Secure Software Modeling Methods for Forensic Readiness

Lukáš Daubner, Tomáš Pitner

LAB OF SOFTWARE ARCHITECTURES AND INFORMATION SYSTEMS

FACULTY OF INFORMATICS
MASARYK UNIVERSITY, BRNO

lasaris

Content

- Security modelling
- Security Modeling Methods
- Forensic Readiness
- Security Modeling Methods for Forensic Readiness

lasaris

Security by Design

- Defects in design
- Lack of background in cybersecurity
- Security is often considered last
- Reactive patching is not enough

lasaris

Security Modeling

- Model-Driven Security
- UML profiles
- Aspect-Oriented Modeling
- Domain Specific Languages

lasaris

Security Modeling – Model-Driven Security

- Subset of Model-Driven Development
- Semi-automatic transformations between models
- Model verification

lasaris

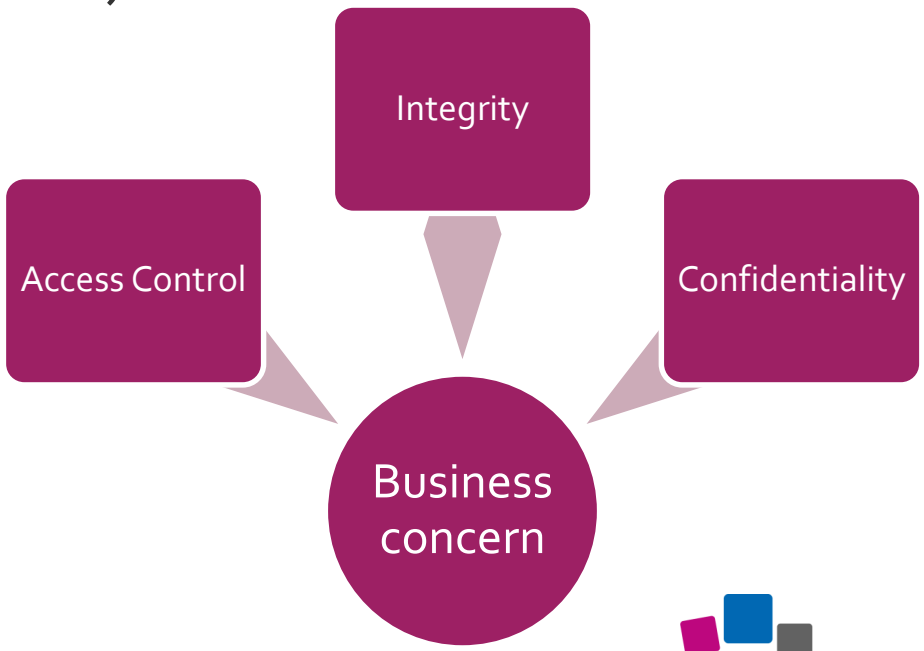
Security Modeling – UML profile

- Extension to UML
- Stereotypes
- Tagged values
- Constraints

lasaris

Security Modeling – Aspect-Oriented Modeling

- Separation of concerns
- Security concerns (aspects)
  - Independently modelled
  - Encapsulated
- Weaving together



lasaris

Security Modeling Methods

UMLsec

- Formulated by J. Jürjens
- UML profile – an extension for security modeling
- Considered as most mature approach
- Support for formal model verification

lasaris

UMLsec – Concerns

- Confidentiality
- Integrity
- Authenticity
- Non-Repudiation
- Access Control
- Information Flow
- Fair Exchange
- Etc.

lasaris

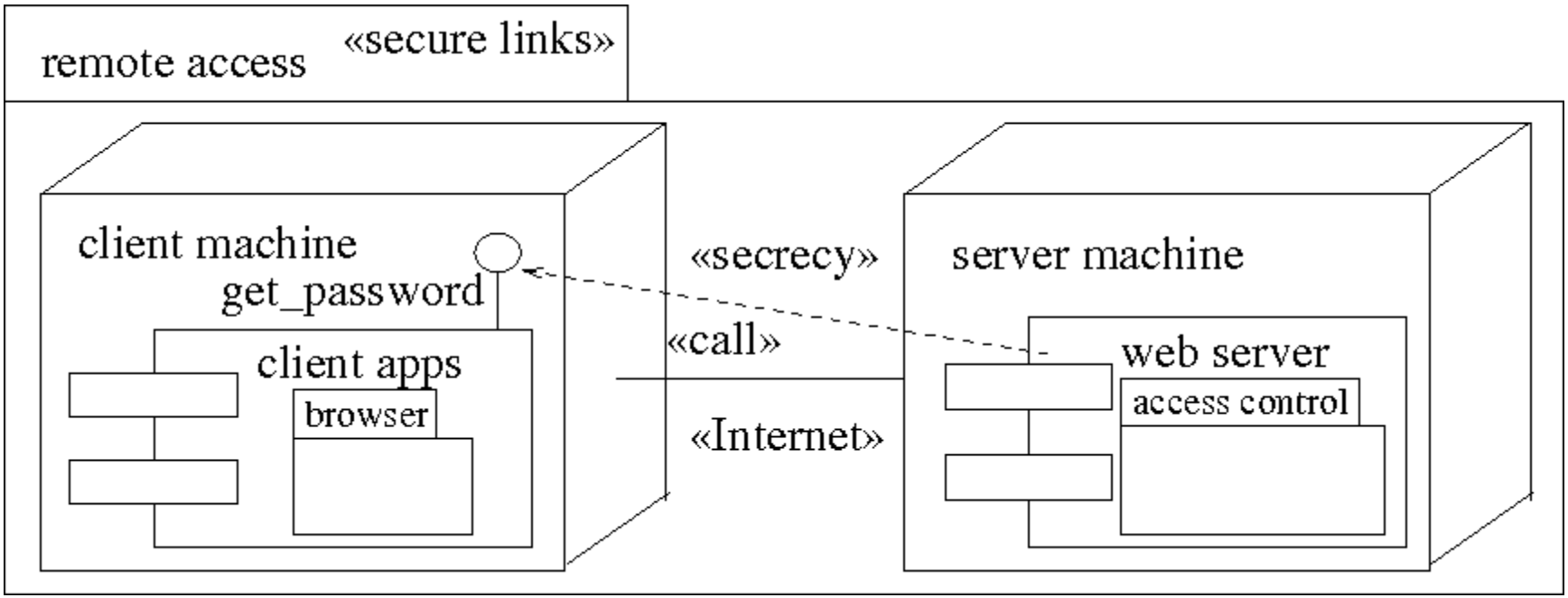
UMLsec – Example

Stereotype	Base class	Constraints	Description
secure links	subsystem	dependency security matched by links	enforces secure communication links
secrecy	dependency	$read \notin Threats_A(s)$	assumes secrecy
Internet	link		Internet connection
encrypted	link		encrypted connection

- Threat rules:
  - Internet - $Threats_A(s) \in \{delete, read, insert\}$
  - encrypted - $Threats_A(s) \in \{delete\}$

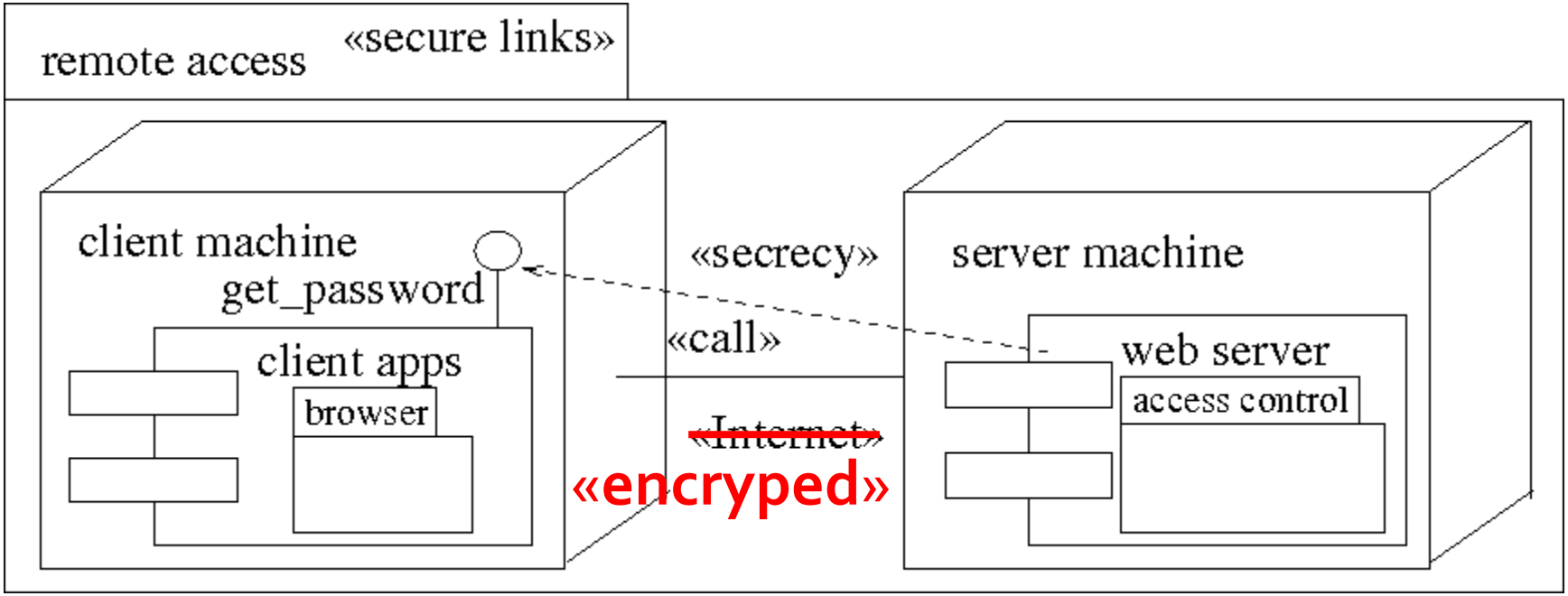
lasaris

UMLsec – Example



lasaris

UMLsec – Example



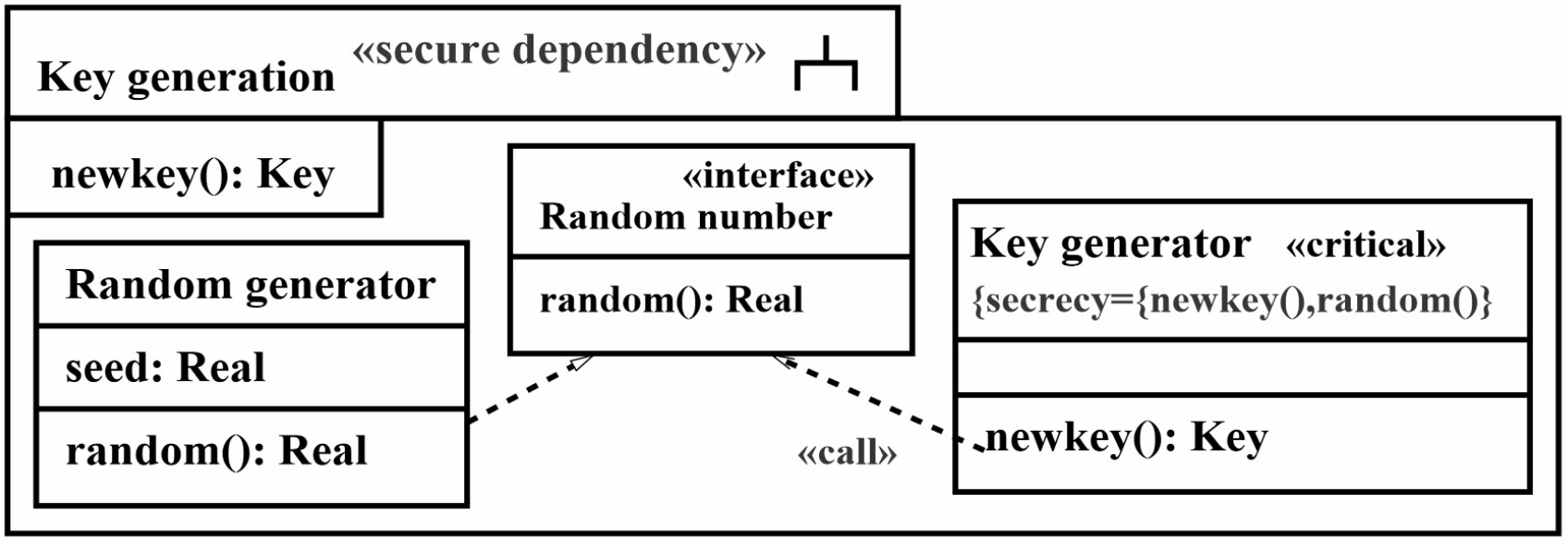
UMLsec – Example II

Stereotype	Base class	Constraints	Description
secure dependency	subsystem	«call» and «send» respect data security	structural interaction data security
critical	object		critical object

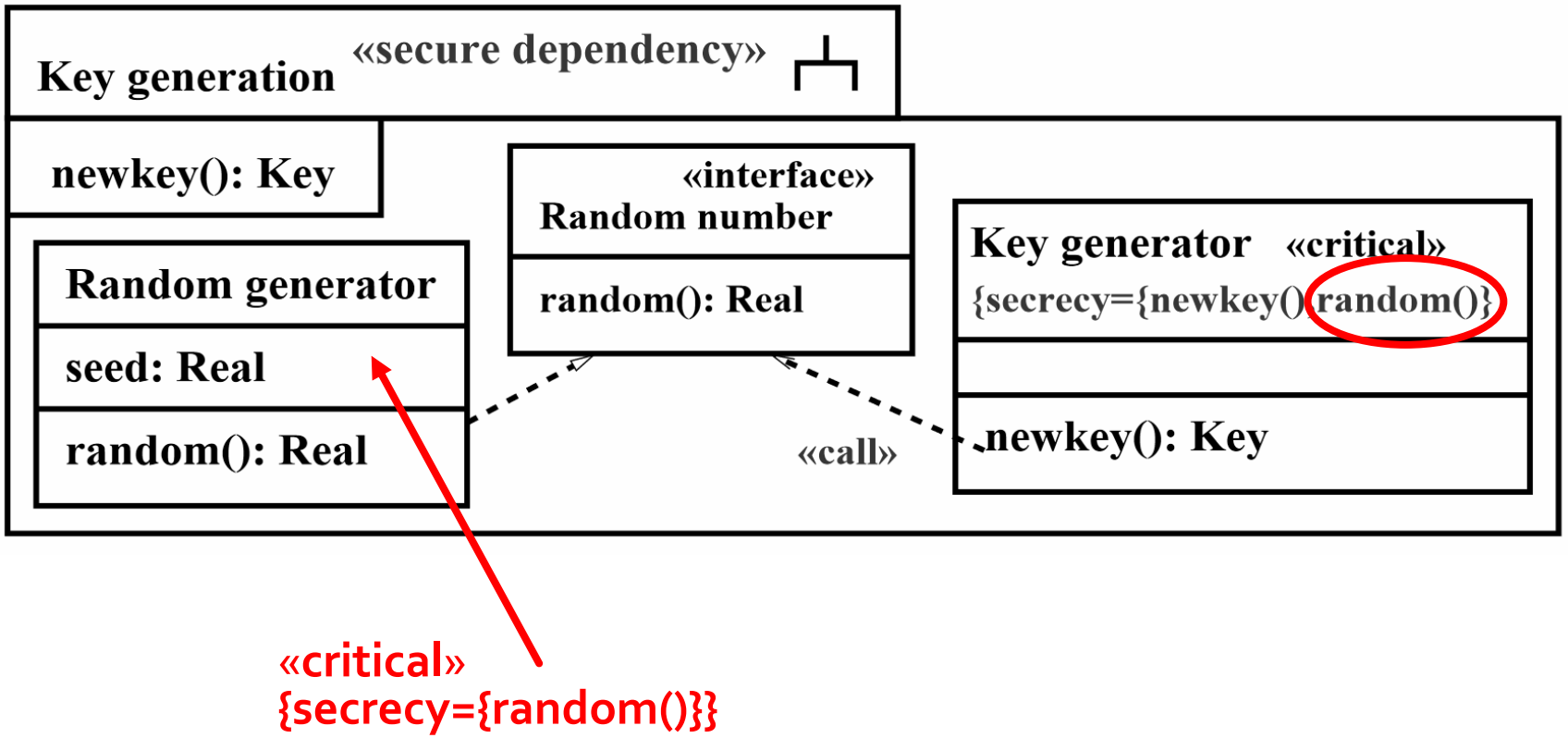
Tag	Stereotype	Description
secrecy	critical	Secrecy of data

lasaris

UMLsec – Example II



UMLsec – Example II



SECTET

- UML profile
- Object Constraint Language
- Aimed at distributed, inter-organizational workflows
- Model-Driven

lasaris

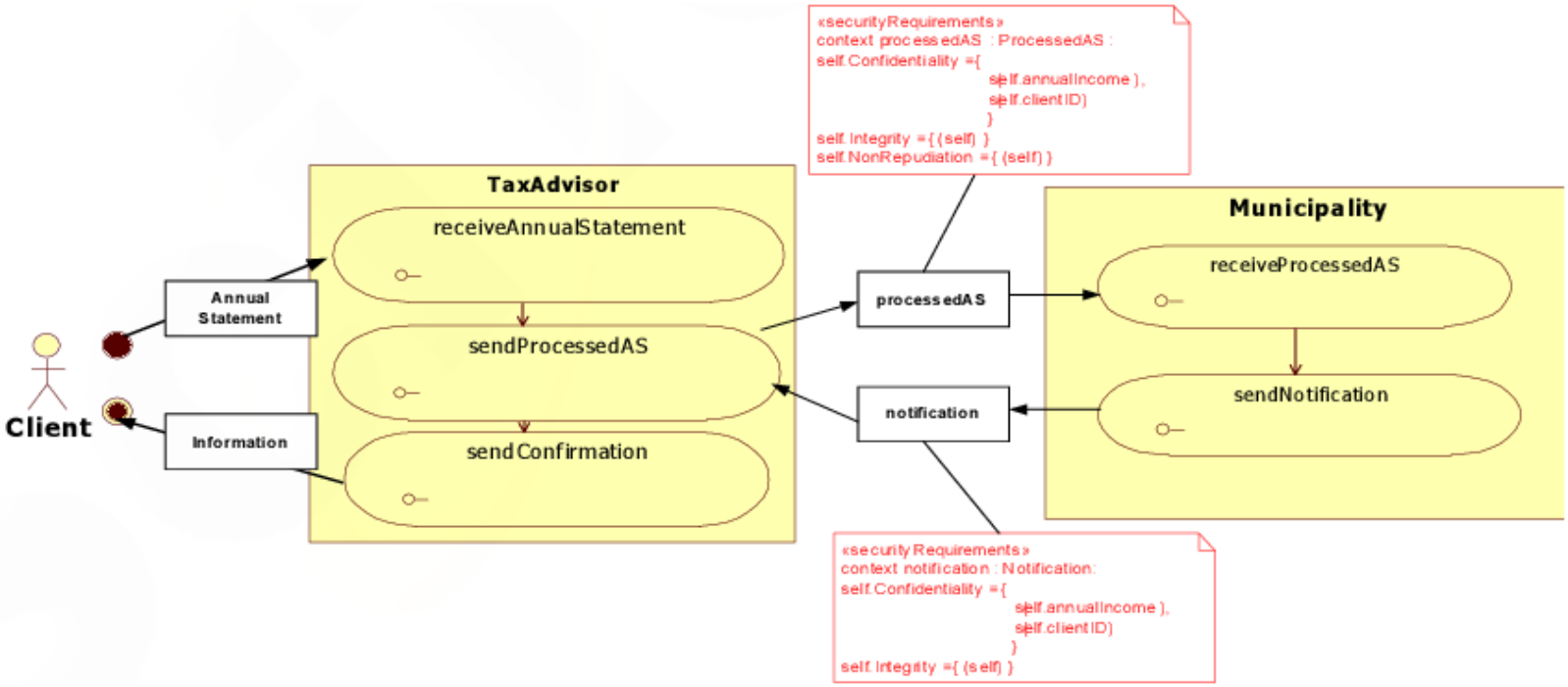
SECTET

- Workflow view
  - Global workflow
  - Local workflow
- Interface view
  - Document model
  - Interface model
  - Role model
  - Access model

lasaris

SECTET – Example

- Global workflow model



lasaris

SECTET – Example

- BPEL file for each partner-role
- Security configuration

```
<process name="Sectino_TaxAdvisor_LWfM">
  <partnerLinks>
    <partnerLink name="MS_Provider" partnerLinkType="Municipality_LWfM"
     partnerRole="Municipality_LWfM"/>
    <partnerLink name="TS_Provider" partnerLinkType="TaxAdvisor_LWfM"
    partnerRole="TaxAdvisor_LWfMRequester"
    myRole="TaxAdvisor_LWfMProvider"/>
  </partnerLinks>
  <variables>
    <variable name="input" messageType="AnnualStatement"/>
    <variable name="output" messageType="Confirmation"/>
    <variable name="input_MU" messageType="ProcessedAS"/>
    <variable name="output_MU" messageType="Notification"/>
  </variables>
  <sequence name="main">
   <receive name="receiveInput" partnerLink="TS_Provider"
    portType="TaxAdvisor_LWfM"
    operation="sendAnnualStatement" variable="input" createInstance="yes"/>
   <invoke // !!! INSERT CALLS TO LOCAL SERVICES !!! //>
   <invoke partnerLink="MS_Provider" portType="Municipality_LWfM"
    operation="sendProcessedAS" inputVariable="input_MU"
    outputVariable="output_MU" name="sendProcessedAS"/>
   <invoke // !!! INSERT CALLS TO LOCAL SERVICES !!! //>
   <invoke name="callbackClient" partnerLink="TS_Provider"
    portType="TaxAdvisor_LWfMCallback"
    operation="onResult" inputVariable="output"/>
  </sequence>
</process>
```

```
PolicySet {(target=<AnnualStatement>)
 PolicySet { target=<outbound>
   PolicySet {(target=<processedAS>)

    Policy (Aspect = "Confidentiality") {
      Rule {
        Signature-Algorithm = "RSA-SHA1",
        Node1 = "/self/annualIncome",
        Node2 = "/self/clientID",
        Recipient = "Municipality"} }
    Policy (Aspect = "Integrity") {
      Rule {
        Signature-Algorithm = "RSA-SHA1",
        Node1 = "/self/",
        Recipient = "Municipality"}
    }
 PolicySet { target=<inbound>
   PolicySet {(target=<processedAS>)

     Policy (Aspect = "Qualified Sign") {
      Rule {
        Signature-Algorithm = "RSA-SHA1",
        Node1 = "/self/",
        Source = "Municipality"
        Signatories = 2}
}}}}
```

lasaris

UML4SOA-NFP

- UML profile
- Extension to UML4SOA
- Aimed on Service Oriented Architectures
- Non-functional requirements

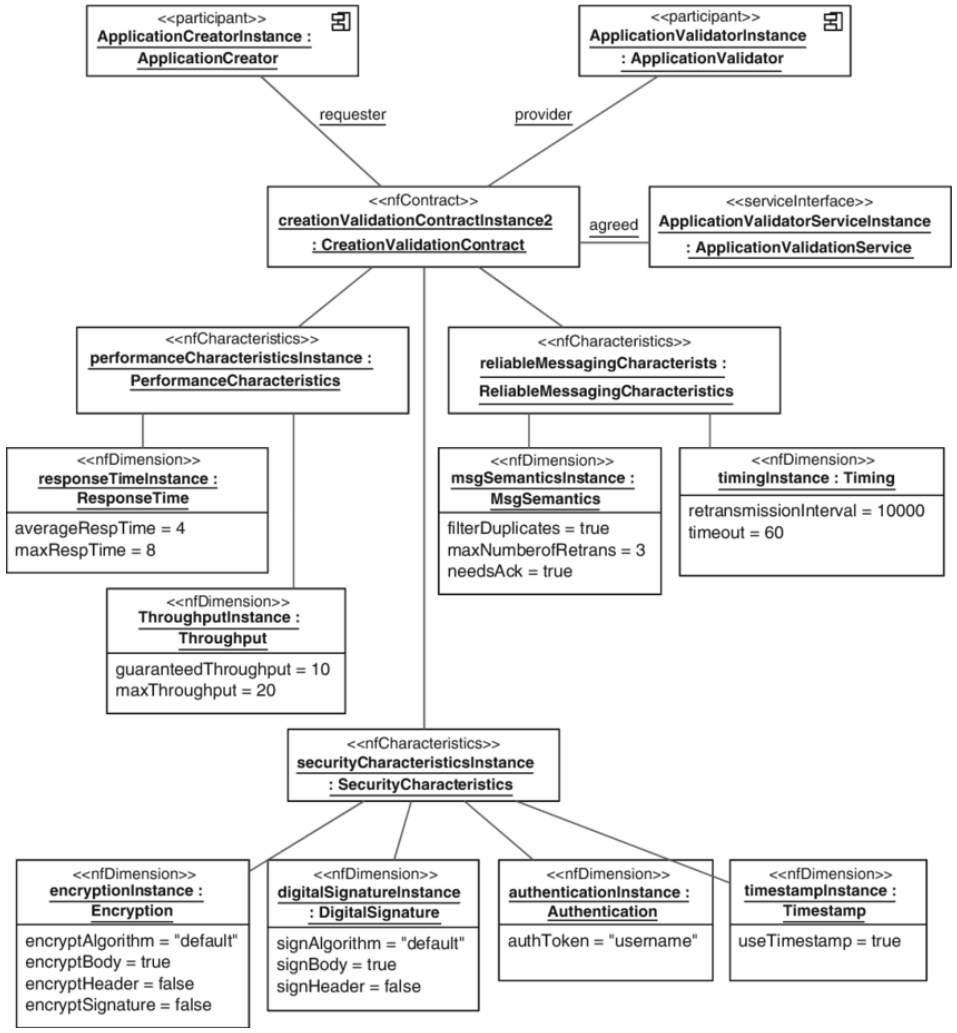
lasaris

UML4SOA-NFP

- Performance
- Dependability
- Reliable messaging
- Security
  - Confidentiality
  - Integrity
  - Non-repudiation
  - Privacy
  - Access Control

lasaris

UML4SOA-NFP – Example



lasaris

UML4SOA-NFP – Example

```
<?xml version='1.0'?>
<service name="ApplicationValidationService">
  <operations>
  </operations>
   <wsp:Policy wsu:Id="ApplicationValidationServiceSecurityPolicy"
         xmlns:wsu="http://docs.oasis-open.org/wss/
           2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"
         xmlns:wsp="http://schemas.xmlsoap.org/ws/
           2004/09/policy">
    <wsp:ExactlyOne>
      <wsp:All>
        <sp:Authentication
            xmlns:sp="http://schemas.xmlsoap.org/ws/
              2005/07/securitypolicy">
          <wsp:Policy>
            <wsp:authToken>
              <wsp:Policy>
                <sp:Username/>
              </wsp:Policy>
            </wsp:authToken>
          </wsp:Policy>
        </sp:Authentication>
              ~~~
        <sp:Timestamp ..
          <wsp:Policy>
            <wsp:useTimestamp/>
          </wsp:Policy>
        </sp:Timestamp>
      </wsp:All>
    </wsp:ExactlyOne>
  </wsp:Policy>
  <wsp:Policy wsu:Id="ApplicationValidationServiceRMPolicy"
   xmlns:wsp="http://schemas.xmlsoap.org/ws/2004/09/policy"
   xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401
   -wss-wssecurity-utility-1.0.xsd"
   xmlns:wsrm="http://ws.apache.org/sandesha2/policy">
    <wsp:ExactlyOne>
      <wsp:All>
        <wsrm:filterDuplicates>true</wsrm:filterDuplicates>
        <wsrm:needsAck>true</wsrm:needsAck>
        <wsrm:maxNumberOfRetrans>3</wsrm:maxNumberOfRetrans>
        <wsrm:retransInterval>10000</wsrm:retransInterval>
        <wsrm:timeout>60</wsrm:timeout>
      </wsp:All>
    </wsp:ExactlyOne>
  </wsp:Policy>
</service>
```

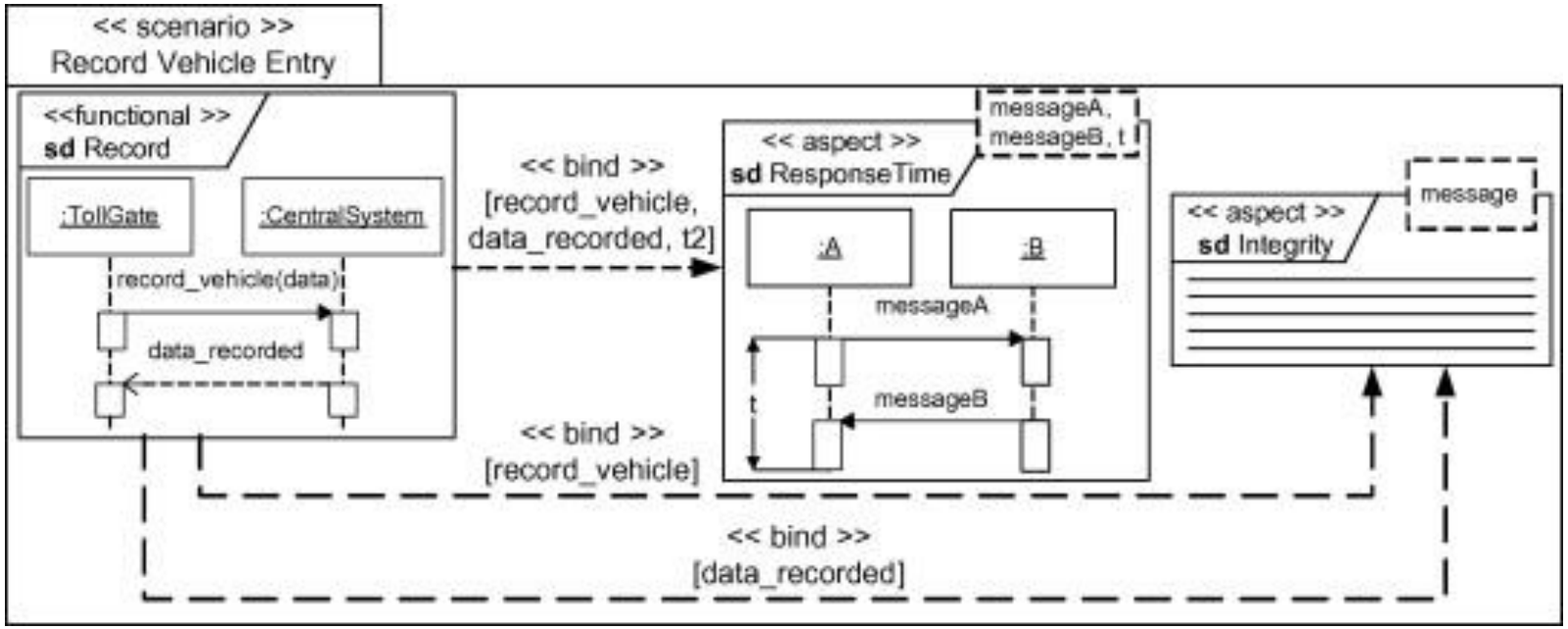
lasaris

AOMsec

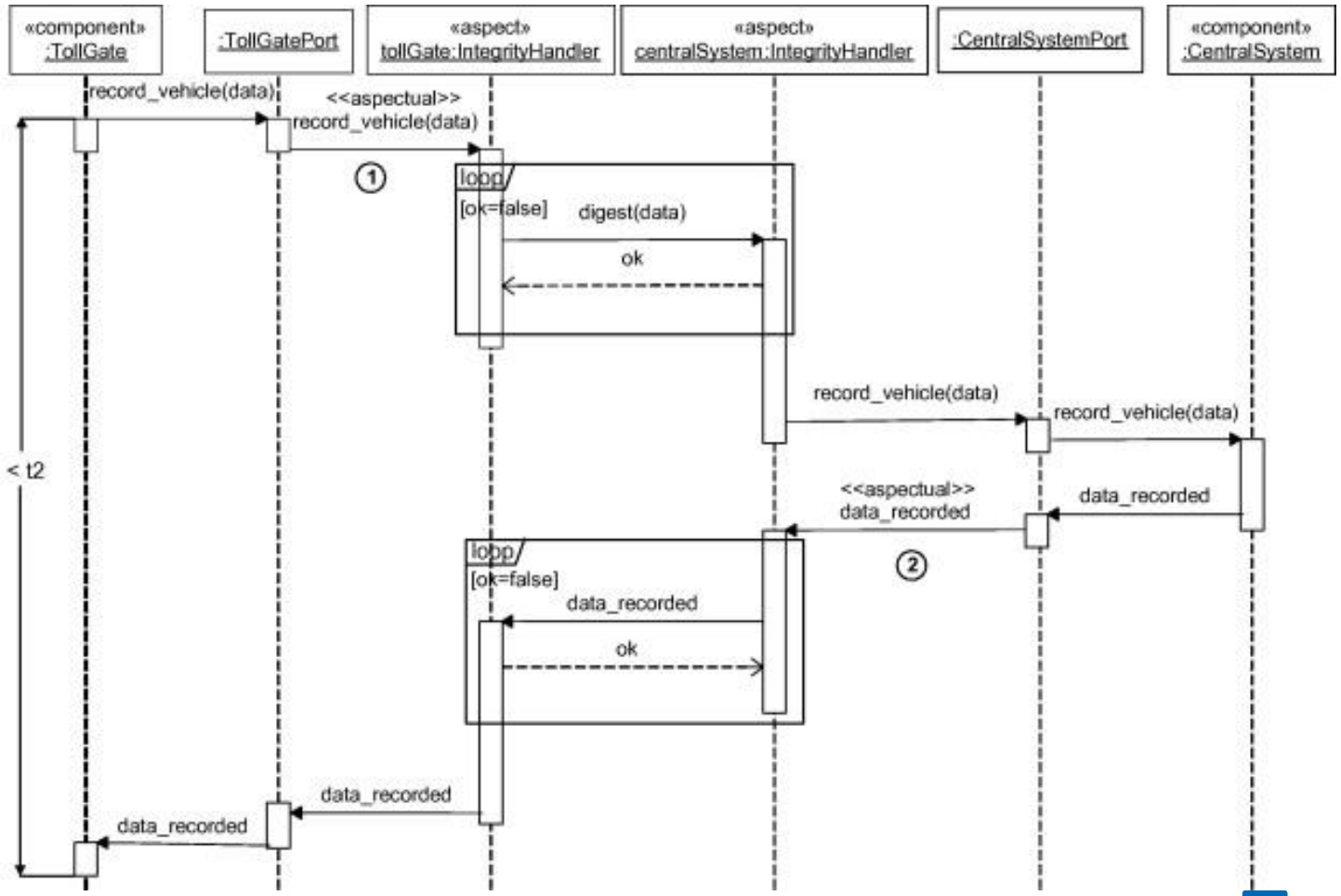
- Aspect-Oriented approach
- UML profile
- Non-functional requirements
- Model-Driven

lasaris

AOMsec – Example



AOMsec – Example



lasaris

Sec@Runtime

- Aspect-Oriented approach
- UML profile
- Runtime weaving
- Platform and toolset

lasaris

SecureDWs

- UML profile
- Aimed at Data Warehouses
- Tackles auditing concern
- Access control, privacy, integrity, etc.

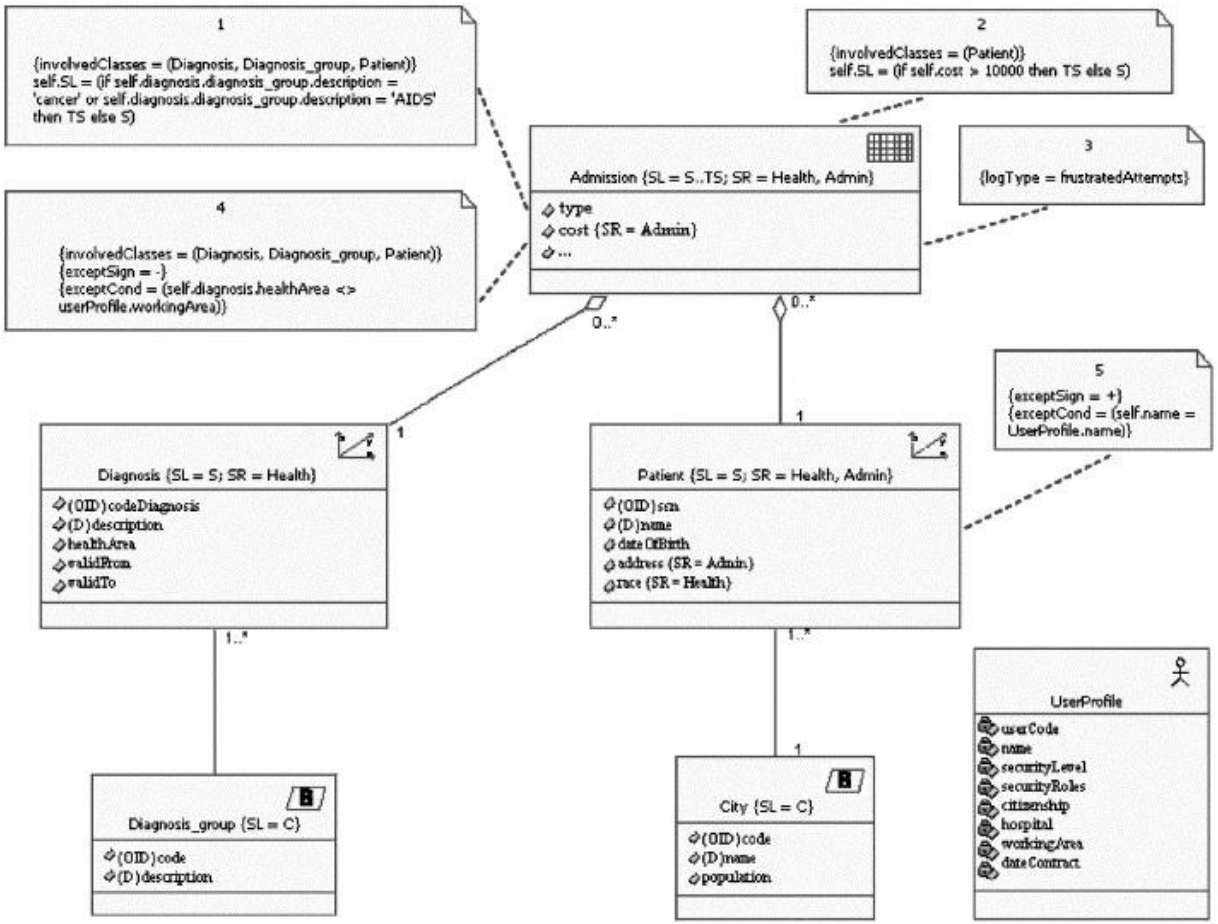
lasaris

SecureDWs – Example

Tag	Stereotype	Description	Type
LogType	class	Specifies if access should be recorded	Attempt
LogCond	class	Specifies condition when is access recorded	OCLExpression
ExceptSign	class	Allow/deny access if constraint applies	{+,-}
InvolvedClasses	class	Constraint applicable if query contains given classes	Set(OCLType)

lasaris

SecureDWs – Example



Forensic Readiness

What is Forensic Readiness?

- Definition by J. Tan (2001)
  - Maximizing the usefulness of incident evidence data
  - Minimizing the cost of forensics during an incident response
- Systematic preparation for forensic investigation
- Proactive measures
  - Opposed to actual investigation, which is reactive
- Increases likelihood of successful investigation

lasaris

Forensic Readiness in Software Engineering

- Formulated by Pasquale et al. (2018)
- Prepare software system during its development
  - Forensic-by-design
- Support for:
  - Proactive evidence securing
  - Data provenance
  - Ensuring chain of custody
- Non-functional requirement

lasaris

Forensic Readiness Concerns

- Availability
- Relevance
- Minimality
- Linkability
- Completeness
- Non-repudiation
- Data provenance
- Legal compliance

lasaris

Forensic Readiness Concerns Meets Security

- Partial overlap with security concerns
- Typically specialized applications of concerns
- Difference between technical and legal understanding
  - Both needs to be addressed

lasaris

Forensic Readiness Concerns Meets Security

- **Availability**
- Relevance
- Minimality
- Linkability
- Completeness
- **Non-repudiation**
- **Data provenance**
- Legal compliance

lasaris

Relevant Security Modeling Methods

Method	Domain	Approach	Security concerns
UMLsec	General	UML profile	Integrity, Non-repudiation
SECTET	Distributed workflows	UML profile	Integrity, Non-repudiation
AOMsec	General	AOM, UML profile	Integrity
Sec@Runtime	General	AOM, UML	Integrity
SecureDWs	Data Warehouses	UML profile	Integrity, Non-repudiation, Auditing
UML4SOA-NFP	SOA	UML profile	General non-functional requirements

lasaris

Relevant Security Modeling Methods

- UMLsec
  - Most promising basis
- AOMsec
  - Lower overhead for designer
  - Patterns
- SecureDWs
  - Auditing description

lasaris

Conclusion

- Security-by-design is important to avoid defects
  - Similar motivation for forensic readiness
- Secure modeling methods are promising in forensic readiness
  - There are overlaps in concerns
  - Although they are not directly applicable
  - They can be used as a basis for forensic readiness modeling

lasaris

References

- Jürjens J. (2002) UMLsec: Extending UML for Secure Systems Development. In: Jézéquel JM., Hussmann H., Cook S. (eds) ≪UML≫ 2002 — The Unified Modeling Language. UML 2002. Lecture Notes in Computer Science, vol 2460. Springer, Berlin, Heidelberg
- Hafner, Michael, Ruth Breu, Berthold Agreiter and Andrea Nowak. "SECTET - An Extensible Framework for the Realization of Secure Inter-Organizational Workflows." WOSIS (2006).
- Gilmore, Stephen & Gönczy, László & Koch, Nora & Mayer, Philip & Tribastone, Mirco & Varro, Daniel. (2010). Non-functional properties in the model-driven development of service-oriented systems. Software and System Modeling. 10. 287-311. 10.1007/s10270-010-0155-y.
- Sánchez, Pablo & Moreira, Ana & Fuentes, Lidia & Araújo, João & Magno, José. (2010). Model-driven development for early aspects. Information & Software Technology. 52. 249-273. 10.1016/j.infsof.2009.09.001.
- Eduardo Fernández-Medina, Juan Trujillo, Rodolfo Villarroel, and Mario Piattini. 2007. Developing secure data warehouses with a UML extension. Inf. Syst. 32, 6 (September 2007), 826-856. DOI=http://dx.doi.org/10.1016/j.is.2006.07.003

lasaris