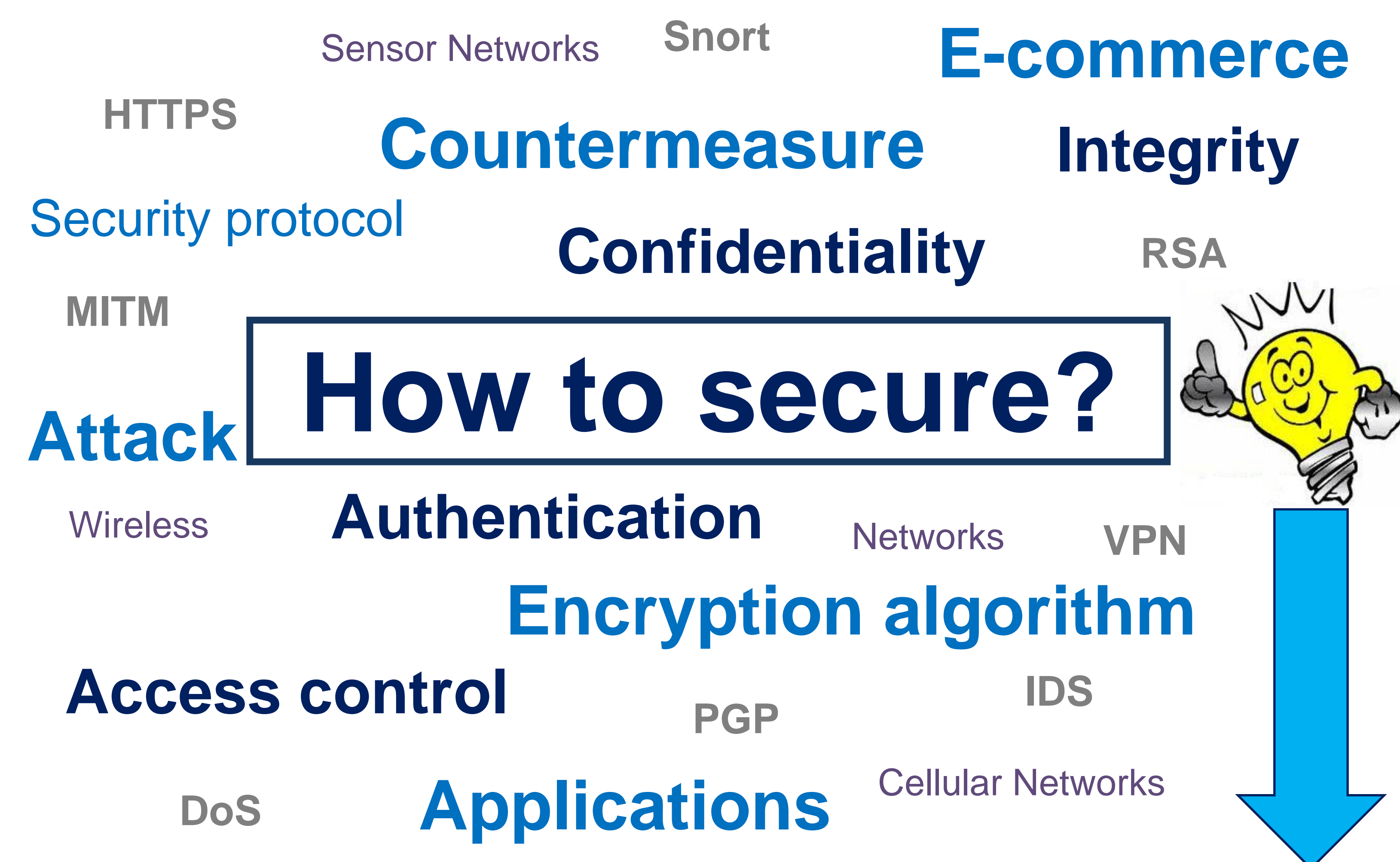


# The STAC ontology

## (Security Toolbox: Attacks & Countermeasures)

Amelie Gyrard, Christian Bonnet and Karima Boudaoud  
{amelie.gyrard, christian.bonnet}@eurecom.fr, karima@polytech.unice.fr

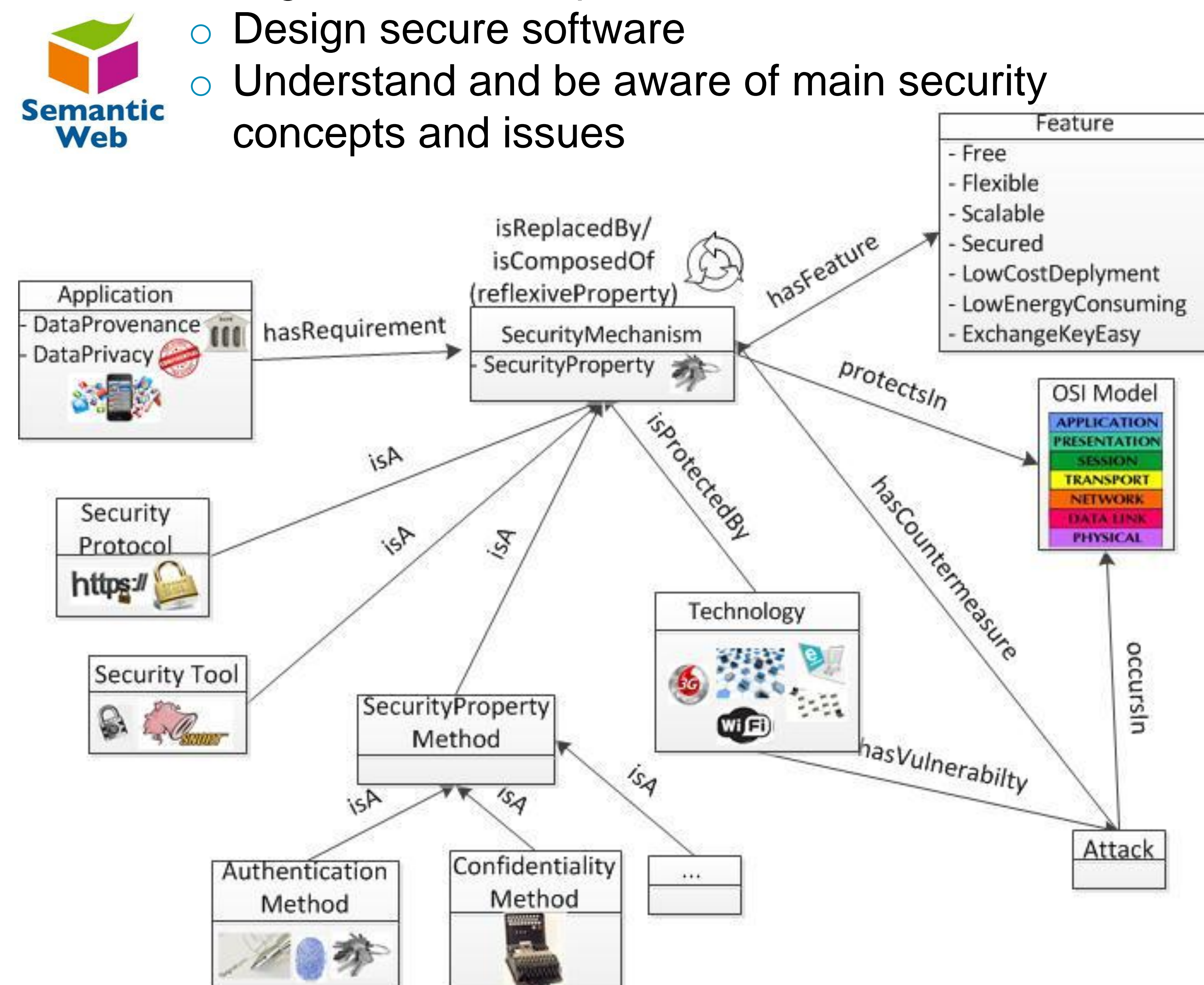
### Motivating scenario



### The STAC ontology

- An ontology to help non-security-expert software designers or developers to:

- Design secure software
- Understand and be aware of main security concepts and issues



### Related works

#### □ Drawbacks of existing ontologies:

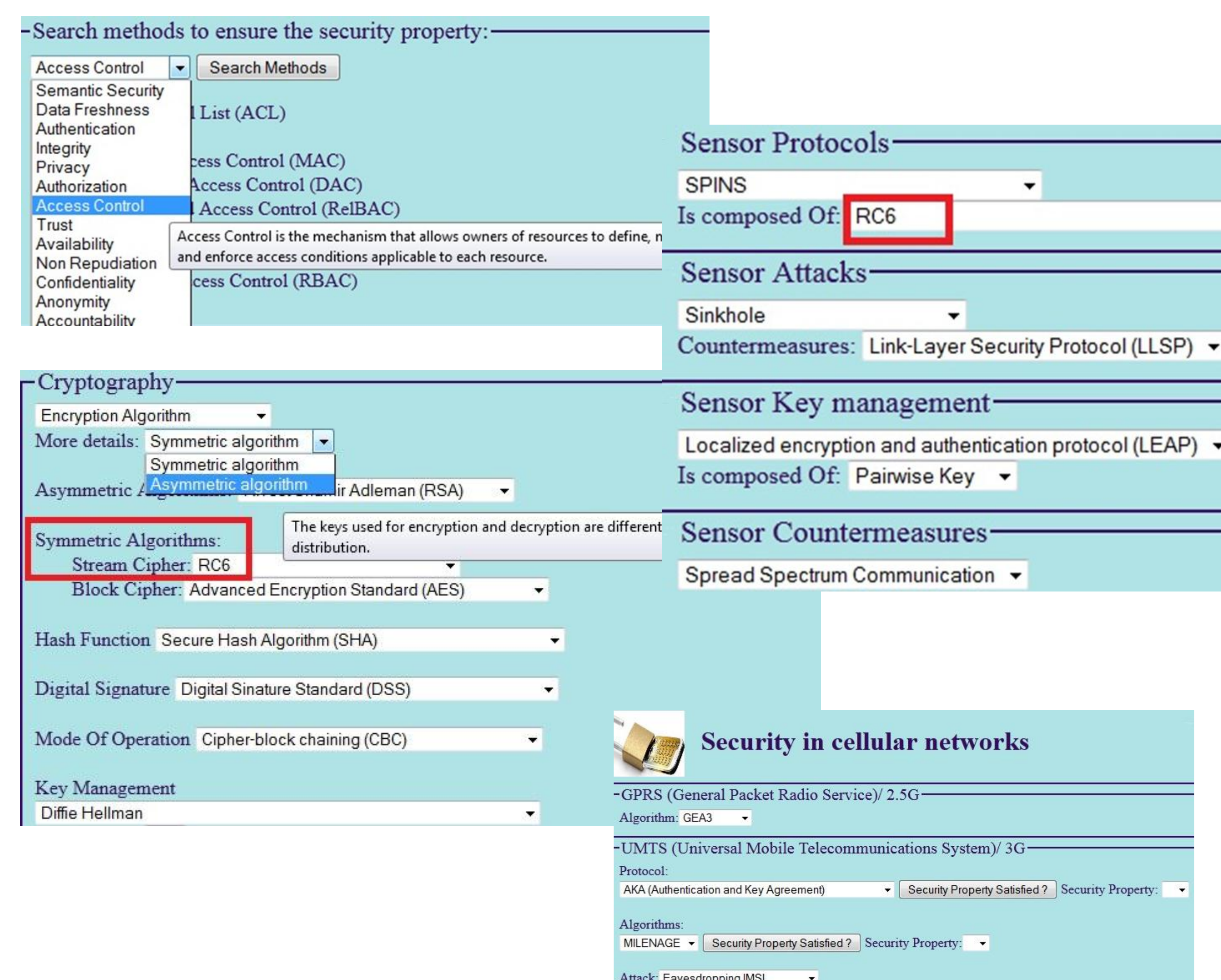
- Most of them are not available online
- Do not consider the previous ontologies
- No descriptions of countermeasures
- No relationships between attacks, security mechanisms, security properties, technologies and OSI Model.
- Do not classify security mechanisms according to security properties



### Implementation

#### □ User interface & Ontology:

- <http://securitytoolbox.appspot.com/>



The screenshot shows the Security Toolbox user interface. It includes sections for:
 

- Search methods to ensure the security property:** A dropdown menu for "Access Control" with options like "Access Control (MAC)", "Access Control (DAC)", "Access Control (RelBAC)", and "Access Control (RBAC)".
- Sensor Protocols:** A dropdown menu for "SPINS" with "Is composed Of: RC6" selected.
- Sensor Attacks:** A dropdown menu for "Sinkhole" with "Countermeasures: Link-Layer Security Protocol (LLSP)" selected.
- Sensor Key management:** A dropdown menu for "Localized encryption and authentication protocol (LEAP)" with "Is composed Of: Pairwise Key" selected.
- Sensor Countermeasures:** A dropdown menu for "Spread Spectrum Communication".
- Cryptography:** A section for "Encryption Algorithm" with "Symmetric algorithm" selected, showing "Stream Cipher: RC6" and "Block Cipher: Advanced Encryption Standard (AES)".
- Hash Function:** "Secure Hash Algorithm (SHA)".
- Digital Signature:** "Digital Signature Standard (DSS)".
- Mode Of Operation:** "Cipher-block chaining (CBC)".
- Key Management:** "Diffie Hellman".
- Security in cellular networks:** A section for "GPRS (General Packet Radio Service)/ 2.5G" with "Algorithm: GEA3" and "Protocol: AKA (Authentication and Key Agreement)".

#### □ Technologies used:

- Semantic Web: OWL, RDF, RDFS, SPARQL, Jena.
- User interface: Java, Google Application Engine (GAE), HTML5, Javascript, AJAX, RESTful (Jersey)

### Conclusion & Future works

- An ontology to help developers to design secure software
- Improve the user interface
- Create templates to secure the application
- Use STAC to secure our Machine-to-Machine architecture (see Doctoral Consortium)