Policy-Based Language for Autonomous and Adaptive Security

Frédéric Cuppens
Professor, Télécom Bretagne
Activity at Télécom Bretagne

- Professor in the LUSSI department
  - Training of graduate engineer students in Telecommunications with specialization in computer security
  - In-service training in cyber security track “Security administrator”.

- Responsible for the CNRS Team SFIIS
  - Security, reliability and integrity of information and systems
  - Joint team with Télécom Bretagne, UVO and ENSTA Bretagne
  - 12 professors
  - 1 CNRS researcher
  - 5 research associates
  - 20 PhD students
Activity at Télécom Bretagne

- Professor in the LUSSI department
  - Training of graduate engineer students in Telecommunications with specialization in computer security
  - In-service training in cyber security track “Security administrator”

- Responsible for the CNRS Team SFIIS
  - Security, reliability and integrity of information and systems
  - Joint team with Télécom Bretagne, UBO and ENSTA Bretagne
  - 12 professors
  - 1 CNRS researcher
  - 5 research associates
  - 20 PhD students
Activity at Institut Mines-Télécom

- Leader of the Thematic Network on Security of Digital Services and Systems
  - Cluster of competency
    - Telecom Paristech, Telecom SudParis, Telecom Bretagne
    - Mines ParisTech, Mines de Nancy, Mines de Nantes, Mines de Saint-Etienne
    - Eurecom
  - 52 permanent staff
    - Largest and strongest research group in Computer Security in France
  - Strengthen collaboration through joint project and research lab with industrial partners
On going collaborative projects

- European projects (FP7)
  - Intertrust: Trusted Interoperable Infrastructure
  - Demons: Decentralized, cooperative and privacy-preserving monitoring

- European projects (ITEA)
  - Predykot: Policy REfined DYnamically and Kept On Track
  - Adax: Intrusion Detection and counter-measure simulation

- National projects (ANR)
  - Pairse: Preservation of confidentiality in Web services environments:

- National projects (FUI and PIA)
  - Frag&Tag: Fragmentation and watermarking of sensitive databases
  - Austral: Security policy for distribution of TV on open network over the top
  - MO3T: Cloud infrastructure for open and interoperable digital library
  - ISER: Secure interoperability for multi-source intelligence systems
Joint labs with industrial partners

- **Cyber Security Lab**
  - With Airbus Group / Cassidian

- **Secure Compression Lab**
  - With Secure IC and DOREMI

- IDentity & Security Alliance Lab (TPT)
  - With SAFRAN / MORPHO

- SEIDO Lab (TPT)
  - With EDF R&D
  - Security of Internet of Things in Electric Plants

- On going negotiation with Thales
Research project

- Policy-Based Language for Autonomous and Adaptive Security
  - Concept of autonomous and adaptive security
  - Policy-Based language for adaptive security
  - Autonomous policy deployment
  - Policy interoperability and negotiation
Concept of Autonomous and Adaptive Security
Concept of Autonomous and Adaptive Security

« Classical » Security

- Security policy specification
- Deployment
- Configuration
- Intrusion detection
- Response

Autonomic Security

- Security policy interoperability
- Self deployment
- Self configuration
- Self evaluation (Risk, Impact)
- Autonomic response
A typical infrastructure to operate security policies …
The policy is administered and enforced -downwards- ...
The result is measured and reported upwards...
Enforcement and reporting are independent and un-correlated.
Objective of adaptive security management
Closing the loop of security policy
Key issues

- Contextual policy-based language
- Self evaluation of risk and impact
- Self deployment and configuration
- Autonomous negotiation of policy and trust
Policy-Based language for adaptive security
Modeling contextual security policies
The OrBAC model

- Organization based access control

[Diagram showing OrBAC model with nodes labeled as follows:
- Context
- Organization: Hospital
- Doctor
- Consult
- Med_record
- Role
- Activity
- View
- Subject
- Action
- Object
- Bob
- read
- Mary_record
- Attending Physician]
Modeling contexts

- Key component of policy adaptation
  - Policy changes when new contexts are activated
  - Activation of new security rules

- Adaptation to the user’s behavior
  - Location based context
  - Provisional context

- Adaptation to the system environment
  - Temporal context
  - Emergency context

- Adaptation to risk evolution
  - Threat based context
Context based language

- State based context
  - Logical rule: \( \text{Hold(Org,S, A, O, Ctx)} : - f1, \dots, fn \)
  - Example:
    \( \text{Hold(Hosp,S,_,_, in operating room)} : - \text{Location(S, L), Type(L, operating\_room)} \)

- Event based context
  - \( \text{Start(Ctx)}: \) moment at which Ctx begins to hold
  - \( \text{End(Ctx)}: \) moment at which Ctx stops to hold

- Context based language
  - \( \text{CE}_S: \) set of state context expression
  - \( \text{CE}_E: \) set of event context expression

- \( \text{CE}_S ::= \text{Always} | \text{Never} | C_S | \text{CE}_S \& \text{CE}_S | \text{CE}_S \oplus \text{CE}_S | - \text{CE}_S | [ \text{CE}, \text{CE} ] \)
- \( \text{CE}_E ::= \text{start(CE}_S) | \text{end(CE}_S) | \text{CE}_S \& \text{CE}_E | \text{CE}_E \& \text{CE}_S \)
- \( \text{CE} ::= \text{CE}_S | \text{CE}_E \)
Modeling contextual security policies
Part 1: Access control

- Permission and Prohibition

- Examples
  - Prohibition(Hosp, Nurse, Consult, Med_record, Always)
  - Permission(Hosp, Nurse, Consult, Med_record, Emergency)

- Key issues and contribution
  - Detection of anomalies
    - Shadowing, Redundancy
  - Detection and management of conflicts
    - Derivation of a policy free of conflict
    - Consistent management of exceptions
  - Administration and delegation
    - AdOrBAC
    - Detection of anomaly in a delegation chain

### Table Example

<table>
<thead>
<tr>
<th>Type</th>
<th>Derives from</th>
<th>Subject</th>
<th>Action</th>
<th>Object</th>
</tr>
</thead>
<tbody>
<tr>
<td>permission</td>
<td>perm1</td>
<td>Gerard</td>
<td>configure serv1</td>
<td>computer2</td>
</tr>
<tr>
<td>prohibition</td>
<td>prohib1</td>
<td>Gerard</td>
<td>edit www config</td>
<td>computer1</td>
</tr>
<tr>
<td>prohibition</td>
<td>prohib2</td>
<td>Gerard</td>
<td>edit www config</td>
<td>computer1</td>
</tr>
</tbody>
</table>

### AdOrBAC

- Detection of anomaly in a delegation chain

### MotOrBAC

- Lab-STICC
Modeling contextual security policies
Part 2: Usage control

- Obligation and dispense
- Examples
  - Obligation(Hosp, Nurse, Write, Med_report, Emergency_consult, Delay(3days))
  - Obligation(Hosp, Nurse, Check_up, Patients,
    Start(Working_hours), End(clinic_hours), groupContext(∀o∃a∃s))
- Key issues and contribution
  - Reference monitor for usage control
    - Based on Event-Condition-Action rules specification
    - Proof of determinism and termination of the decision
  - Conflict in obligations with deadline
    - Situation calculus for planning obligations with deadline
  - Collective obligations
  - Delegation of obligations
    - Formal model for responsibility, liability and accountability
Response Policy

Step 1: Threat pre-characterization

OrBAC security rules by use cases and referenced alerts
Step 2: Threat characterization

- **Context of applicable response**
- **Rules**
- **OrBAC**
- **Information Matcher**
- **Alert**
- **Context parameters**

Organization rules of applicable response
Response Policy

Step 3: Policy Instantiation

Context of applicable response

Rules
OrBAC

Information Matcher

Context parameters

MotOrBAC

Organization rules of applicable response

Policy instances

Alert

Lab-STICC
Response policy

- Impact evaluation
  - Taxonomy of countermeasures based on their effect on the system and on the attack
  - Model of attack likelihood based on attack graphs
  - Model of response parameterized by the intruder’s level of skill and knowledge

- Analysis of dependencies
  - Service Dependency Framework Model in AADL (Architecture Analysis and Design Language)
  - Management of alternative response
  - Management of logical and physical dependencies in policy based response
Autonomous policy deployment
Security policy deployment and configuration

- Problem

Global policy

- Self policy deployment and configuration
  - Network
  - Operating system
  - Database
  - Service
Security policy deployment and configuration

- Different approaches
  - Pushing configuration
    - Network, Operating systems and web services
  - Rewriting queries
    - Database management systems
  - Weaving security aspects
    - Trusted service interoperability
    - Security and privacy by design
Some contributions

- Global OrBAC policy
- Pushing network configuration
- XACML Translation
- Query rewriting
- Secure Service Interoperability
- Access control To web services
- fQuery
fQuery
Secure rewriting of SPARQL queries
"Instrumentation" with OrBAC

Simple example

```
SELECT ?name ?age
WHERE{
  FILTER EXISTS{
    ?doc rdf:type O:Doctor.
    ?doc O:hasId ?id.
    FILTER(?id=$bob_id)
  }
}
```

Permission(Hospital, Doctor, Read, Med_record, Attending_Phasician)
Hold(Hospital, s, a, o, Attending_Phaician) \(\Leftarrow\)
patient_data(o,p) \& doctor(s,p)
### Privacy preferences

<table>
<thead>
<tr>
<th>Data Owner</th>
<th>Field</th>
<th>Consent</th>
<th>Accuracy</th>
<th>Purpose</th>
<th>Recipient</th>
</tr>
</thead>
<tbody>
<tr>
<td>Safaa</td>
<td>Age</td>
<td>Yes</td>
<td>K_anonym, k=5</td>
<td>Medical_treatment</td>
<td>Bob</td>
</tr>
<tr>
<td>Safaa</td>
<td>Name</td>
<td>Yes</td>
<td>-</td>
<td>Medical_treatment</td>
<td>Bob</td>
</tr>
</tbody>
</table>

![Diagram of privacy preferences](image-url)
Rewriting a query by joining each field with its preference, then we apply the accuracy

```
1. SELECT ?name ?age
2. FROM dt:infos WHERE {
3.   ?p rdf:type dt:Patient;
4.   dt:id ?id;
5.   dt:name ?n;
7. }
8. SERVICE ps:preferences {
9.   ?dp rdf:type P:DataOwner;
10.   P:hasId ?id;
12.   ?pref P:hasPurpose ‘Medical_treatment’;
13.   P:hasRecipient ‘Bob’;
15.   ?tp1 P:hasName `name’;
16.   P:hasDecision ?nameDecision.
17.   OPTIONAL{ ?tp1 P:hasAccuracy ?nameAccuracy.}
18.   ?tp2 P:hasAge `age’;
19.   P:hasDecision ?ageDecision.
20.   OPTIONAL{ ?tp2 P:hasAccuracy ?ageAccuracy.}
21. }
22. BIND(IF(?nameDecision=’No’,null,
23.     IF(bound(?nameAccuracy),
24.       udf:eval(?n,?nameAccuracy),?n)
25.     ) AS ?name).
26. BIND(IF(?ageDecision=’No’,null,
27.     IF(bound(?ageAccuracy),
28.       udf:eval(?a,?ageAccuracy),?a)
29.     ) AS ?age).
30. FILTER(?age >= 25)
31. }
```
Application to AGGREGO: Security & privacy in Semantic Mediator
Application to AGGREGO: Security & privacy in Semantic Mediator

Business Applications

Smart-Query Component

fQuery-AC (SPARQL 1.0)

fQuery-Privacy (SPARQL 1.1)

SPARQL Engine (SPARQL 1.1)

AGGREGO Server

Q_0

Q_1

Q_2

Q_{data}

Q_{pref}

Access Control Rules

MotOrBAC

Security Policy

PrivOrBAC SPARQL Service

29/04/13
Policy interoperability and negotiation
Policy interoperability

- Problematic
  - Distributed systems managed by different organizations
  - Need to share and exchange information

- Each organization has its own security policy
O2O: Organization to Organization

- Virtual private organization B2A
  - Control interoperability from B to A
  - Resources are owned by A (Ograntor)
  - Subjects come from B (Ograntee)
O2O: Organization to Organization

- VPO and Principle of Confinement
  - The scope of a security rule should be limited to the organization it applies to
  - O2O enforces the principle of confinement

- Policy of interoperability
  - Based on contract definition
  - Policy compatibility based on ontology alignment

- Model of VPO administration
  - Centralized administration
  - Decentralized administration
  - Hybrid administration
Trust Negotiation with XeNA

Service requester

- Policy evaluation
- Exception treatment module
- Exception treatment policies
- Access policies

Service provider

- Policy evaluation
- Exception treatment module
- Exception treatment policies
- Access policies

Negotiation module

Request

Negotiation

Response
XeNA

- Resource classification based negotiation
  - Classification of resources
    - Class 1 – with direct access (no negotiation)
    - Class 2 – with indirect access (negotiation based on internal security rules)
    - Class 3 – with indirect strategic access (negotiation based on obfuscated security rules)
  - Negotiation policies through derivation process
  - Negotiation and obfuscation strategies
  - Exceptions and treatment strategies

- Policy rewriting
  - Definition of an algebra
  - Rewriting based algorithm to detect and solve conflicts
  - Approach to derive negative attributes from positive attributes

- Implementation of the XeNA framework
  - Partially based on TrustBuilder
  - OrBAC profile of XACML
On-going work and conclusion
On-going work and conclusion

- **Policy mining**
  - Mining firewall configuration to extract a global policy
  - Autonomous process to compare configurations

- **Policy negotiation**
  - Autonomous negotiation to derive interoperability policies
  - Integration to Secure SLA

- **Response policy to coordinated attacks**
  - Appropriate measures to evaluate risk and impact
  - Strategies to derive consistent responses

- **Application to SCADA systems**
  - Adaptive configuration for industrial automata
  - Response policies in case of intrusion