CISTRANA

Identity and Trust in Security-aware SW architectures

Riccardo Scandariato

DistriNet, K.U. Leuven

Observation (1)

- Software architecture is the corner-stone of software development
  - First step into solution space
  - Place where stakeholders' needs are harmonized
- Driven by software qualities (a.k.a. NFR)
  - E.g., security is of growing importance

Observation (2)

- Support for security at architecture phase in secure software process is very limited
  - Microsoft SDL, OWASP CLASP, McGraw Touchpoints
- So far, only threat modeling

De Win, Scandariato, Buyens, Grégoire, Joosen, On the Secure Software Development Process, Journal of Information and Software Technology *(to appear)*

Security
What do we need?

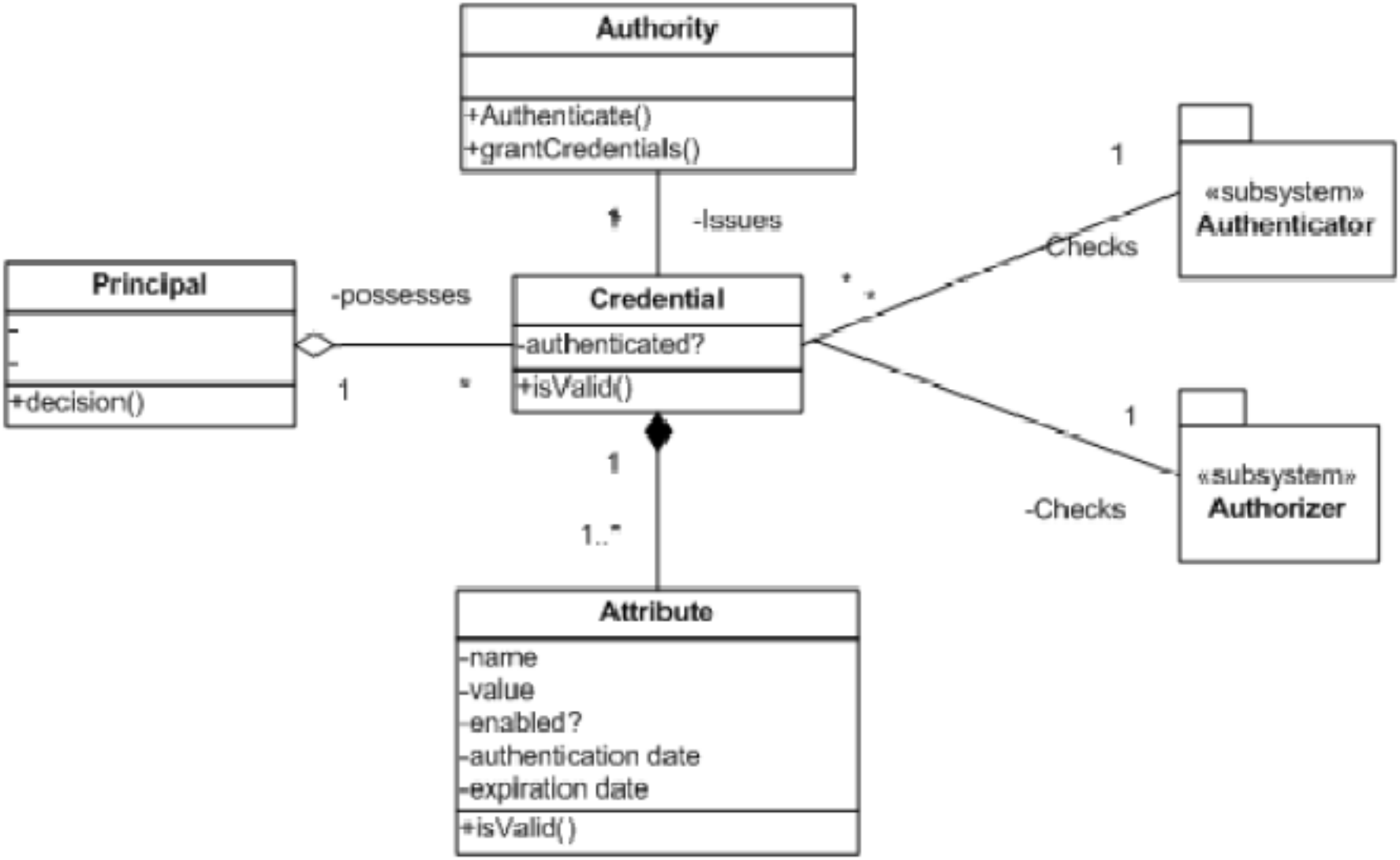
- A systematic methodology guiding the transition from security requirements to architecture
  - E.g., similarly to ADD (performance, reliability, etc.)
- An engineered catalog of architectural building blocks
  - E.g., security patterns

Pattern

- Well-known (and sound) solution for a recurring problem, whose pros and cons are known in advance
  - Pipes&Filters, Blackboard, Layers

"A pattern is a relationship between a certain context, a certain system of forces which occurs repeatedly in that context, and a certain spatial configuration which allows these forces to resolve themselves" [Coplien]

Security patterns
Credential



IDM patterns (1)

- C. Steel, et al, Core Security Patterns: Architectural Patterns and Best Practices, 2005, Prentice Hall
  - Assertion builder
  - Credential tokenizer
  - Single sign-on delegator
- SAML (and J2EE) oriented

IDM patterns (2)

- N. Delessy, E. Fernandez, M. Larrondo-Petrie, A pattern Language for Identity Management, ICCGI 2007
  - Identity Provider
  - Identity Federation
  - Circle of Trust
- Using
  - Authenticator [Schumacher] and Credential [PLoP06]
- Interaction with other security features
  - E.g., attribute-based authorization

Software architectures
Research agenda

- Architectural building blocks
  - More systematic catalog(s) of patterns
  - E.g., distilled IDM knowledge out of standards and technologies

- Architecture definition
  - Tools and techniques to embed security concerns in software architectures

Software architectures
Research agenda

- Architectural trade-offs
  - Interaction of security sub-features (IDM vs. authZ)
  - Interference with others qualities (e.g., IDM vs. usability)
  - Security-oriented evaluation
- Architectural notations
  - Extensions to support communication, trade-off analysis, and consistency analysis

Software architectures
Synergies

- Supporting automation
  - Req → Archi
  - Archi → Design
- Process improvement
  - Construction activities
  - Verification activities
- Towards requirements
  - Which RE methodology fits better?
  - Requirement patterns to bridge the gap?

CISTRANA

Identity and Trust in Security-aware SW architectures

Riccardo Scandariato

DistriNet, K.U. Leuven