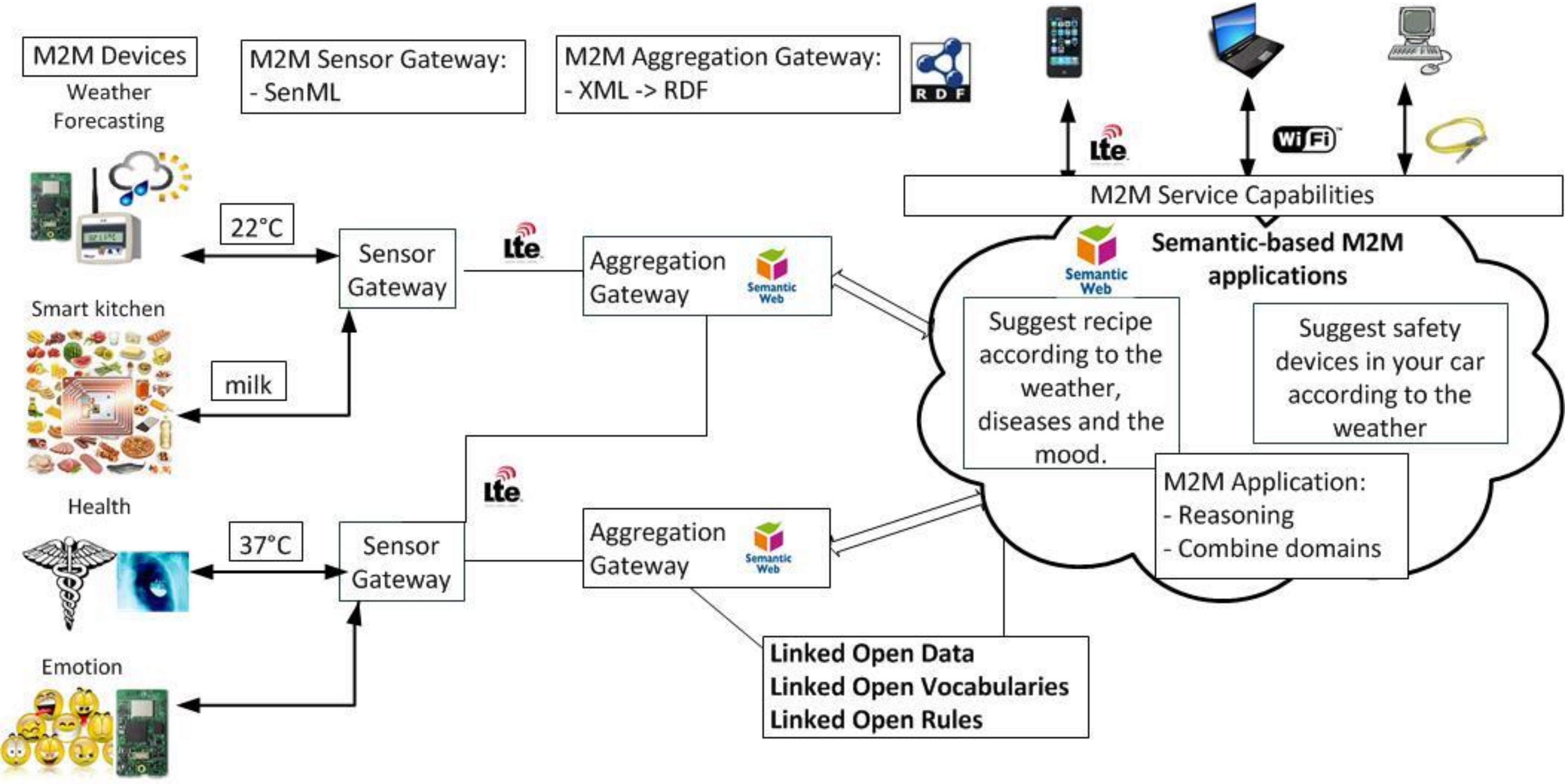
A leading institution at the heart of the digital society

An Ontology-Based Approach for Helping to Secure the ETSI Machine-to-Machine Architecture

Amelie Gyrard

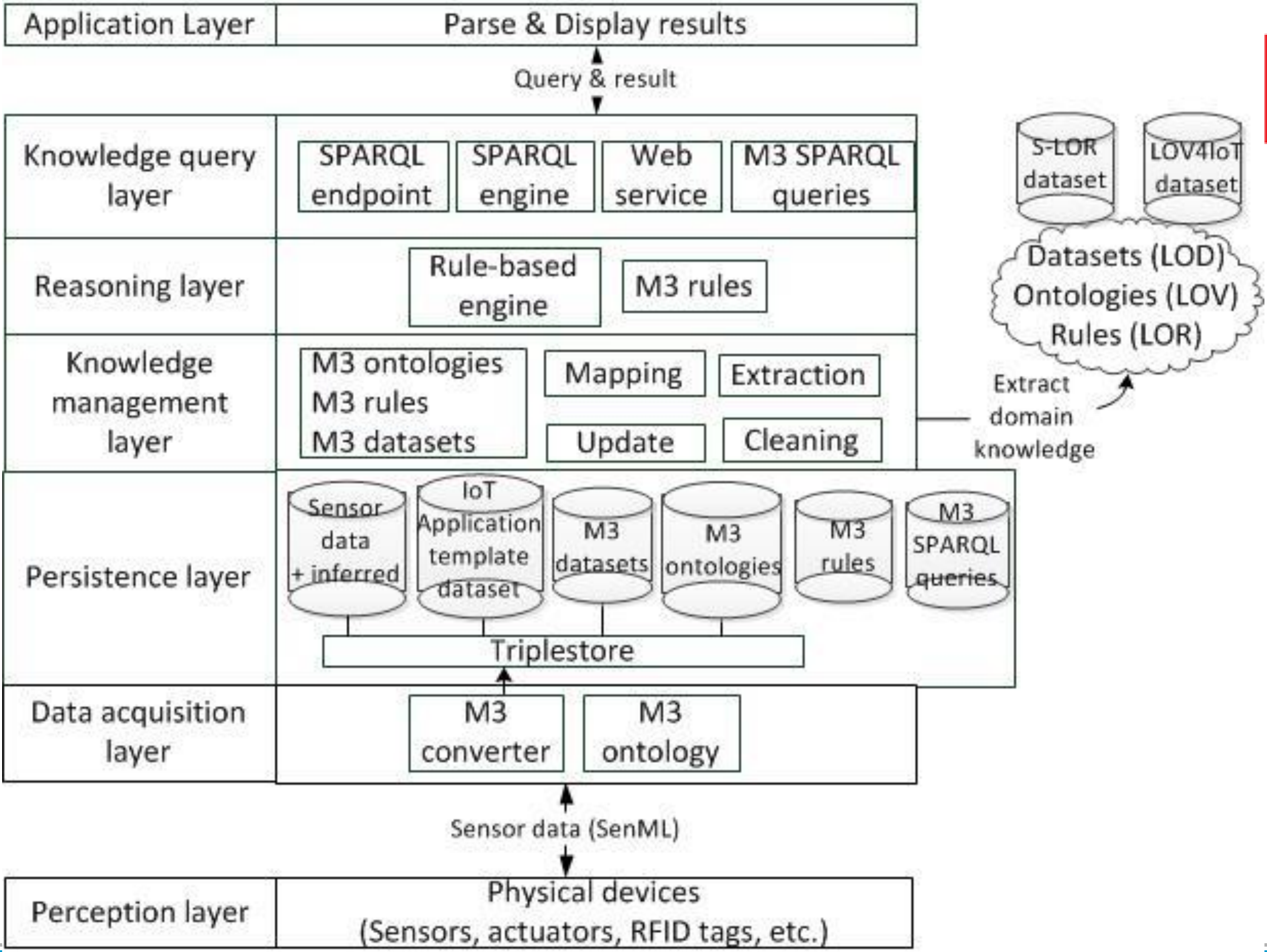
- Christian Bonnet (Eurecom, Mobile Communication)
- Karima Boudaoud (I3S, Security)

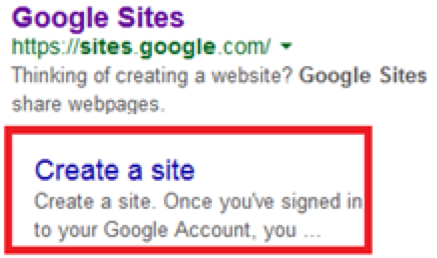
Semantic-based M2M Architecture



Paper: A Machine-to-Machine Architecture to Merge Semantic Sensor Measurements [Gyrard et al., WWW 2013]

Machine-to-Machine (M3) framework: Build IoT applications





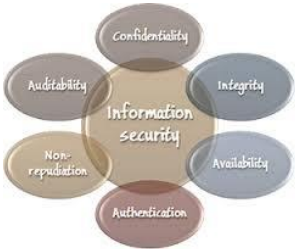
Google Sites
https://sites.google.com/
Thinking of creating a website? Google Sites share webpages.

Create a site
Create a site. Once you've signed in to your Google Account, you ...

http://www.sensormeasurement.appspot.com/

Motivation

- **How to secure IoT architectures and applications?**
  - ○ Communications
  - ○ Data
  - ○ Technologies employed
  - ○ Security properties satisfied



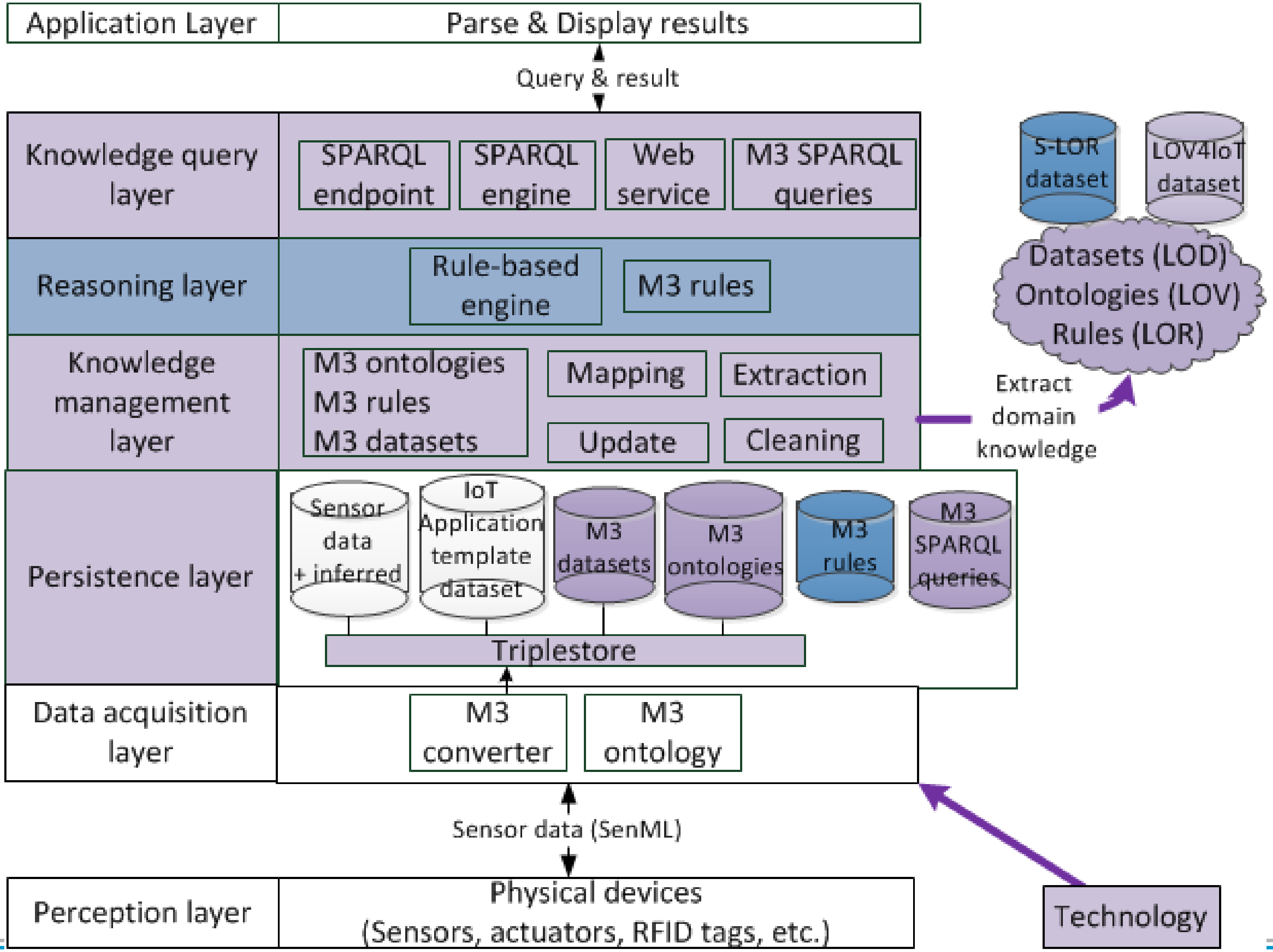
- **Time-consuming to be familiar with:**
  - ○ Attacks
  - ○ Security mechanisms

- **“Security by design”**

⇒**Reuse M3 for another purpose: security context**

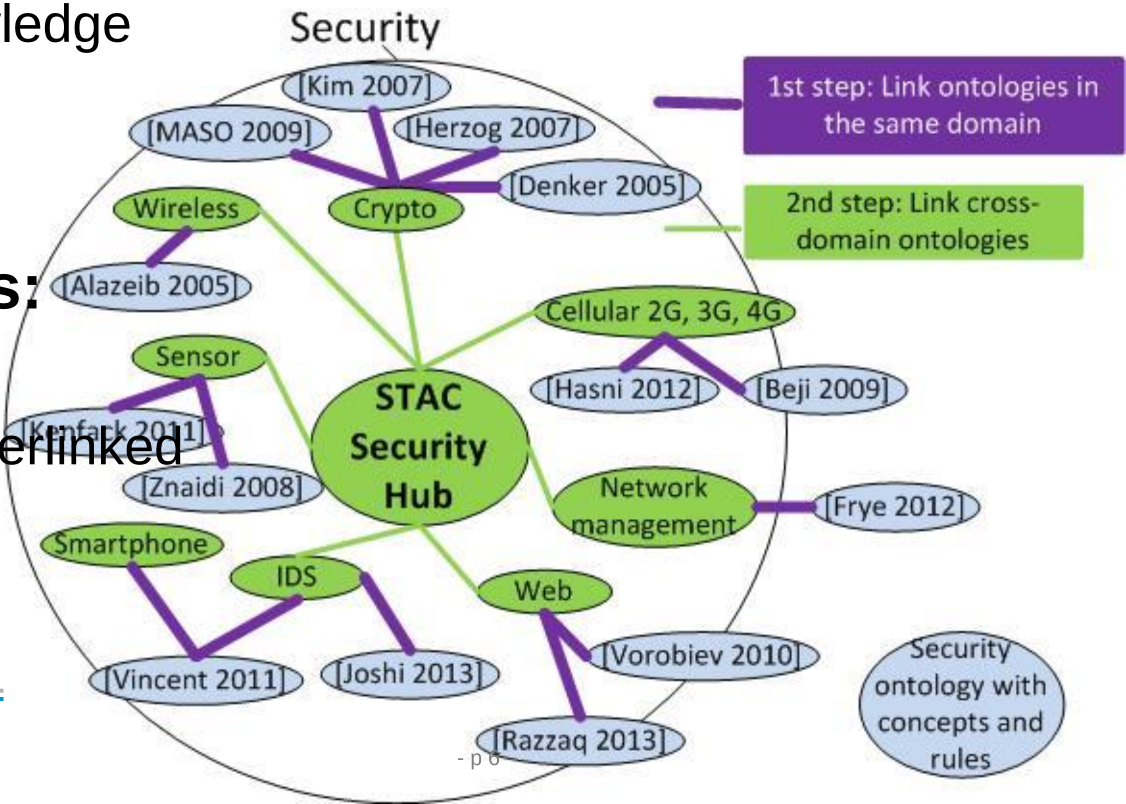
⇒**A tool to help choose the best security mechanism fitting our needs**

Reuse M3 to secure IoT applications or architectures



Security knowledge base

- **Reusing security knowledge:**
  - 24 works referenced in various domains:
    - IDS, Web, Sensor networks, Smart phones, Network communications, Cryptography
  - Use semantic web technologies (ontologies)
    - Reuse domain knowledge
    - Reasoning engine
    - Flexibility
- **Lack of best practices:**
  - Not published online
  - Domain-specific, Not interlinked
  - Heterogeneous terms

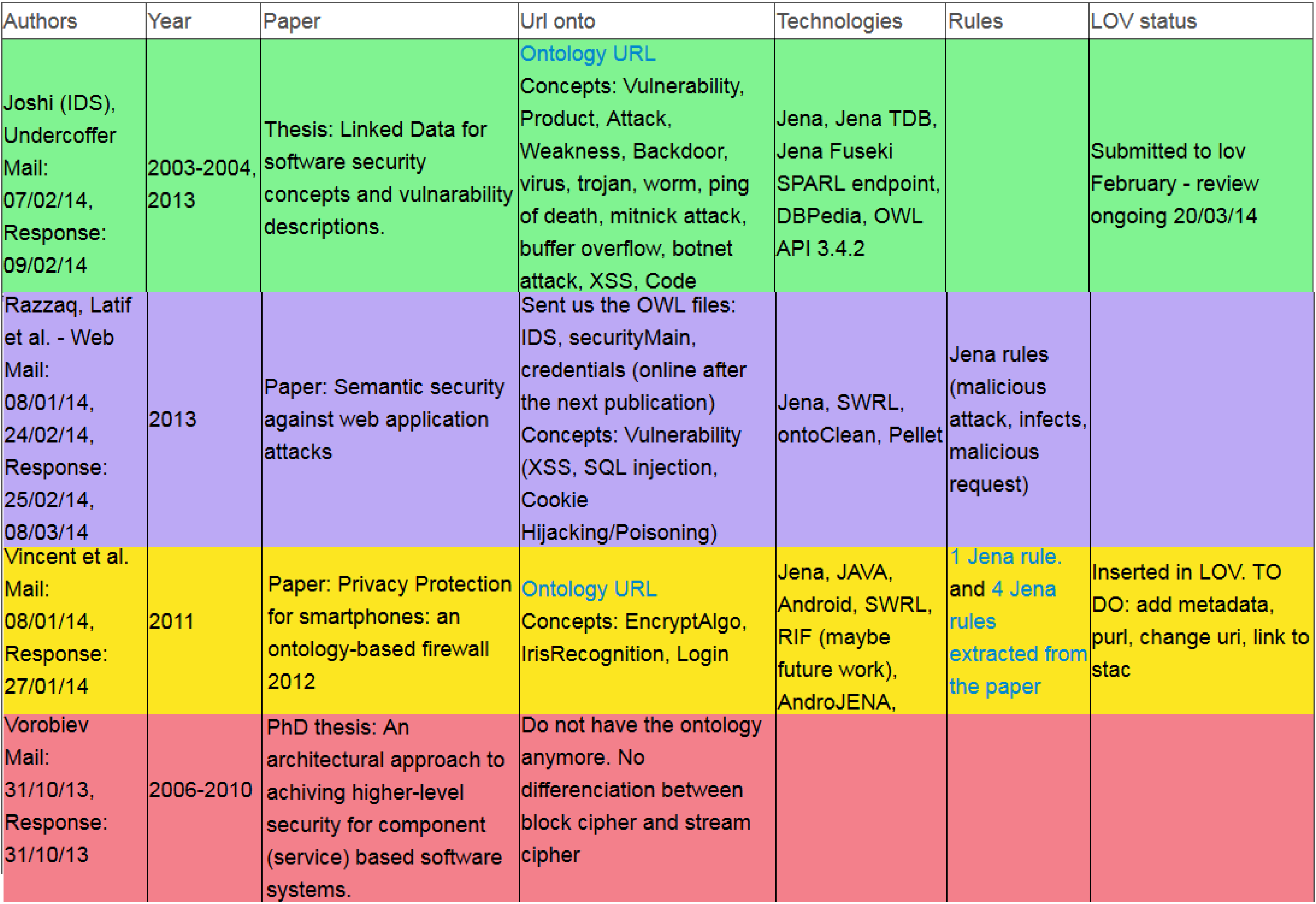


1st step: Link ontologies in the same domain

2nd step: Link cross-domain ontologies

Security ontology with concepts and rules

Security ontologies



Authors	Year	Paper	Url onto	Technologies	Rules	LOV status
Joshi (IDS), Undercoffer Mail: 07/02/14, Response: 09/02/14	2003-2004, 2013	Thesis: Linked Data for software security concepts and vulnarability descriptions.	Ontology URL Concepts: Vulnerability, Product, Attack, Weakness, Backdoor, virus, trojan, worm, ping of death, mitnick attack, buffer overflow, botnet attack, XSS, Code	Jena, Jena TDB, Jena Fuseki SPARL endpoint, DBPedia, OWL API 3.4.2		Submitted to lov February - review ongoing 20/03/14
Razzaq, Latif et al. - Web Mail: 08/01/14, 24/02/14, Response: 25/02/14, 08/03/14	2013	Paper: Semantic security against web application attacks	Sent us the OWL files: IDS, securityMain, credentials (online after the next publication) Concepts: Vulnerability (XSS, SQL injection, Cookie Hijacking/Poisoning)	Jena, SWRL, ontoClean, Pellet	Jena rules (malicious attack, infects, malicious request)	
Vincent et al. Mail: 08/01/14, Response: 27/01/14	2011	Paper: Privacy Protection for smartphones: an ontology-based firewall 2012	Ontology URL Concepts: EncryptAlgo, IrisRecognition, Login	Jena, JAVA, Android, SWRL, RIF (maybe future work), AndroJENA,	1 Jena rule. and 4 Jena rules extracted from the paper	Inserted in LOV. TO DO: add metadata, purl, change uri, link to stac
Vorobiev Mail: 31/10/13, Response: 31/10/13	2006-2010	PhD thesis: An architectural approach to achiving higher-level security for component (service) based software systems.	Do not have the ontology anymore. No differenciation between block cipher and stream cipher			

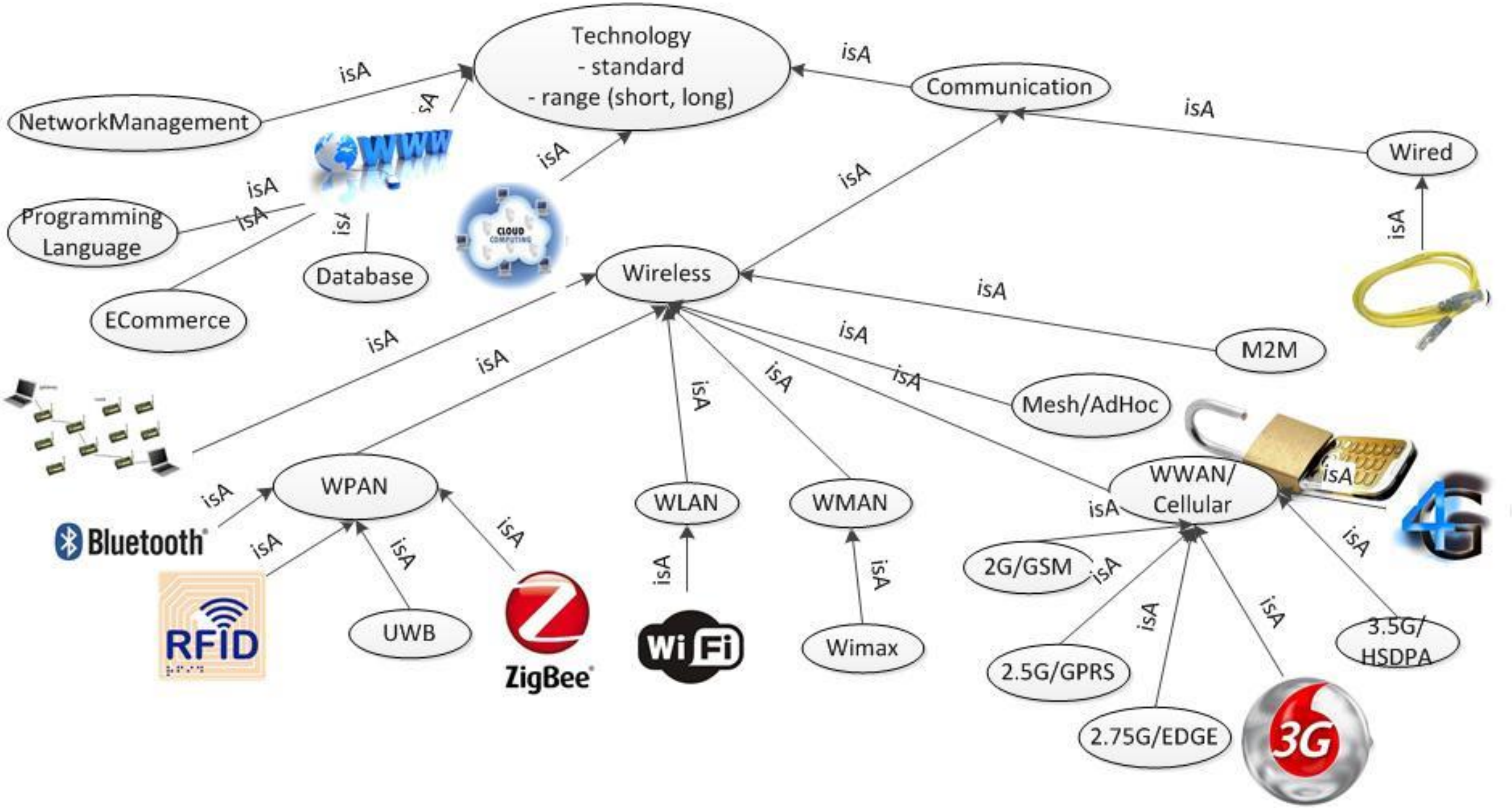
http://www.sensormeasurement.appspot.com/?p=ontologies

The STAC ontology

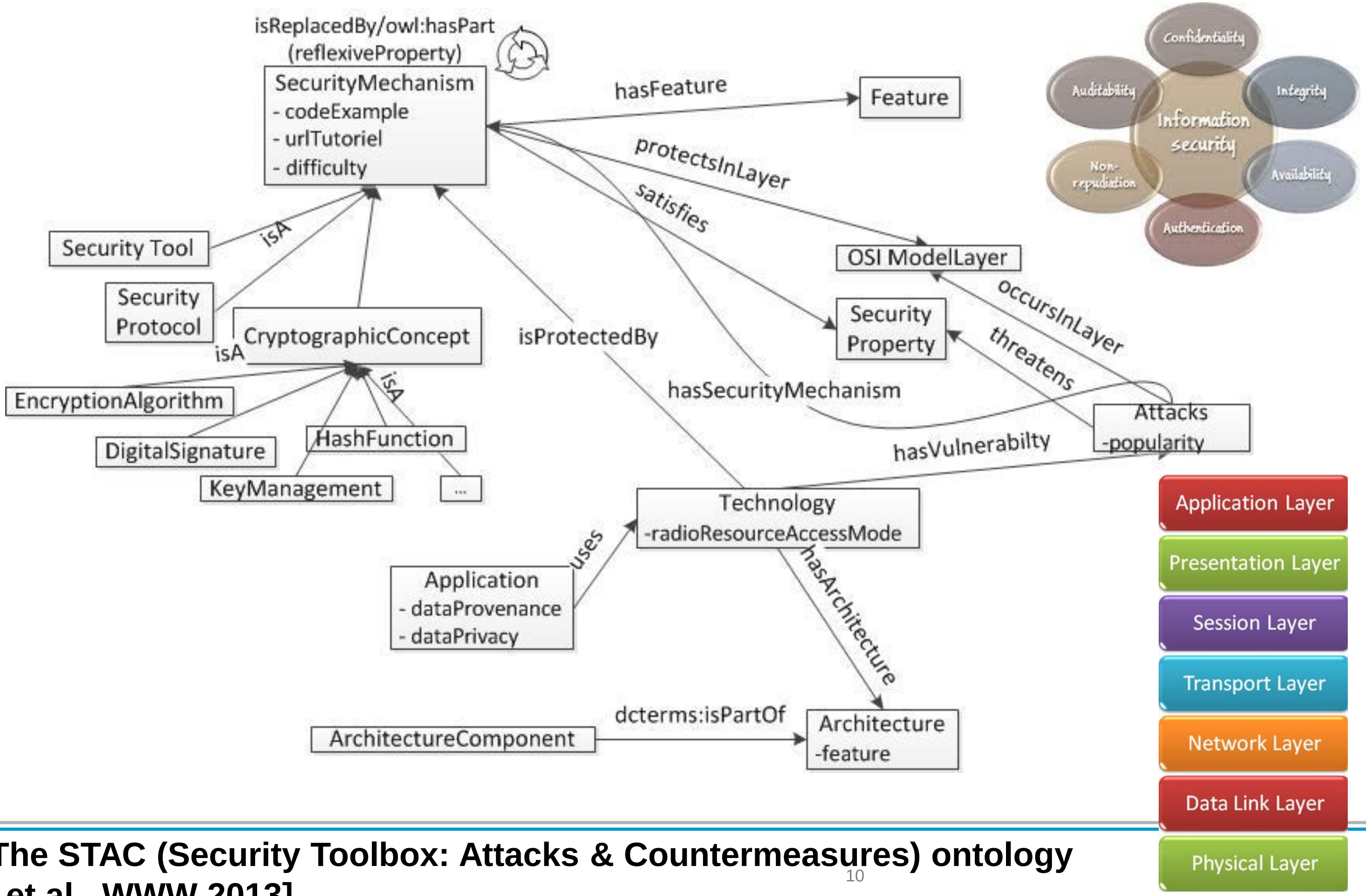
- STAC (Security Toolbox: Attacks & Countermeasures)
  - ○Ontology is a vocabulary to describe concepts and properties in a particular domain
  - ○http://securitytoolbox.appspot.com/stac#
  - ○Referenced by Linked Open Vocabularies (LOV)

- Help the developer choose security mechanisms to secure IoT applications.

How to secure heterogeneous technologies?



The STAC ontology



Paper: The STAC (Security Toolbox: Attacks & Countermeasures) ontology [Gyrard et al., WWW 2013]

The STAC application

- A semantic-based application to help the developer to design a secure software:
  - ➢The STAC ontology
  - ➢The user interface

Semantic Web

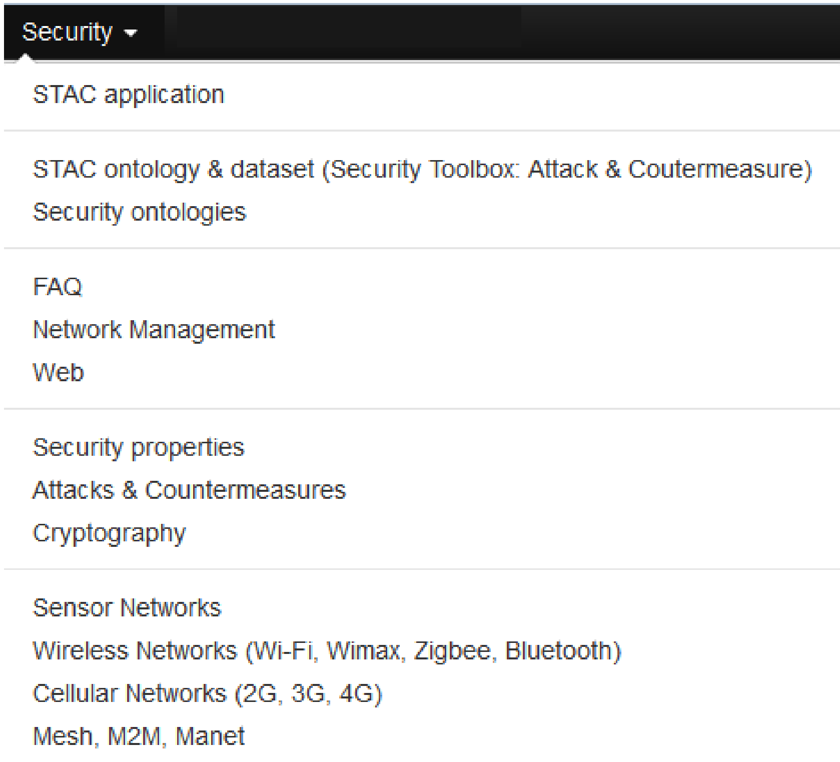
JAVA

semantic web framework Jena

HTML

CSS

JavaScript



STAC application

STAC ontology & dataset (Security Toolbox: Attack & Coutermeasure)

Security ontologies

FAQ

Network Management

Web

Security properties

Attacks & Countermeasures

Cryptography

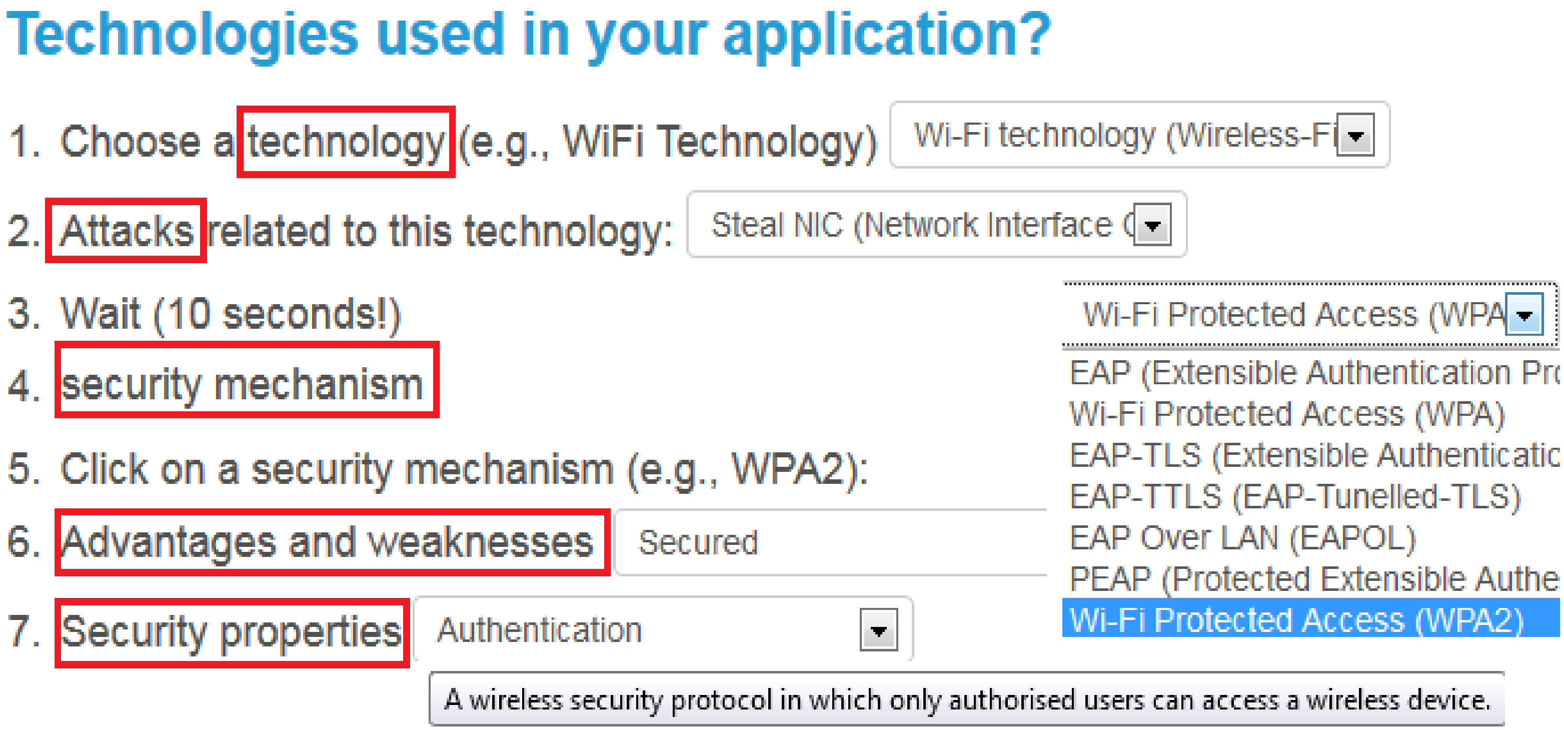
Sensor Networks

Wireless Networks (Wi-Fi, Wimax, Zigbee, Bluetooth)

Cellular Networks (2G, 3G, 4G)

Mesh, M2M, Manet

STAC template



Technologies used in your application?

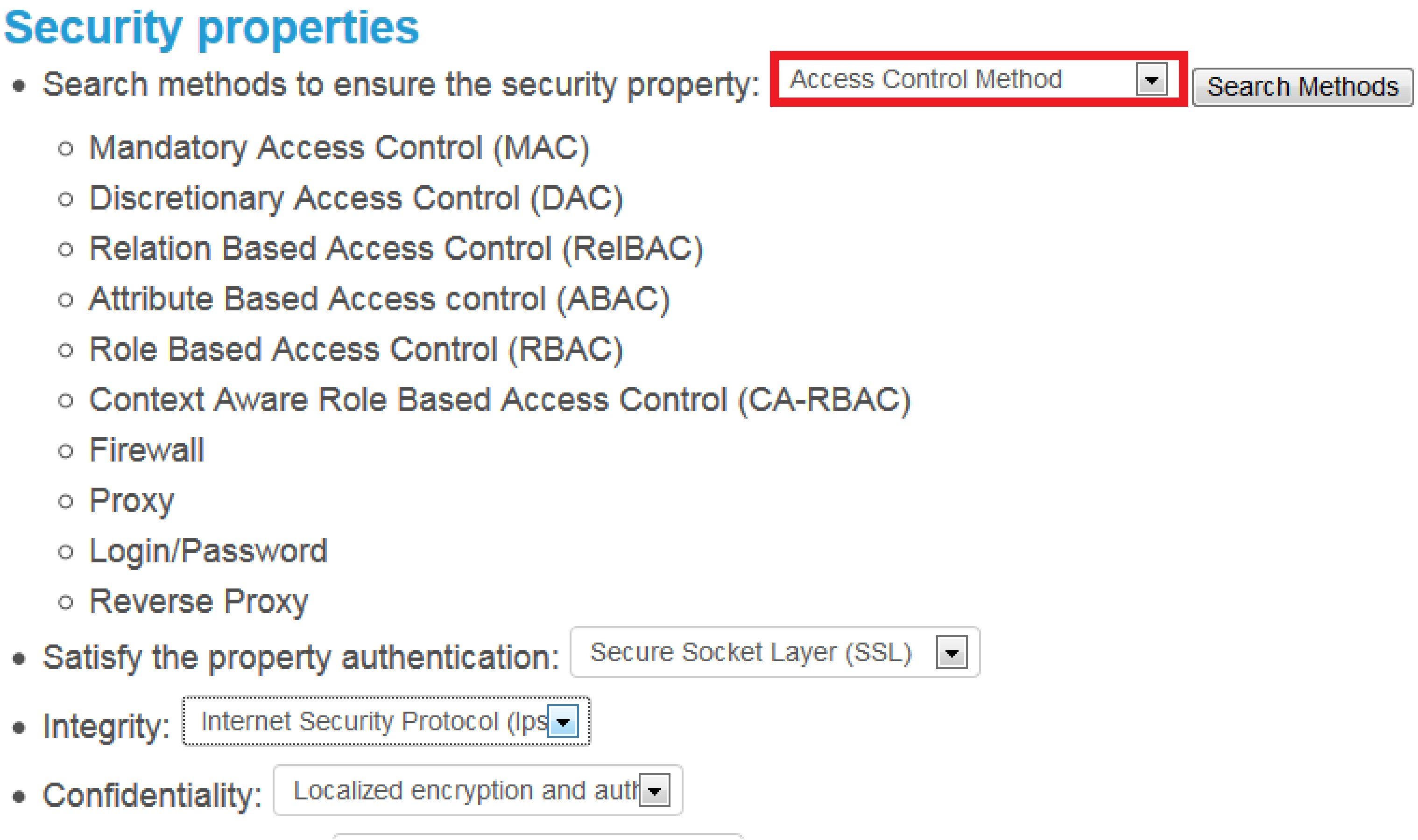
1. Choose a technology (e.g., WiFi Technology) Wi-Fi technology (Wireless-Fi
2. Attacks related to this technology: Steal NIC (Network Interface C
3. Wait (10 seconds!)
4. security mechanism
5. Click on a security mechanism (e.g., WPA2):
6. Advantages and weaknesses Secured
7. Security properties Authentication

A wireless security protocol in which only authorised users can access a wireless device.

Wi-Fi Protected Access (WPA
EAP (Extensible Authentication Pro
Wi-Fi Protected Access (WPA)
EAP-TLS (Extensible Authenticatic
EAP-TTLS (EAP-Tunelled-TLS)
EAP Over LAN (EAPOL)
PEAP (Protected Extensible Authe
Wi-Fi Protected Access (WPA2)

http://www.sensormeasurement.appspot.com/?p=stac

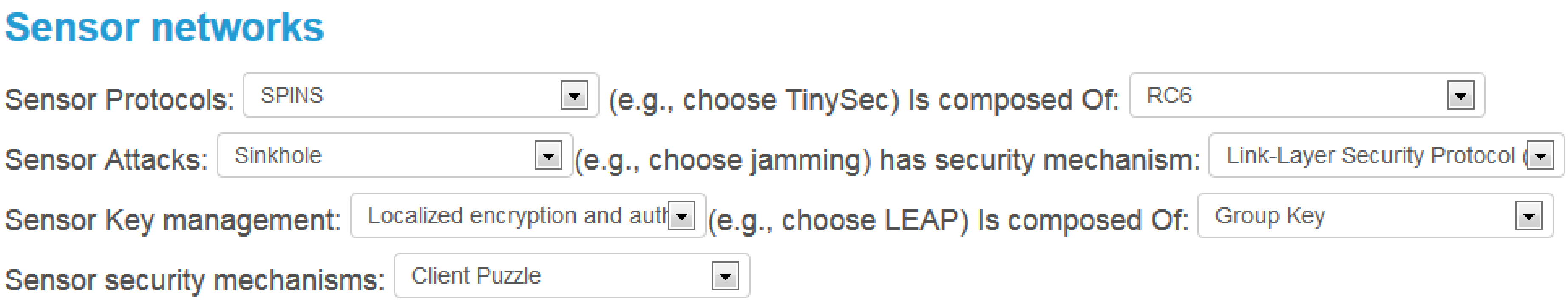
Security properties



Security properties

- Search methods to ensure the security property: Access Control Method
  - Mandatory Access Control (MAC)
  - Discretionary Access Control (DAC)
  - Relation Based Access Control (RelBAC)
  - Attribute Based Access control (ABAC)
  - Role Based Access Control (RBAC)
  - Context Aware Role Based Access Control (CA-RBAC)
  - Firewall
  - Proxy
  - Login/Password
  - Reverse Proxy
- Satisfy the property authentication: Secure Socket Layer (SSL)
- Integrity: Internet Security Protocol (Ips
- Confidentiality: Localized encryption and auth

STAC to secure communications



Sensor networks

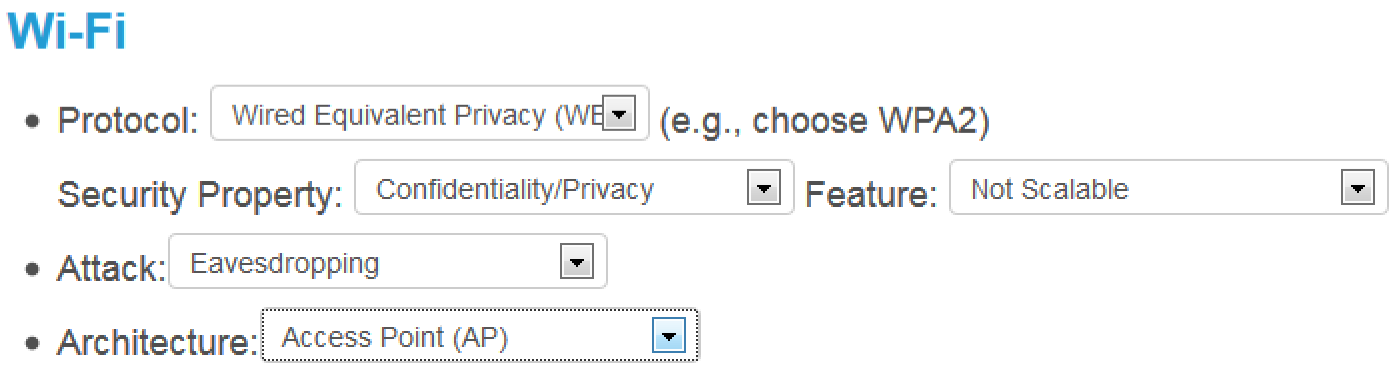
Sensor Protocols: SPINS (e.g., choose TinySec) Is composed Of: RC6

Sensor Attacks: Sinkhole (e.g., choose jamming) has security mechanism: Link-Layer Security Protocol (

Sensor Key management: Localized encryption and auth (e.g., choose LEAP) Is composed Of: Group Key

Sensor security mechanisms: Client Puzzle

http://www.sensormeasurement.appspot.com/?p=sensor



Wi-Fi

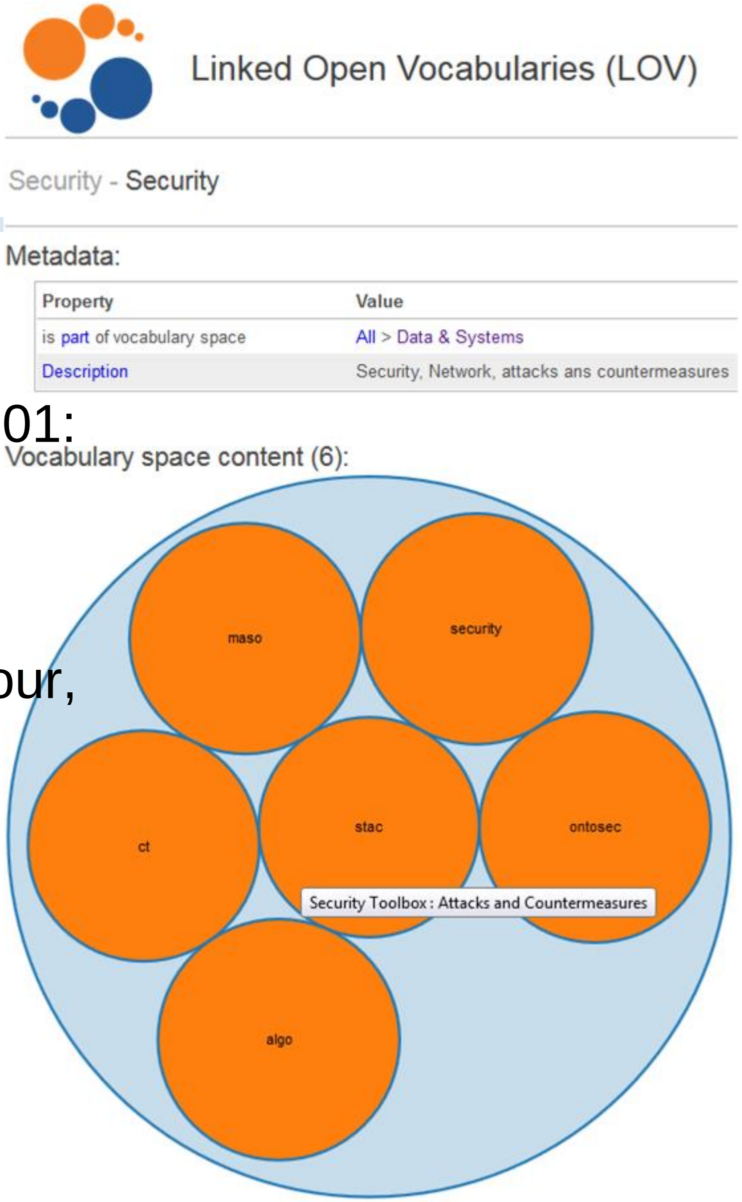
- Protocol: Wired Equivalent Privacy (WE (e.g., choose WPA2)

  Security Property: Confidentiality/Privacy Feature: Not Scalable
- Attack: Eavesdropping
- Architecture: Access Point (AP)

http://www.sensormeasurement.appspot.com/?p=wireless

Evaluation

- **Methodologies**
  - [Noy et al. 2001]: Ontology development 101: A guide to creating your first ontology
- **Semantic web tools**
  - Oops, TripleChecker, RDF Validator, Vapour,
  - Linked Open Vocabularies (LOV), Linked Open Data (LOD)
- **24 security ontologies**
  - More than 14 ontologies are online
- **User form:**
  - 24 responses
  - Updated STAC with new security domains



Linked Open Vocabularies (LOV)

Security - Security

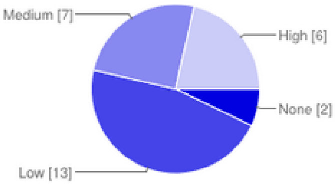
Metadata:

Property	Value
is part of vocabulary space	All > Data & Systems
Description	Security, Network, attacks ans countermeasures

Vocabulary space content (6):

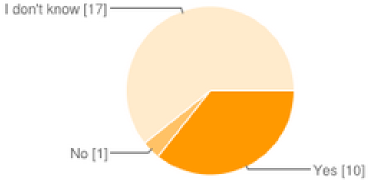
STAC evaluation form

Your knowledge in security?



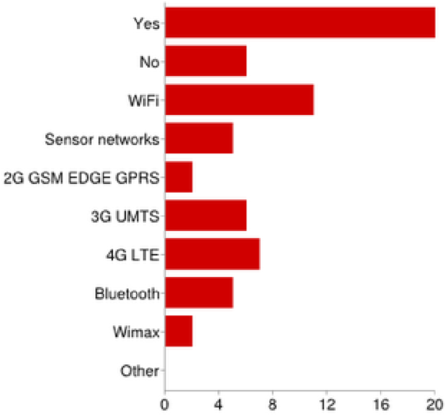
None	2	7%
Low	13	46%
Medium	7	25%
High	6	21%

Is STAC a useful application (securitytoolbox.appspot.com/)?



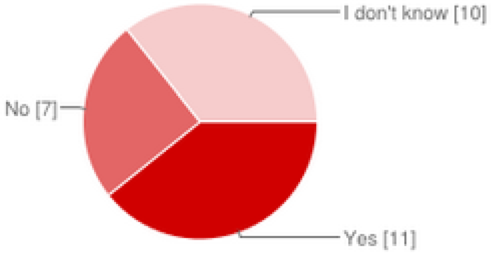
Yes	10	36%
No	1	4%
I don't know	17	61%

Are you interested in security for wireless networks?



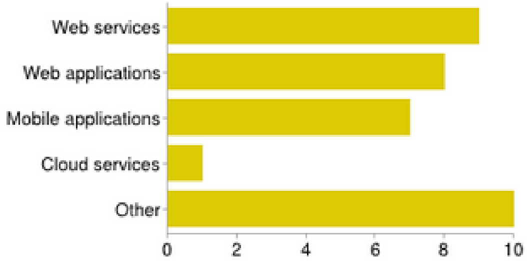
Yes	20	31%
No	6	9%
WiFi	11	17%
Sensor networks	5	8%
2G GSM EDGE GPRS	2	3%
3G UMTS	6	9%
4G LTE	7	11%
Bluetooth	5	8%
Wimax	2	3%
Other	0	0%

Are the concepts intuitive and easy to understand ?



Yes	11	39%
No	7	25%
I don't know	10	36%

What kind of applications do you need to secure ?



Web services	9	26%
Web applications	8	23%
Mobile applications	7	20%
Cloud services	1	3%
Other	10	29%

https://docs.google.com/forms/d/1NKiMQPVR6X6Reioud0-WBZu1bmo3T1Ah7PZm9De-apk/viewform

Conclusion & Future works

- **M3 framework:**
  - Build IoT applications to reason on cross-domain data
  - STAC
    - A security knowledge base
    - Helping developers choose security mechanisms to secure IoT applications.
  - Linked Open Rules to share and reuse rules

Thank you!

- **We have more demonstrations for:**
  - STAC
  - Linked Open Rules
  - M3 framework
- **gyrard@eurecom.fr**
- **http://www.sensormeasurement.appspot.com/**