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 II)

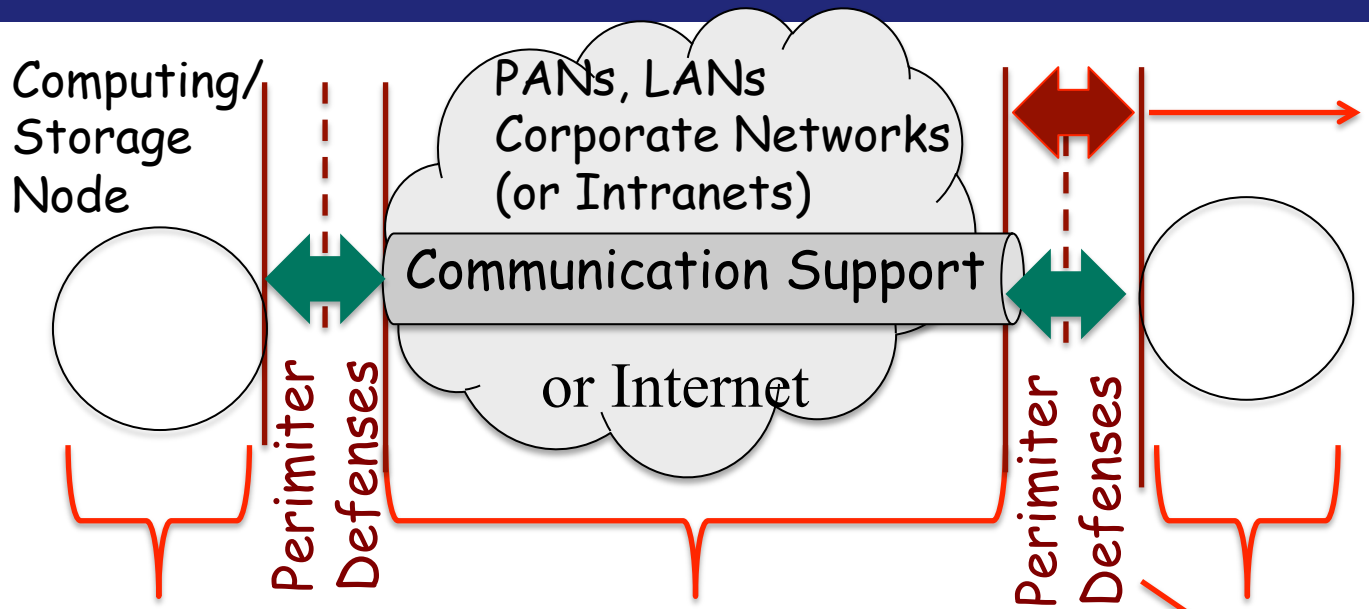
Concepts, Terminology
Frameworks

Introduction: complementary questions …

- How to address **Security in Distributed Systems**?
- **Typology of defenses** for distributed systems security ?
- What is the **OSI X.800 Framework** ? What are the main **features and orientations** in the OSI X800 framework ?
- What is a **secure communication channel** ? How to define a secure communication channel, how to address its security properties and threats, and what are the level of abstraction?
- What are the **security services and standards in the TCP/IP security Stack** ?
- What is a **layered secure channel** ? What is **tunneling security modes and security transport modes** established for **end-to-end communication security**

Computer Systems and Networks Security (A Distributed Systems Security Approach)

Distributed Systems Security Dimensions



Access Networks:
LAN, WLAN
PAN, WPAN
Net. Technology, and Network Gateways

Perimeter Defenses:
(Switches, Routers, Traffic Filters, FWs, IPSs and IDSs:
- NIDS
- HIDS

Scope of Communications Security (Traffic, Data Flows, Message-Exchanges Communication Endpoints)

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

Protection of involved dimensions

2 dimensions involved

(Distributed System Approach):

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

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

- Security Stack, with different layers of approach

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

Secure Data Storage
Software and OS Security +
Software Attestation +
Isolation and Containment
Trusted Execution

Computer Systems and Network Security

Network (or Internetwork) Security Level

- **Communications' Protection**
  - Private/Dedicated/Shared/Public/Outsourced
  - Wired, Wireless, Supervised, Non-Supervised …
  - Internet Communication

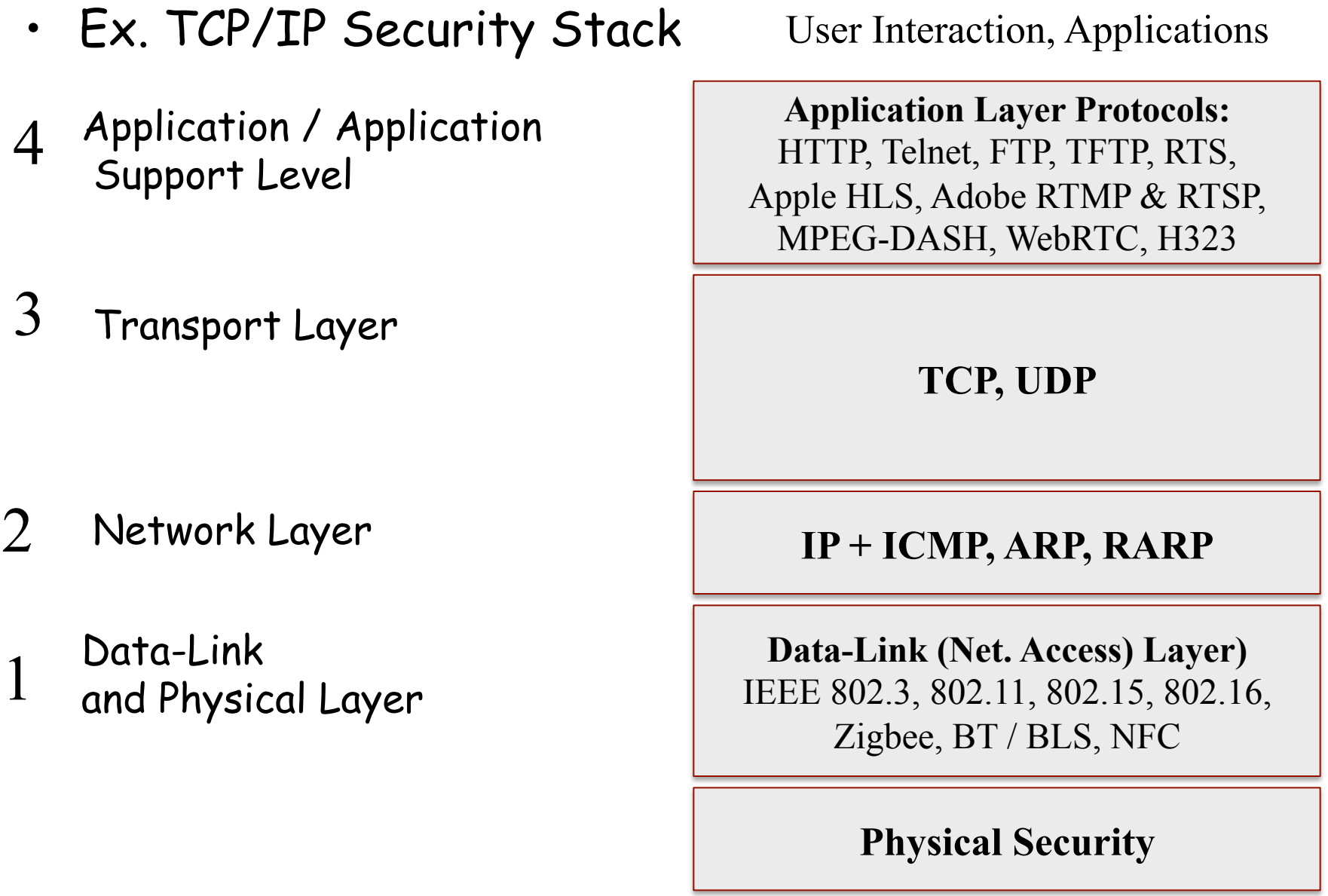
- Physical Level (Physical Resources)
- Access Level (Data Link)
- Traffic Flow Level (Net Level)
- Transport Level
- Session/Representation Level
- Application-Protocol Level

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

TCP/IP Security Stack (and Related Standards)

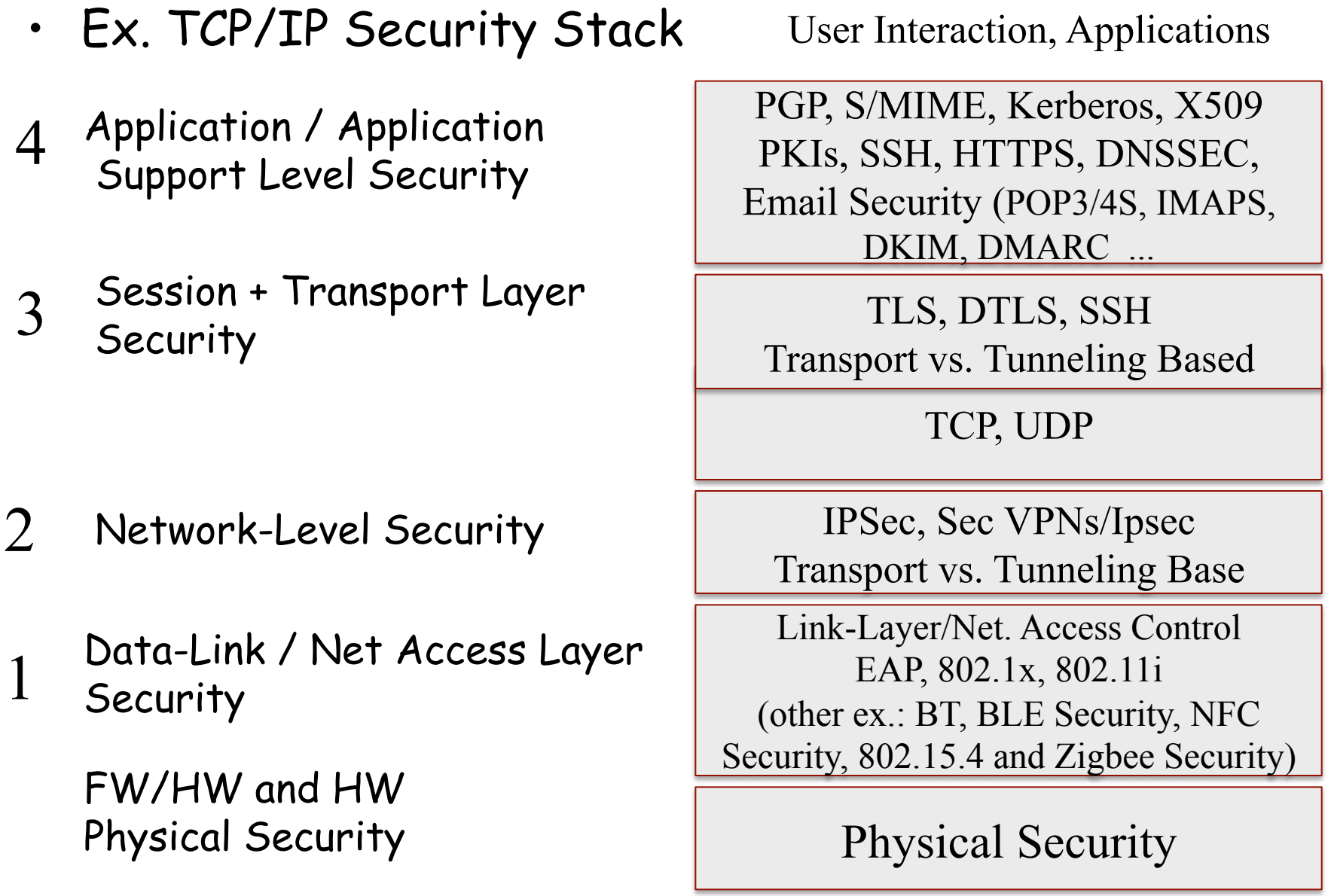
Communication Security Services and Protocols

- Ex. TCP/IP Security Stack



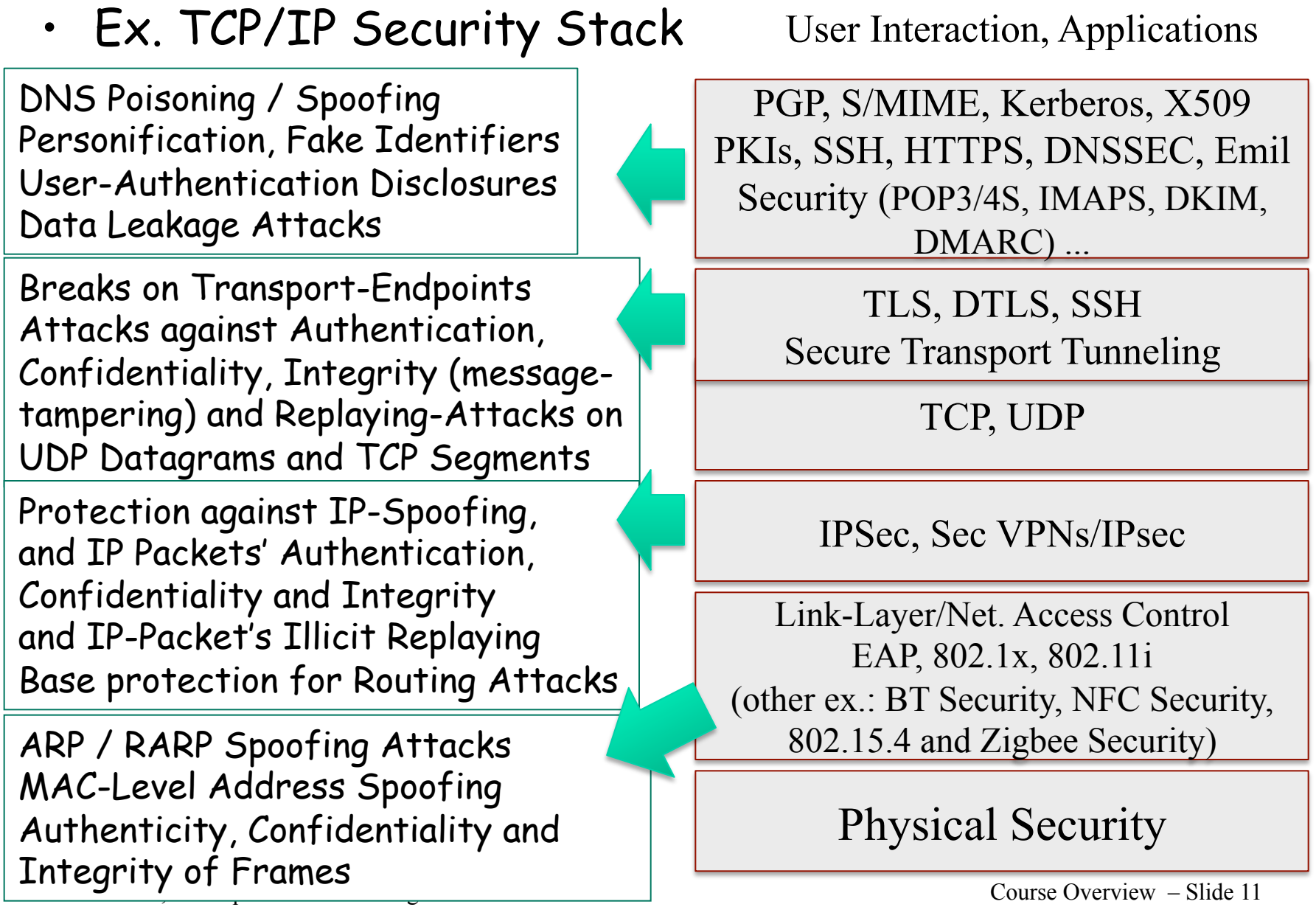
Communication Security Services and Protocols

- Ex. TCP/IP Security Stack



Some examples of countermeasures

- Ex. TCP/IP Security Stack



DoS and DDoS Threats and Protection

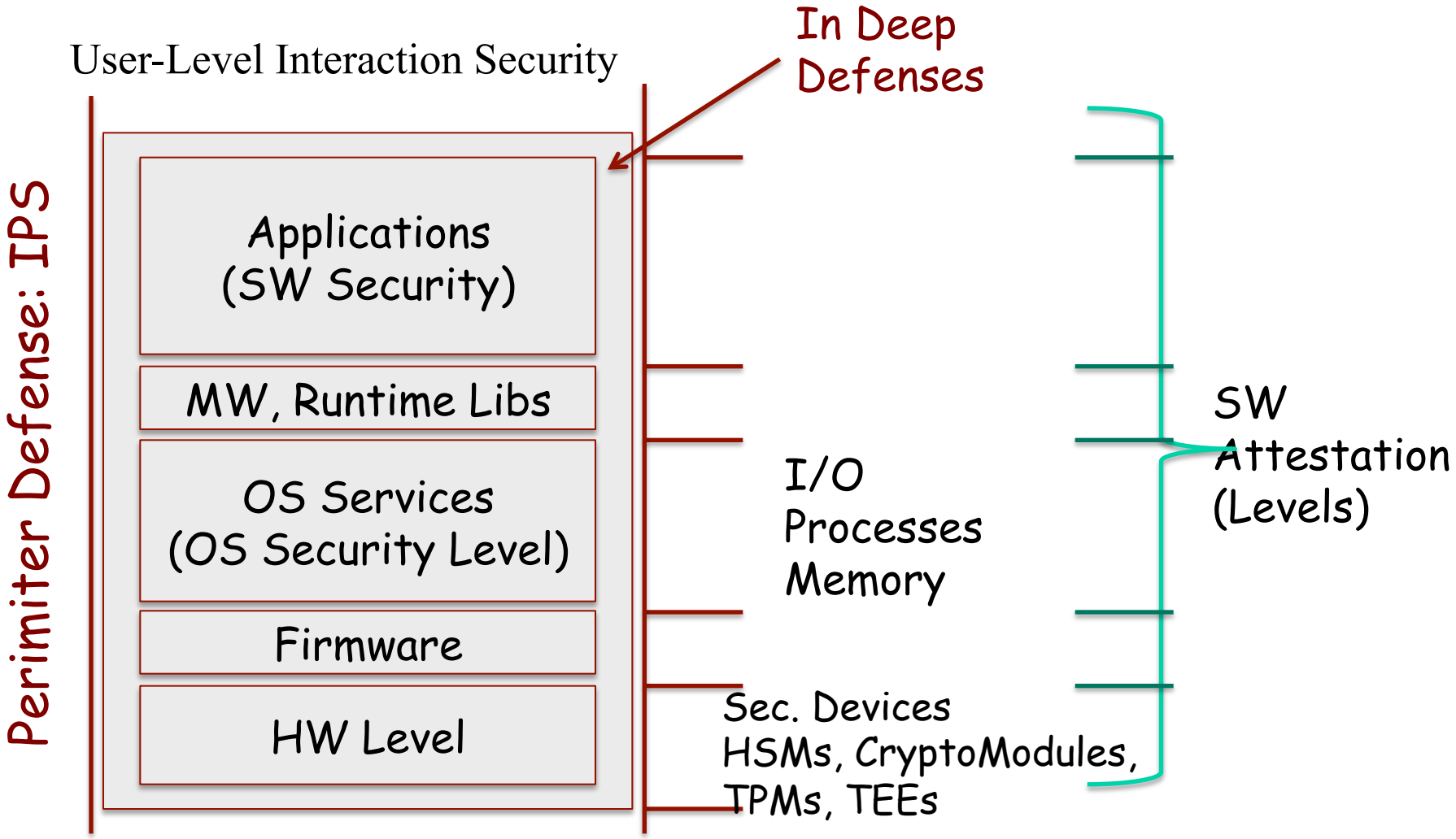
Mitigation in TCP/IP Stack Implem. and Runtime

Complex Defenses combining many Defense Types (Ex., Perimeter Defenses, Cloud DDoS Protection)

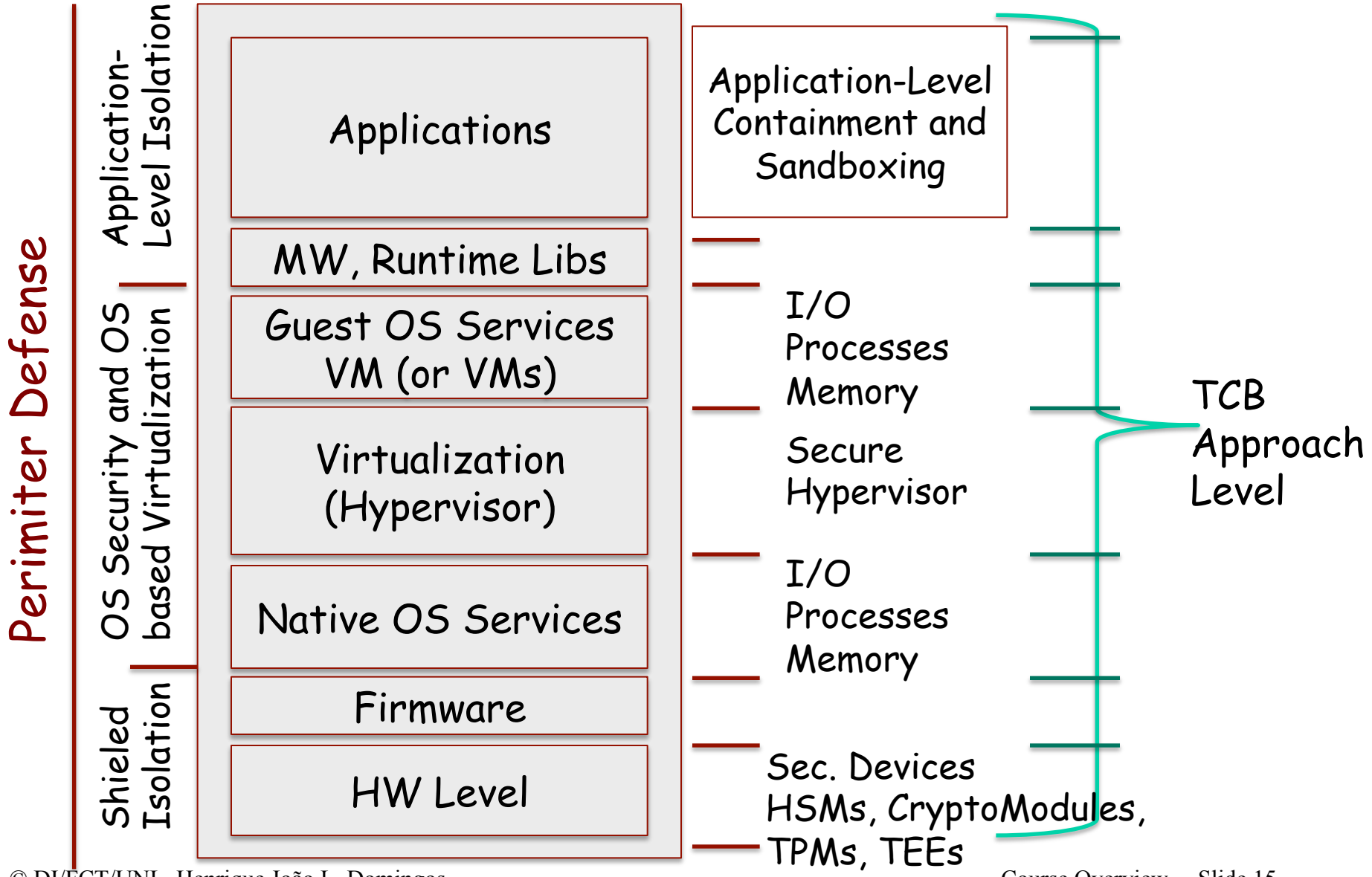
- What about not included countermeasures on TCP/IP Security Stack Standards ? Discussion
  - Simple (common) examples
    - Land Attacks, Teardrop Attacks
    - ECHO-CHARGEN and SYN Flooding Attacks
    - IP Ping-of-Death Attacks
    - Stack Smashing Attacks
    - Format/Data Representation Formats and Endpoints' Processing
  - More complex …:
    - Large-Scale DDoS / Cloud-Based DDoS Vectors of Communication Overloads ☹
      - Need Specific Network Perimeter Defense and In-Deep Defense Mechanisms
      - …. OR Cloud-Enabled Defenses ;-)

Computer Security Services and Mechanisms

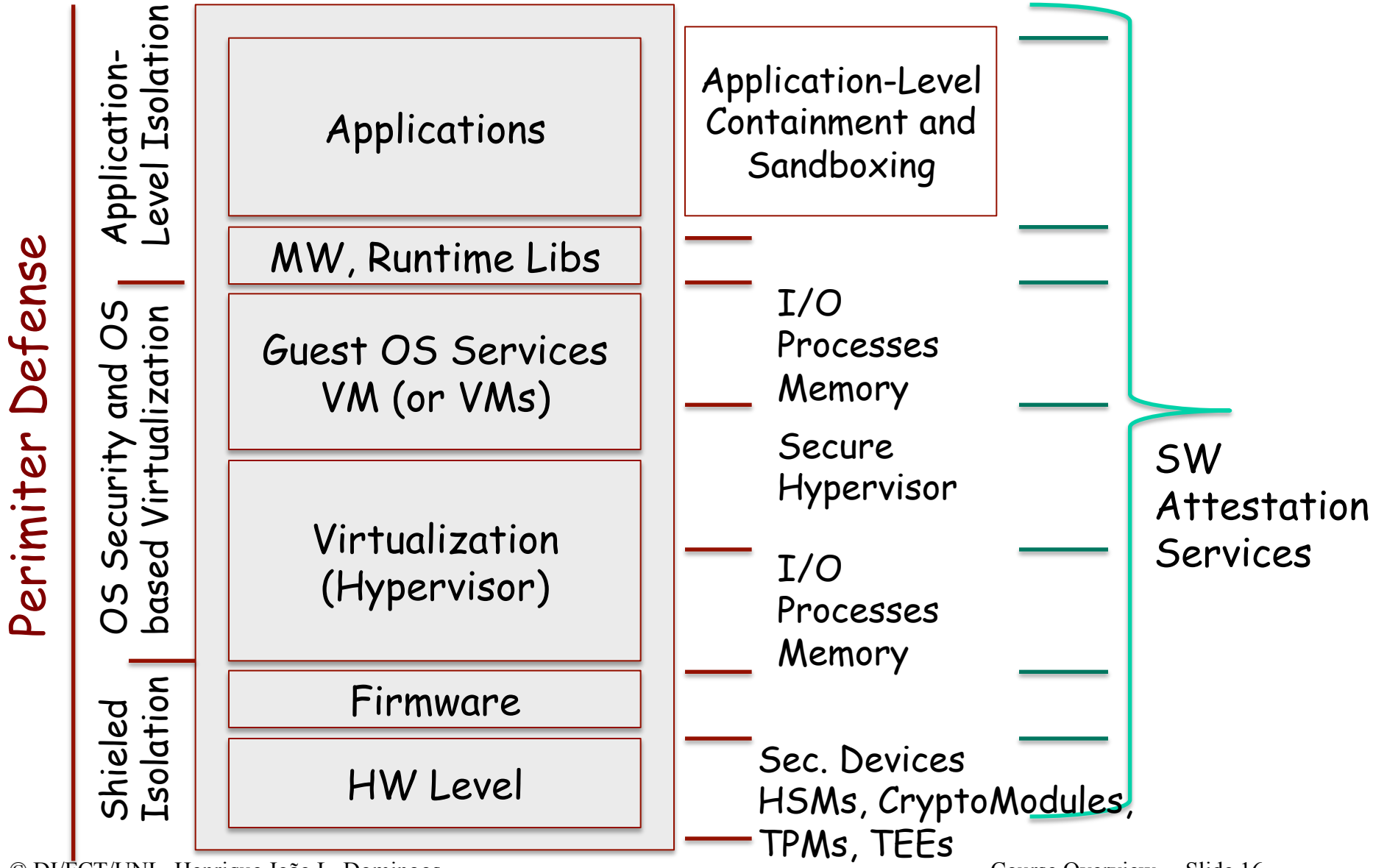
Scope of Computer Security
(involving SW, FW and HW services and mechanisms)



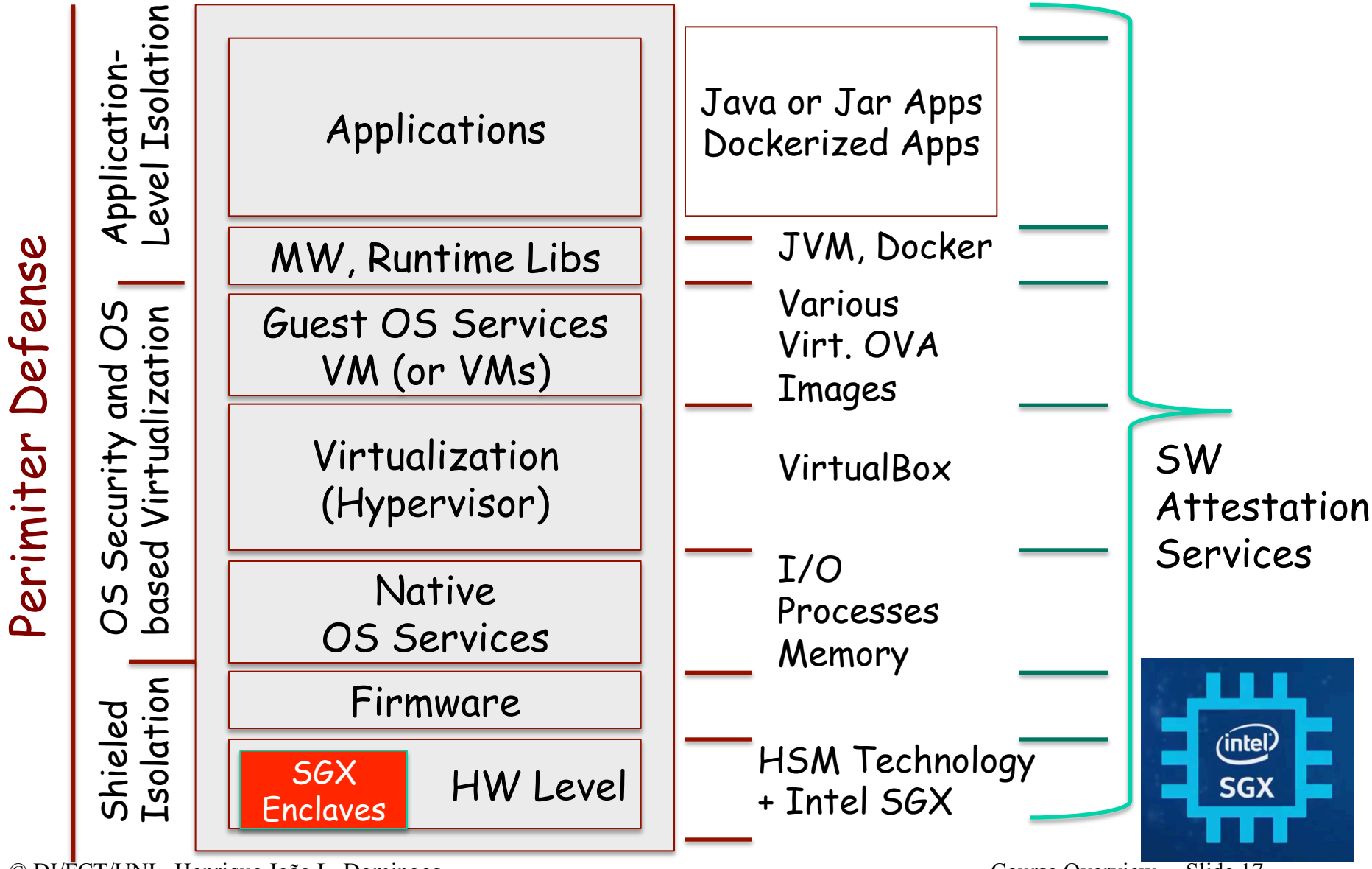
Scope of Computer Security Isolation and TCB Level



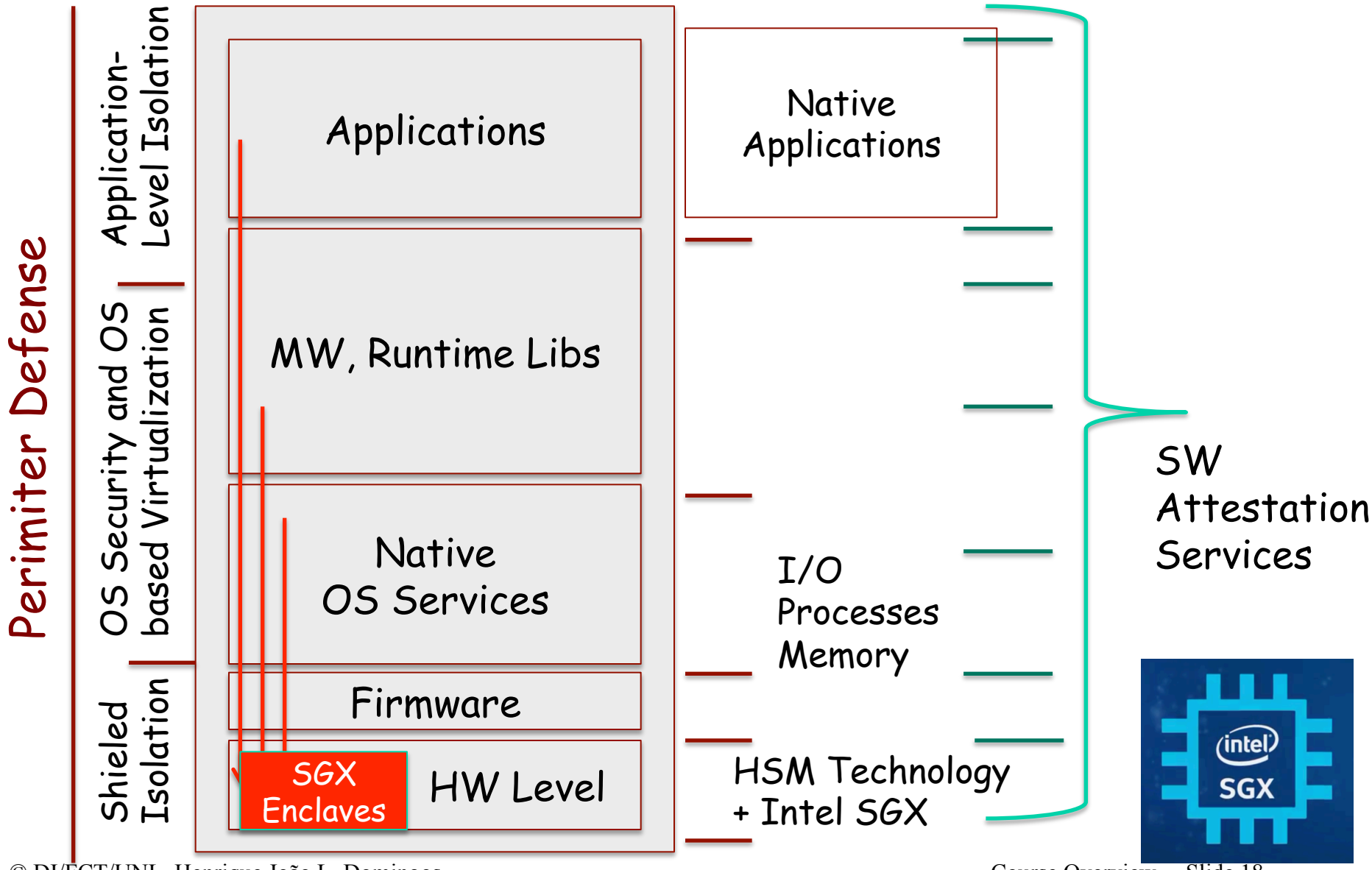
Scope of Computer Security Isolation and TCB Level



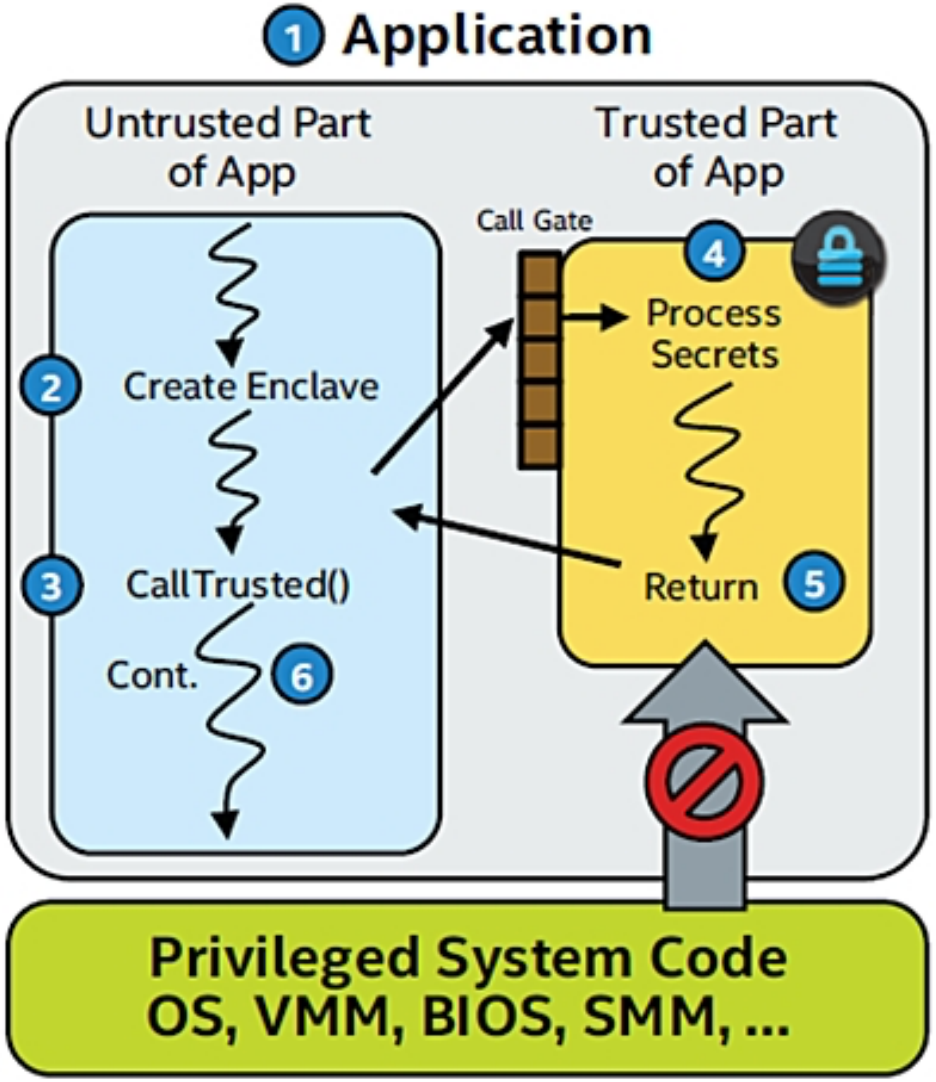
Concrete Implementation

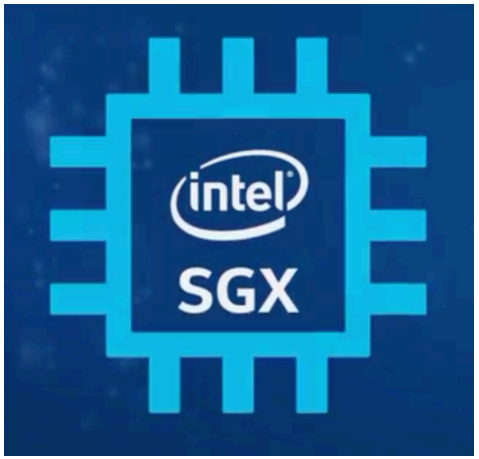


Concrete Implementation

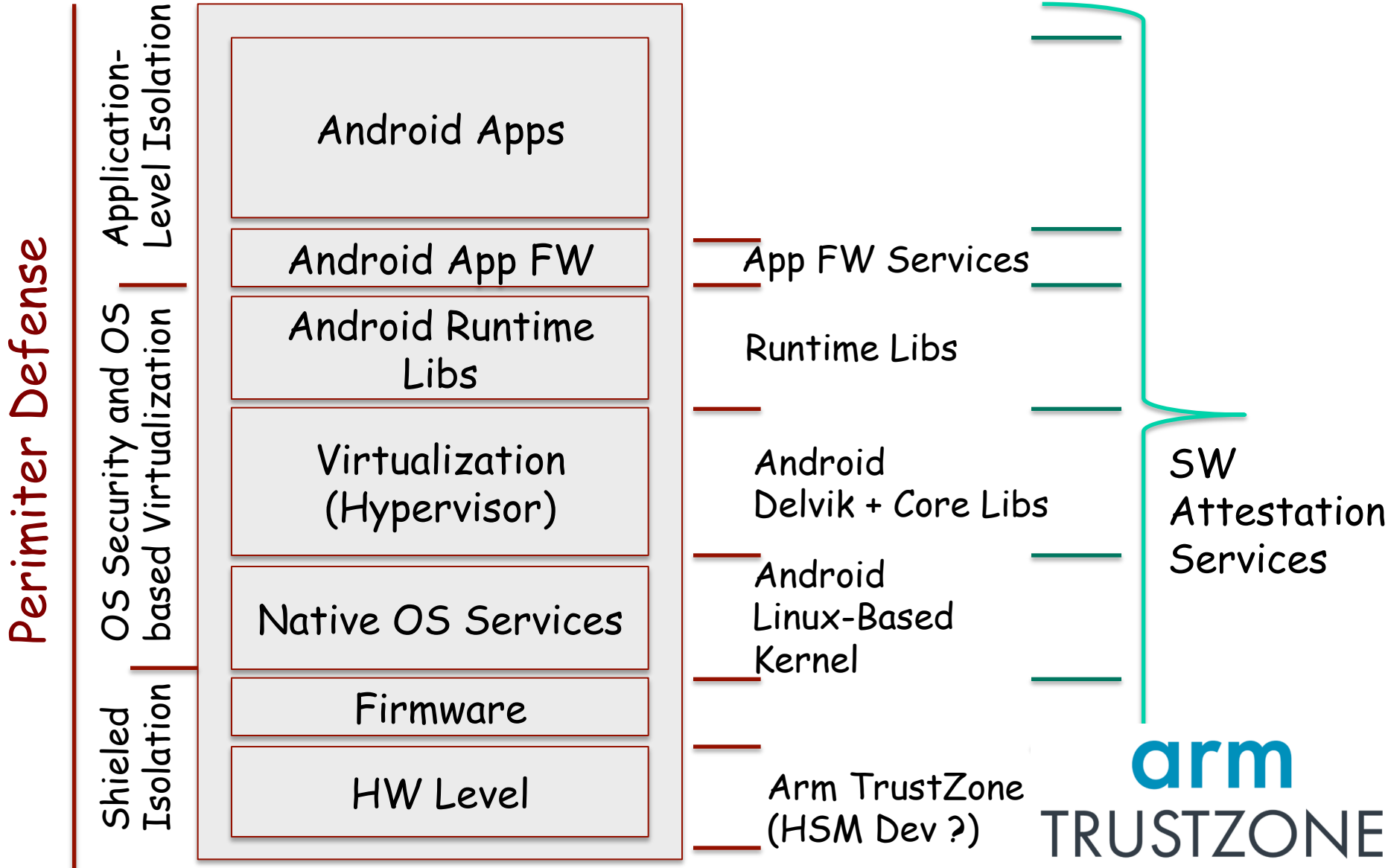


Intel SGX TEE Protection

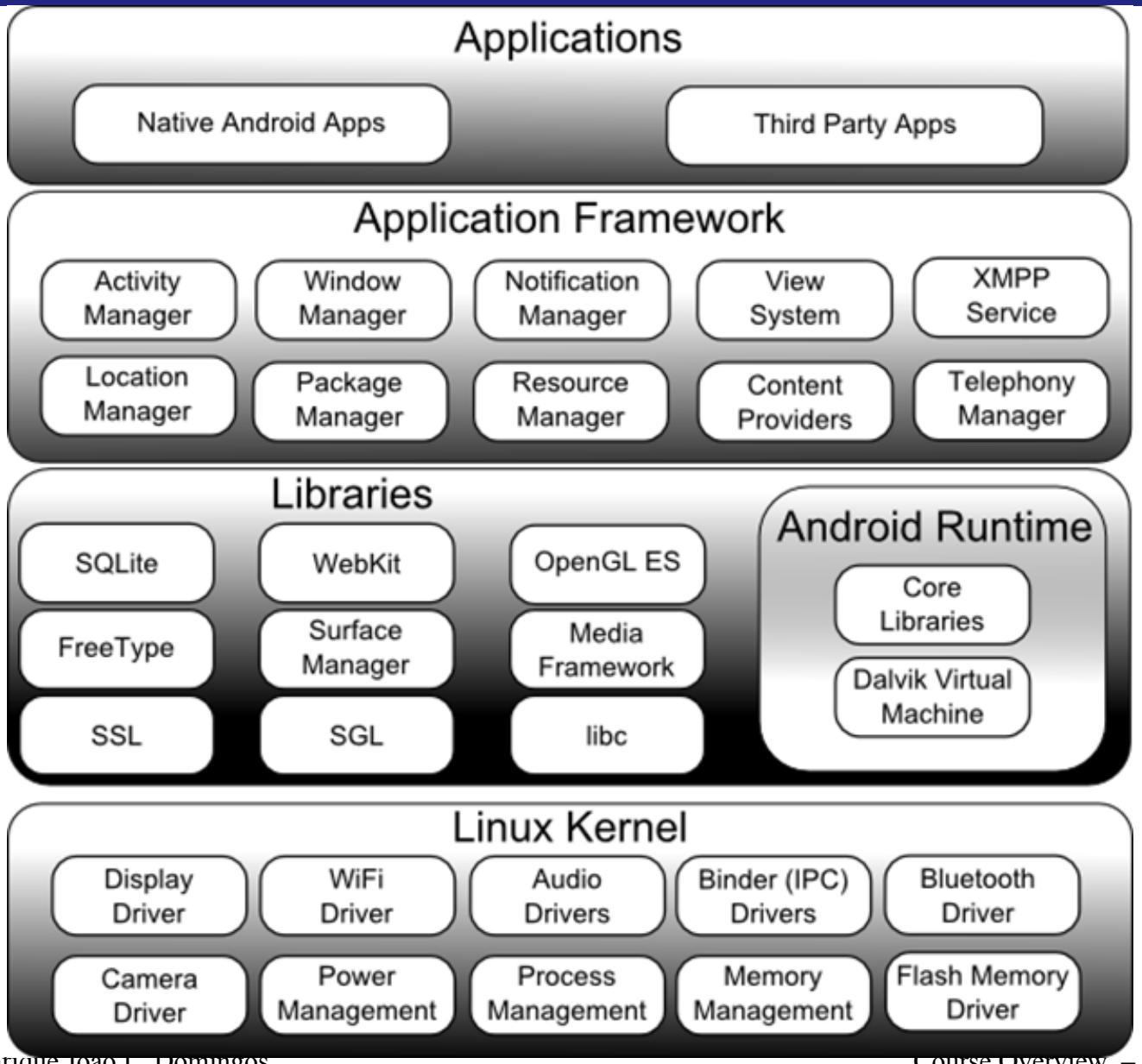




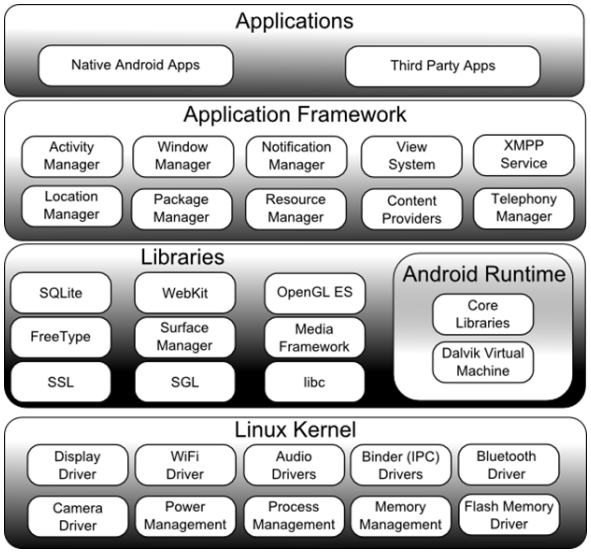
Another concrete Implementation
(ARM / Mobile Oses: Exemple w/ Android)



Android Architecture

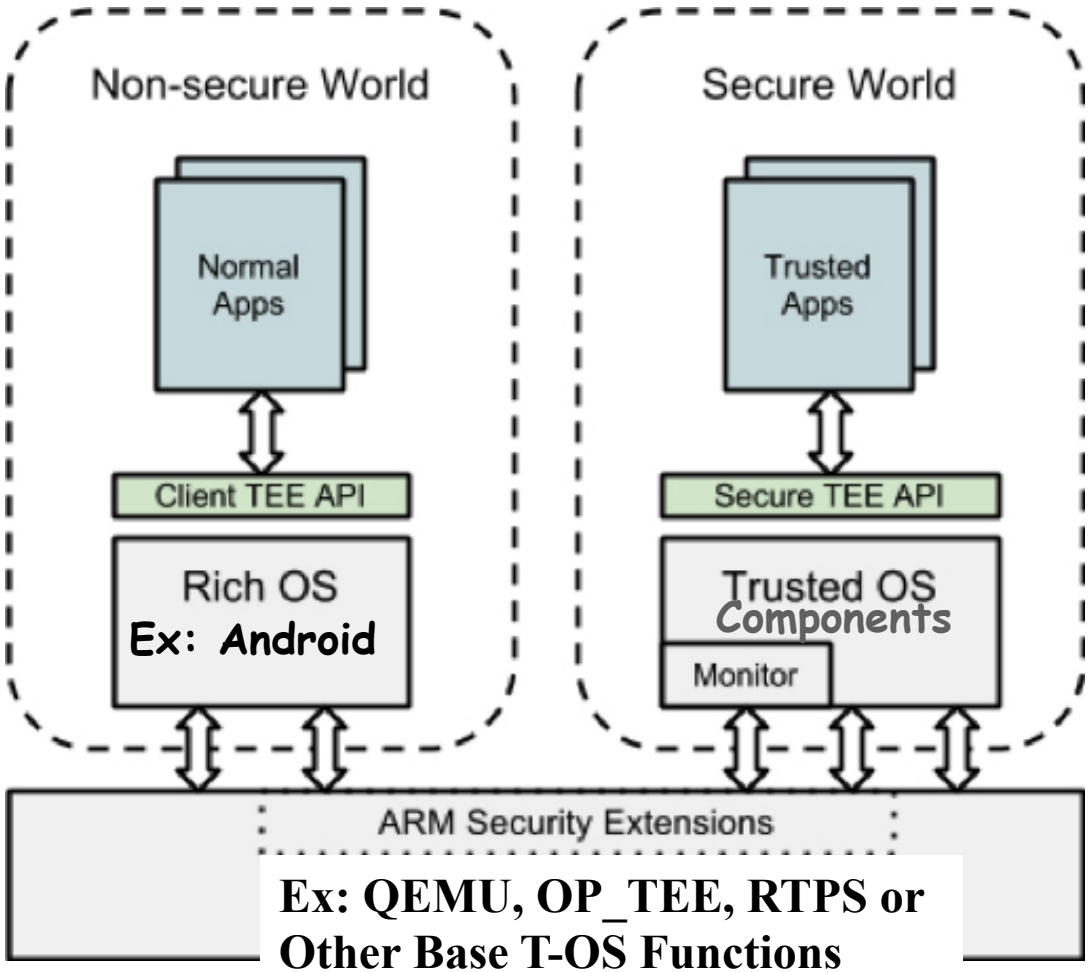


Ex: Android Architecture on HW-Shielded Trust Execution Environment



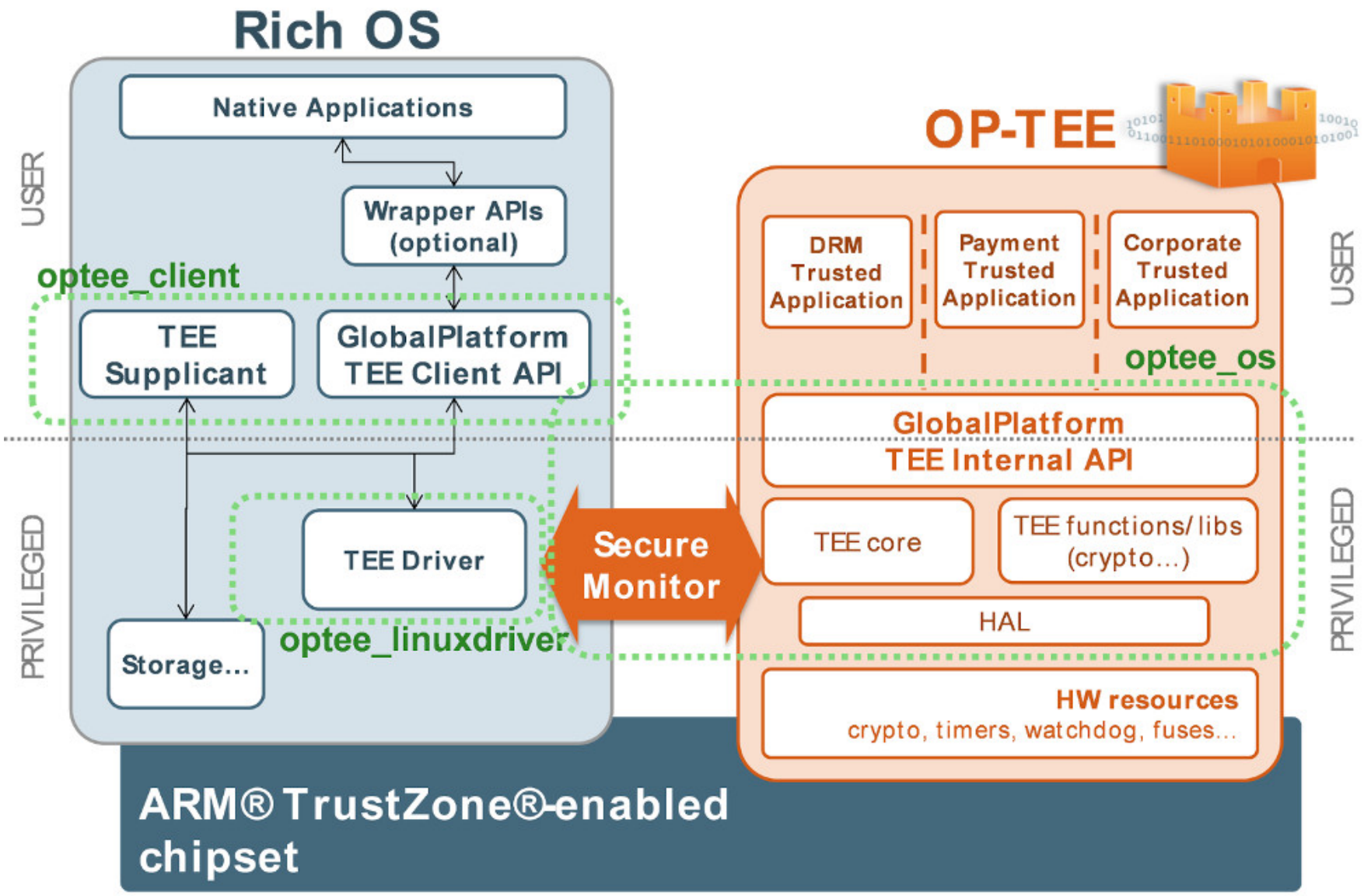
Mapping of Non-Sensitive Components

Mapping of Trusted Components



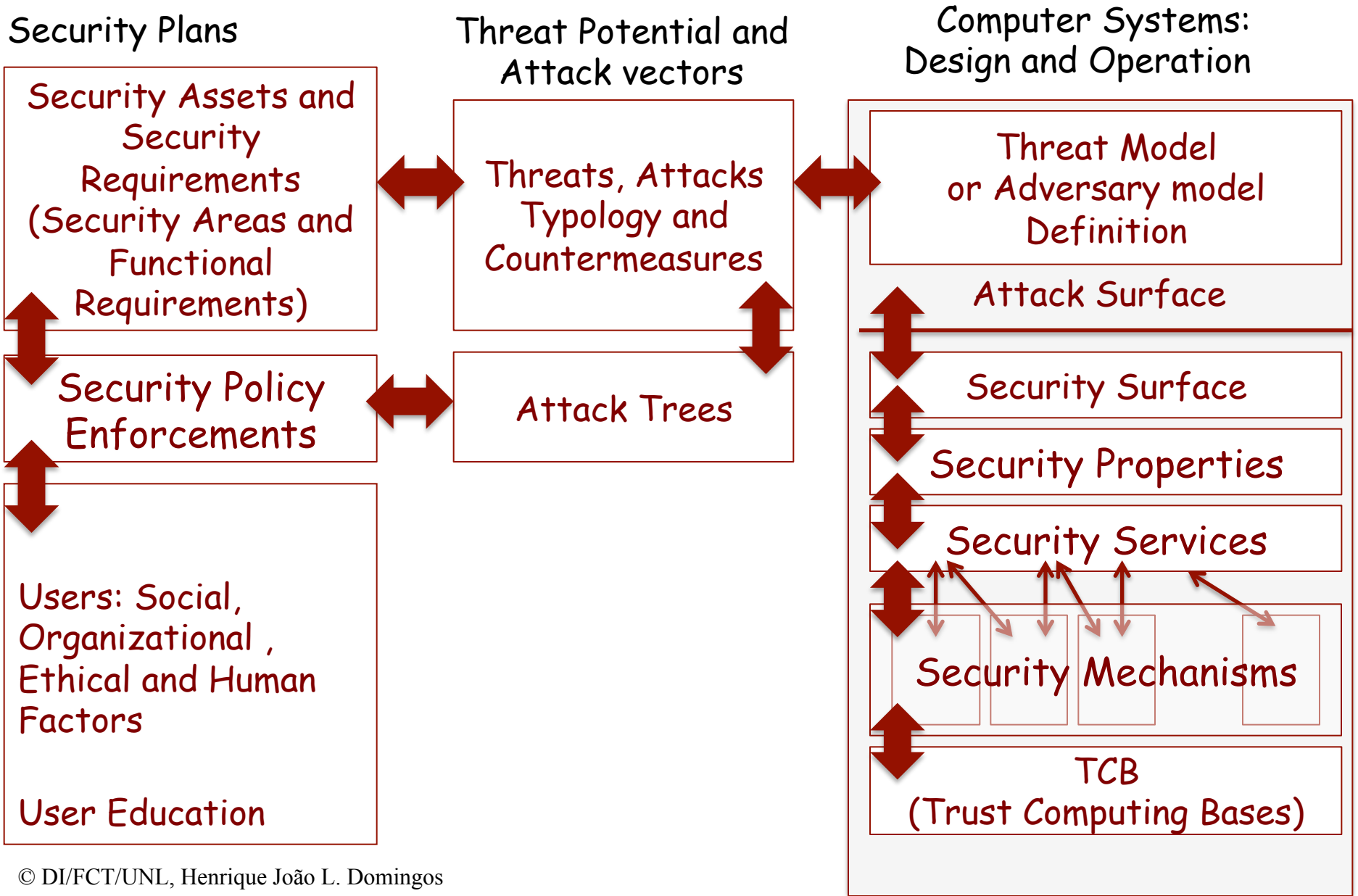
Ex: QEMU, OP_TEE, RTPS or Other Base T-OS Functions

TEE Architecture



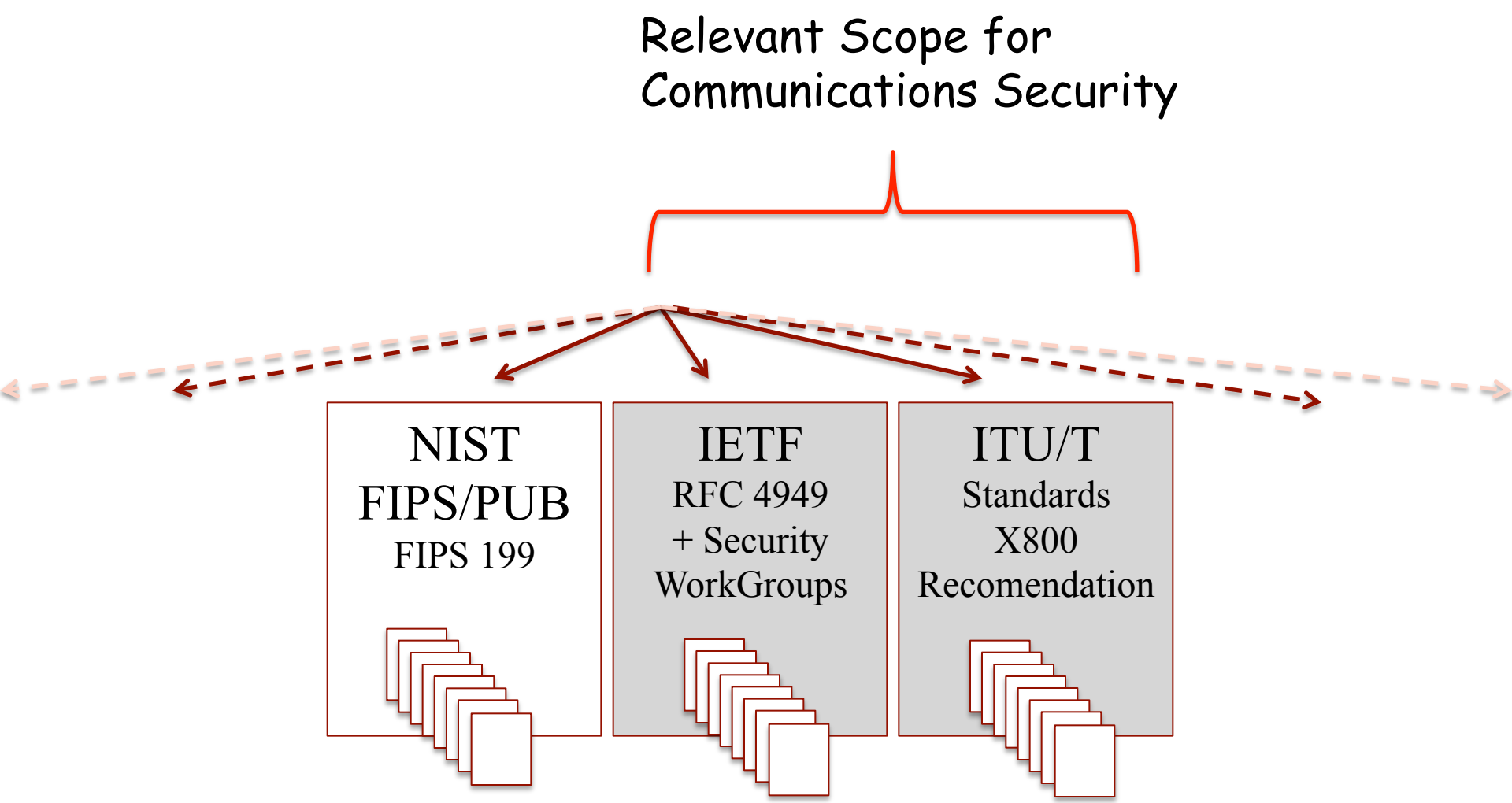
OSI X.800 Rec. IETF RFC 4949 + IETF Security Standards (RFC)

Remembering our initial (conceptual) Security Framework



Instantiation of standard frameworks

Technical Security Standardization Frameworks



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

Typology of Attacks

Communication Attack Typology

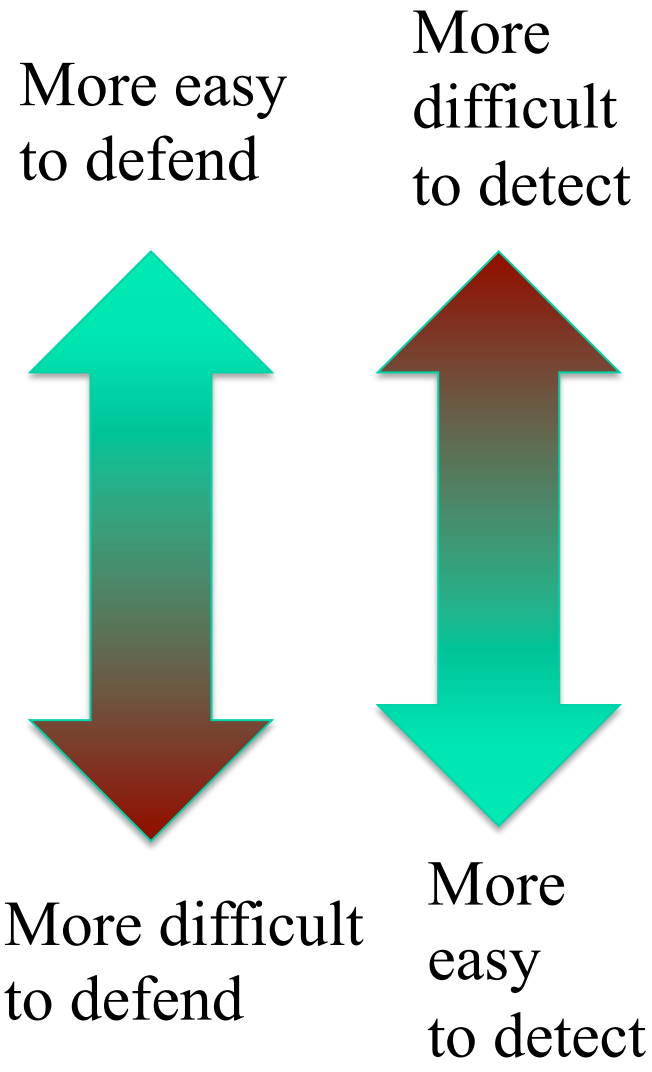
- **Passive Attacks**
  - Release of Message Contents (Payload Data Leakage)
  - Packet Analysis (Frame/Datagrams/Packet Sniffing)
    - Specific Targeted Data Packets
  - Traffic Analysis (at different stack layers)
    - Traffic Flow Inspection and Reconnaissance
- **Active Attacks**
  - Masquerade (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: Attacks

Communication Attack Typology

- **Passive Attacks**

- **Active Attacks**



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

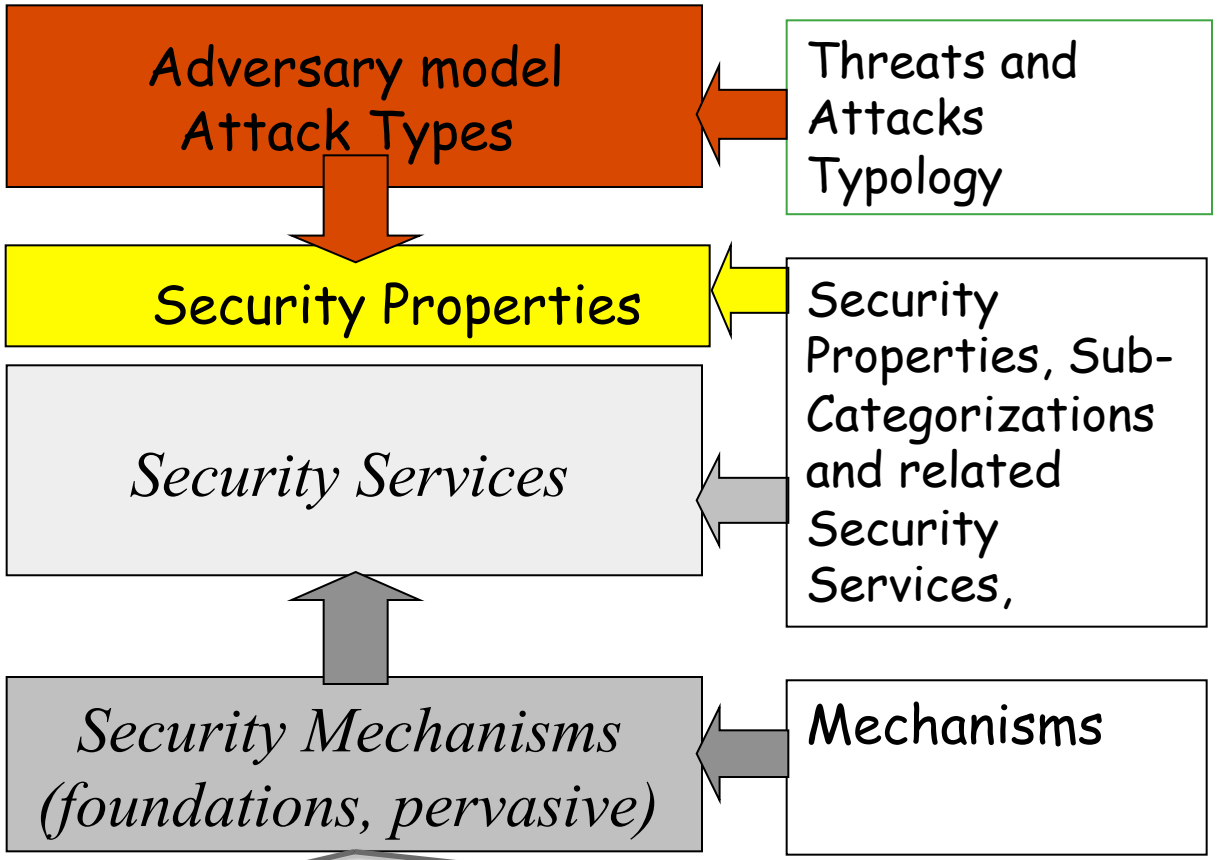
- Encipherment
- Digital Signatures
- Data Integrity
- Authentication Exchanges
- Access Control
- Traffic Padding
- Routing Control
- Notarization

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

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

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, Algorithms, 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 mechanisms

Authentication and Key Distribution Protocols

Service	Encipherment	Digital signature	Access control	Data integrity	Authentication exchange	Traffic padding	Routing control	Notarization
	Mechanism							
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

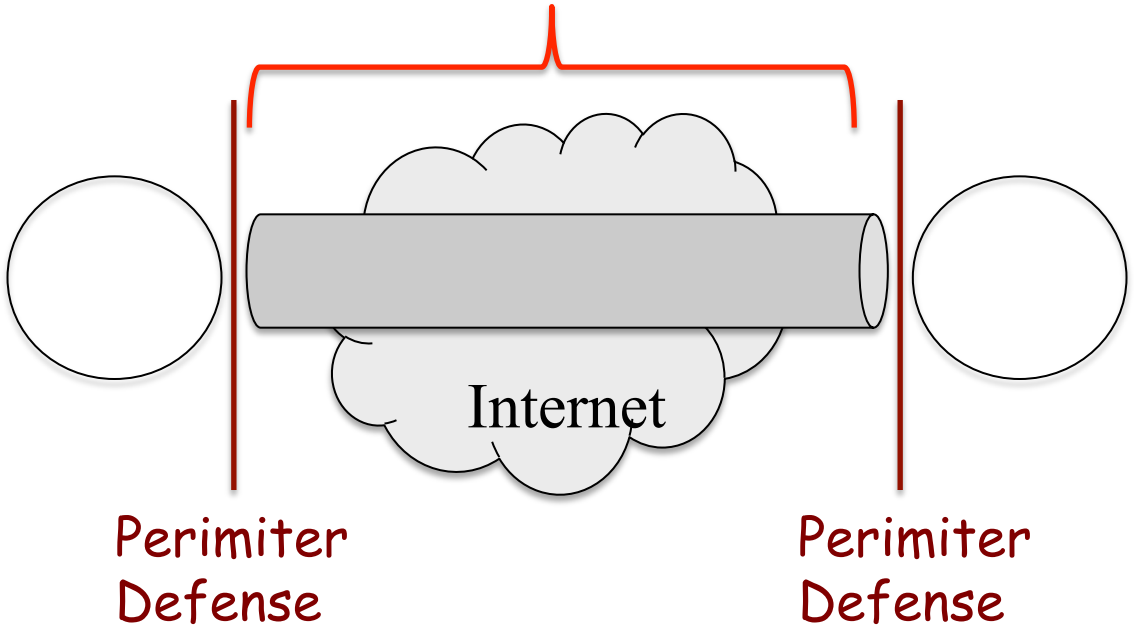
Asymmetric Crypto Methods

Secure Hash Funtions, HMACs or CMACs

Security Channel
(Definition using the OSI X.800 Reference)

How to define a Secure Channel ?

- Definition in the scope of the OSI X.800 framework
  - A communication channel immune to the Attack Typology and MiM threats, according to the OSI **X.800 attack typology and OSI X.800 defined services and mechanisms**
  - **PtP (Point-Point) vs. End-to-End Security Arguments**

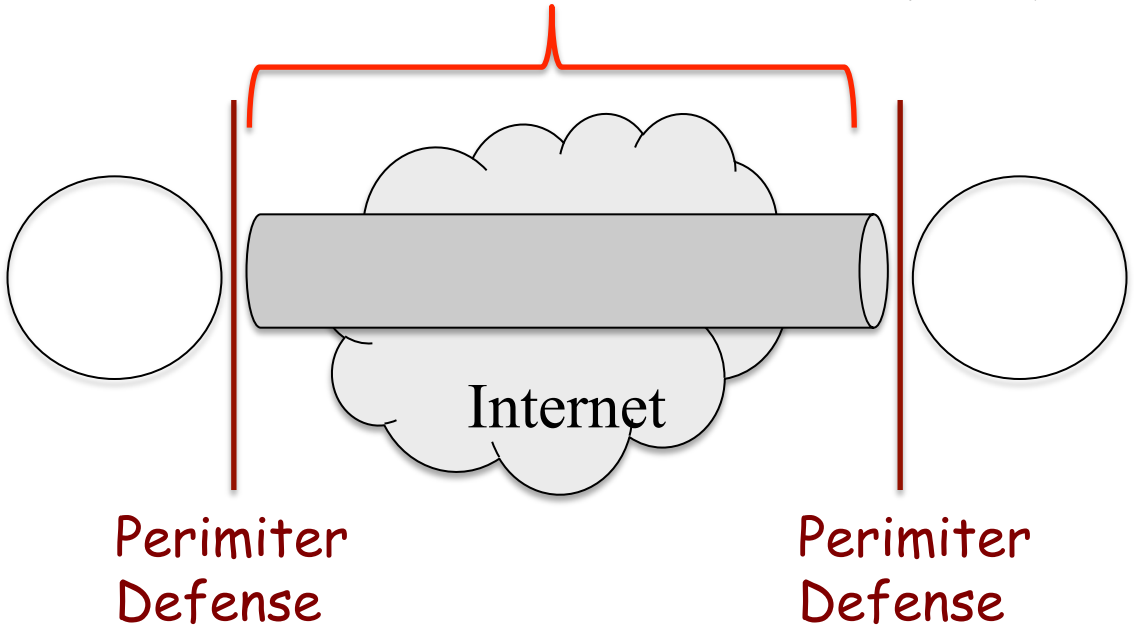


Properties in a Secure Channel ?
See the Security properties in the OSI X.800

- Authenticated endpoints (principals, mutual authentication, peer-authentication and data-authentication)
- Traffic and data flow confidentiality
  - Connection-oriented vs. Connectionless
- Traffic and data flow integrity
  - Connection-Oriented vs. Connectionless
- No replaying

Cryptography plays an important role !

Protection can be addressed at different Levels of Approach (in the Communication Stack)

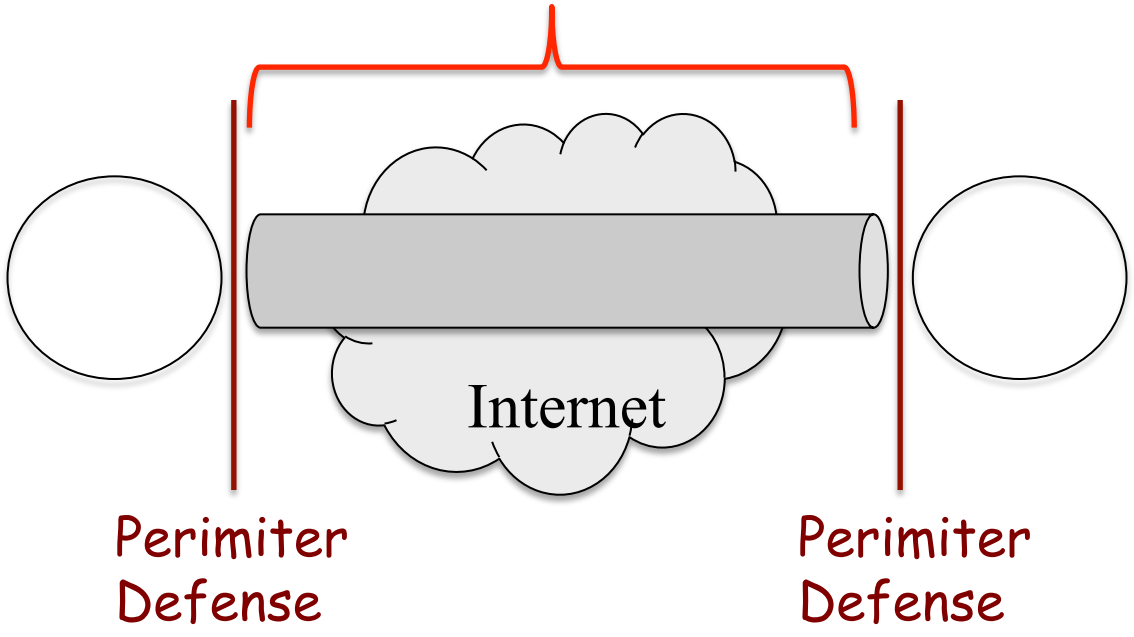


Properties in a Secure Channel ?
See the Security properties in the OSI X.800

What about …

- No Repudiation
- Routing Control
- Availability
- Net Access and Connection control
- Reliability
- …

Complementary Mechanisms and Services (out of the cryptography scpe)



The Role of Cryptographic Tools, Methods and Techniques

Important:

Cryptography is very important for Computer Systems and Network Security ! ...
... but it is not a PANACEA

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
  - Message authentication Codes
    - Sometimes called "Lightweight" Signatures
    - MACs, HMACs or CMACs

  Authentication

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 fopr Integrity Checks:
      - Cryptographic Hash Functions
      - Use of Cryptographic Hash Functions in HMACs

Integrity

Mappings in the X.800 framework

	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

	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			

Dependable Distributed Systems

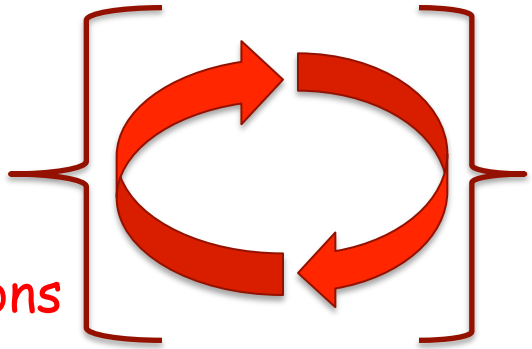
Computer Systems and Network Security

- 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

Dependable Systems

- **Dependable system:**
  - **a system we can depend on**
  - *A system is dependable if reliance can justifiably be placed on the service it delivers.*
  - **dependability** as the ability to provide services that can defensibly be trusted within a time-period.

Dependability

- In Systems Engineering: **dependability** as a measure (metrics) of the provided attributes

- In Software Engineering, **dependability** as the **ability to provide services that can defensibly be trusted within a time-period** (a certain life cycle)

- See, for ex: https://en.wikipedia.org/wiki/Dependability

Dependability and Dependable Systems

- Dependable systems are characterized by dependability attributes and metrics of their attributes:
  - **Availability:** continuity of correct operation
  - **Reliability:** readiness for correct operation
  - **Maintainability** and **maintenance support:** ability and functions for maintenance and repair (recovery)
  - **Performance:** operation provided in useful time
  - **Durability:** ability to remain functional and usable, with minimal or non-excessive maintenance or repair in a lifetime period
  - **Safety:** absence of bad / catastrophic consequences on the users and environment
  - **and Security:** Confidentiality, Integrity, Availability, Authenticity, Access Control,

    and also more and more … Privacy (including Data Privacy Privacy-Enhanced Computation)

Typology of Defenses in Distributed Systems Security for Dependability Criteria

Typology of Defenses (1)

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

Typology of Defenses

- **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

Typology of Defenses

- **Complexity Issues**
- **Realistic Approaches**

- **Perimeter Defenses vs. "in deep" Defenses**

Typology of Defenses

- **Complexity Issues**
- **Realistic Approaches**

- **Perimeter Defenses vs. "in deep" Defenses**
- **Perimeter Defenses (ex., IPS or FWs: NIPS, HIPS; IDS: HIDS, NIDS; Hpots 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

Typology of Defenses

- **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 securiry 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

Key-Criteria: 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 organziations (ex., ANSI, NIST, FIPS-PUB, ISO, IEEE, IETF ... IACR,) or Certified Labs (ex., NIST/NVLAP and accreditaded CMTLs, compliant implementations with valid/updated IETF/RFCs , RSA Labs, ...)

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

Complementary reading (*in Portuguese*)

- 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