An Integrated Meta-Model for Cloud Application Security Modelling

K. Kritikos[a] & P. Massonet[b]

a – ICS-FORTH, Heraklion, Greece

b – CETIC, Charleroi, Belgium

Outline

- Problematic
- Contribution
- Security Meta-Model
- Automatic Security Model Production
- Future Work

Co-funded by the European Union

The Facts

- Cloud computing continuously embraced by many organisations
- Migration to cloud via free or proprietary platforms
  - Model-Driven Engineering adopted
    - From generic requirements to cloud agnostic down to cloud-specific solutions
    - model@runtime support
    - Model transformation, reasoning & adaptation support

Co-funded by the European Union

The Problem & Opportunities

- Security is neglected
  - Main prevention factor for cloud migration
- It can be exploited to achieve:
  - Cloud provider filtering & deployment optimization based on security requirements
  - Security-based application adaptation

Co-funded by the European Union

Contribution

- Security meta-model:
  - Minimal but sufficient
  - Well-integrated in CAMEL
  - Coupled with OCL constraints for enforcing the domain semantics
  - Coverage of security requirements/capabilities & application reconfiguration rules
  - Linkage of security requirements for traceability
  - Better metric specification coverage

Co-funded by the European Union

Contribution (cont.)

- Method for producing security models
  - Modelling effort reduced
    - Re-use of security elements derived to specify security requirements/capabilities & reconfiguration rules
  - High-level cloud provider security capability description for provider filtering
- Rely on PaaSage
  - Multi-cloud application management platform
  - Security meta-model well-integrated in CAMEL multi-DSL

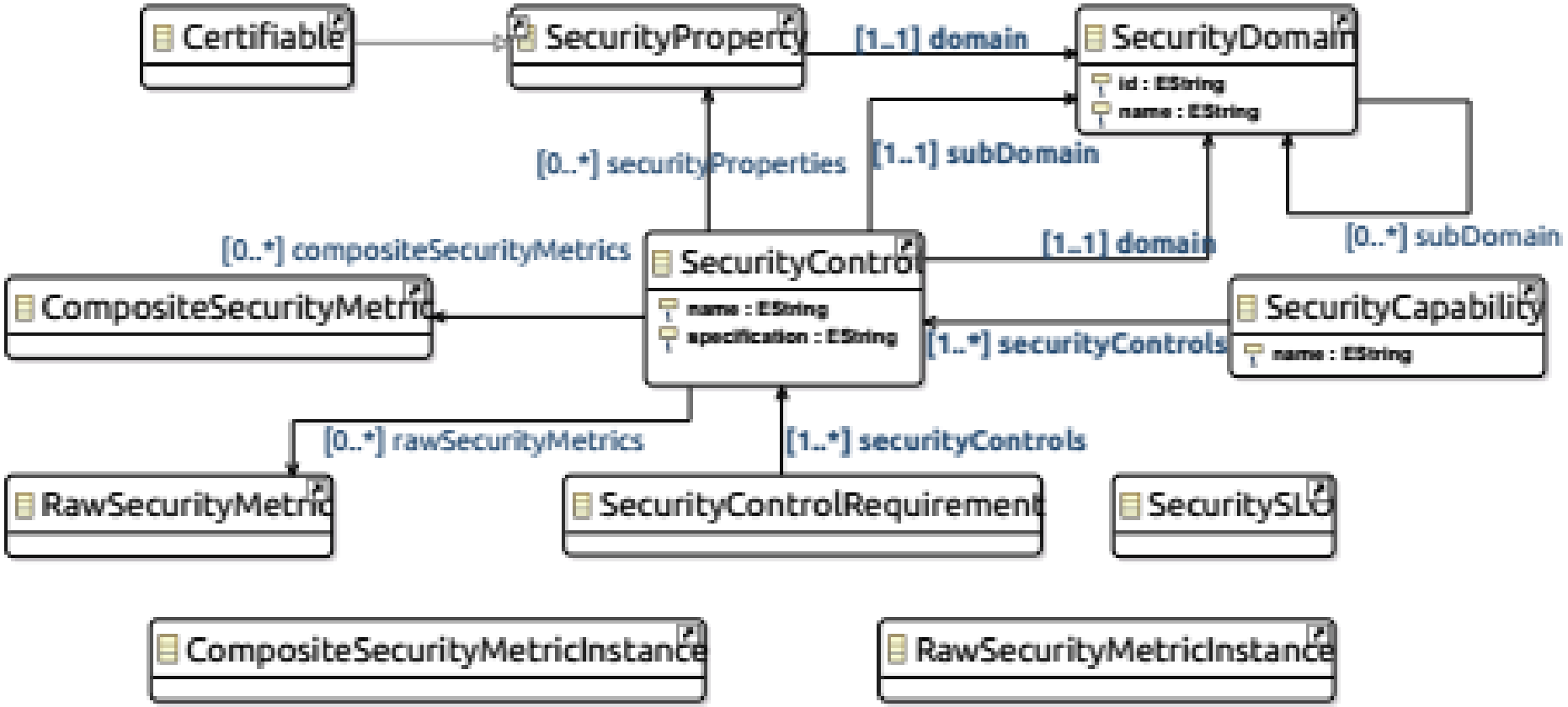
Co-funded by the European Union

Security Meta-Model – Design Requirements

- Cover basic domain concepts & relations
- Specify both high- & low-level security requirements
- Align requirements to CAMEL requirement DSL
  - Security SLOs as SLOs also exploited for scalability rule specification
- Better metric specification via alignment with CAMEL metric model
- Derive OCL constraints to cover domain semantics

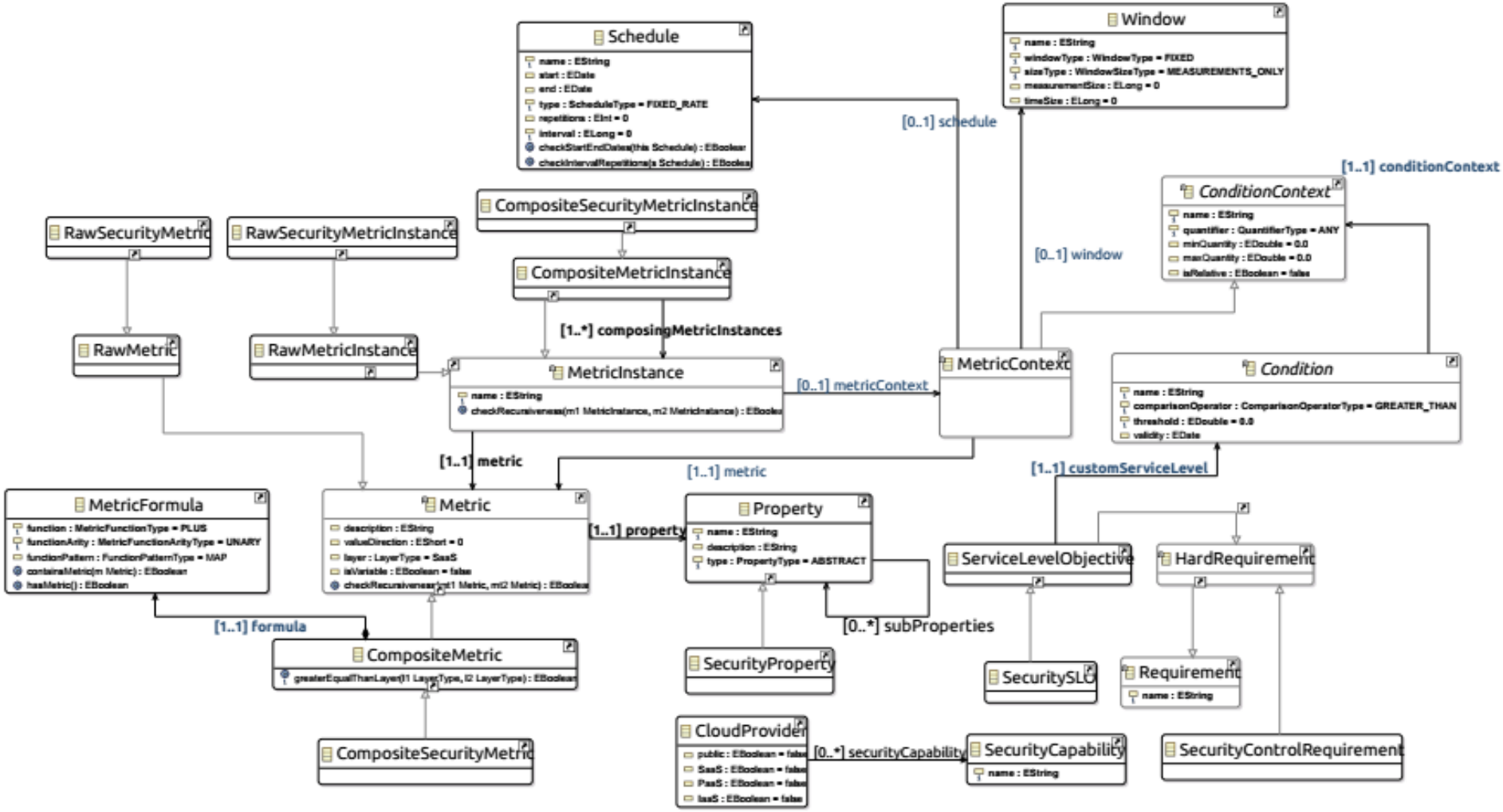
Co-funded by the European Union

Security Meta-Model



Co-funded by the European Union

Security Meta-Model – CAMEL Integration



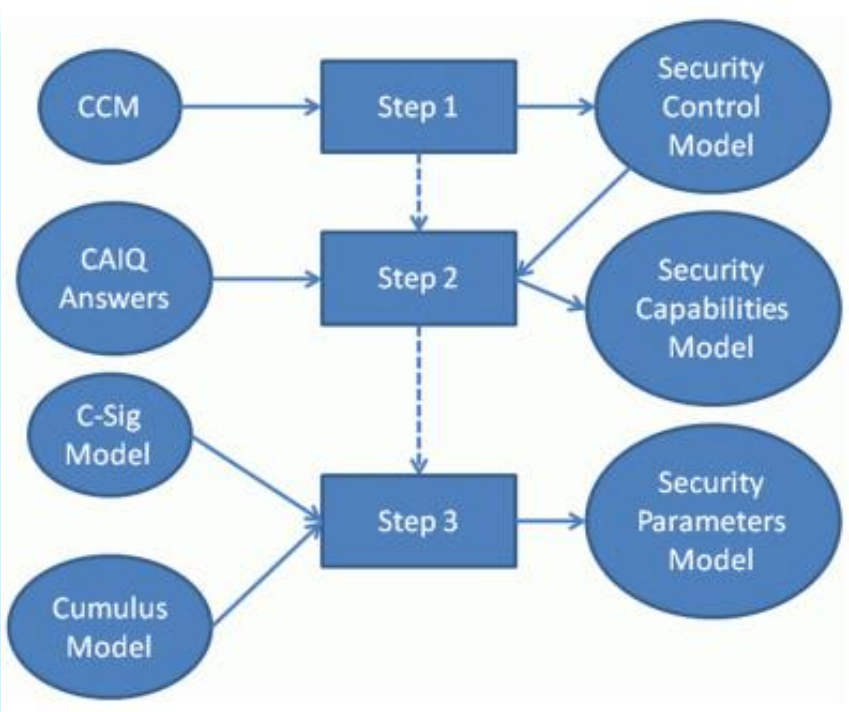
Co-funded by the European Union

Security Model Production Method

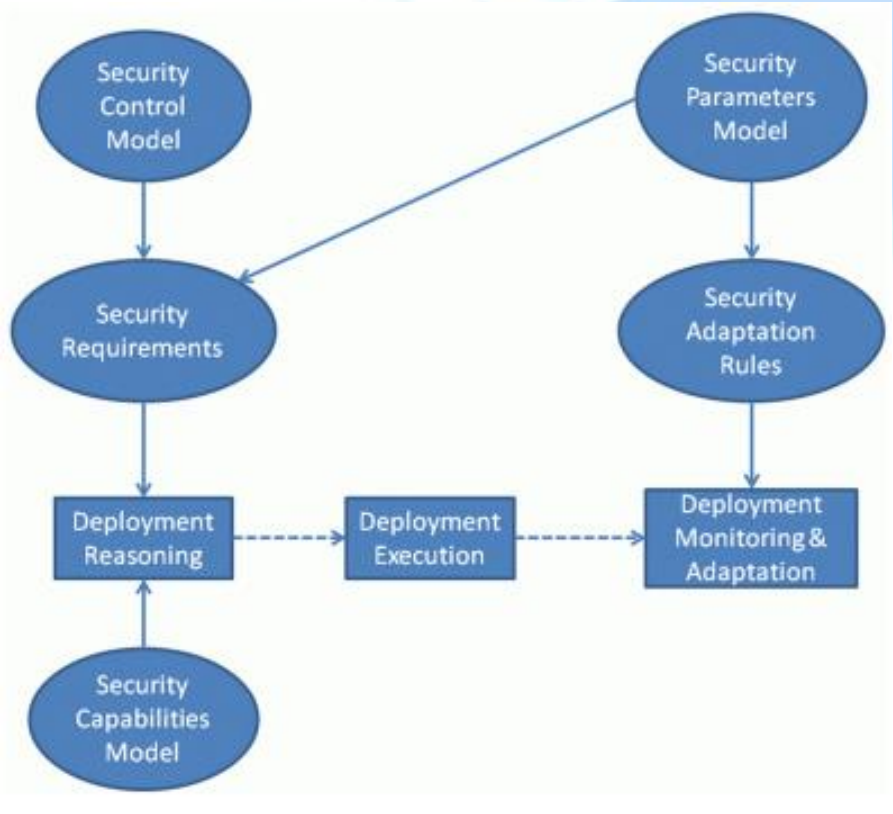
- Input:
  - SCA's Cloud Control Matrix (CCM)
  - SCA's Consensus Assessment Initiative questionnaires (CAIQ) completed by cloud providers
  - Security models (C-Sig, Cumulus) defined in [1-2]
- Steps:
  1. Security Control Model Production
  2. Security Capability Model Production
  3. Basic Security Model Production

Co-funded by the European Union

Security Model Production Method



(a) Method Steps



(b) Connection to PaaSage application deployment & provisioning workflow

Co-funded by the European Union

Security Model Production Method – Step 2

- Main idea:
  - question partitions related to security controls
  - Check answers & assess security control realization
    - Simple acceptance rule: positive question answer percentage > T (0.65)
    - Associate cloud provider to respective security control capability
- Issue – different versions of CAIQ
  - Old version with no yes/no answer field
    - Manual question inspection to derive simple yes/no answer

Co-funded by the European Union

Security Model Production Method – Step 3

- Main idea:
  - Start with existing models
  - Link elements together to form partitioned hierarchies with security controls on top
    - Cover conceptual gaps, when needed
    - Select the most suitable security controls per security element covered
- Resulting model can be used to specify hierarchies of security requirements

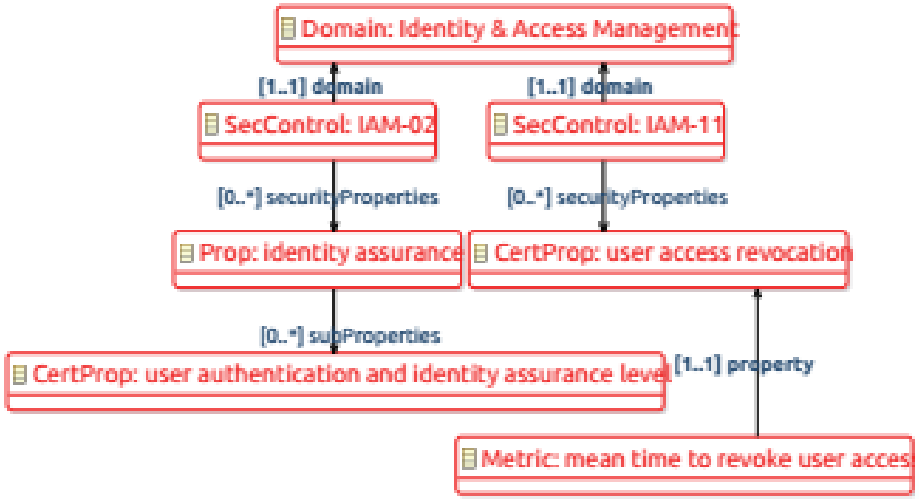
Co-funded by the European Union

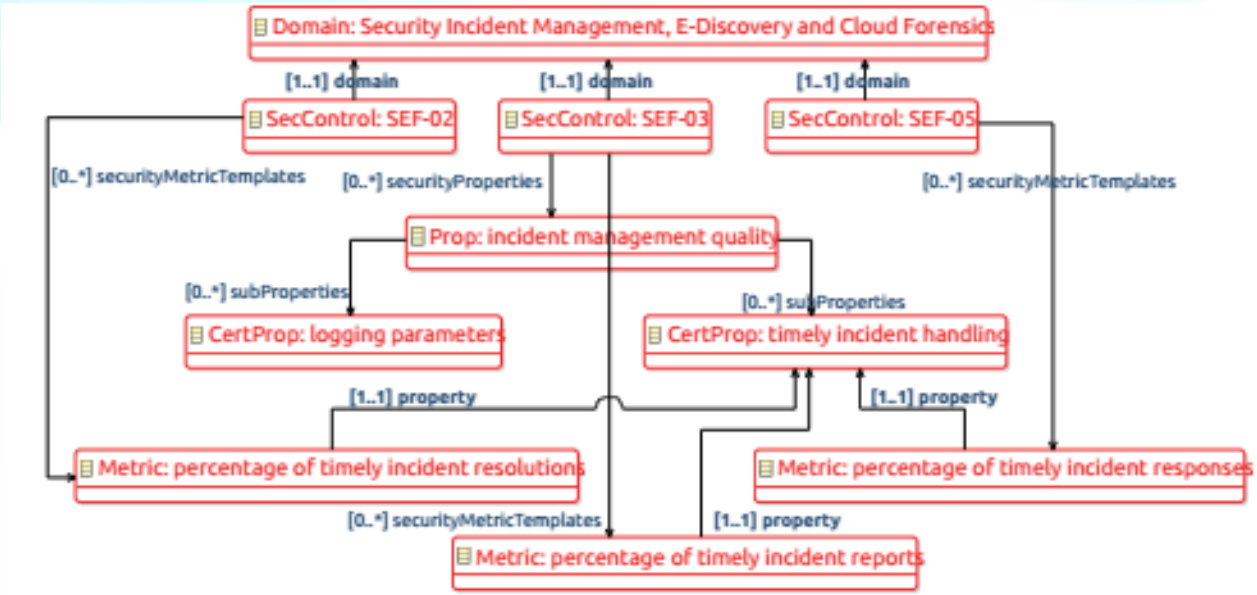
Security Model Production Method – Step 3

- Main Algorithm:
  - Input: Model1 as C-SIG model & Model2 as Cumulus model
  - Steps:
    - For each p (security metric of property) in Model1
      - Create respective security meta-model instances
      - Find equivalent element in Model2
        - » If exists, copy Model2 hierarchy on top of this element & match its domain with top security domains in security control model. Then, check which security control mapping to the match domain is the most appropriate
        - » If not, cover the gap by introducing a new property α which will be linked to a respective hierarchy by following a similar approach to the previous sub-case

Co-funded by the European Union

Security Model Production Method – Snapshots





Co-funded by the European Union

Future Work

- Extend security DSL to cover additional aspects or improve modelling of current aspects
- Consider additional prominent security models in the production of the basic security model
- Enhanced evaluation of degree of satisfaction of security controls
  - Query relative significance, levels of satisfaction for “yes” answers
- Couple security DSL with other (cloud) standards like TOSCA & WS-Agreement

Co-funded by the European Union

References

1. Cloud Select Industry Group (C-SIG), . Cloud Service Level Agreement Standardization Guidelines. Technical Report; 2014. URL: http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?action=display&doc_id=6138.
2. Pannetrat, A.. D2.1: Security-aware SLA specification language and cloud security dependency model. Cumulus Project Deliverable; 2013.

Co-funded by the European Union