




UNIVERSITY
OF TRENTO - Italy




Cyber Security Risk Assessment
Spring 2018

Lecture 7
Preventive Controls

11/03/18 Fabio Massacci - Cyber Risk Assessment 1





UNIVERSITY
OF TRENTO - Italy



Sample of Controls

- **Functional Classification**
 - Preventive
 - System Hardening → reduce opportunities
 - Software Patching → remove vulnerabilities
 - Detective
 - Intrusion Detection Systems → reduce likelihood
 - Likelihood (of exploit going unnoticed), may reduce impact (if corrective actions taken)
 - Audit Trails (as before, for humans)
 - Corrective
 - Back-up → it is done before the incident but it doesn't forbid the incident to happen → reduce impact
 - File Recovery → recover from impact
- **Conceptual Classification**
 - Procedural → organization level, related to humans operating system
 - Technical → system and software level
 - Physical → related to facilities



11/03/18 Fabio Massacci - Cyber Risk Assessment 2

 UNIVERSITY OF TRENTO - Italy 

Procedural Control Examples

- Policies and procedures
- Security plans
- Insurance and bonding
- Background and financial checks



11/03/18 Fabio Massacci - Cyber Risk Assessment 3

 UNIVERSITY OF TRENTO - Italy 

Procedural Control Examples (Cont.)

- Data loss prevention program
- Awareness training
- Rules of behavior
- Software testing



11/03/18 Fabio Massacci - Cyber Risk Assessment 4

 UNIVERSITY OF TRENTO - Italy 

Technical Control Examples

- Login identifier
- Session timeout
- System logs and audit trails
- Data range and reasonableness checks
- Firewalls and routers
- Encryption
- Public key infrastructure (PKI)

11/03/18 Fabio Massacci - Cyber Risk Assessment 5

 UNIVERSITY OF TRENTO - Italy 

Physical Control Examples

- Locked doors, guards, CCTV
- Fire detection and suppression
- Water detection
- Temperature and humidity detection
- Electrical grounding and circuit breakers

11/03/18 Fabio Massacci - Cyber Risk Assessment 6

UNIVERSITY OF TRENTO - Italy eit Digital MASTER SCHOOL

NIST SP 800-53 Control Families

- **Access Control (AC)**
- **Audit & Accountability (AU)**
- **Awareness & Training (AT)**
- **Configuration Management (CM)**
- **Contingency Planning (CP)**
- **Identification & Authentication (IA)**
- **Incident Response (IR)**
- **Maintenance (MA)**
- **Media Protection (MP)**
- **Personnel Security (PS)**
- **Physical & Environment Protection (PE)**
- **Planning (PL)**
- **Program Management (PM)**
- **Risk Assessment (RA)**
- **Security Assessment & Authorization (CA)**
- **System & Communications Protection (SC)**
- **System & Information Integrity (SI)**
- **System & Services Acquisition (SA)**


11/03/18 Fabio Massacci - Cyber Risk Assessment 7

UNIVERSITY OF TRENTO - Italy eit Digital MASTER SCHOOL


Preventive Controls

- **Countermeasures reduce risk and loss**
 - Reduce Threats
 - Reduce Chances and Vulnerabilities
 - Reduce impact of loss

11/03/18 Fabio Massacci - Cyber Risk Assessment 8




UNIVERSITY
OF TRENTO - Italy




Key Idea of Preventive Controls

- ***To prevent “stuff” from happening you must***
 - Mediate actions between system & rest of world
 - Attribute actions to good or bad actors
 - Understand what is right and what is wrong
- ***OASIS XAML Key “Logical” Components***
 - Policy Enforcement Point
 - Policy Decision Point
 - Policy Information Point
 - Policy Administration Point
- ***Invented for Web access control but concepts are pretty general.***

11/03/18 Fabio Massacci - Cyber Risk Assessment 9




UNIVERSITY
OF TRENTO - Italy




XACML Model’s Actors

- ***PAP – Policy Administration Point***
 - The (logical) system entity that creates a *policy* or *policy set*
- ***PEP – Policy Enforcement Point***
 - The (logical) system entity that performs access control, by asking decision requests and enforcing authorization decisions
- ***PDP – Policy Decision Point***
 - The (logical) system entity that evaluates applicable policy and renders an authorization decision
- ***PIP – Policy Information Point***
 - The (logical) entity that acts as a source of attribute values
 - Attributes describing subjects (users), resources, environments (contexts) used to decide whether a control process apply
- ***Conceptually distinct entities but implementation can be instantiated by single entity***

11/03/18 Fabio Massacci - Cyber Risk Assessment ▶ 10



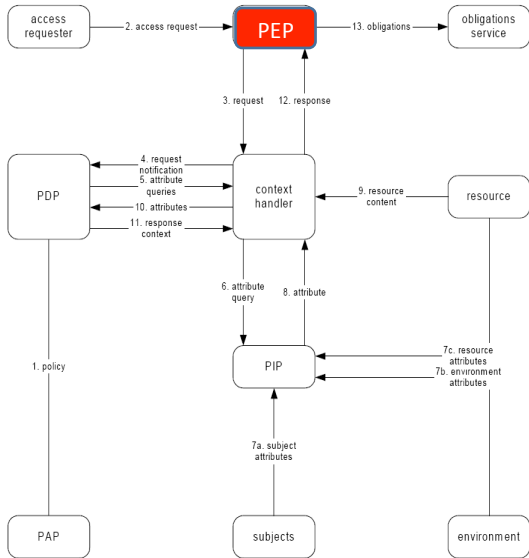
UNIVERSITY OF TRENTO - Italy



XACMI Main Actors

Policy Enforcement Point


- Entity protecting the resource (e.g. file system)
- Performs access control by making decision requests and enforcing authorization decisions and executing obligations




The diagram illustrates the XACMI Main Actors in a Policy Enforcement Point (PEP) scenario. The actors and their interactions are as follows:

- access requester** sends an **access request** (2) to the **PEP**.
- PEP** sends a **request** (3) to the **context handler**.
- context handler** sends a **request notification** (4) to the **PDP**.
- context handler** sends **attribute queries** (5) to the **PDP**.
- PDP** returns **attributes** (10) to the **context handler**.
- context handler** sends a **response context** (11) to the **PDP**.
- context handler** sends an **attribute query** (6) to the **PIP**.
- PIP** returns **attribute** (8) to the **context handler**.
- context handler** sends **resource content** (9) to the **resource**.
- resource** sends **resource attributes** (7c) and **environment attributes** (7b) to the **PIP**.
- subjects** send **subject attributes** (7a) to the **PIP**.
- PIP** sends a **response** (12) to the **PEP**.
- PEP** sends **obligations** (13) to the **obligations service**.
- PAP** provides **policy** (1) to the **PDP**.
- environment** provides **resource** to the **context handler**.

11/03/18
Fabio Massacci - Cyber Risk Assessment
► 11



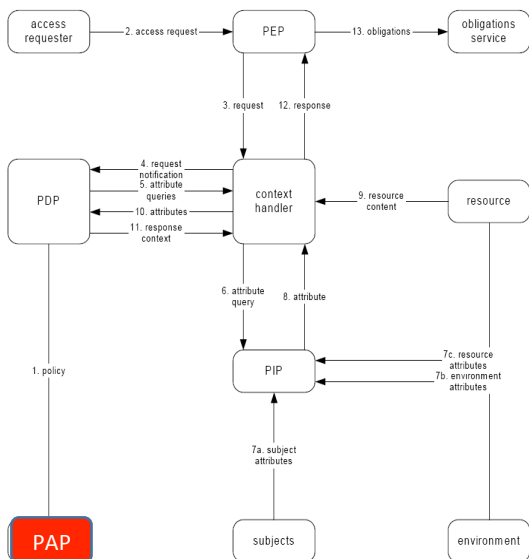
UNIVERSITY OF TRENTO - Italy



XACMI Main Actors

Policy Administration Point

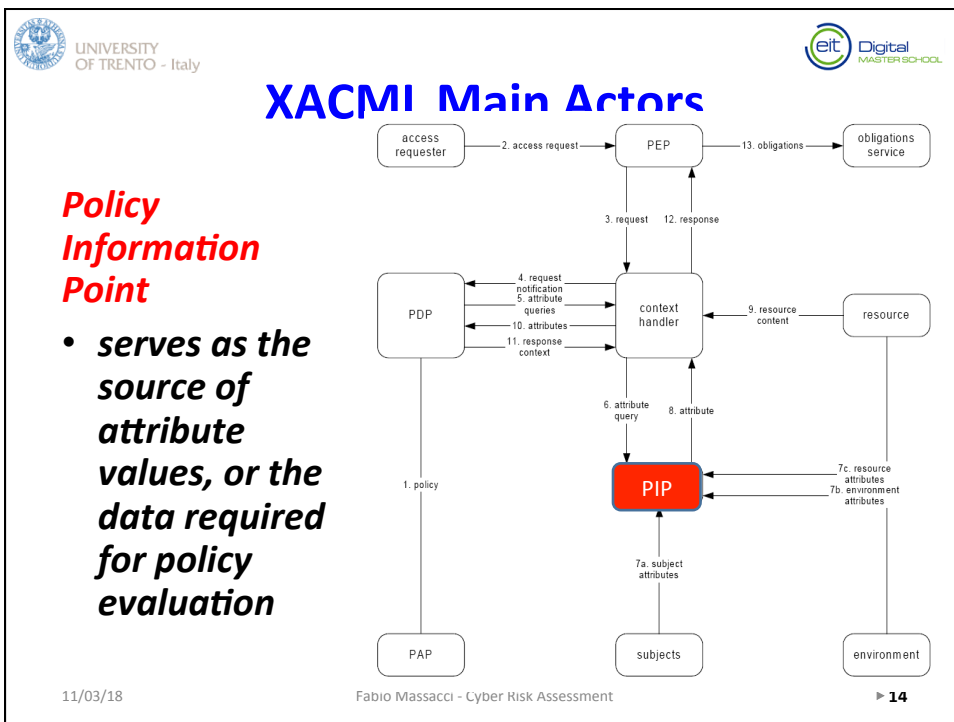
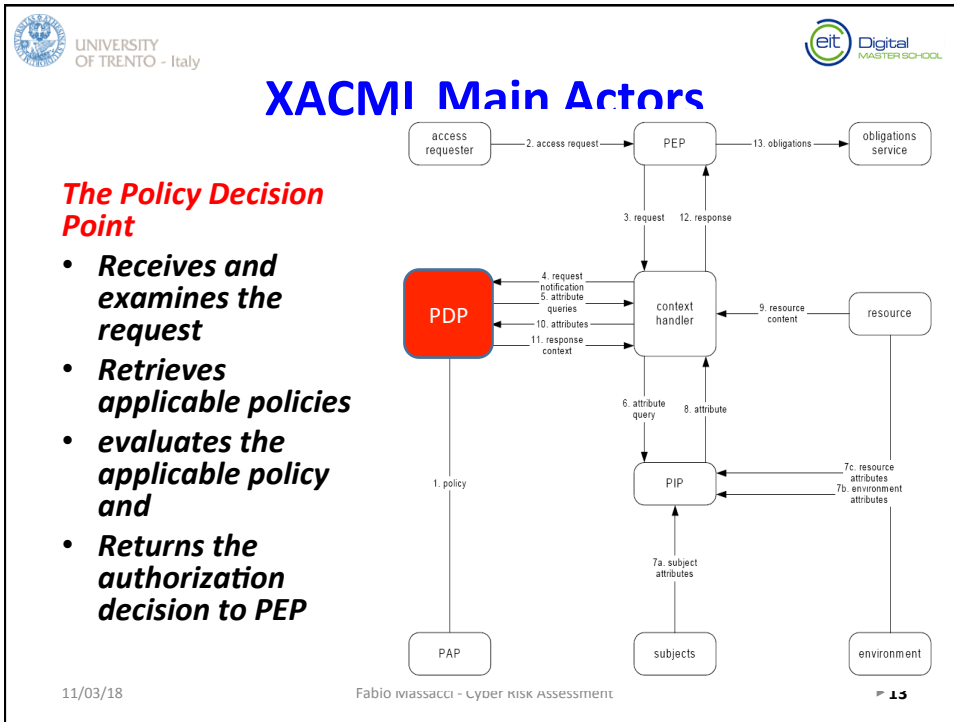
- creates security policies and stores these policies in the repository

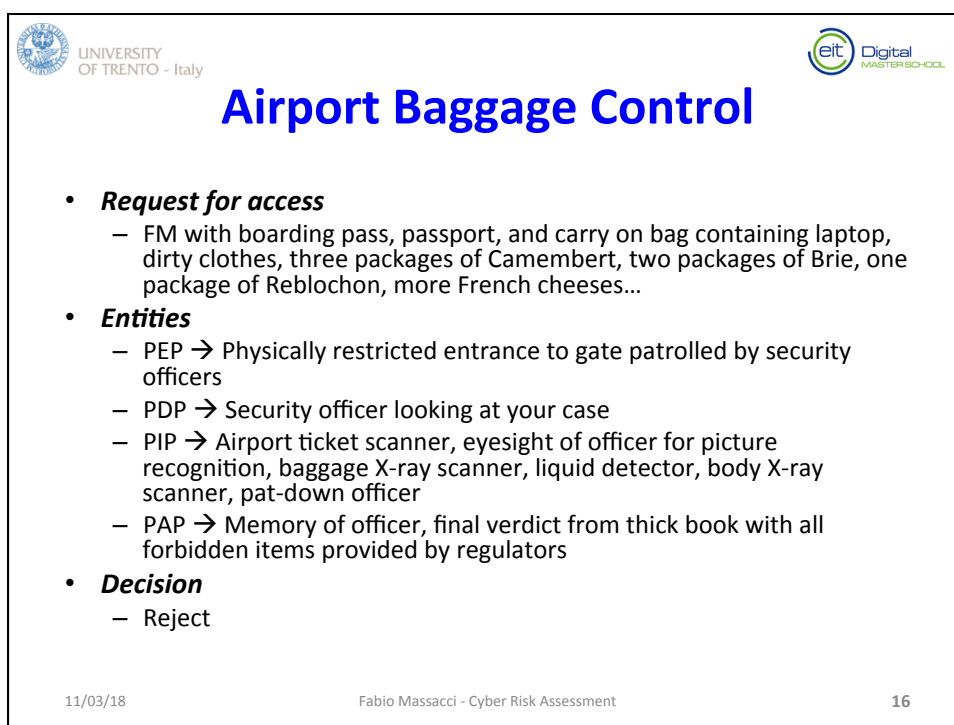
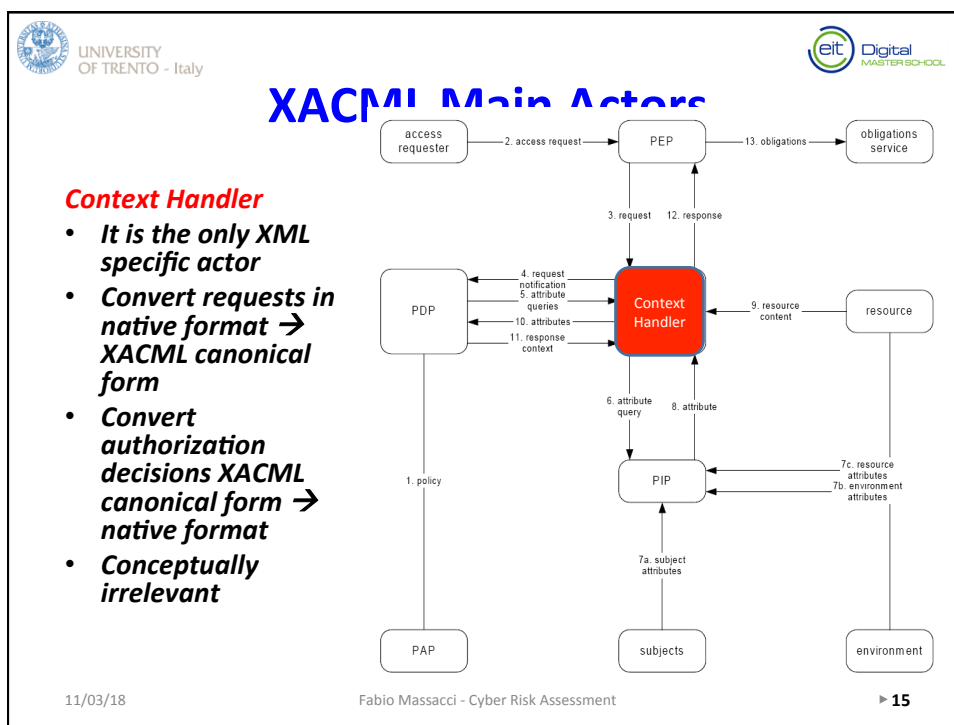



The diagram illustrates the XACMI Main Actors in a Policy Administration Point (PAP) scenario. The actors and their interactions are as follows:

- access requester** sends an **access request** (2) to the **PEP**.
- PEP** sends a **request** (3) to the **context handler**.
- context handler** sends a **request notification** (4) to the **PDP**.
- context handler** sends **attribute queries** (5) to the **PDP**.
- PDP** returns **attributes** (10) to the **context handler**.
- context handler** sends a **response context** (11) to the **PDP**.
- context handler** sends an **attribute query** (6) to the **PIP**.
- PIP** returns **attribute** (8) to the **context handler**.
- context handler** sends **resource content** (9) to the **resource**.
- resource** sends **resource attributes** (7c) and **environment attributes** (7b) to the **PIP**.
- subjects** send **subject attributes** (7a) to the **PIP**.
- PIP** sends a **response** (12) to the **PEP**.
- PEP** sends **obligations** (13) to the **obligations service**.
- PAP** provides **policy** (1) to the **PDP**.
- environment** provides **resource** to the **context handler**.


11/03/18
Fabio Massacci - Cyber Risk Assessment
► 12








UNIVERSITY
OF TRENTO - Italy




Airport Baggage Control - II

- **Identification**
 - Valid Boarding Pass associate name to entity
- **Authentication**
 - Officer links claimant to entity identified by boarding pass by looking at (a) presence of passport linked to entity, (b) presence of picture linked to claimant
- **Authorization**
 - Identify all material requests brought by claimant
 - Bring in dirty clothes → ok
 - Bring in laptop → check laptop for explosive → ok
 - Bring in Reblochon → ok
 - Bring in Camembert → No → repeated request → check big 100 pages book → Camembert forbidden → reject
 - Make final decision
 - Policy = any item rejected → reject claimant
 - Enforce decision

11/03/18 Fabio Massacci - Cyber Risk Assessment 17



UNIVERSITY
OF TRENTO - Italy



Firewalls

- **Network Firewall (PEP, PDP, PIP, PAP)**
 - PEP = Mediate all input and output traffic arriving to a subnet
 - PIP = values in IP packet, provenience physically authenticated
 - either incoming cable or outgoing cable
 - PDP = reject based on port and provenance
- **Application Firewall**
 - PEP → mediate all requests arriving to application
 - PIP → reconstruct instruction from individual network packets

11/03/18 Fabio Massacci - Cyber Risk Assessment 18

UNIVERSITY OF TRENTO - Italy eit Digital MASTER SCHOOL

Where to actually deploy a PEP

- Different forms of interaction are possible**

kernel supported
(e.g. in O/S)

interpreter

modified application: inline
reference monitor (IRM)

11/03/18
Fabio Massacci - Cyber Risk Assessment
19

UNIVERSITY OF TRENTO - Italy eit Digital MASTER SCHOOL

Enforcement Design Choices (II)


- Reference monitor**
 - may not capture all "high-level" events
 - More difficult to escape
- Wrapper/interpreter**
 - performance overhead
 - Example is request for water on the plane → access mediated by airport crew
- Instrumentation: merge monitor into program**
 - different security policies != different merged-in code
 - pay only for what you use
 - Impossible for humans
- What happens if things don't work? Is the program or the security fault?**

Reference monitor


Interpreter

Program instrumentation

11/03/18
Fabio Massacci - Cyber Risk Assessment
20




UNIVERSITY
OF TRENTO - Italy




Ideal Properties

- **Perfect Mediation**
 - It is impossible to bypass the security mechanism
- **Transparency**
 - If your request is legitimate it should go true “as if” the system did not exist → ideally you shouldn’t even realize you are being monitored
- **Soundness (or Security)**
 - All allowed actions should respect the security policy (or made eventually to do so)

11/03/18 Fabio Massacci - Cyber Risk Assessment 21




UNIVERSITY
OF TRENTO - Italy




Enforcement Design Choices (III)

- **Reference Monitor as the “Default” PEP**
 - Observes the execution of a program/process and halts the program if it’s going to violate the security policy.
- **Most enforcement mechanisms are reference monitors**
 - They are “simple” to build and understand
 - But can miss the semantics of events
- **Common Examples:**
 - O.S. memory protection
 - Access control checks
 - Routers and Firewalls
 - Security officer at airport gates

11/03/18 Fabio Massacci - Cyber Risk Assessment 22




UNIVERSITY
OF TRENTO - Italy




Enforcement Design Choice IV

- **Beijing 1995 – UN Women’s Conference**
 - My (now) wife was an official delegate to the conference on behalf of the European Youth Forum
 - You don’t want nosy NGOs stepping into something they shouldn’t (e.g. China is still very poor) or talking to somebody they shouldn’t (eg human right)
- **Enforcement Mechanism → interpreter**
 - All delegate accompanied by volunteers who will show them around and steer them throughout in the right “shiny” places
- **Not perfect though**
 - By casual conversation found “volunteers” were members of Chinese Army
 - Lack of transparency
 - At some point my wife and her friend went out for lunch “unattended”, turned the wrong way and went into into a poor restaurant (the owner took orders, then took the bike and went to buy the ingredients) → later people arrived and were involved in a western-movie-style tavern brawl
 - Lack of perfect mediation → led to failure of security policy

11/03/18 Fabio Massacci - Cyber Risk Assessment 23



UNIVERSITY
OF TRENTO - Italy



Additional Reading

- **Ross Anderson’s book**
- **NIST SP 800-53 Control Families**
 - Don’t just pick random controls from there → think first: do they apply to you?

11/03/18 Fabio Massacci - Cyber Risk Assessment 24