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, 2020/2021

1. Introduction (Part II)

Part II – Complementary Concepts and Notions

Last Lecture … (Introduction, Part I)
Preliminary concrpts and terminology …

- How to define a Secure System and Its Security Properties and Dimensions (Network vs. Systems Security)
- Computer Security Strategy and Security Policies
- Important concepts, notions and terminology …
  - Security vs. Risk vs. Vulnerability
  - Threats vs. Attacks vs. Incidents
  - Passive Attacks vs. Active Attacks
  - Insider Attacks vs. Outsider Attacks
  - Owners/Subjects, Risk, Countermeasures, Asset, Threats and Threat Agents: relation between these notions
  - Attacks Typology
  - Notion of "Principal" (or Subject)
  - Attack Surface and Attack Trees
  - Adversary (or Threat) Model Definition
  - Trust Computing Base

- W. Stallings, L. Brown, Computer Security – Principles and Practice, Person, Ch.1 (§ 1.1- § 1.3)
- W. Stallings, Network Security Essentials – Applications and Standards, Ch.1 (§ 1.1- § 1.6)

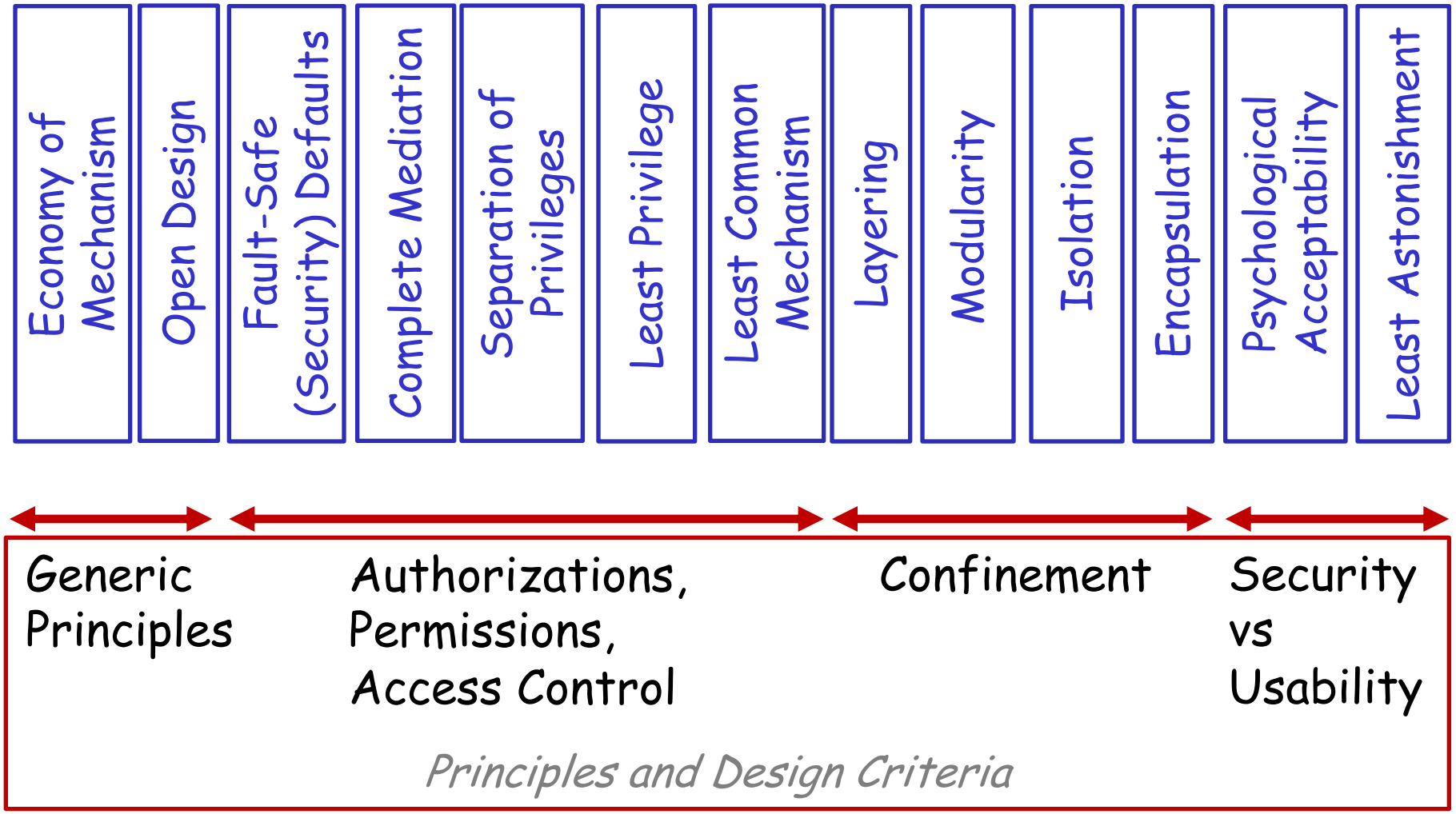
Today … (Introduction, Part II)
More relevant concepts and notions

Topics today :

- Fundamental Security Design Principles
- Differences between Security, Safety and Privacy, Trust/Trustworthiness and Dependability
- CNS (a.k.a, DS) Security Model
- Anatomy of Attacks against Computer Systems
- Security Frameworks and Standards
  - ISO 27001, NIST / FIPS PUB, OSI X.800
  - OSI X.800 definitions: Attack Typology, Security Properties, Security Services and Security Mechamisms
- How to define a Secure Channel
- Role of Cryptgraphic Tools, Alg., and Techniques
- TCP/IP security stack: security protocols and standards

Fundamental Security Design Principles and Choice of Mechanisms

Fundamental Security Design Principles



Fundamental Security Design Principles (1)

- **Principle of Economy of Mechanism**
  - Keep it Small as possible, Keep it Simple, Keep it Verifiable/Auditable, Keep It Maintenable, avoid unacessary complexity, Keep it Parameterizable, Keep it Replaceable
- **Principle of Fault Safe Defaults**
  - Access decisions based on explicit permissions rather that on exclusions
  - For more security: what is not explicitly authorized is forbiden
- **Principle of Complete Mediation**
  - Well-controlled, coordinated and synchronized acces control policies entirely mediated by trustable access control component/service (reference monitor)
  - No indirect authorizations and incorrect delegation control, examples: uncontrolled caches, uncontrolled copies of authorizations

Fundamental Security Design Principles (2)

- **Principle of Open Design**
  - Open rather than Secret: No security by obscurity
  - Ex., open/auditable sofrware for white-box based analysis, reputable and secure cryptographic algorithms

- **Principle of Separation of Privileges**
  - Multiple privilege attributed defined to achieve access to restricted resources
  - Appropriate access-control granularoty of protected resources (ex., file system resources with separated permisisons based on specific operations
  - Avoidance of policies defines in a "all or nothing" base
  - Another example: multifactor authentication and degress of permissions based on progressive authentication factors as proofs
  - Avoindance of escalation of privileges based on the same access control and authentication factors

Fundamental Security Design Principles (3)

- **Principle of Least Privilege**
  - Every process and every user should perform under the least set of privileges necessary to operate
  - Ex., a user with a specific role, can only use the minimal operatons and access the minimcal resources to perform her/his specific tasks
  - Ex., a web server (ex., apache) must execute with low privileges and can only access to resources (files, documents) with the minimal read privileges for its purpose
- **Principle of Least Common Mechanism**
  - Design should minimize functions and resources shared by different entities
- **Principle of Psychological Acceptability (Usability)**
  - No interference unduly with users' work and poductivity
  - Users' adherence to system security is a very important factor ... otherwise the most certain thing is that it will be reversed

Fundamental Security Design Principles (4)

- **Principle of Isolation**
  - Isolation of critical resources, critical processing to assure its integrity
  - Isolation can be address at different levels and different approaches:
    - Logical and Sofware Componentization (language-based)
    - Logical organization of isolated services (Rest-Servers, WebServices, Architectures of Micro-Services, …)
    - Isolation between storage and processing
    - Logical Language based runtime virtulalization (Ex., JVM, CLR)
    - Logical Containerization (ex., dockered components)
    - Logical OS-based virtualization by Hypervisors (Guest isolated VMs)
    - Physical-Isolation (inside a Computer Platform) of Trusted HW Execution Environmets
    - Physical isolartion with specialized HW devices (ex., HW Crypto Modules)
    - Physical Isolation (with multiple Computer Platforms segregated in Data Centers and isolated by Intrusion Prevention Systems)
    - Sometimes, some authors also refer: vertical vs. horizontal virtualization solustions

Fundamental Security Design Principles (5)

- **Principle of Encapsulation**
  - Specific form of isolation (language-based: isolated components and objects in OO-Languages or Component-Composition Languages (ex., Objects/Classes with Private Resources …)
- **Principle of Modularity**
  - Use of separate security services or functions as separated modules
  - Use of common and (well-known/verified) trustable security modules
- **Principle of Layering**
  - Multiple and overlapping of multiple and independent protection approaches for security enforcements
  - Ex., Multi-factor authentication (that can include different SW and HW factors and devices)
  - Ex., Onion-Encryption using the same crypto algorithm with different keys, or using different algorithms with different keys
  - Ex., Onion-Routing and forms of encapsulation of security channels as inner payloads of other outer security channels

Fundamental Security Design Principles (6)

- **Principle of Least Astonishment**
  - The behaviour of componets must be consistent, responding or used always in the same way and without user's disturbance and not astonishing the users

Choice of base mechanisms (1)

- **Confinment Mechanisms** (isolation, sandboxing, modularization, encapsulation of resources and execution environments)
- **Access-Control Mechanisms** (complete mediation, separation of provileges, least-privilege, least-common access)
  - Access control to resources
  - Privileged execution
- **Filtering mechanisms** (forms of primary confinment and access-control, for example permimiter defenses
- **Registration and logging mechanisms** (event-logging)
- **Inspection mechanisms** (Operation Analysis, Vulnerability Assessment, Functions of SIEM Platforms, etc)

Choice of base mechanisms (2)

- **Auditing mechanisms** (Log/Forensic Analysis Tools
- **Cryptography** and Related Mechanisms and Techniques (as Specific Mechanisms)
- **Cryptographic Protocols** (Protocolos using Criptographic Primitives and Constructions for the Implementation of Secure Communication Channels
  - Different approach levels: Phisical/Data-Link/Network Level/Transport Level/Application-Level)

Security, Safety, Privacy,Trust and Dependability

Security vs Safety vs. Privacy
(Closely related terms but … inherent differences)

- **Security: Protection from malocious activities**
  - prevention of malicious activities by attack agents (attackers, adversaries, opponents, malicious users)
- **Safety: Sate of being safe**
  - Protection of correct users (principals), prevention of accidents (accidents which may or may not involve human agents, but are in any case not intentional).
    - Avoidance of equipment, computers, processes, situations of use, from inherent dangers/chances of being hurt, safe from injuries
- **Privacy**
  - Privacy is the ability of an individual or group (as principals) to seclude themselves or information (and even more … their computations) revealing about themselves, and thereby express themselves selectively (require different security properties under the control of principals owning the involved resources or computations)

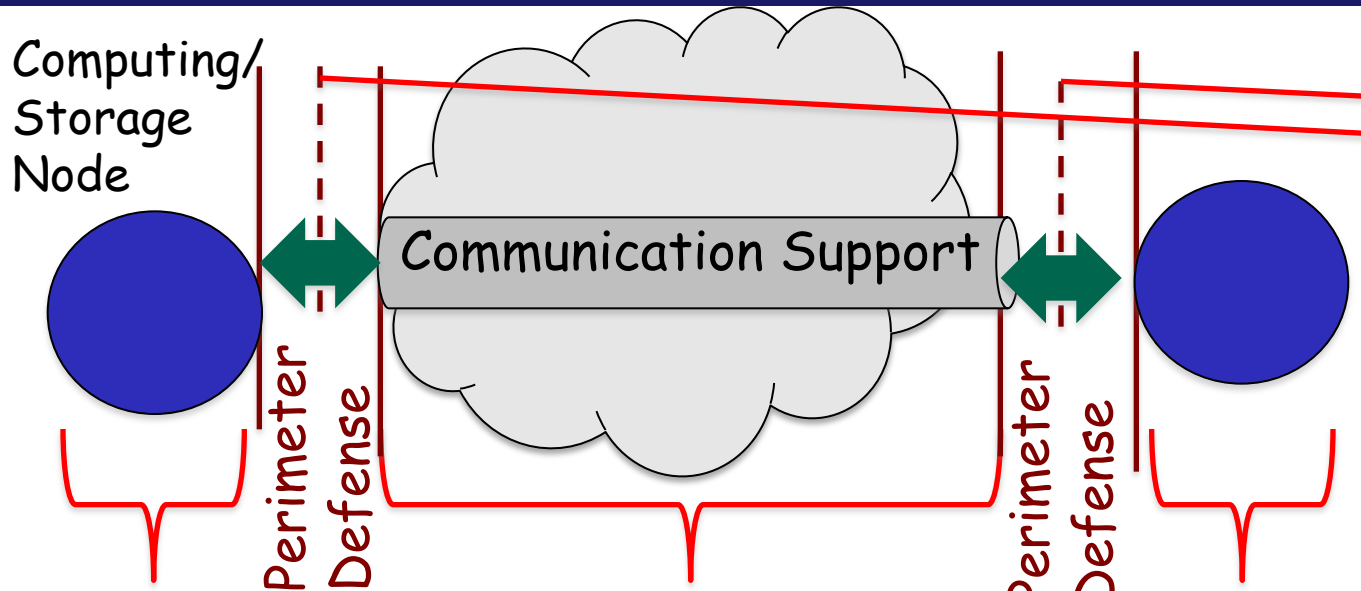
Security vs Safety vs. Privacy
(Closely related terms but … inherent differences)

- **Trust, Trustworthiness and Trustworthy Computing**
  - Trust: firm belief of reliability, truth, correct behaviour of someone or something, to perform correctly as expected …
  - Trustworthiness the property of being trust
  - Trustworthy Computing (**TwC**): a term that has been applied to computing systems that are inherently secure available and reliable
- **Dependability**
  - A property of someone or something from who/what/which we can depend
  - Dependable system or component: a system of component from which we can depend for trust
  - Dependable solution: a solution that inherently is **reliable, secure and trust**

Computer Networks and Systems Security Model

(*a.k.a*: Distributed Systems Security Model)

Distributed Systems Security Dimensions



Perimeter Defense:

(Switches,

Routers

IPSs:

- FWs,

IDSs:

- NIDS
- HIDS

Communications Security
(Traffic, Data Flows, Message-Exchange) and Communication Endpoints

Computer Systems Security
(Applications and SW Processing/Execution, Data Management, MW Services. OS Resources and FW/HW Devices

Network Access Security Model

Opponent

— human (e.g., hacker)

— software (e.g., virus, worm)

Access Channel

Gatekeeper function

Information System

Computing resources (processor, memory, I/O)

Data

Processes

Software

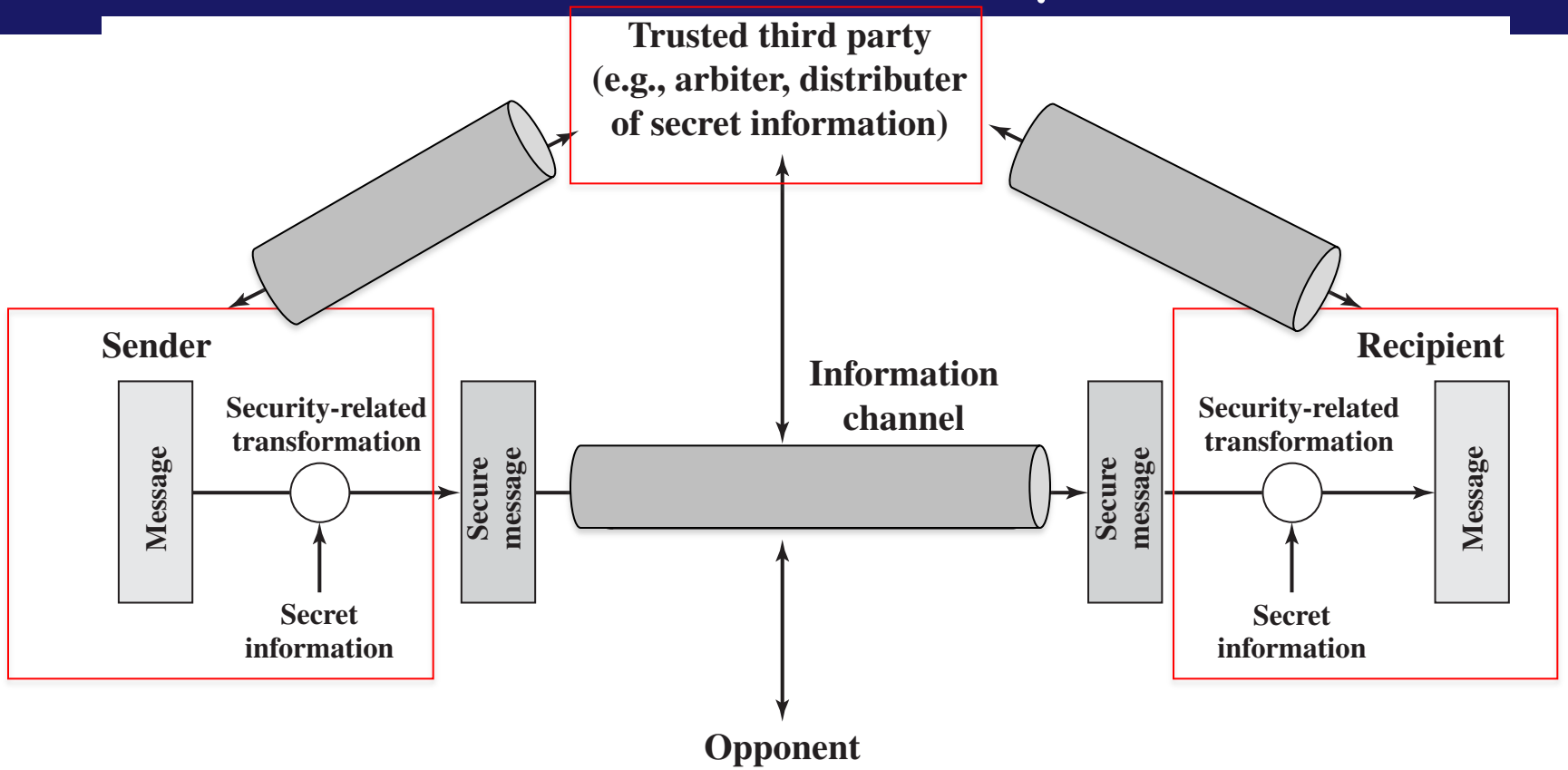
Internal security controls

IDS Intrusion Prevention
IPS Intrusion Detection

Node Perimeter Defence
(Intrusion Prevention)

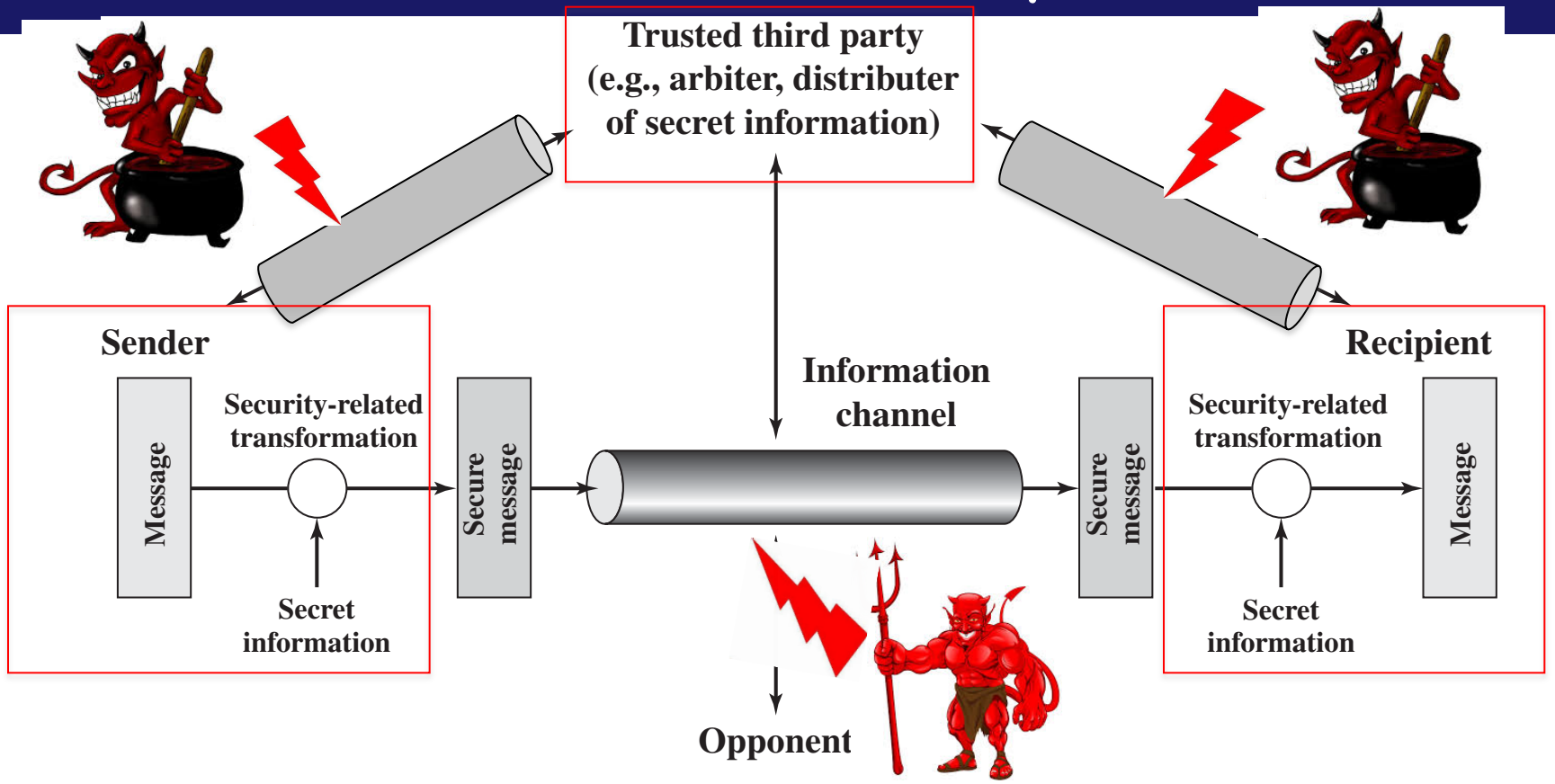
Packet Filtering + FWs, App. GWs + Traffic Shapers + IDSs

Model for Network Security



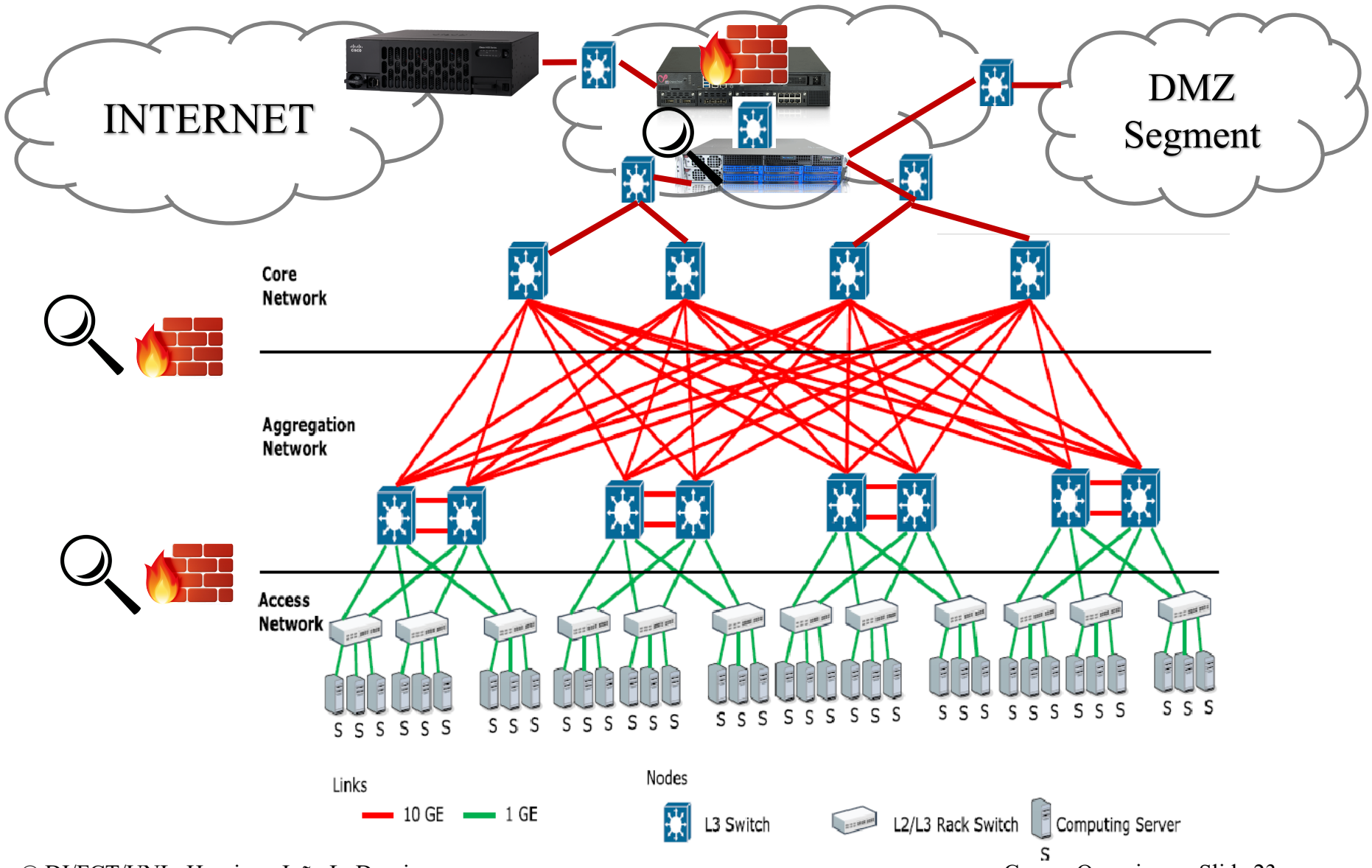
Problem:
How to establish **secure communication channels**
How to design and implement security services
(**security protocols**) to protect the communications

Model for Network Security

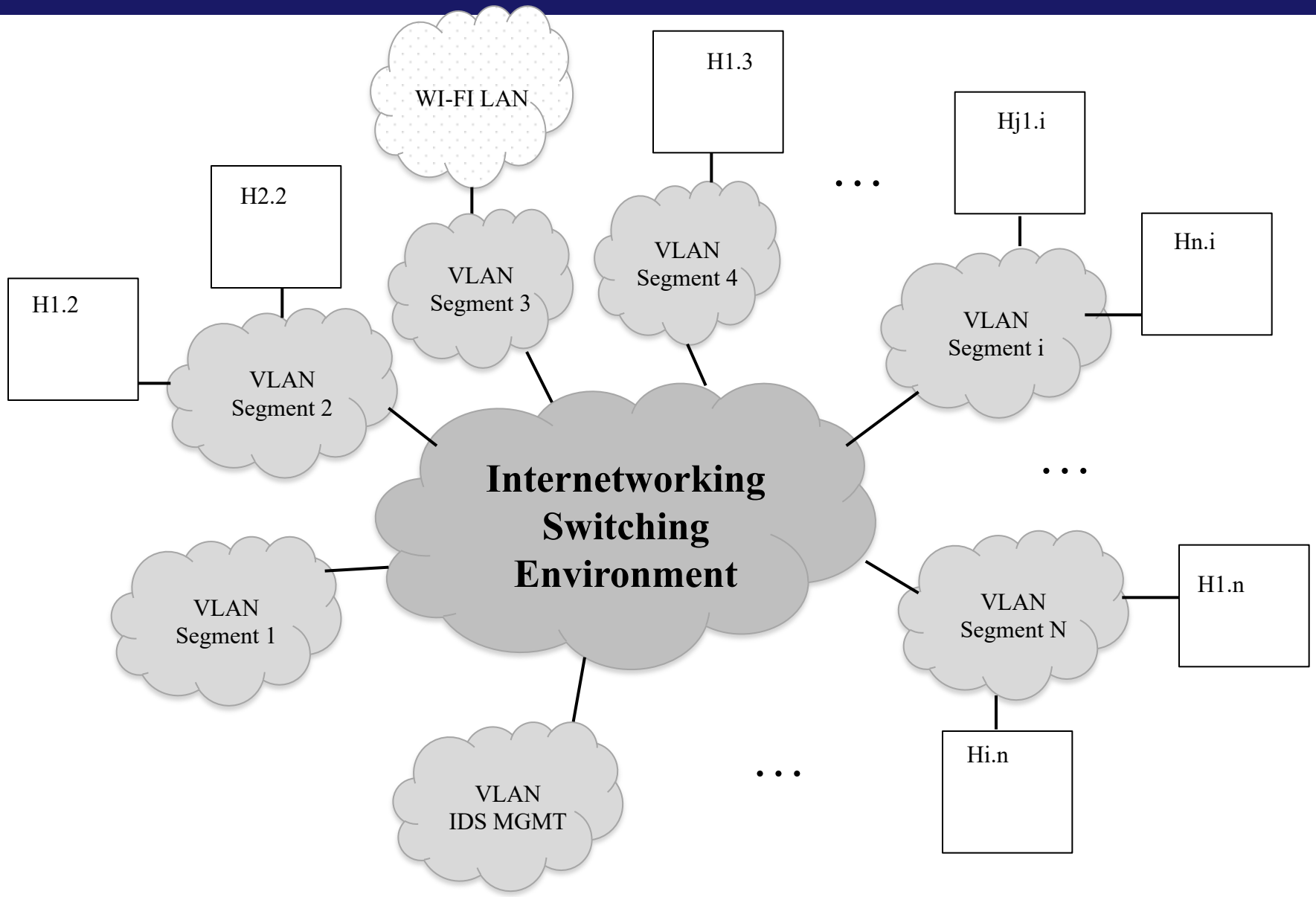


Initial Hypothesis (simple approach/analysis):
Trusted Nodes: Senders, Receivers and TTPs
(Out of the adversary model hypothesis)
What does this means ? Ex., Crypto WORKS FINE !

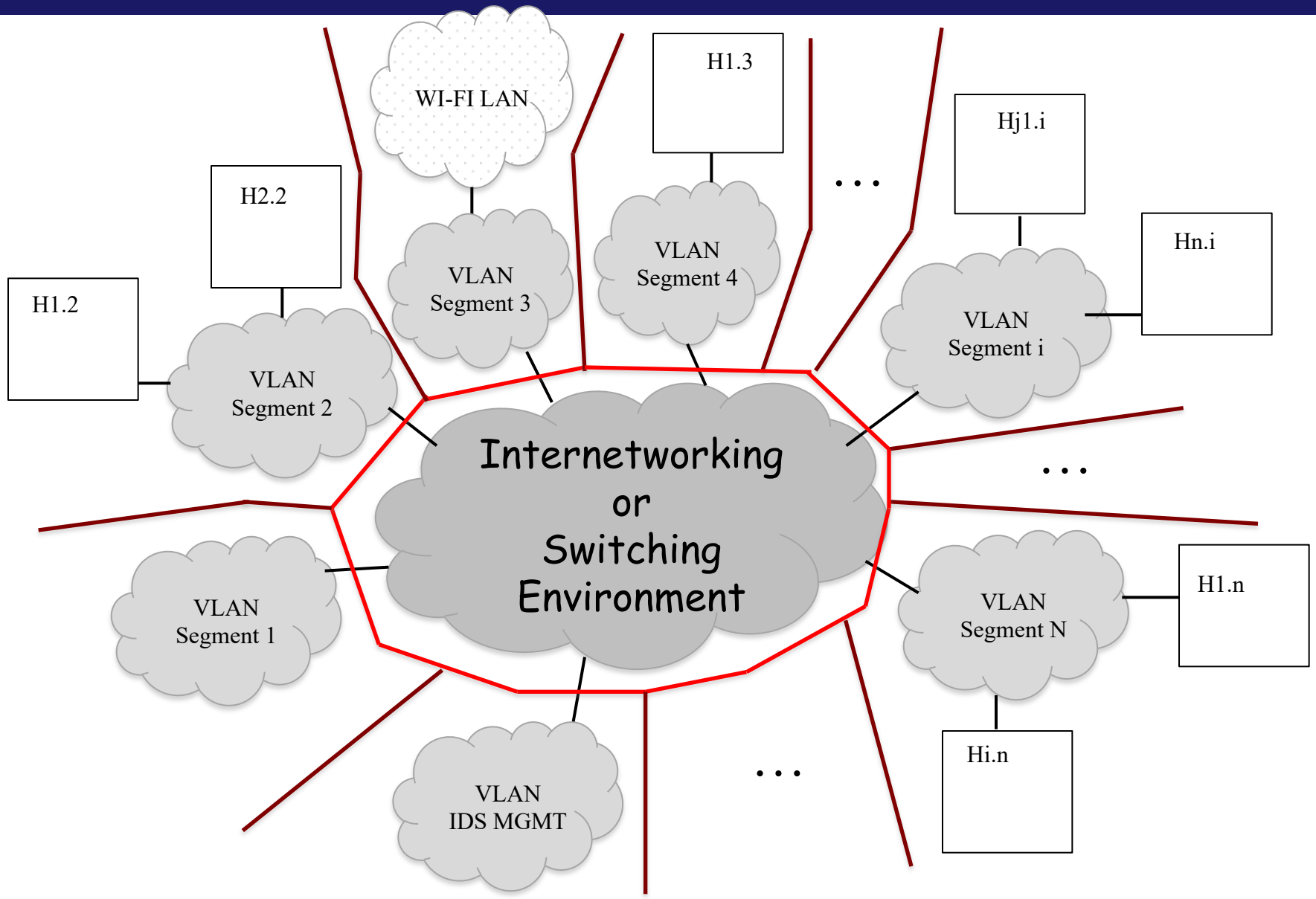
Network Perimeters (ex.: Datacenter)



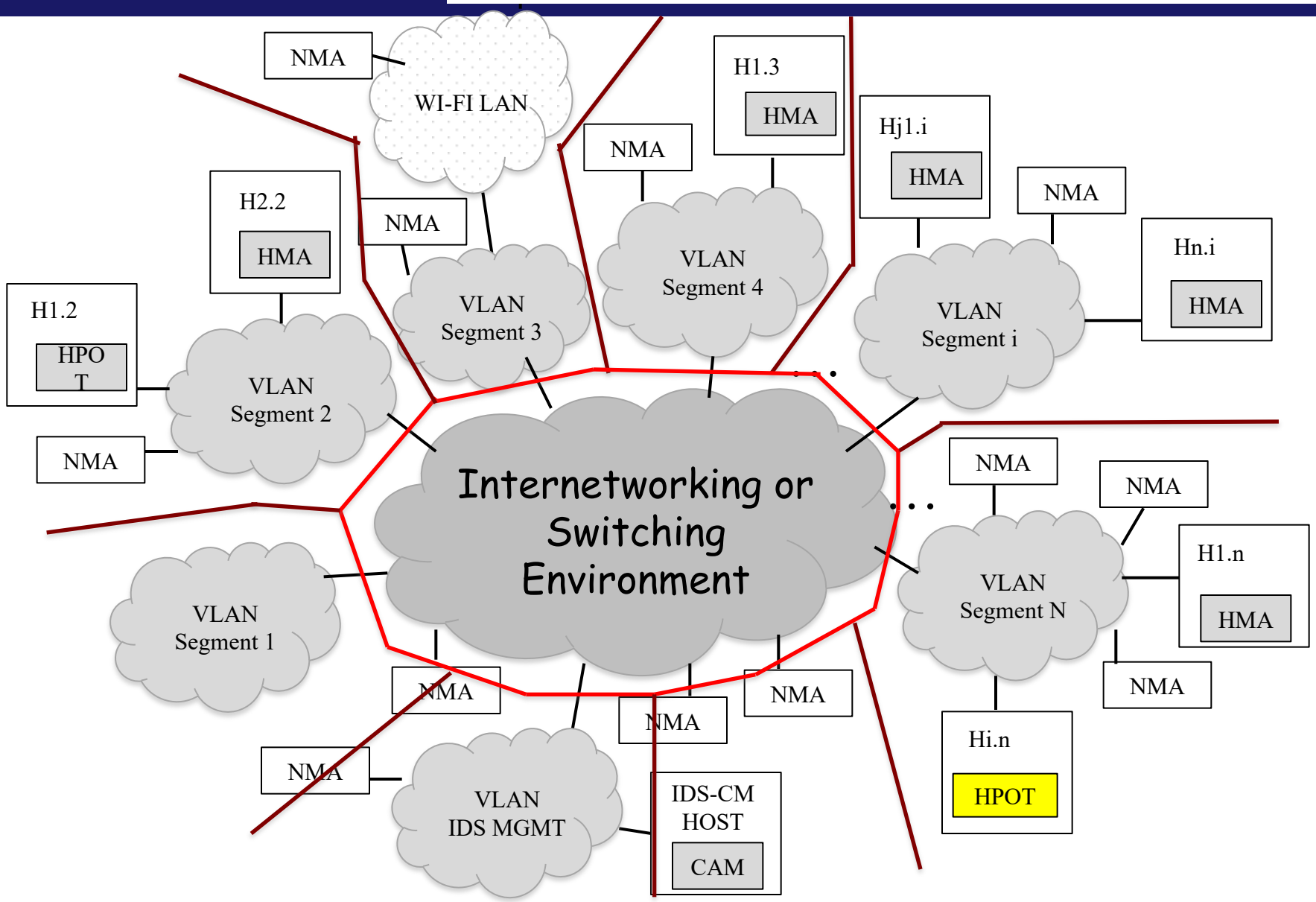
Internetworking Topology



Network Perimeters: Segmentation and Segregation



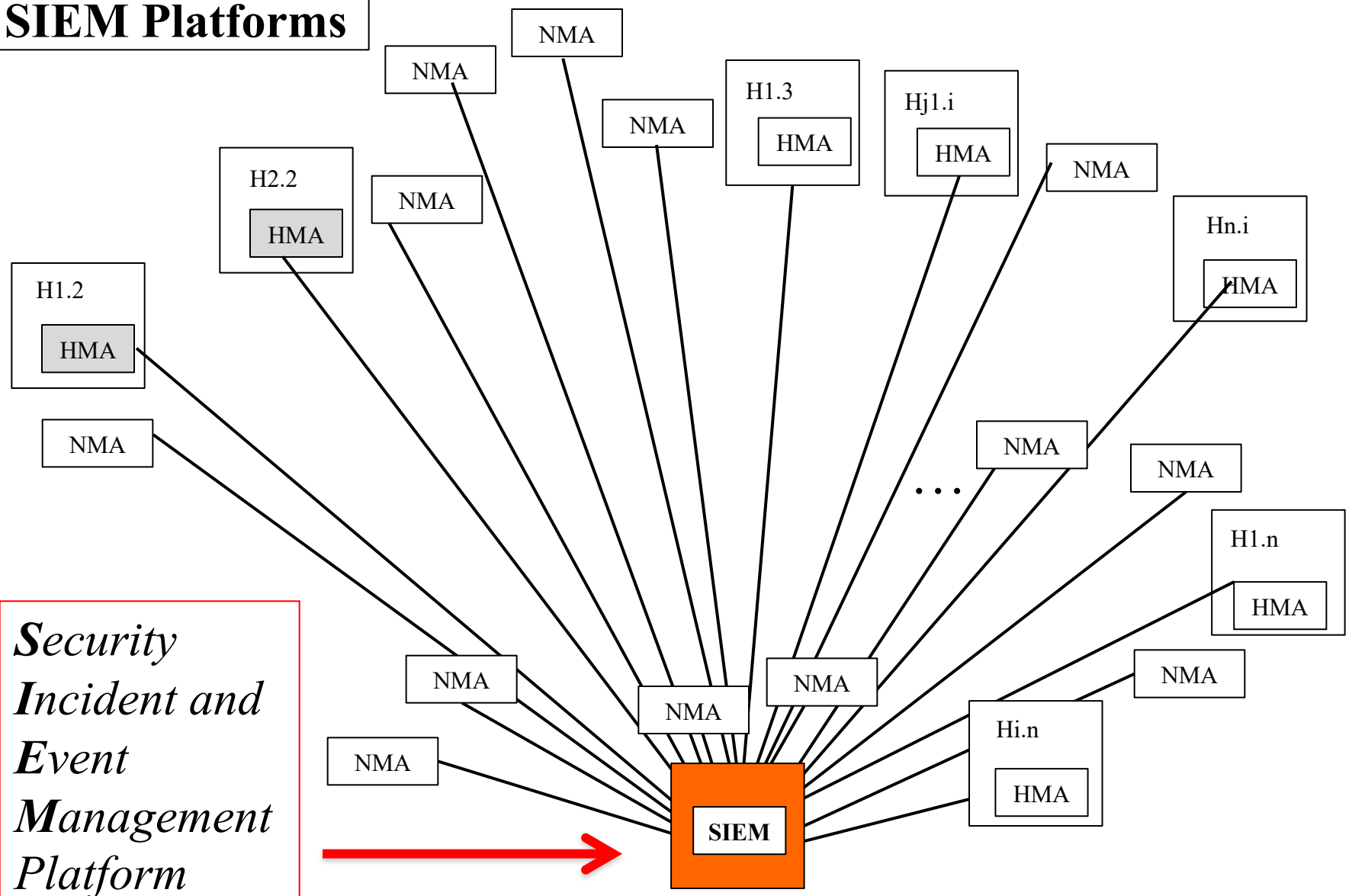
Distributed Hybrid Intrusion Detection: Honeypots, NIDS, HIDS w/ NMAs and HMAs (



SIEM

Distributed Hybrid Intrusion Detection: Honeypots, NIDS, HIDS w/ NMAs and HMAs (

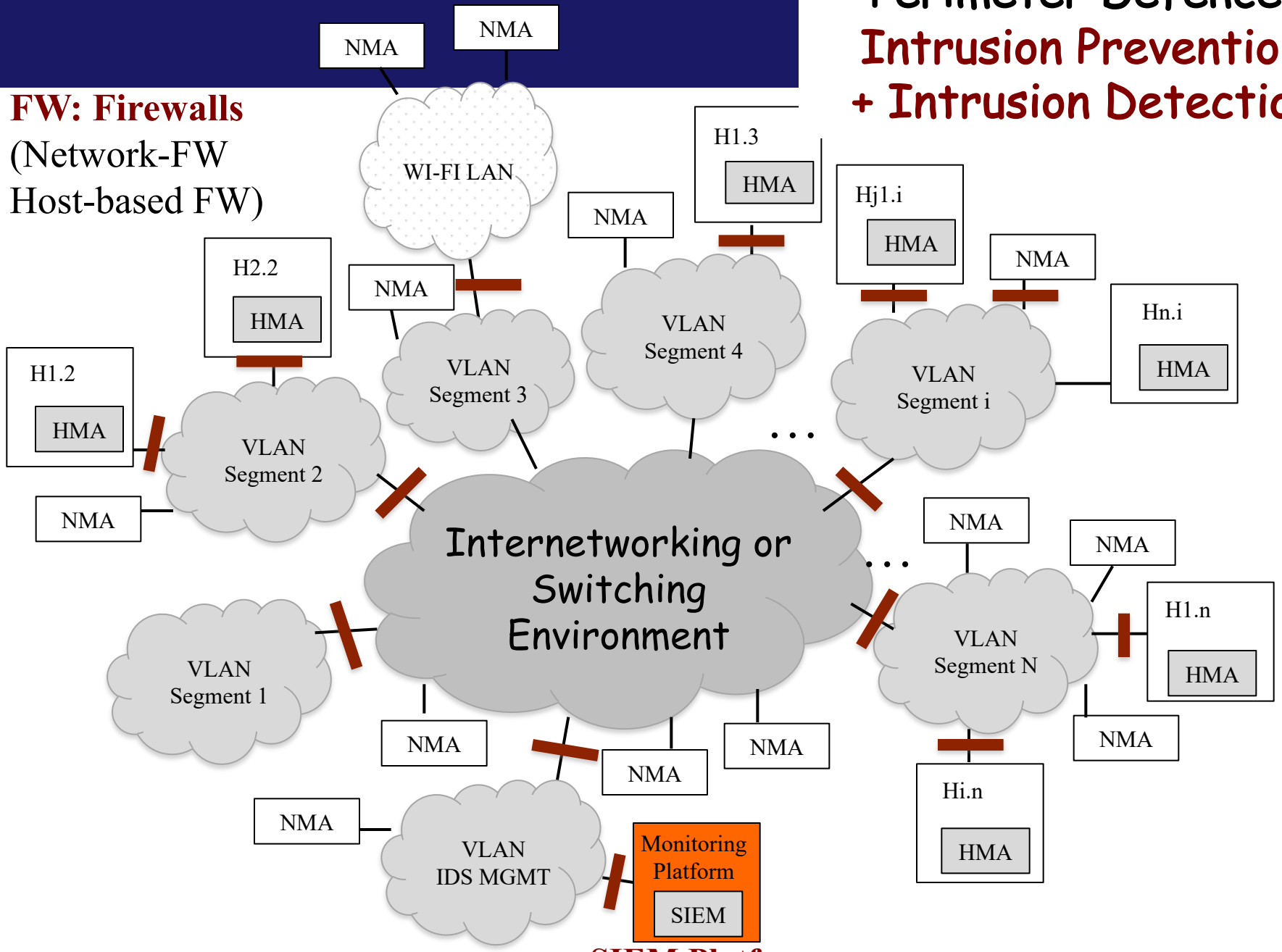
SIEM Platforms



Security Incident and Event Management Platform

Perimeter Defences:
Intrusion Prevention + Intrusion Detection

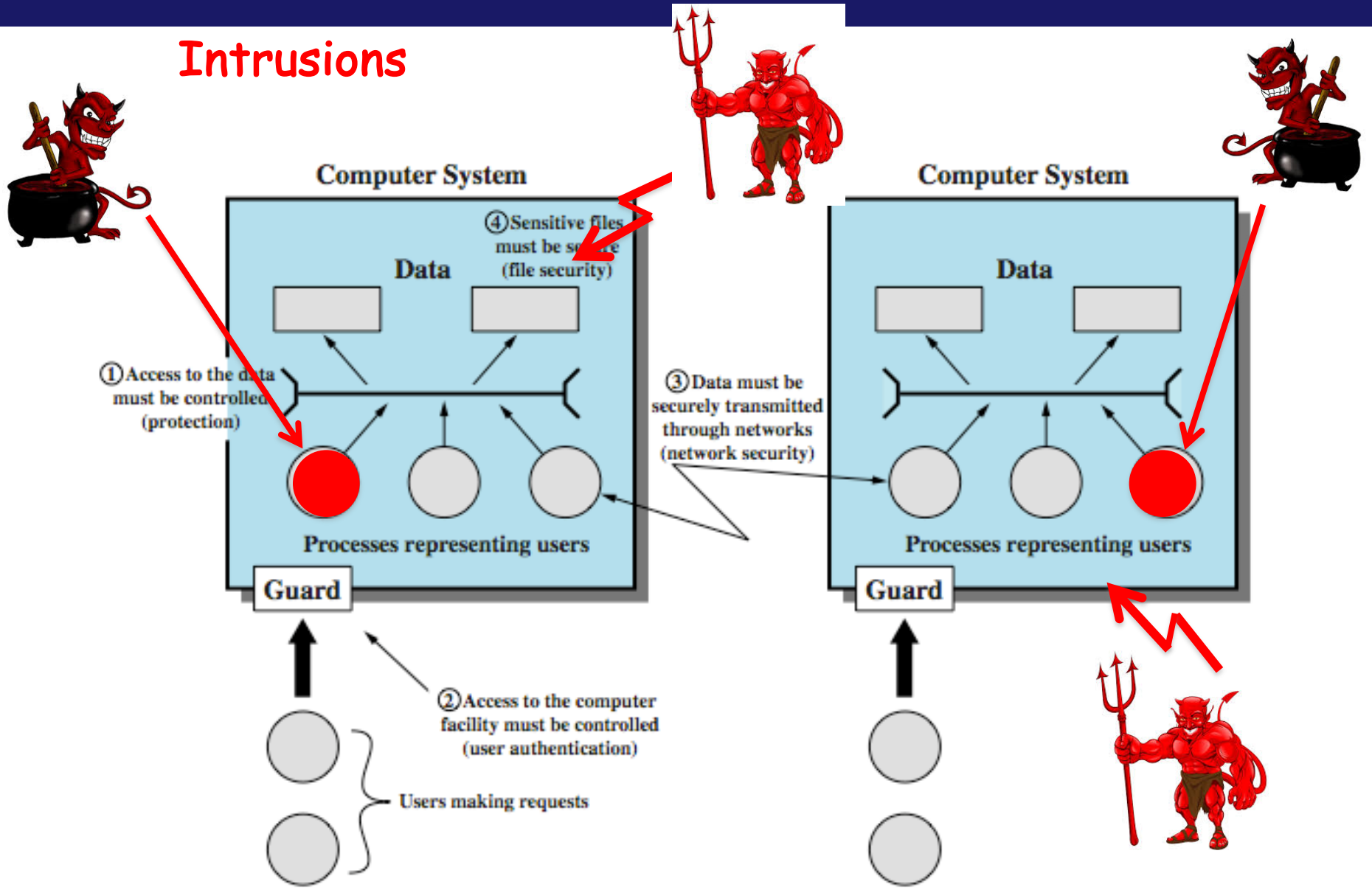
FW: Firewalls
(Network-FW
Host-based FW)



SIEM Platform

Computer Systems Security

Intrusions



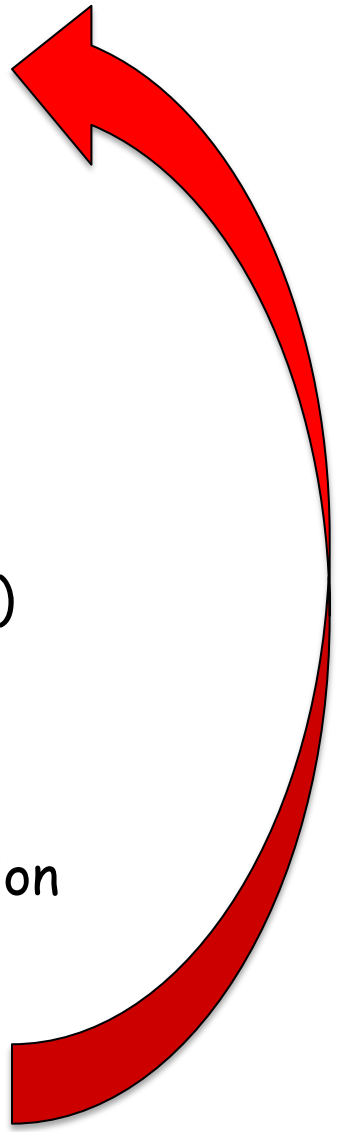
Typical anatomy of attacks

Pre-Attack Phase

1. Information
2. Enumeration
   - Enumeration / Scanning Tools
3. Vulnerability Identification / Checking
   - Vulnerability checkers
4. Exploit
   - Vulnerability Exploiters (outside exploiting attacks)

Attack/Penetration Phase

5. Penetration / Intrusion
   - Insider (In-deep) exploiting attacks
6. Data leakage/corruption and/or Malicious Code Injection (Active vs. Passive Attacks)
7. Maintenance of intrusion/illicit access/use
8. Base for new launching attacks



Anatomy of attacks vs. Tools (examples)

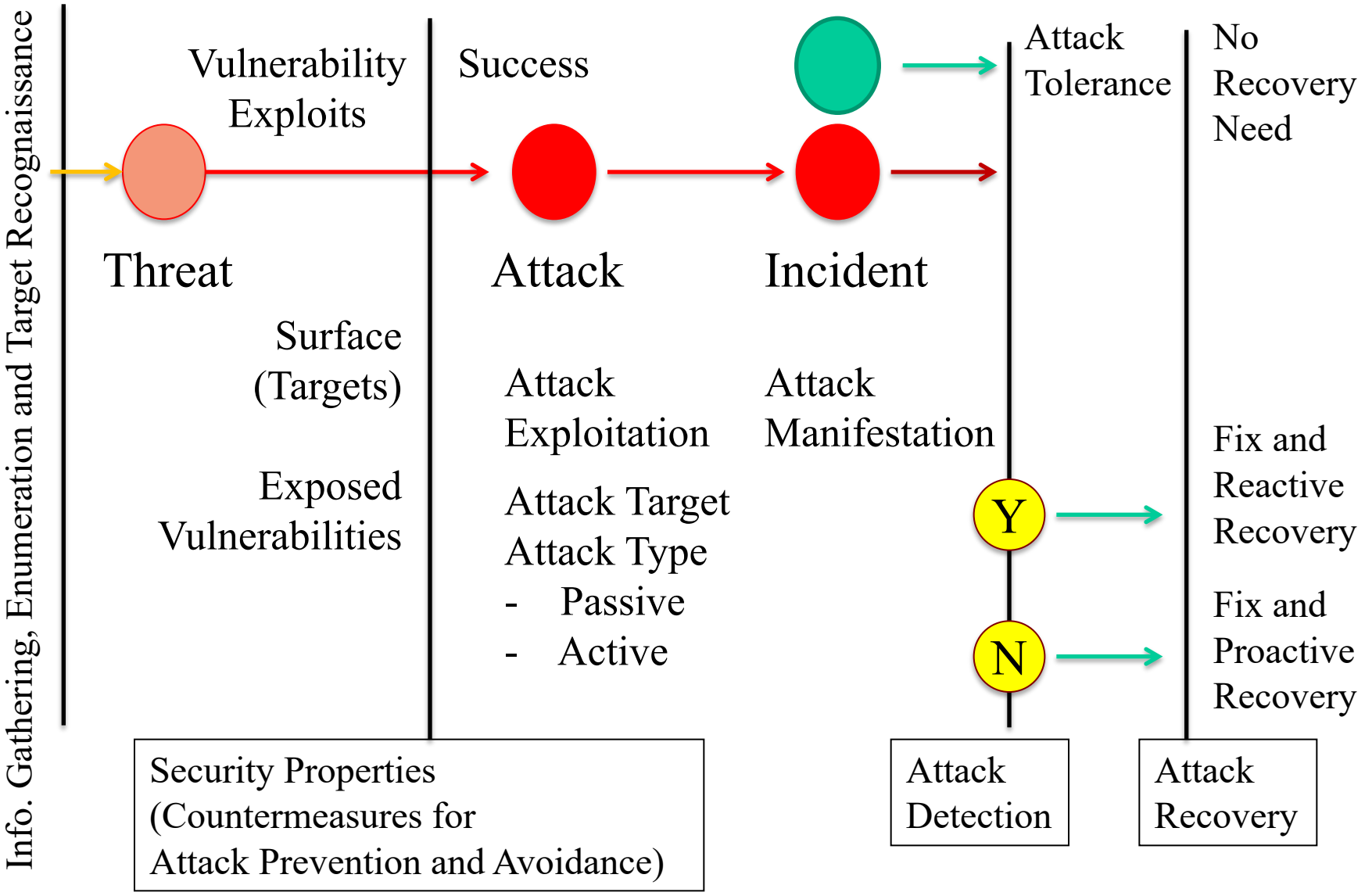
1. Information — **Ex: google searches, whois, dig, nslookup, traceroute**
2. Enumeration — **Ex: nmap & zenmap ettercap, tcpdump, wireshark, AircrackNG, … Nagios**
3. Vulnerability Identification / Checking — **Ex: https://www.owasp.org/index.php/Category:Vulnerability_Scanning_Tools https://resources.infosecinstitute.com/14-popular-web-application-vulnerability-scanners/**
4. Exploit — **Ex: Metasploit, OpenVAS, Maltego, HCONstf, John the Ripper, Caim&Abel, etc., … Ex: arpspoofer, netsparker, accunnetix, core, Hackerone, ZAP, Intruder, Indusface, BreachLock**
5. Penetration / Intrusion — **RATA, W3af, Kali-Based Tools, Nessus, Portswegger, Retina, SQLmap, SQL Ninja, CANVAS,WebscarabNG BeEF,Dradly, Probely, Spyse, SET Toolkit, etc, ...**
6. Data leakage/corruption — **https://blackarch.org/exploitation.html http://www.pentest-standard.org/index.php/PTES_Technical_Guidelines https://pentestbox.org/**

Code Injection (Active vs. Passive Attacks)

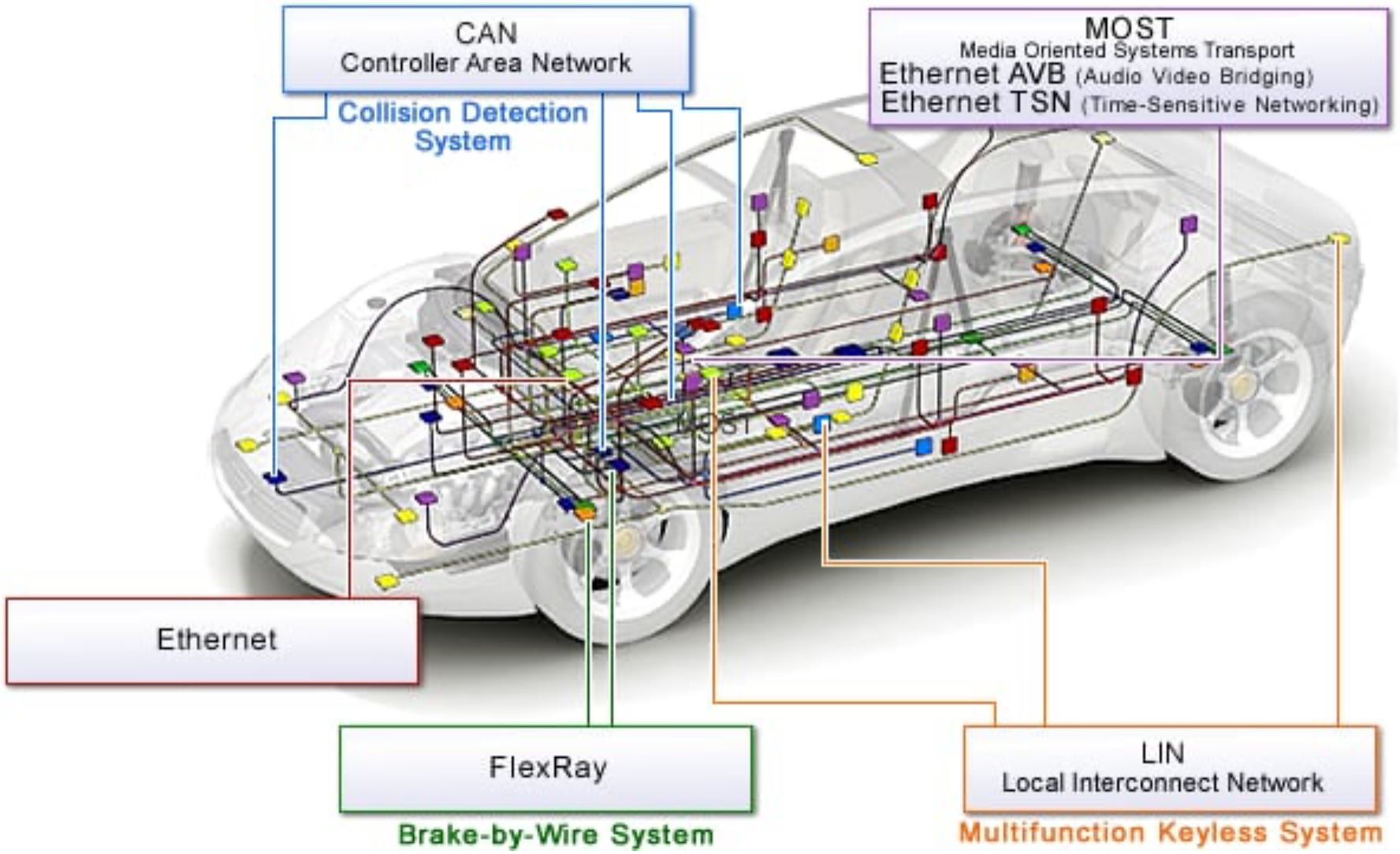
1. Maintenance of intrusion/illicit access/use
2. Base for new launching attacks

Etc, Etc, Etc, …

Vulnerability, Threats, Attacks, Incidents

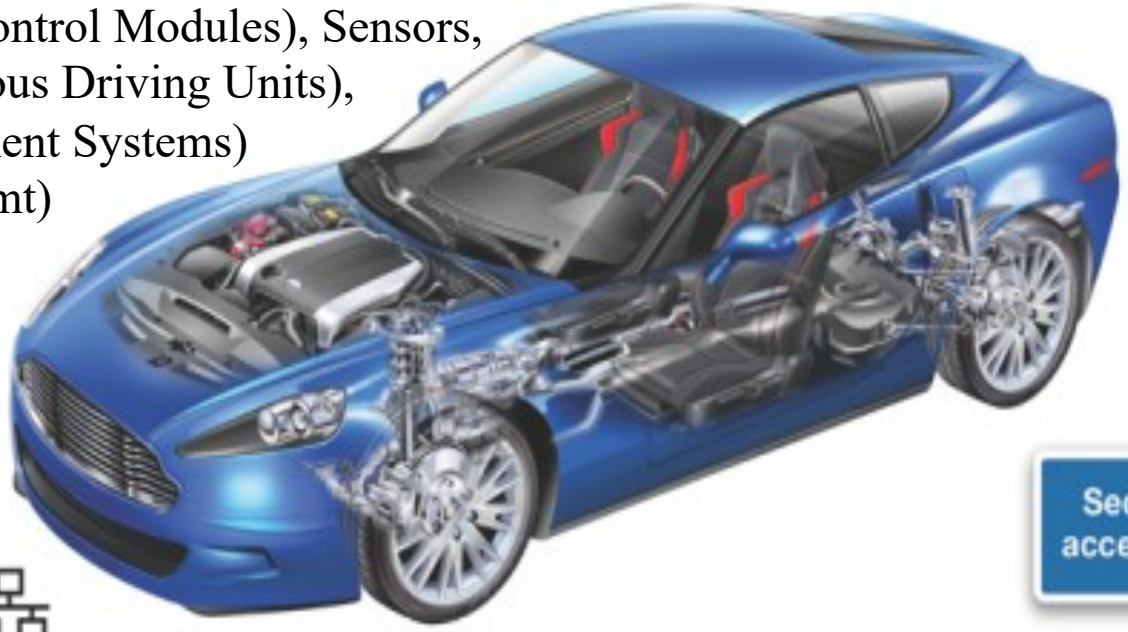


Network Perimeters (ex.: Automotive Network)

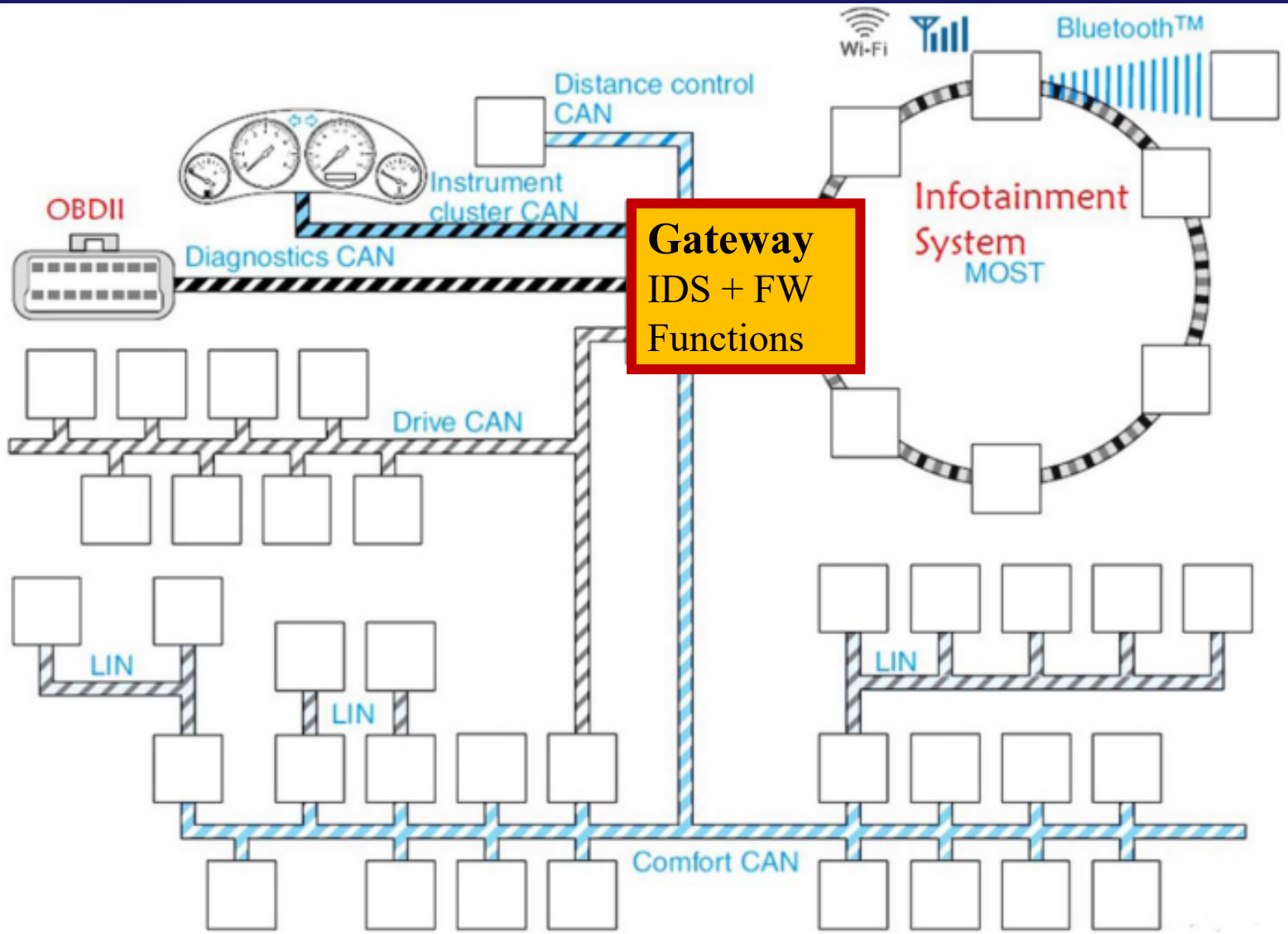


Network Perimeters (ex.: Automotive Network)

Interconnection of ECUs (Engine Control Units), TCUs (Transmission Control Units), ABS (Anti-Lock Breaking Systems), CBM (Body Control Modules), Sensors, AD (Autonomous Driving Units), ES (Entertainment Systems) IS (Infotainmemt) Cameras, Internet/Cloud Commection



Network Perimeters (ex.: Automotive Network)



Protection of involved dimensions

2 main dimensions involved

(Distributed System Approach):

- **Computer Systems Security (Computing Nodes)**
  - Computer Security Services and Mechanisms
  - "In Deep Security Protection"
- **Network / Internetworking (Communication Security)**
  - Secure Communication Channels
  - Point-to-Point vs. End-to-End Security Arguments

In this dimension is particularly relevant the approach of Internet Security Standards and TCP/IP Security Services

- TCP/IP Security Stack (different layers of approach)

Computer Systems and Network Security

Computer Systems Security

Computer Systems (Computing Nodes)

In Deep Defenses

- Physical Level (Phys. Environment)
- HW Level (HW Devices, FW/HW)
- OS Level (SW Services)
- Virtualization Services
- MW / Runtime Libraries' Level
- Application-Support Level

Secure Data Storage

(in Memory vs. Persistency)

Software and OS Security

Software Attestation

Containment, Isolation

Trusted Execution

Host-Based Perimiter Defenses:
Local Firewalls and Host-Based Intrusion Detection

Computer Systems and Network Security

Network (or Internetwork) Security Level

Communications' Protection

- Different Technology
- WSNs, PANs, VNETs, LANs, WLANs, Internet Communication
- Bluetooth, NFC, WSNs

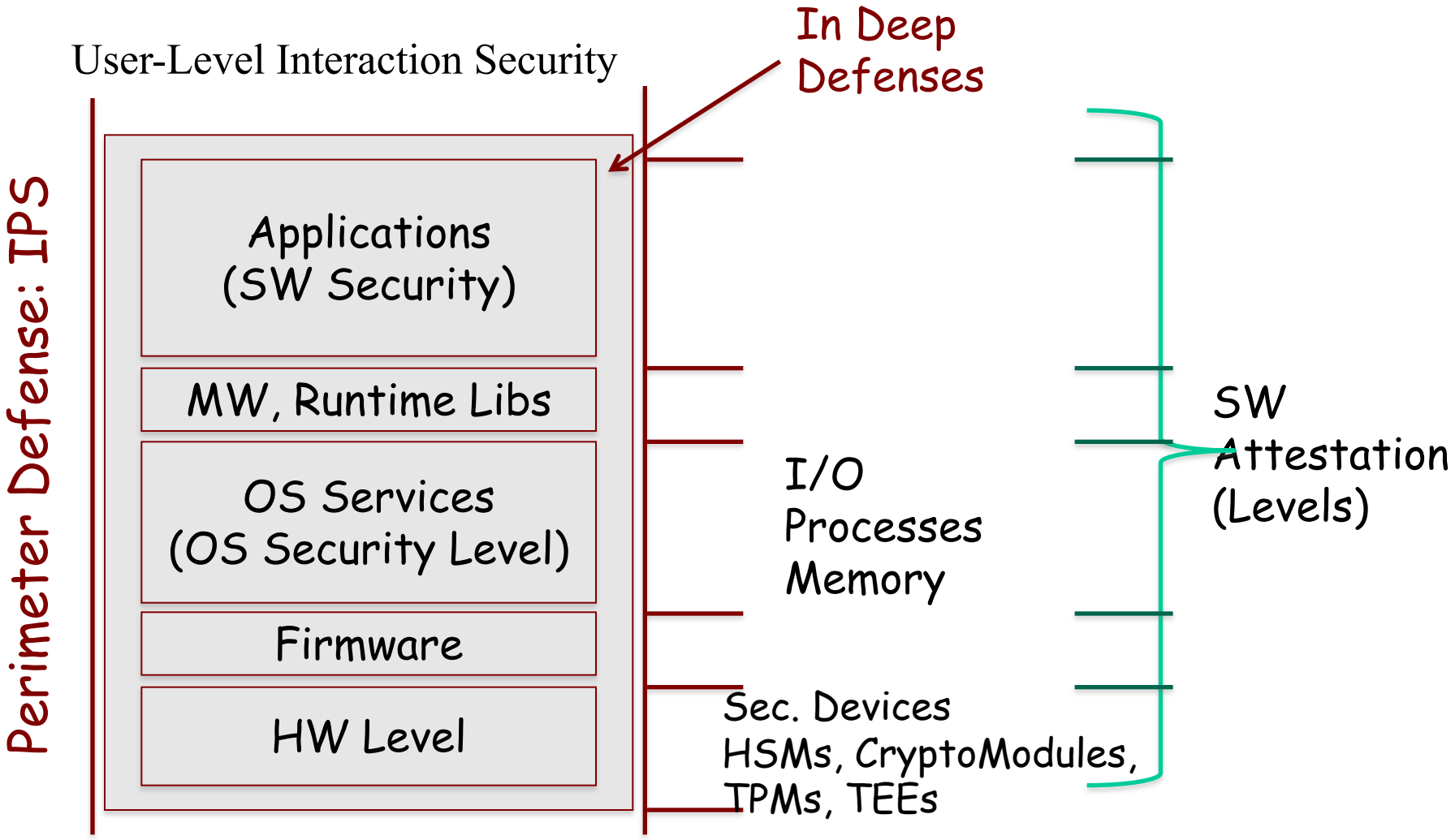
- Physical Level (Physical Resources)
- Access Level (Data Link)
- Traffic Flow Level (Net Level)
- Transport Level
- Session/Representation Level
- Application-Protocol Level

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

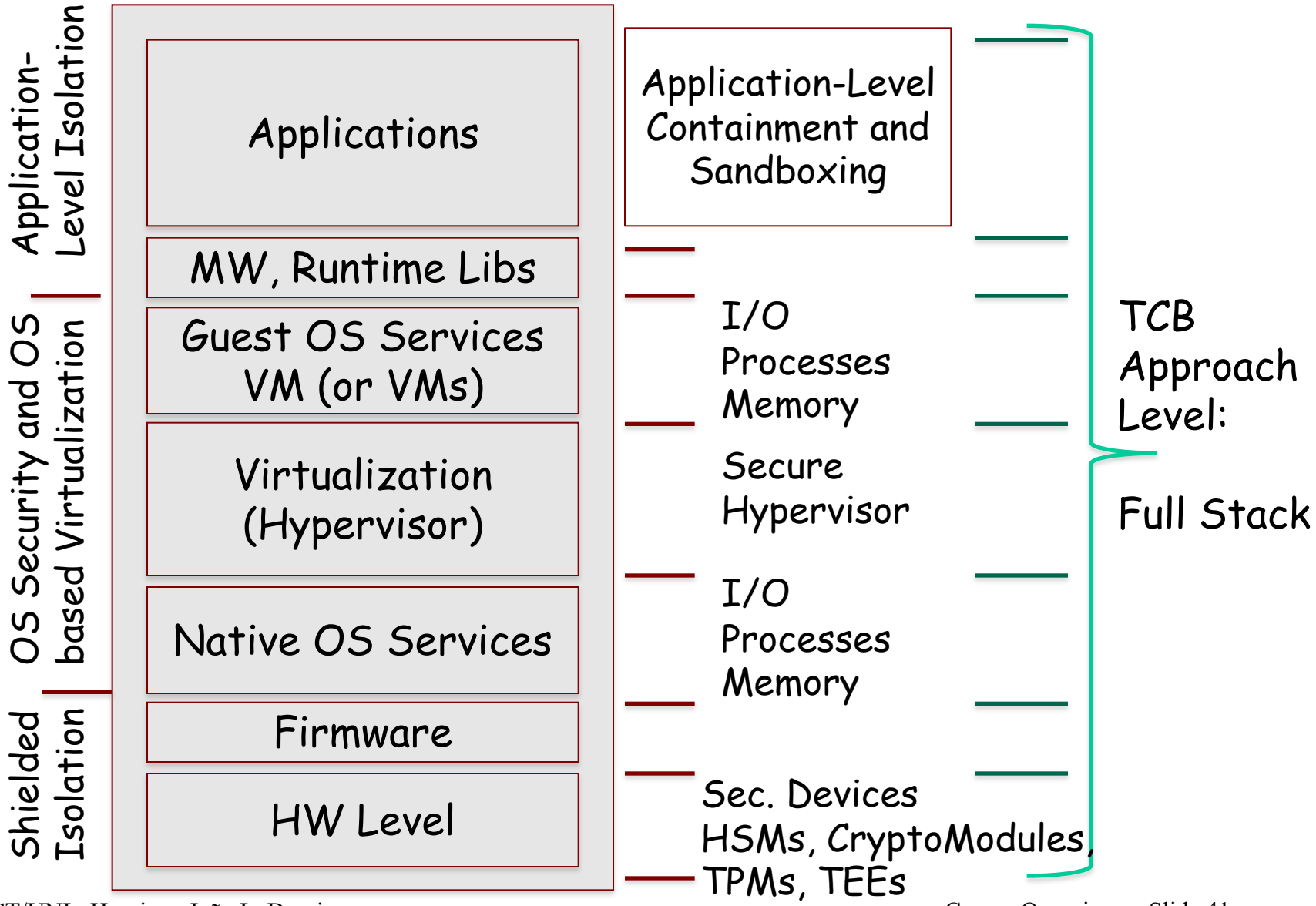
Network Appliances and Network-Based Perimiter Defenses:
Routers/Packet Filters, Firewalls and Netwosk Intrusion Detection

Computer Security Services and Mechanisms: Defense levels and TCB approach levels

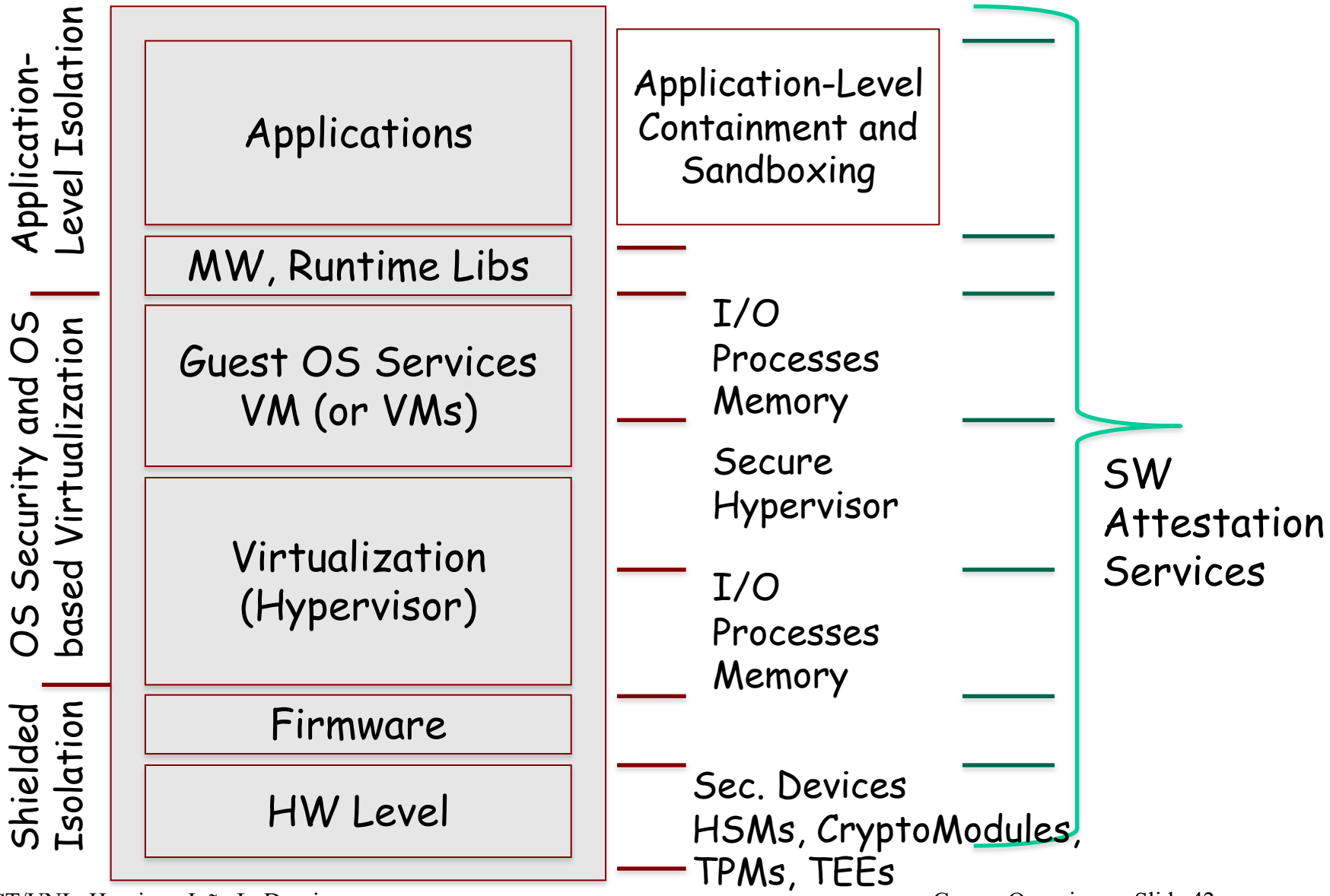
Scope of Computer Security
(involving SW, FW and HW services and mechanisms)



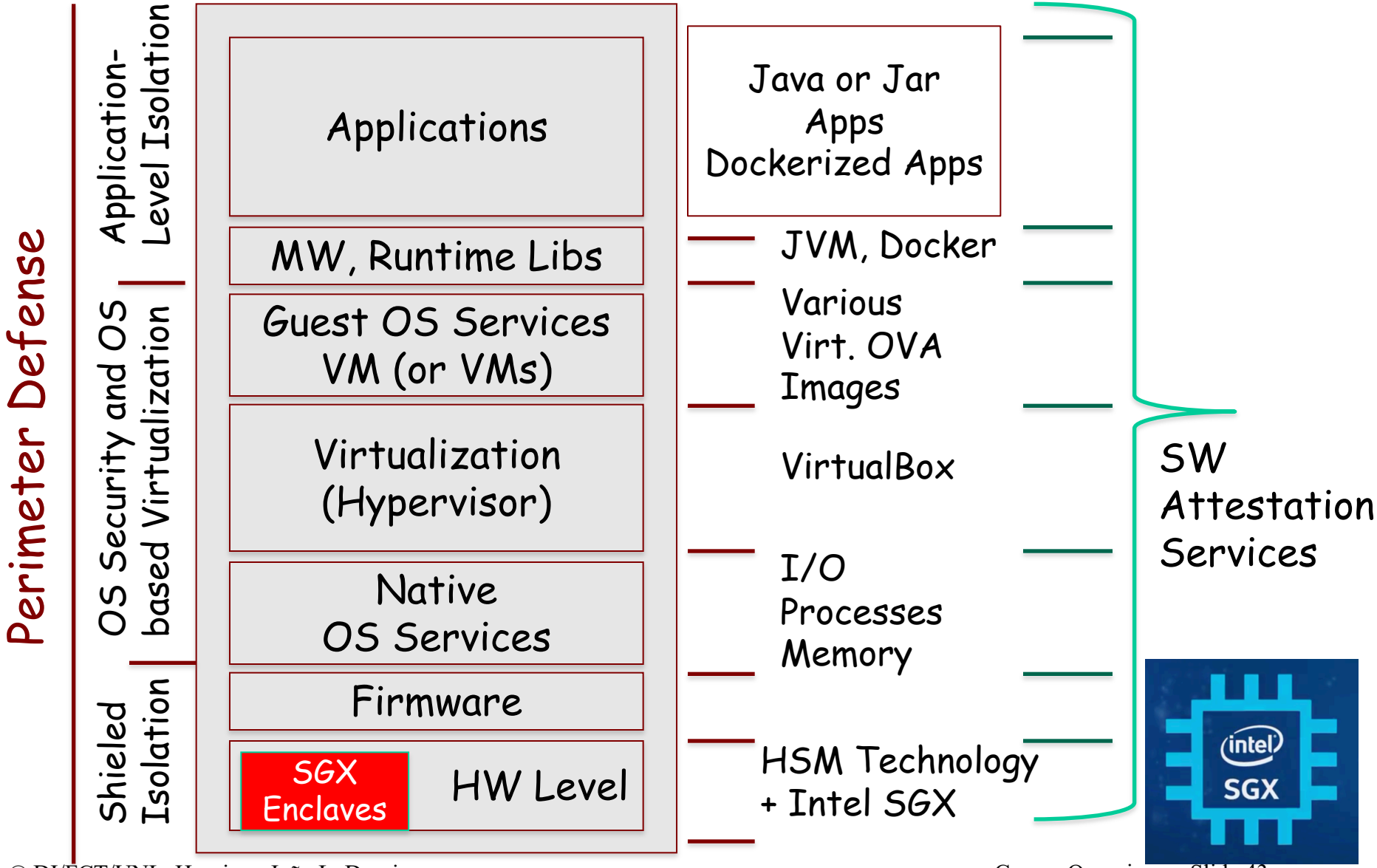
Scope of Computer Security
Isolation and TCB Level; Where is the TCB ?



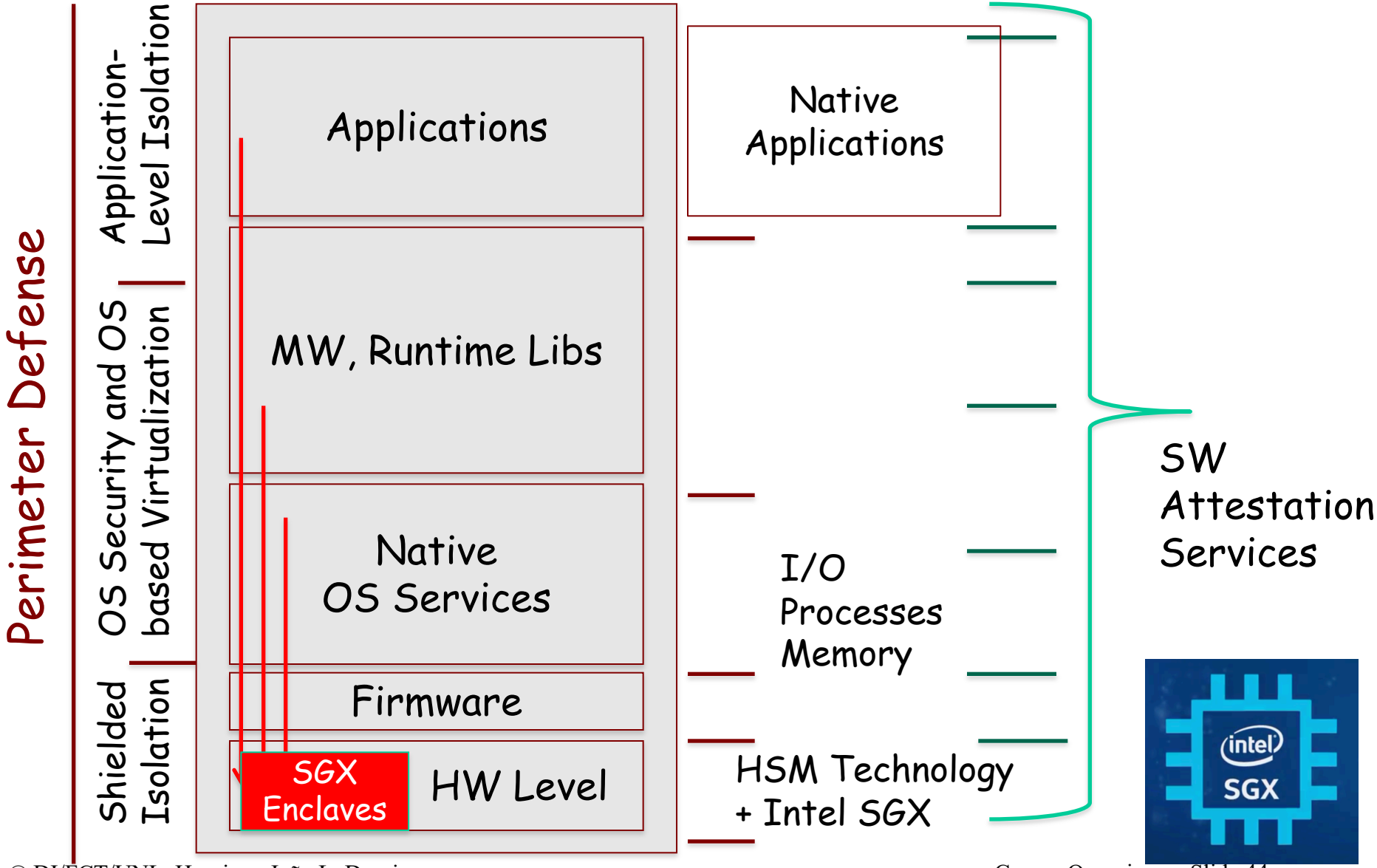
Scope of Computer Security Isolation and TCB Level



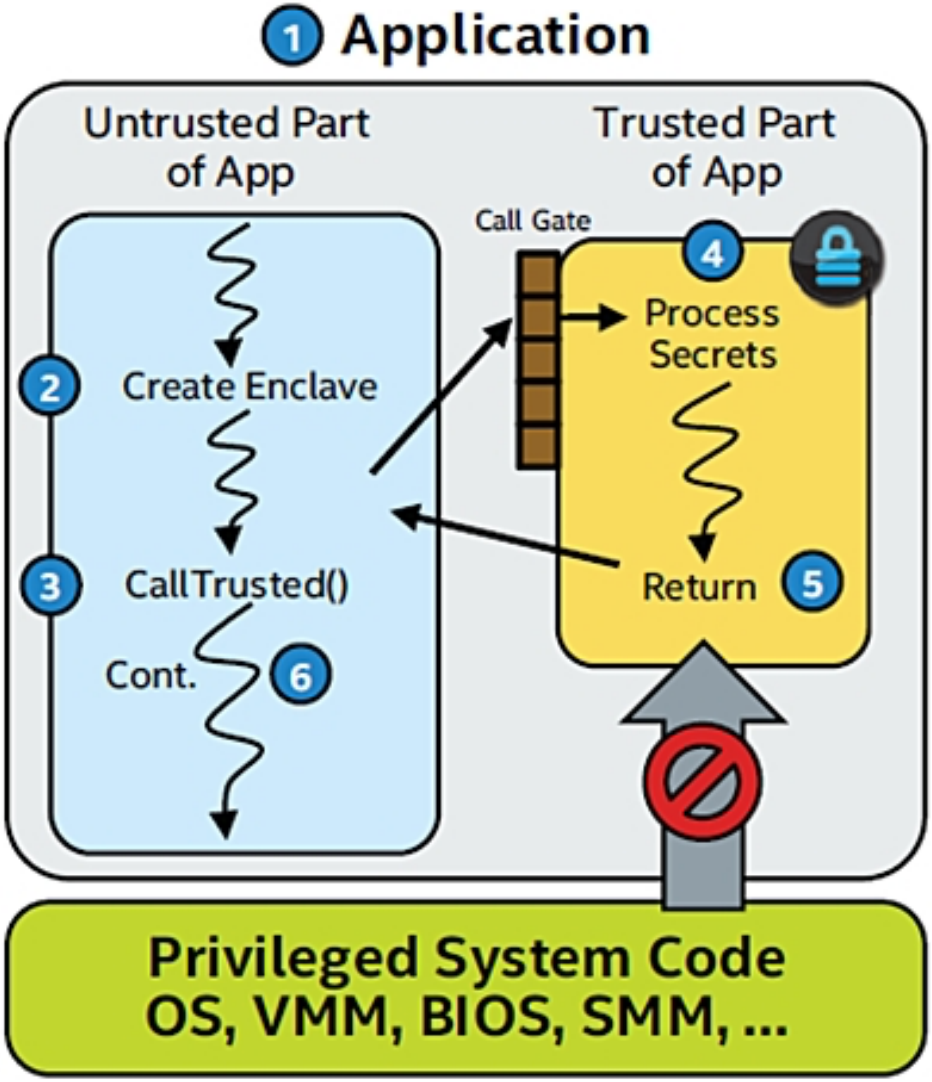
Concrete Implementation: HW Backed Isolation

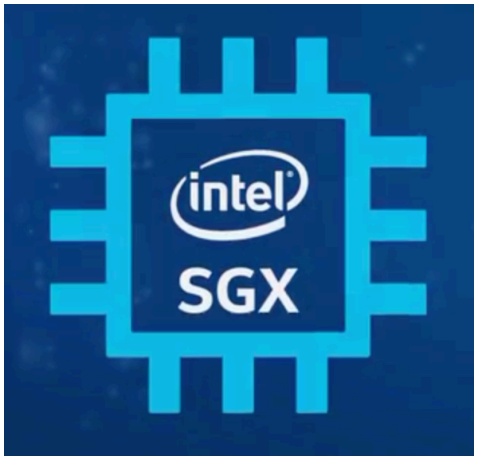


Concrete Implementation: HW Backed Isolation

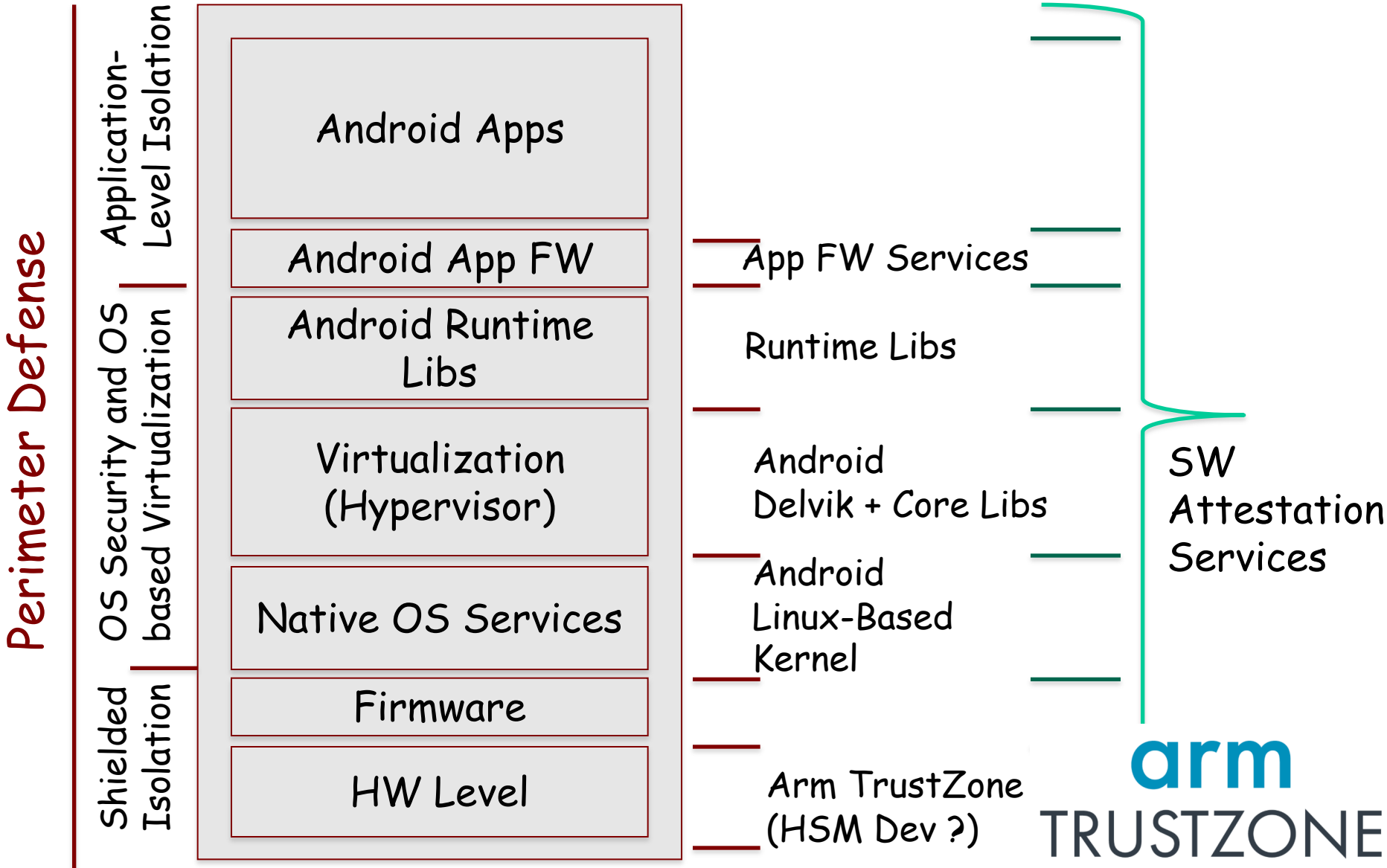


Intel SGX TEE Protection

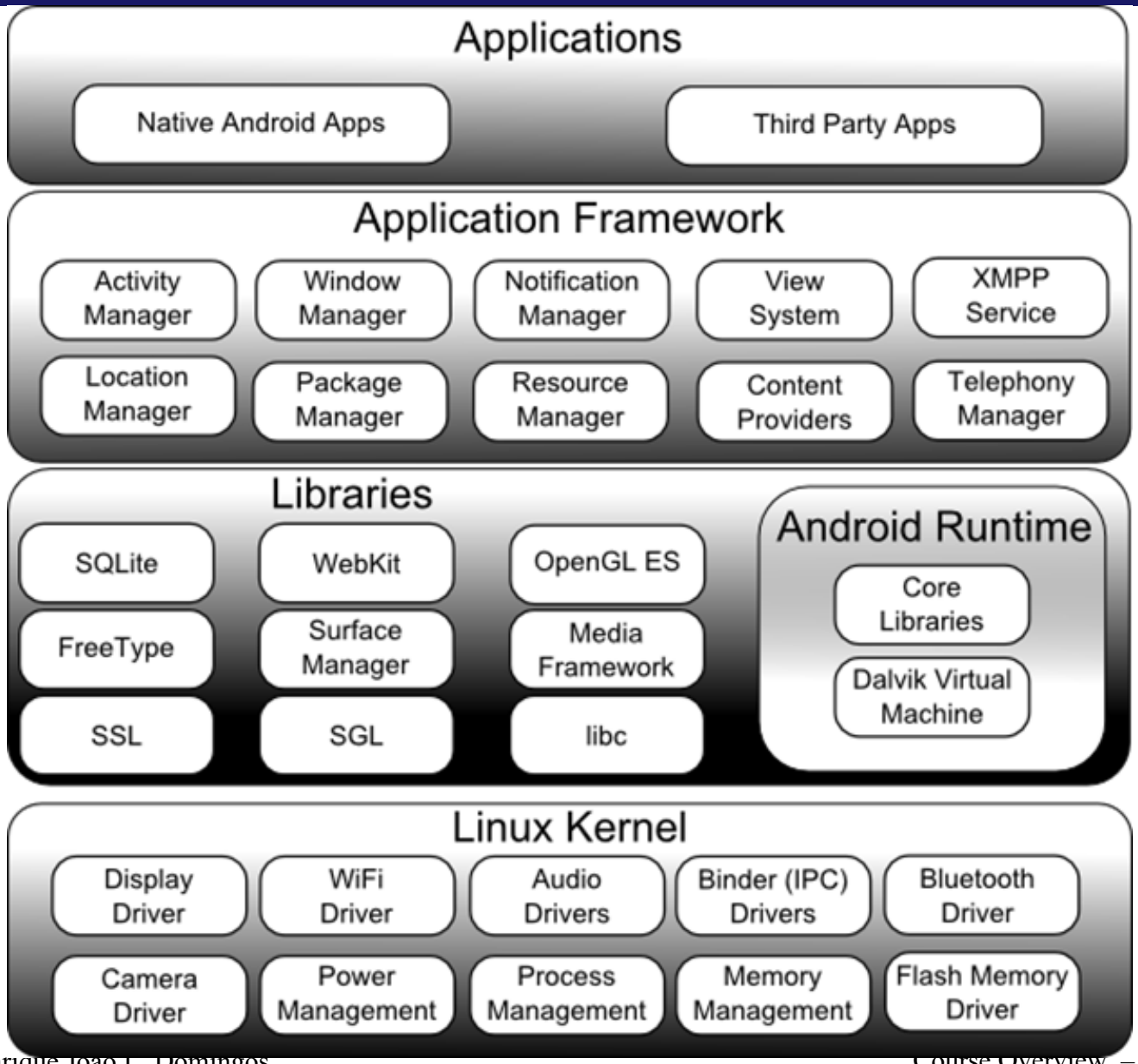




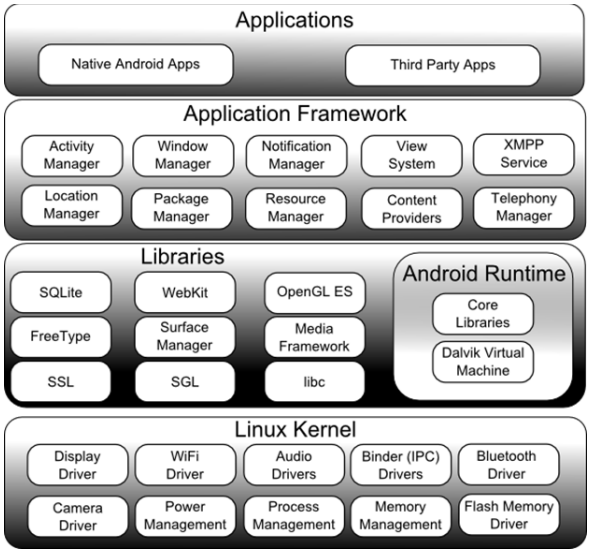
Another Implementation of HW-Backed Isolation (ARM / Mobile OSes: Example w/ Android)

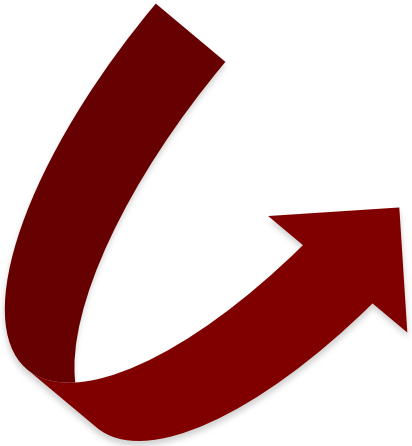


Android Architecture



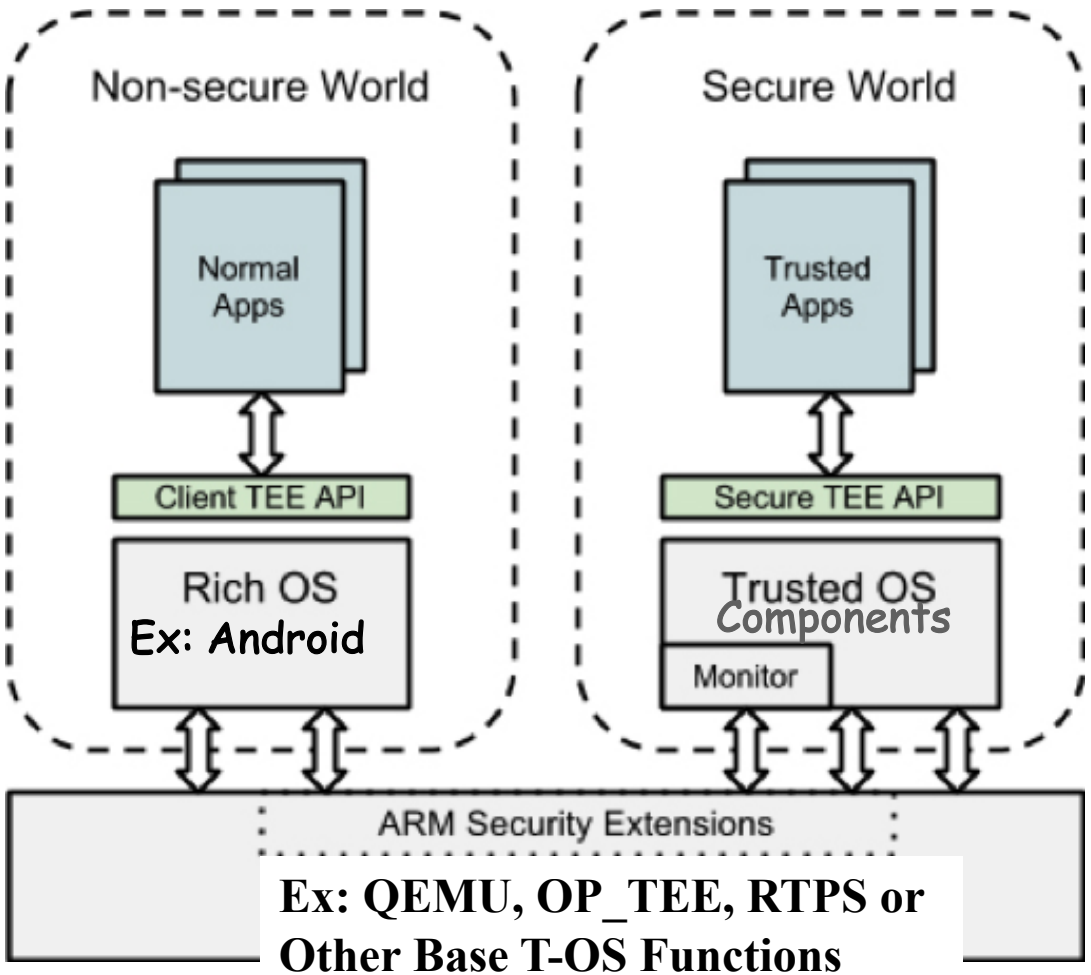
Ex: Android Architecture on HW-Shielded Trust Execution Environment





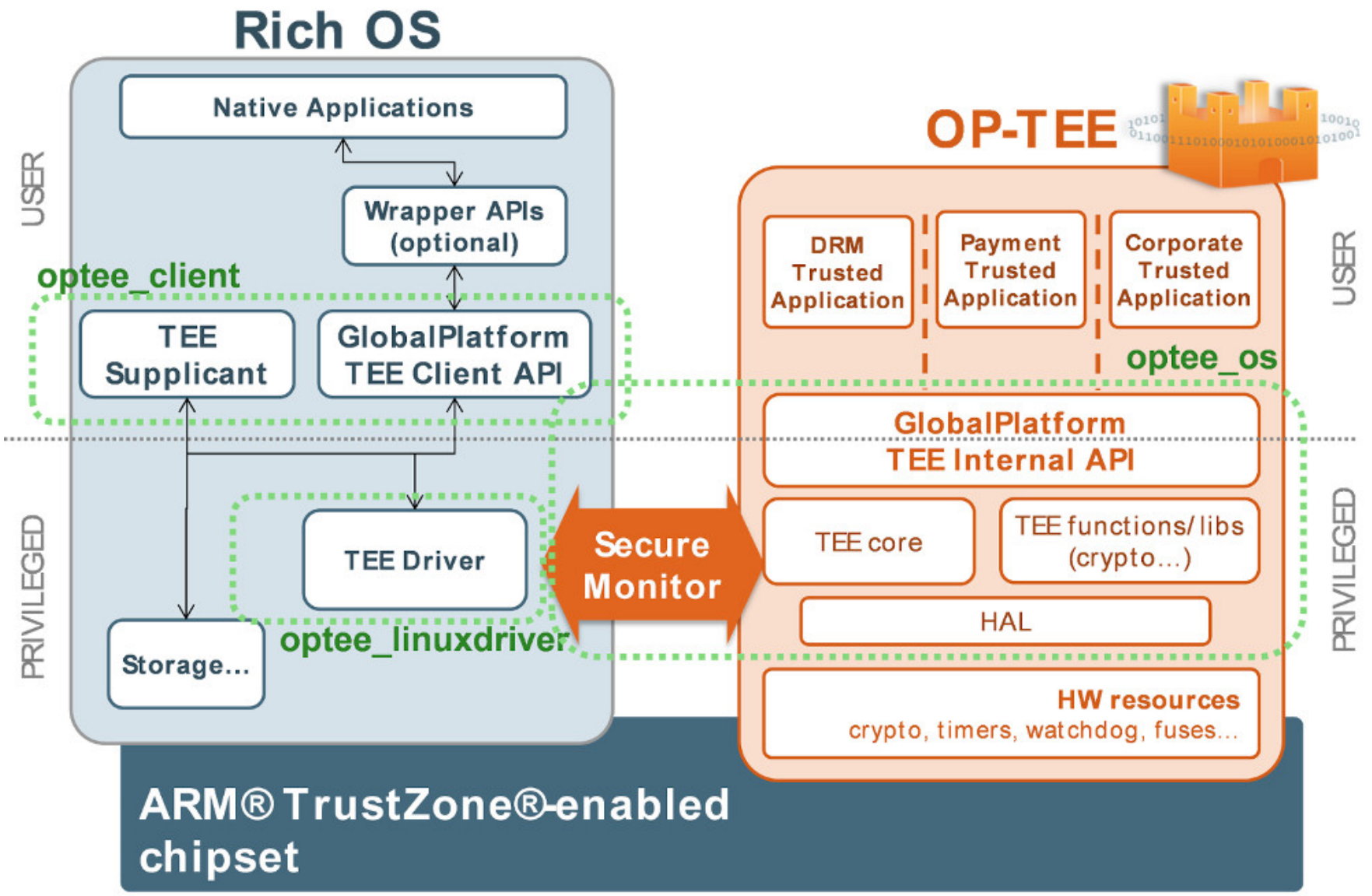
Mapping of Non-Sensitive Components

Mapping of Trusted Components



Ex: QEMU, OP_TEE, RTPS or Other Base T-OS Functions

TEE Architecture



Security Frameworks and Standards

Organizational Security Frameworks [Informative]

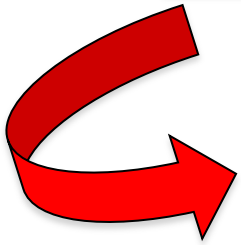
ISO 17999 - 20001 [Informative]

ANSI FIPS PUB (NIST)

OSI X.800

Organizational Security Frameworks

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

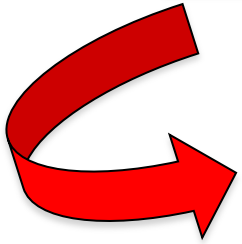


How to organize such mappings ?

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

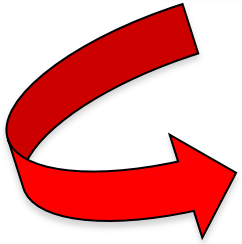
(Some) Examples:

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** (Portuguese Law Frameworks and Transpositions)

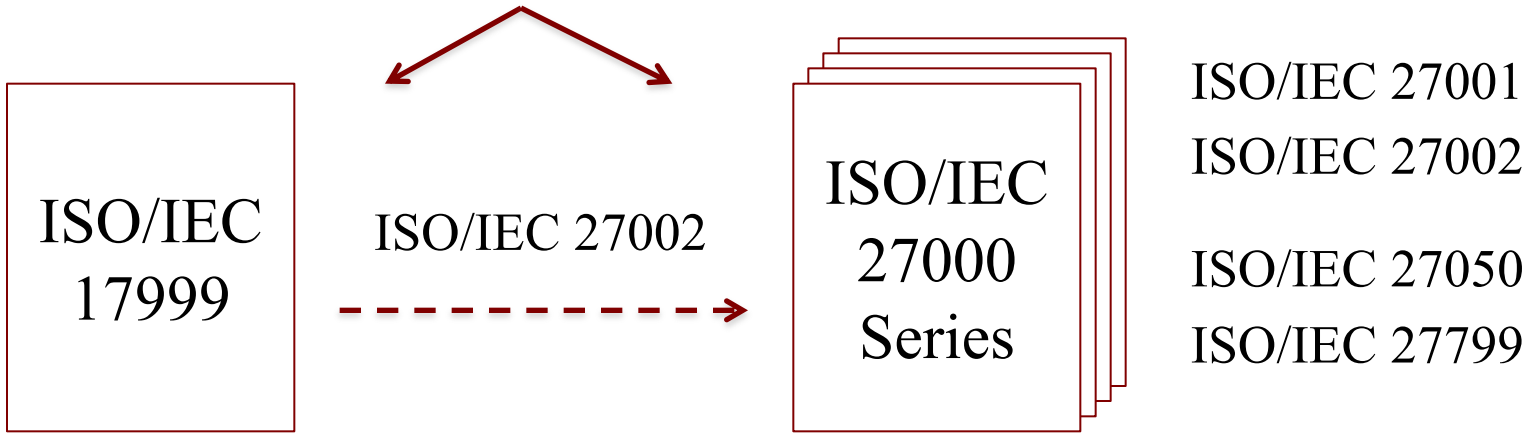
Proteção de Dados Pessoais	Criminalidade Informática	Regime Jurídico de Documentos Eletrónicos e Assinaturas Digitais	Defesa do Consumidor	Comunicações de Emergência e Segurança
Art 35º Constituição sobre utilização de Informática, UE L119/2016,	Lei 199/2009	DL 290-D/99, 62/2003 25/2004, 165/2004, 116-A/2006,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

ISO / IEC Framework
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 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)

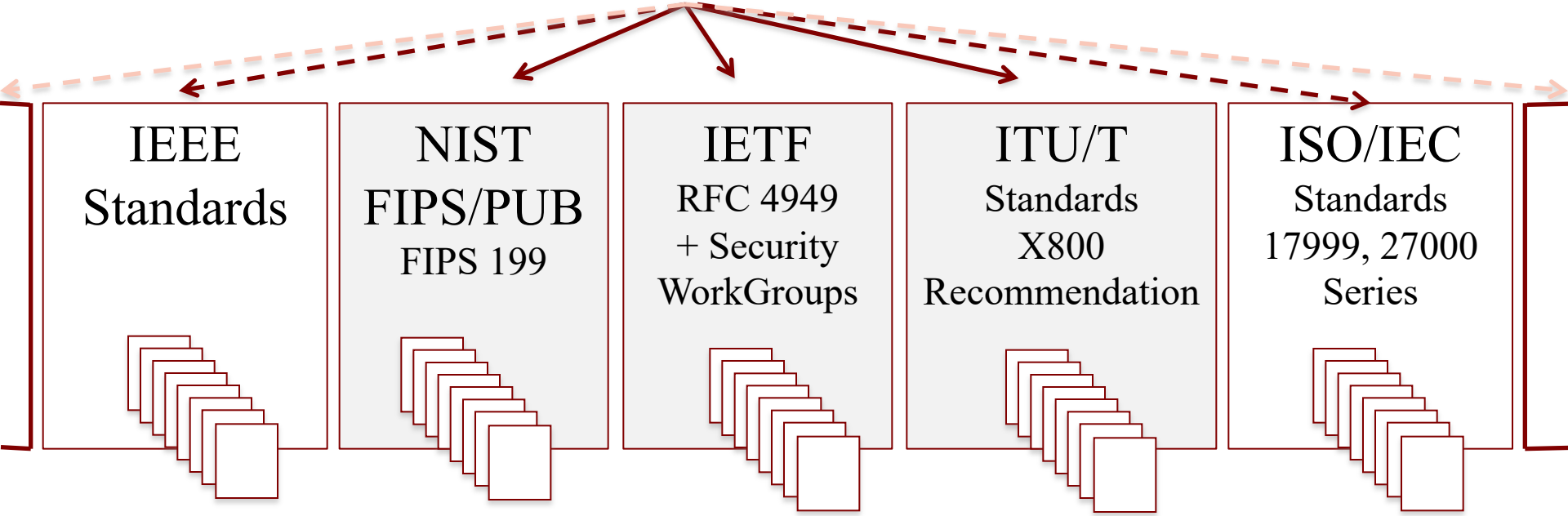
- https://www.iso.org/isoiec-27001-information-security.html
- https://www.iso.org/standard/39612.html

Engineering Frameworks

- 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)



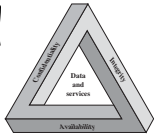
NIST, FIPS PUB 199 Framework

NIST FIPS PUB Framework

- See Introduction (Part I)

- Confidentiality
- Integrity
- Availability

CIA Triad NIST and FIPS PUB Standardization



- Authenticity (or Authentication)
- Accountability (tracing, auditing, logging, forensics)

Extended Properties

OSI X.800 Conceptual Framework

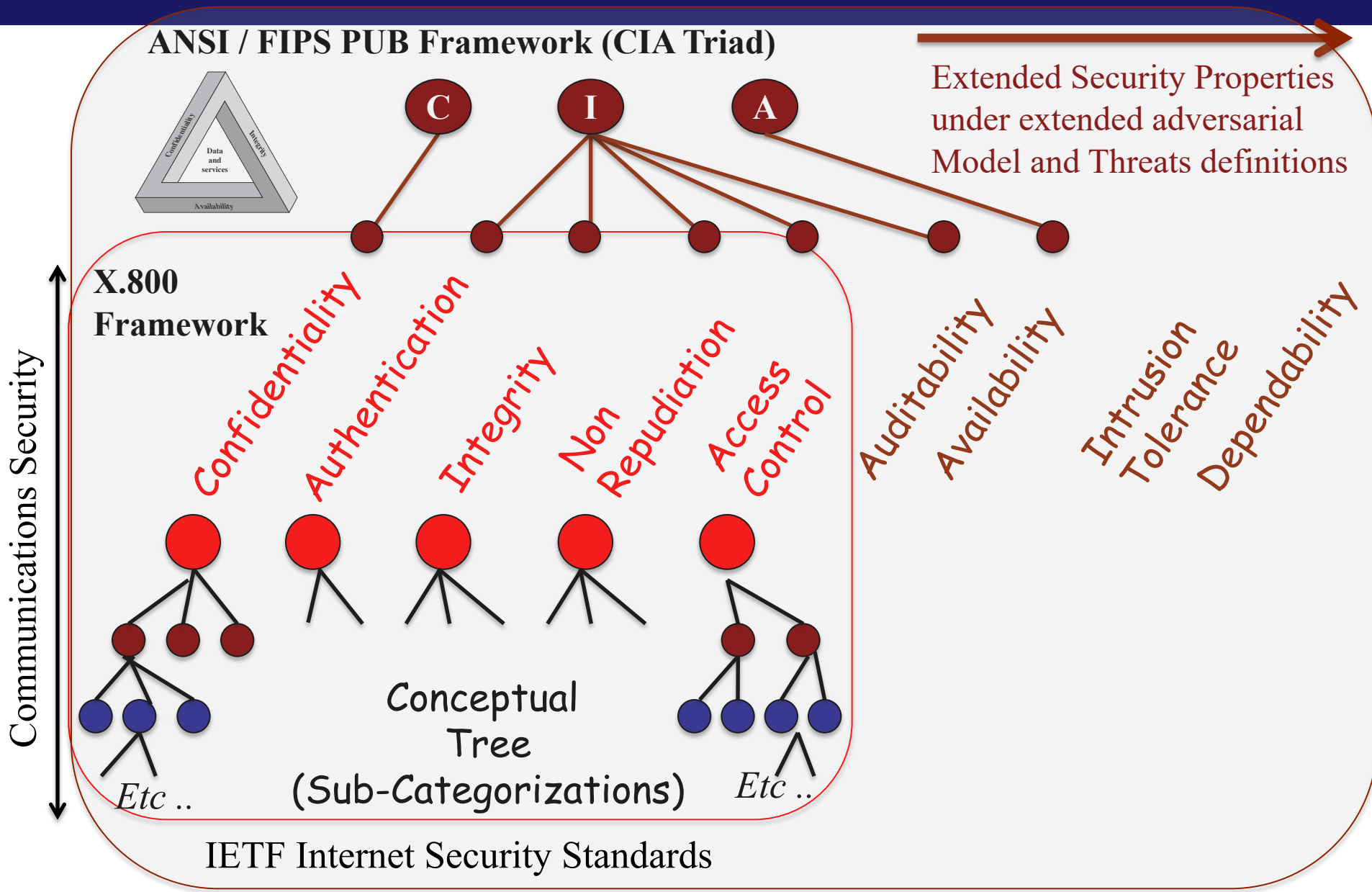
Internet Security Standards (IETF RFCs)

Ex., RFC 2828

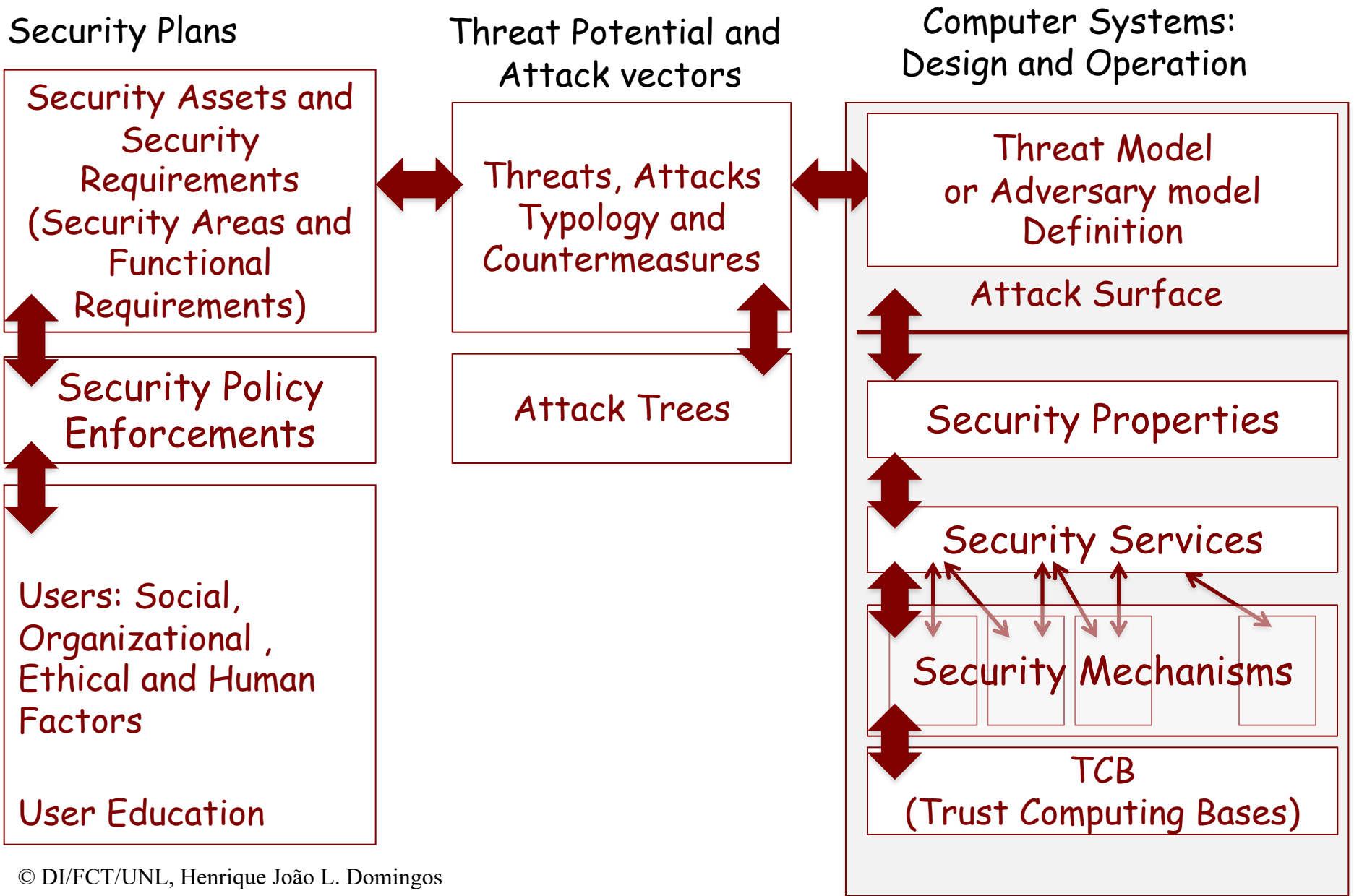
Communications (Network, Internet) Security

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

Base Security Properties: X.800 Framework



Remembering our initial (conceptual) Security Framework



Threats vs. Attacks (OSI X.800)

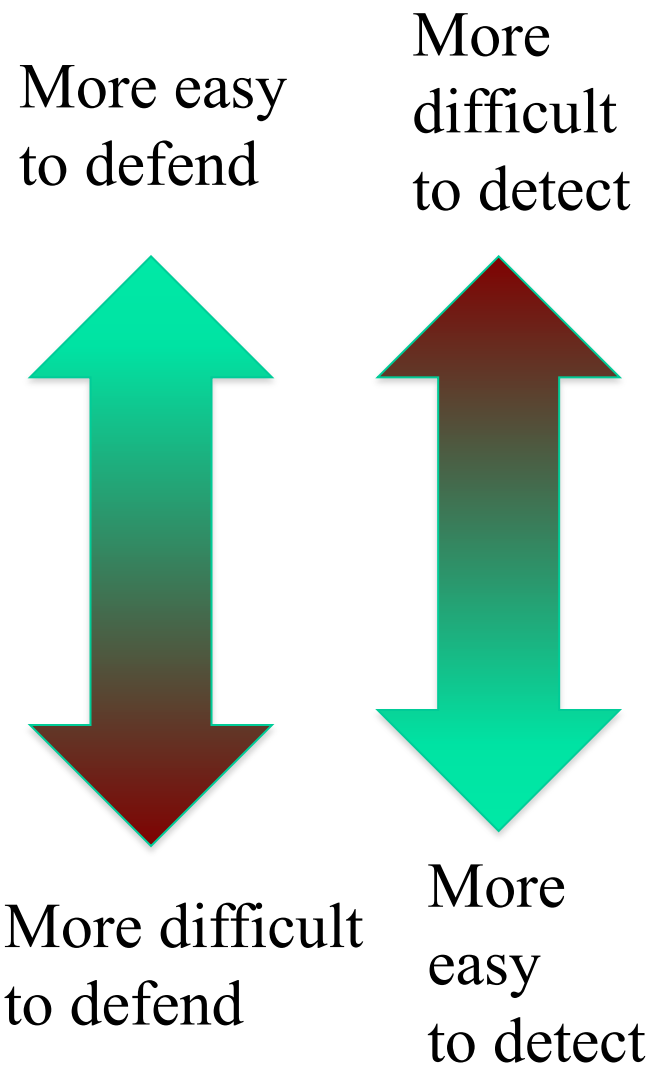
- **Threat:** Potential of security violation, when there is circumstances, vulnerabilities, capabilities, actions or events that could breach security and cause harm
  - Possible danger that might exploit a vulnerability
  - Potential exploits in the attack surface

- **Attack:** Assault/Break on Security, as a concrete manifestation of threats
- Intelligent action as a deliberate attempt (method, technique, use of attack tool) to evade security services and violate security policy (and related security properties) of a system
  - Induction of incorrect (non-secure) behaviour

OSI X.800: Attacks

- **Passive Attacks**

- **Active Attacks**



Typology of Attacks in OSI X.800 Framework

- **Passive Attacks**
  - Release of Message Contents (Payload Data Leakage)
  - Packet Analysis (Frame/Datagrams/Packet Sniffing)
    - Specific Targeted Data Packets
  - Traffic Analysis (at different stack layers)
    - Traffic Flow Inspection and Reconnaissance
- **Active Attacks**
  - Masquerade (Message Forgery)
  - Replay (or Illicit Message-Replay)
  - Modification of Messages (Message Tampering)
    - Can Include Attacks against Message Ordering
  - DoS (Message Discarding, Message Dropping, Overloading and Net. Congestion and/or Saturation)
  - Attacks inducing end-point incorrect processing

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-Repudiation of Destination

OSI X.800: Security Mechanisms

Specific Security Mechanisms

- Encipherment (Encryption)
- 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

Mapping Attacks vs. Security Services

Security Services	Attack Typology: 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

Mapping Attacks vs. Security Mechanisms

Security Mechanisms	Attack Typology: 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

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,
Aalgorithms, models, techniques

	Mechanism							
Service	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			

Cryptographic tools as base specific mechanisms

	Mechanism							
Service	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			

Symmetric Crypto Methods

Asymmetric Crypto Methods

Secure Hash Functions, HMACs or CMACs

Authentication and Key Distribution Protocols

Suggested Readings

- Review the slides …
- Conclude your readings of:
  - W. Stallings, L. Brown, Computer Security – Principles and Practice, Person, Ch.1
  - W. Stallings, Network Security Essentials – Applications and Standards, Ch.1

See the Review Questions and Try to Answer

Check tests and quizzes (CLIP) on questions related to Introduction (Slides Parte I and II)