BABEŞ-BOLYAI UNIVERSITY

24th International Working Conference, REFSQ 2018,
Utrecht, The Netherlands, March 19-22, 2018

Security Requirements Elicitation from Engineering Governance, Risk Management and Compliance

Lect. Dr. Ana-Maria Ghiran

Prof. Dr. Robert Buchmann

Assist Dr. Cristina-Claudia Osman

University Babeş-Bolyai of Cluj Napoca, Romania

Agenda

- Motivation
- The Vision of GRC Security Requirements Engineering
- Key Proposal
- Examples:
  - —Access control policies in RDF
  - —Diagrammatic Knowledge Sources
- Conclusions

Motivation

Security requirements
have heterogeneous sources and representations,
often implied by contextual documentation
(rather than explicitly formulated by stakeholders)

Governance

Internal control policies, Guiding standards
“username must not be related to person”

Risk management

Risk mitigation policies
“username and passwords must not be related”

Compliance

Regulatory obligations
“appropriate safeguards should be in place to protect user data like login credentials” - GDPR

Motivation

Security requirements
have heterogeneous sources and representations,
often implied by contextual documentation
(rather than explicitly formulated by stakeholders)

Governance | **Risk management** | **Compliance** → **GRC**

Internal control policies, Guiding standards
"username must not be related to person"

Risk mitigation policies
"username and passwords must not be related"

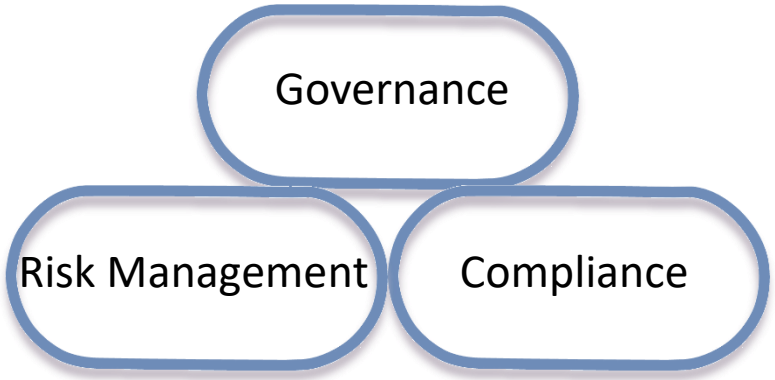
Regulatory obligations
"appropriate safeguards should be in place to protect user data like login credentials" - GDPR

Motivation

GRC advocates integration

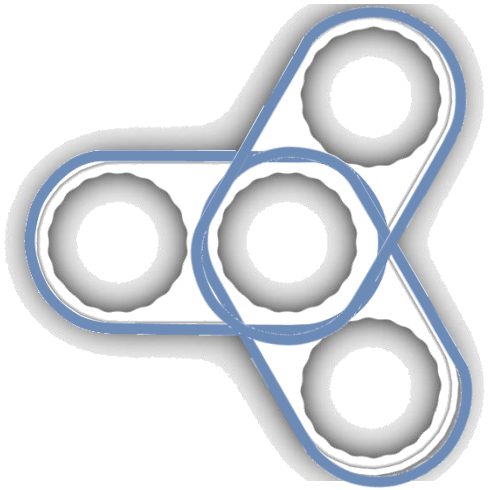
GRC disciplines treated separately:

- some might be unaware by the requirements identified in the other areas
- tasks are repeated, activities and costs are duplicated



Integrated GRC disciplines:

- enable richer and comprehensive requirements
- opportunity for a "**security requirements knowledge base**"



The Vision of GRC Security RE

Proposal:

a security requirements knowledge base that is…

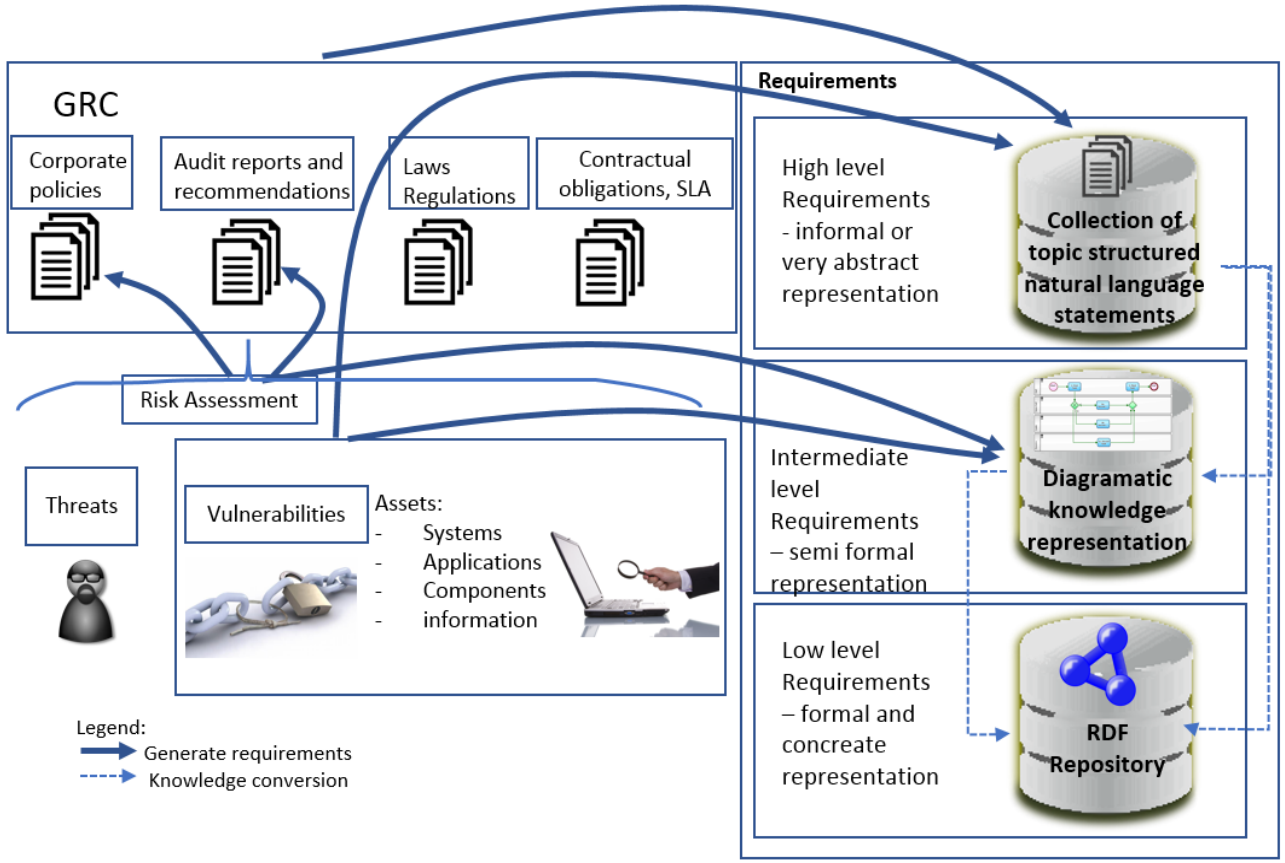
- machine-readable
- linkable to data

Underlying technology:

Semantic technology (RDF, OWL)

Technical Challenge:

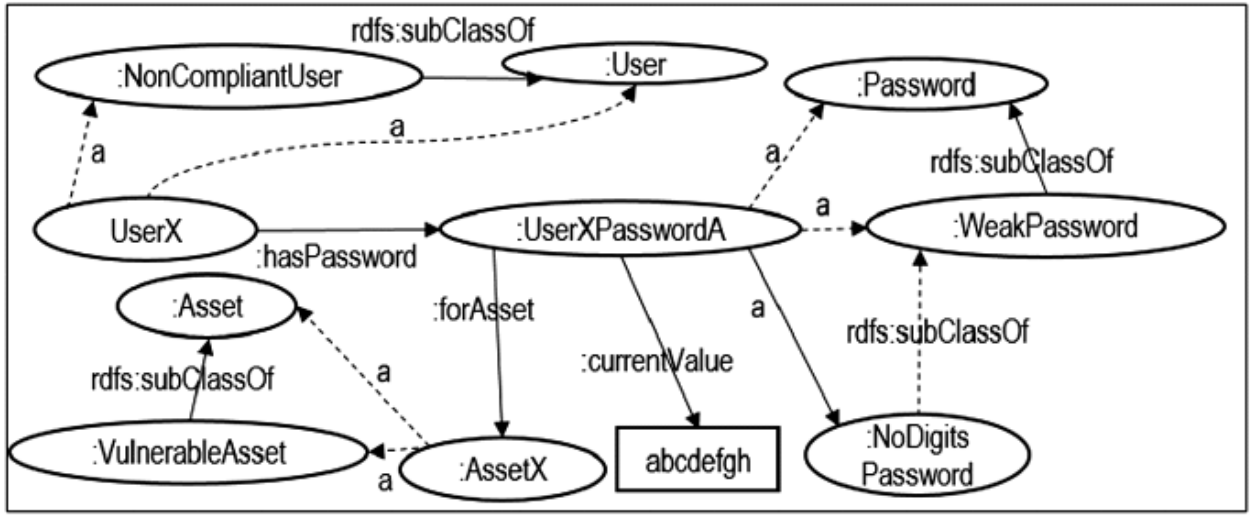
Knowledge conversion processes and adapters (to unify the repository under RDF)



Key proposal

RDF (Resource Description Framework) – unifying format employed here to represent (and semantically link) requirements from heterogeneous sources:

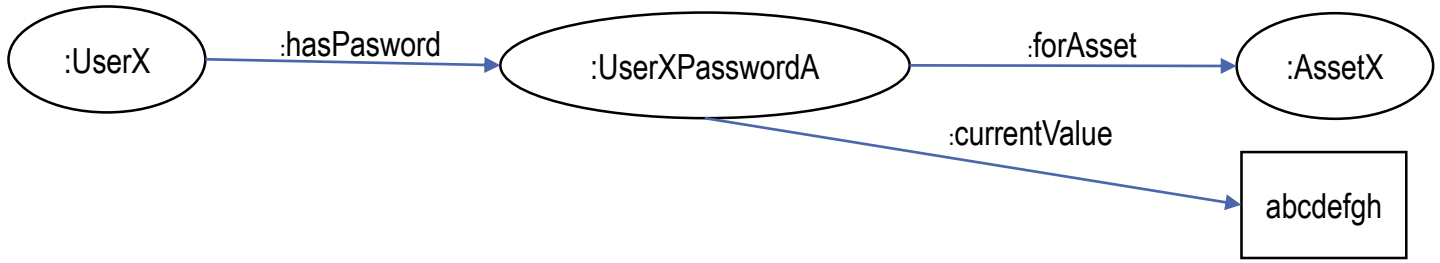
- *textual* sources => manual translation
- *visual* (diagrammatic) sources => automated translation
- *ontology-based* sources => semantic integration with existing knowledge sources



Background on RDF

"Knowledge graphs" are formed by connecting statements:

:UserX	:hasPassword	:UserXPasswordA.
:UserXPasswordA	:currentValue	"abcdefgh".
:UserXPasswordA	:forAsset	:AssetX.



⇒ graph databases can be employed for storage and semantic queries:

Retrieve users that have set a password for asset X

```
SELECT ?user
WHERE { ?user :hasPassword/:forAsset :AssetX }
=> UserX
```

*https://www.w3.org/TR/sparql11-query/

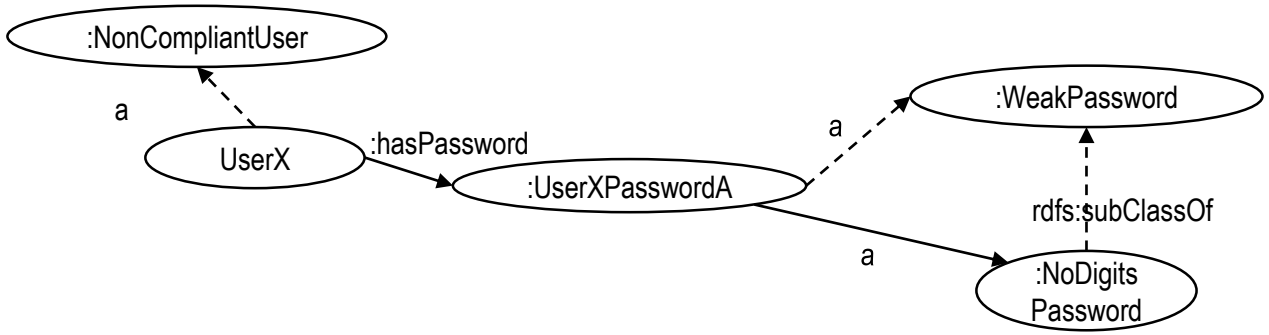
OWL* axioms and inferences on password policies

:WeakPassword owl:unionOf (:NoDigitsPassword :NoSymbolPassword :ShortPassword).
=>NoDigitsPassword rdfs:subClassOf :WeakPassword.

:NonCompliantUser owl:onProperty :hasPassword; owl:someValuesFrom :WeakPassword; rdfs:subClassOf :User.
:UserXPasswordA a :NoDigitsPassword.
=>:UserXPasswordA a :WeakPassword.
=> :UserX a :NonCompliantUser. :AssetX a :VulnerableAsset.

SPARQL Query:
Retrieve the noncompliant users

```
SELECT ?x WHERE
 {?x a :NonCompliantUser}
```

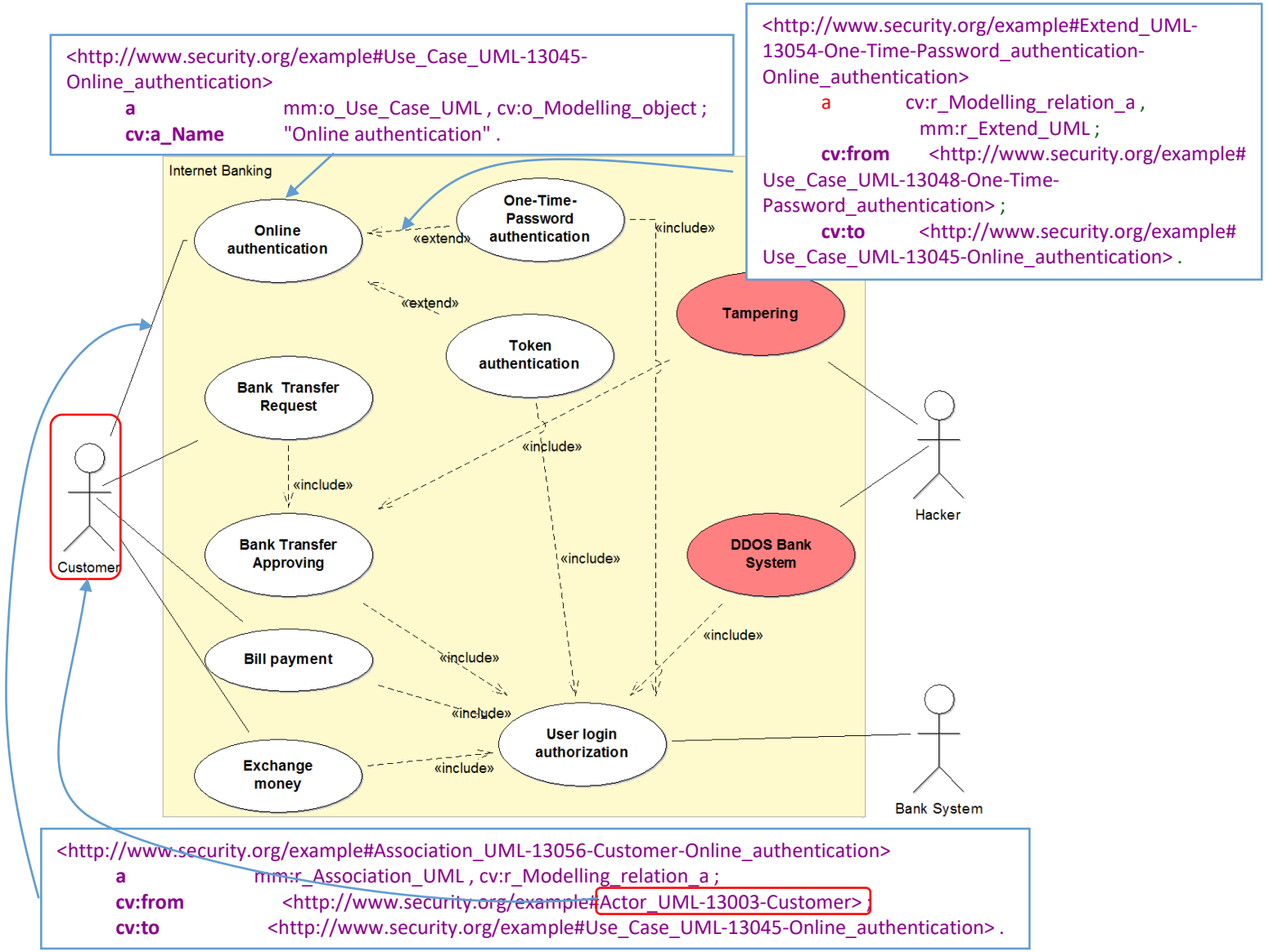


*https://www.w3.org/TR/2012/REC-owl2-overview-20121211/

Converting diagrammatic sources: UML

Online Authentication:

Uses cases and abuse cases described diagrammatically
AND
as a graph amenable to reasoning

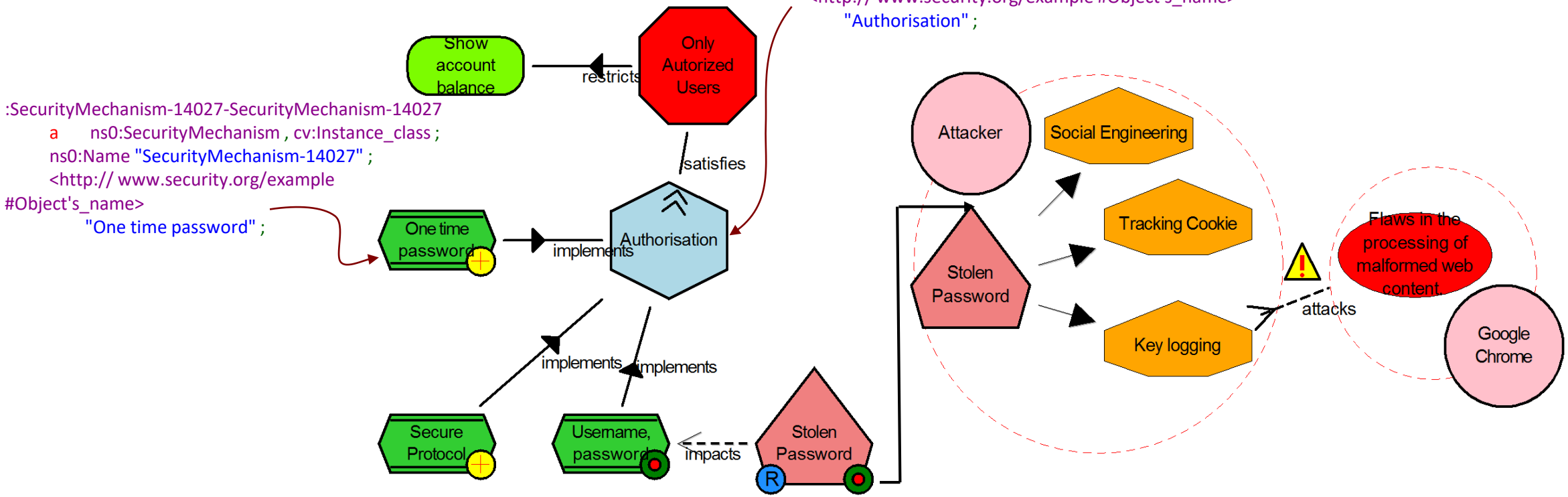


Converting diagrammatic sources: SecureTropos

Threat case description in SecureTropos

```
:SecurityObjective-14036-SecurityObjective-14036
      a      ns0:SecurityObjective , cv:Instance_class ;
      ns0:Name "SecurityObjective-14036" ;
      <http:// www.security.org/example #Object's_name>
           "Authorisation" ;
```

```
:SecurityMechanism-14027-SecurityMechanism-14027
      a      ns0:SecurityMechanism , cv:Instance_class ;
      ns0:Name "SecurityMechanism-14027" ;
      <http:// www.security.org/example
#Object's_name>
           "One time password" ;
```



Conclusions

- Our approach advocates semantic integration of multiple sources for security requirements

- A requirements knowledge base can enable a shared, traceable and formal representation of requirements

On-going work

An integrative schema to unify

- several (security) requirements diagram types (SecureTropos, UML use cases)
- other types of documents that are commonly used in integrated GRC (mostly rules)
- security data that should be assessed against GRC policies

A Question/Answer interface to retrieve information from the hybrid knowledge base

Thank you!

robert.buchmann@econ.ubbcluj.ro