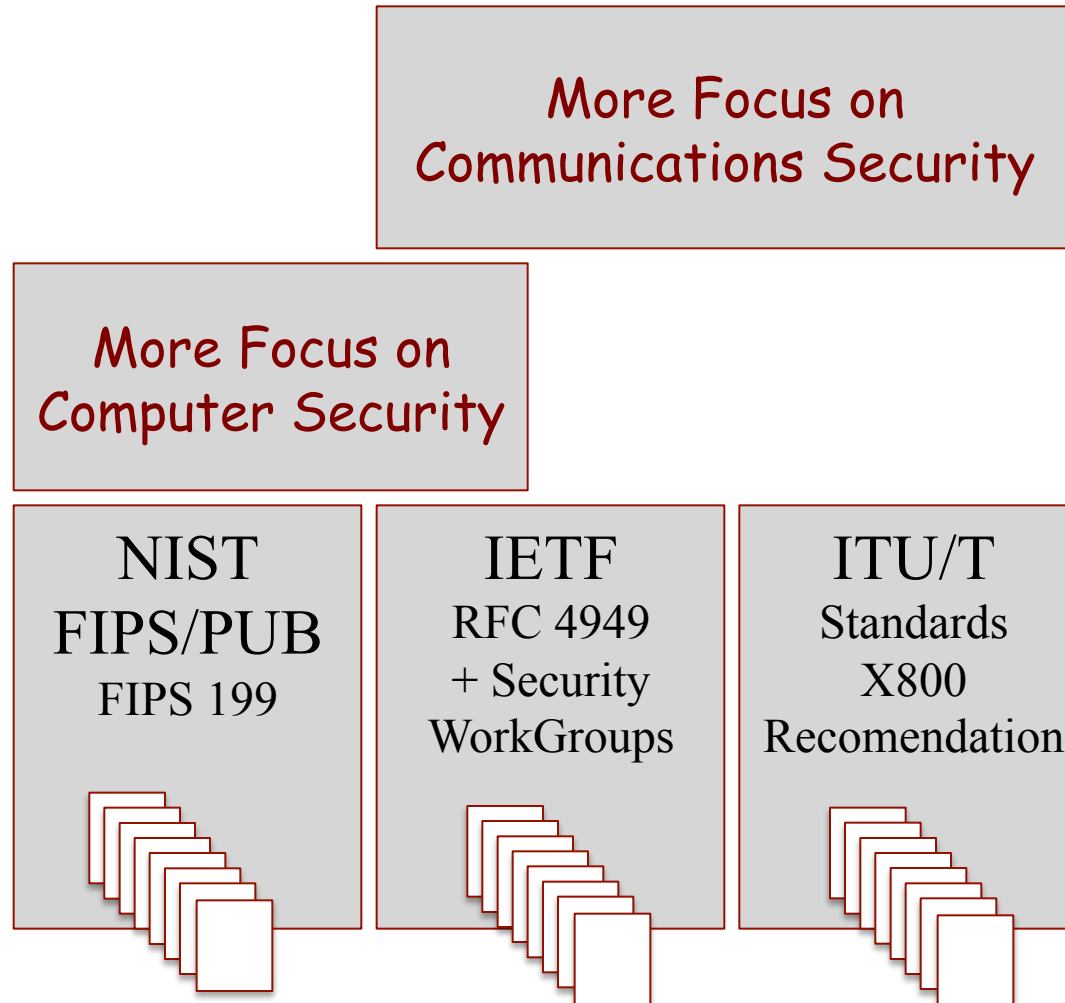
	Release of message contents	Traffic analysis	Masquerade	Replay	Modification of messages	Denial of service
Encipherment	Y					
Digital signature			Y	Y	Y	
Access control	Y	Y	Y	Y		Y
Data integrity				Y	Y	
Authentication exchange	Y		Y	Y		Y
Traffic padding		Y				
Routing control	Y	Y				Y
Notarization			Y	Y	Y	

**Cryptography methods,
Algorithms, models, techniques**

Service	Mechanism							
	Encipherment	Digital signature	Access control	Data integrity	Authentication exchange	Traffic padding	Routing control	Notarization
Peer entity authentication	Y	Y			Y			
Data origin authentication	Y	Y						
Access control			Y					
Confidentiality	Y						Y	
Traffic flow confidentiality	Y					Y	Y	
Data integrity	Y	Y		Y				
Non-repudiation		Y		Y				Y
Availability				Y	Y			

Summary

Technical Security Standardization Frameworks



- Revision of all Suggested Readings

Revision: Suggested Readings

Security Objectives and Challenges

Suggested Readings:

W. Stallings, L. Brown, Computer Security - Principles and Practice, Person, Chap. 1

W. Stallings, Network Security Essentials - Applications and Standards, Chap 1



Additional suggested reading (Port. Language)

- Targets of Defense
- Vulnerability vs. Risk Management Issues
- Typology of Defenses in CSNS
- Perimeter vs. "in Deep" Defenses
- Security Policy Enforcement
- Types of Security Mechanisms
- Distributed Systems Security Principles and Risks



Suggested Reading (Portuguese Language):

A. Zúquete, *Segurança em Redes Informáticas*, Cap. 1 - Introdução (pp 11-16), FCA, 5ª Ed., 2018