dipartimentoinformatica
Università degli Studi dell'Aquila

# Analyzing Tradeoffs between Software Security and Performance

PhD student
Catia Trubiani
catia.trubiani@univaq.it

Advisor
Vittorio Cortellessa
vittorio.cortellessa@univaq.it

Project PRIN PaCo (Performability-aware Computing)
Camerino, 15th September 2010

## Outline



» Motivation

» Our approach

- Security Library
- Enabling Security

» Experimental validation

» Conclusions

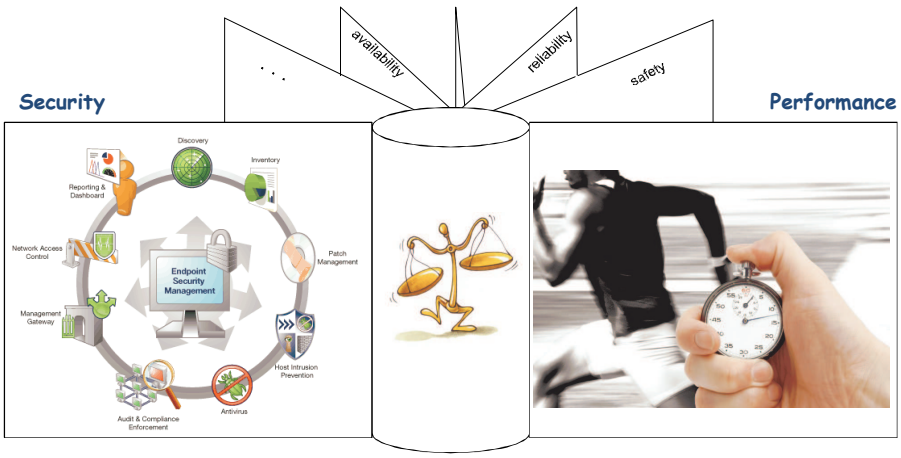
V.Cortellessa, C.Trubiani, L.Mostarda, N.Dulay
"An Architectural Framework for Analyzing Tradeoffs between Software Performance and Security"
@ISARCS – International Symposium on ARchitecting Critical Systems, CompArch 2010

Project PRIN PaCo (Performability-aware Computing)
Camerino, 15th September 2010

## Motivation

3

» Trade-off analysis for critical systems

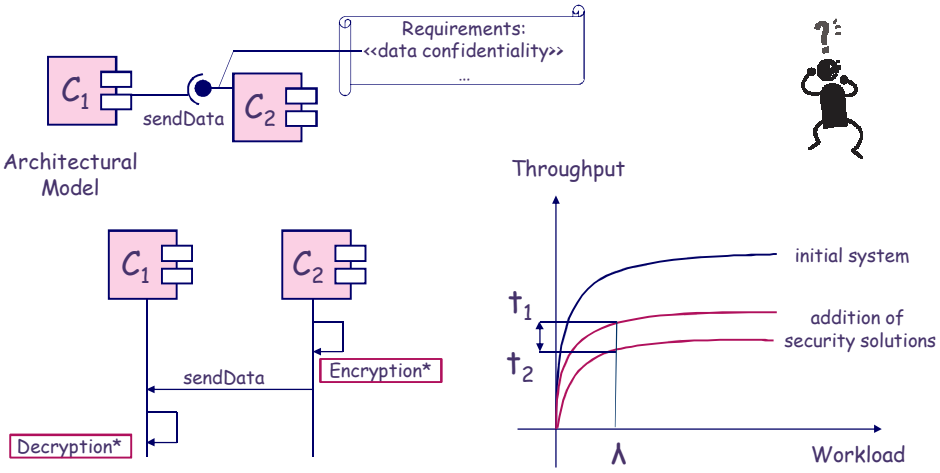





## Problem statement

4

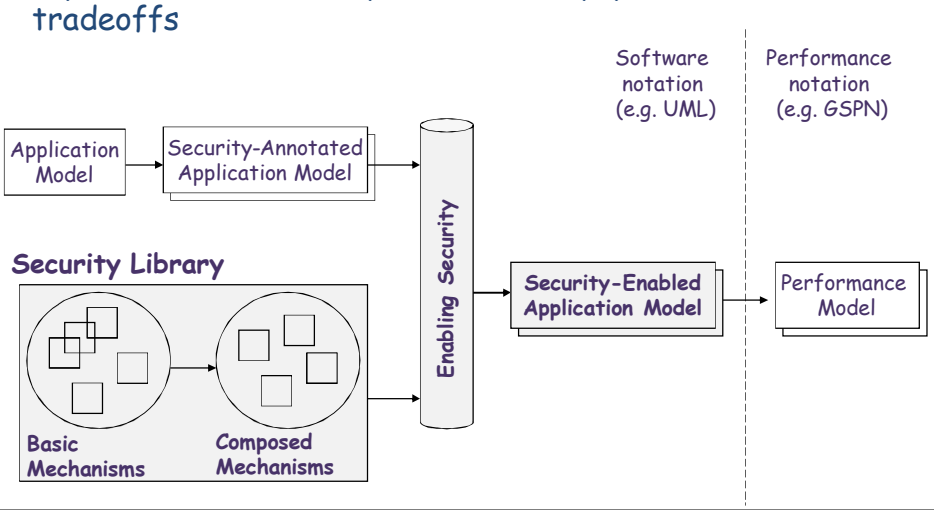
» How much the security solutions degrade performance?



## Our approach

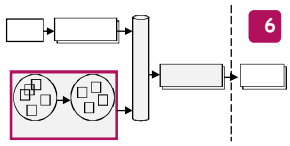
5

» A process for the analysis of security/performance tradeoffs






## A vision of our Security Library

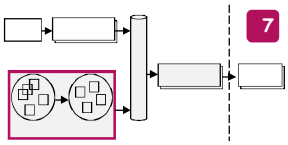


6

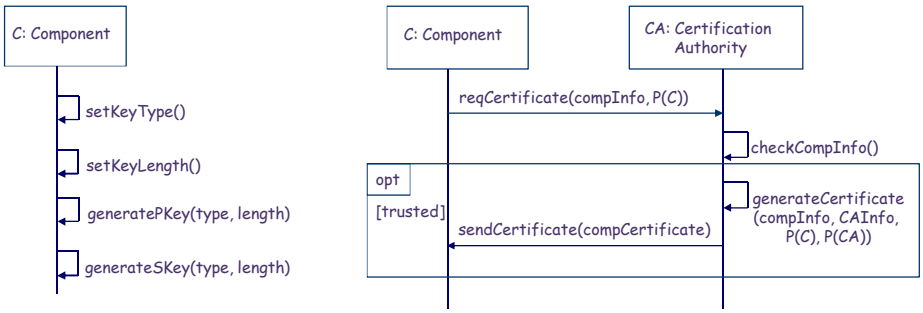
» Dependencies between Mechanisms

| Composed \ Basic | Encryption | Digital Signature Generation | Digital Signature Verification | Decryption |
|---|---|---|---|---|
| Data Confidentiality | X | | | X |
| Data Integrity | | X | X | |
| Peer Entity Authentication | | X | X | |
| Data Origin Authentication | | X | | |

# Security Library (1/3)



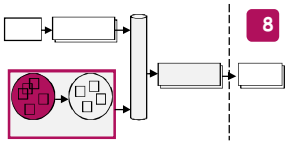

» Some preliminary operations



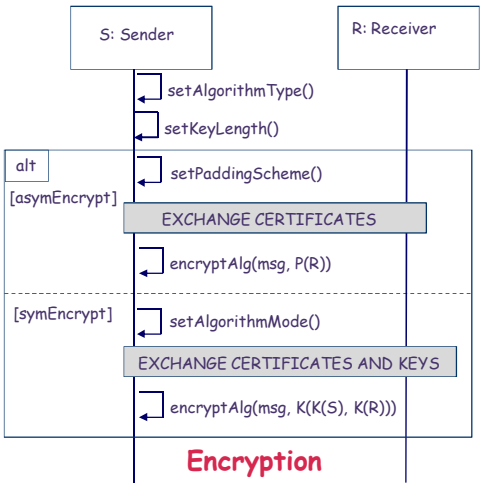

"generateKeys" "getCertificate"



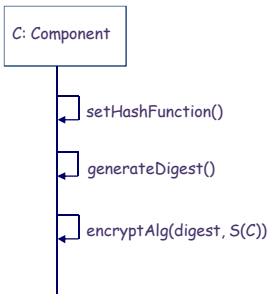
# Security Library (2/3)




» Basic Mechanisms



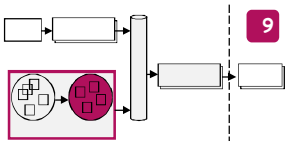

Encryption



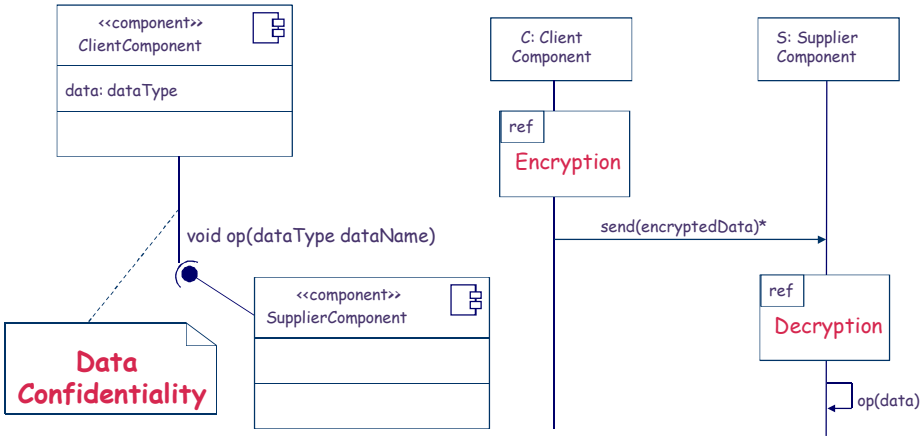

Digital Signature Generation

## Security Library (3/3)





» Composed Mechanisms



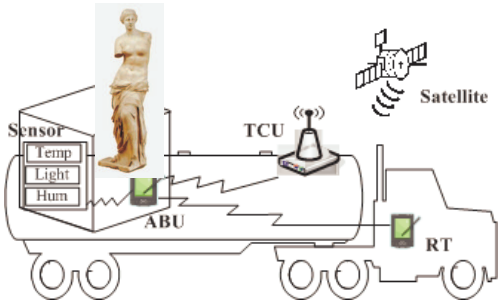



## Our approach at work!

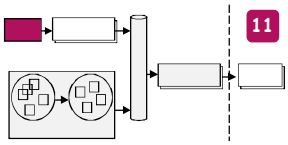


» More details of the approach by means of a driving case study, i.e. the CUSPIS system:

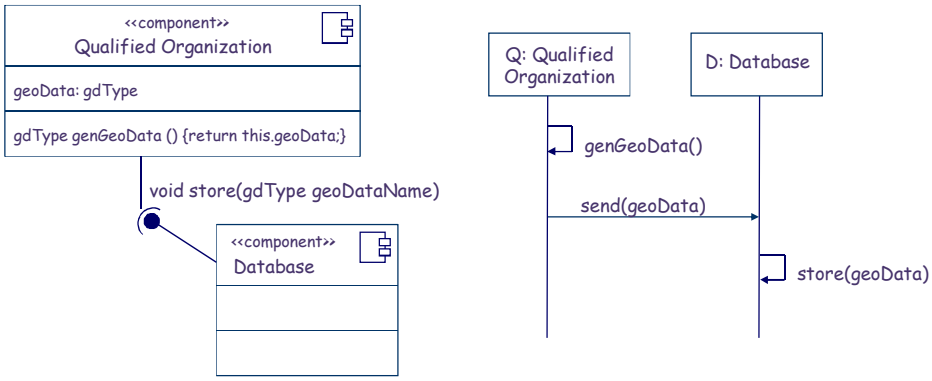
- Cultural asset authentication (CAA)
  - "GeoDataGeneration" scenario
- Cultural asset transportation (CAT)



## Application Model

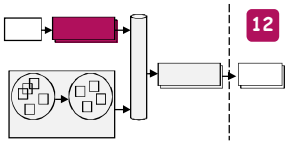



» The Application Model is a static and dynamic representation of a software architecture

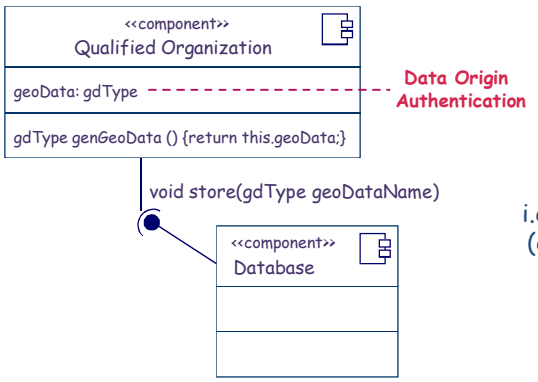





## Security-Annotated App.Model(s)

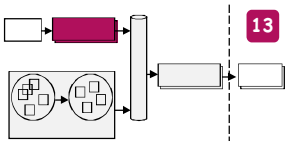



» A Security-Annotated model is obtained by introducing security annotations



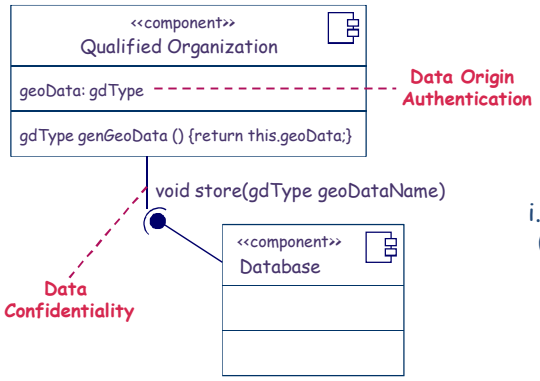

**System Configuration $SC_1$,**
i.e. the required security settings
(e.g. Data Origin Authentication)

## Security-Annotated App.Model(s)



13

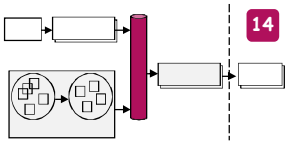
» A Security-Annotated model is obtained by introducing security annotations




**System Configuration $SC_2$**, i.e. the required security settings (e.g. Data Origin Authentication and Data Confidentiality)



## Enabling Security



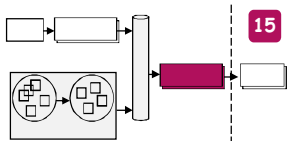
14

» Operational steps:

1. Interpretation of security annotations
   - **Key-aspect**: composability of models
   (i) Entry points unambiguously defined
   (ii) Security models easily composable

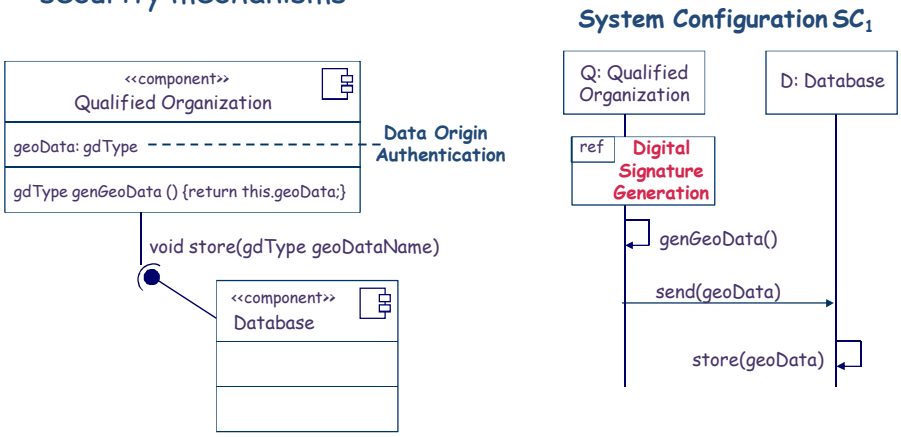
2. Evaluation of security mechanisms at the application level
   - **Key-aspect**: application-independent parameters are specified in the Security Library
   (i) Implementation options unambiguously defined
   (ii) Estimation of application-dependent Security Mechanisms

## Security-Enabled App. Model(s)



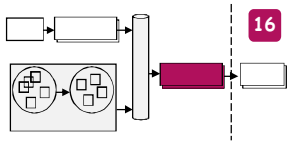
15

» A Security-Enabled model is obtained by embedding the appropriate security mechanisms



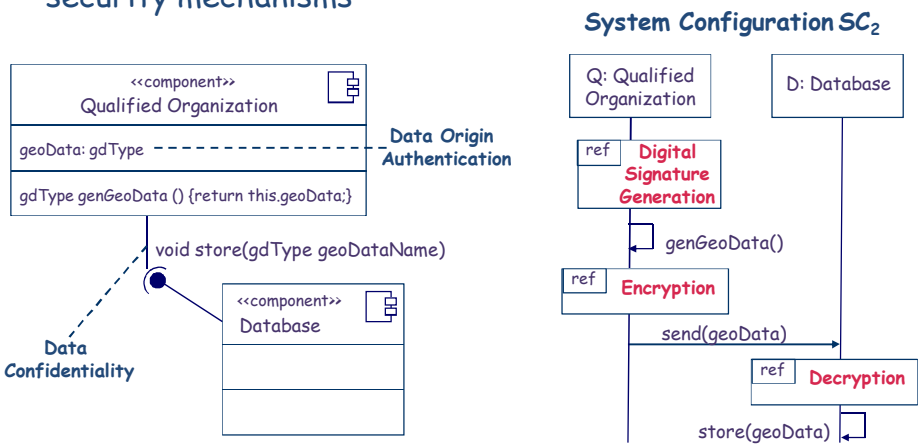



## Security-Enabled App. Model(s)

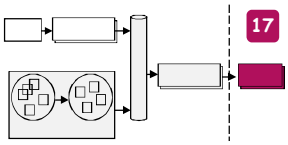


16

» A Security-Enabled model is obtained by embedding the appropriate security mechanisms

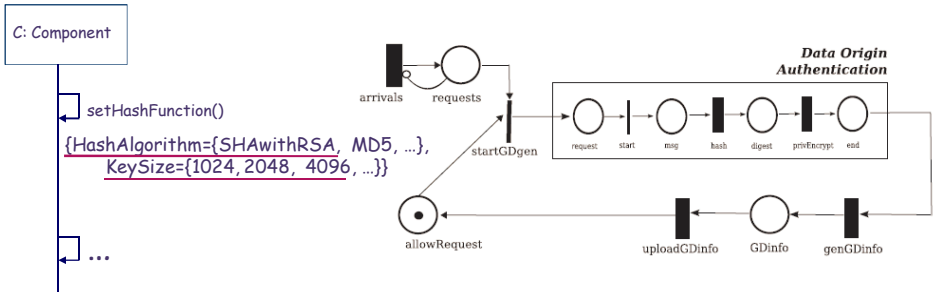


# Performance Model(s)



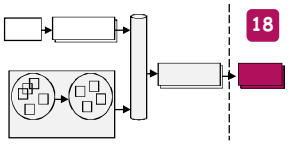

» A Performance model is obtained by transforming a software model into a performance model

**System Configuration $SC_1$**



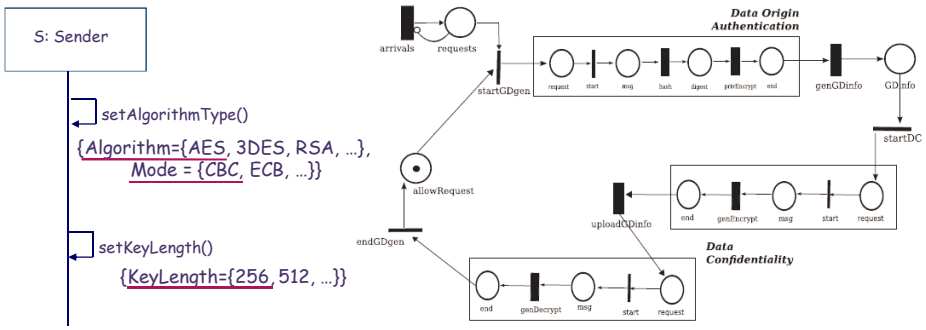



# Performance Model(s)




» A Performance model is obtained by transforming a software model into a performance model

**System Configuration $SC_2$**



## Validation of the case study

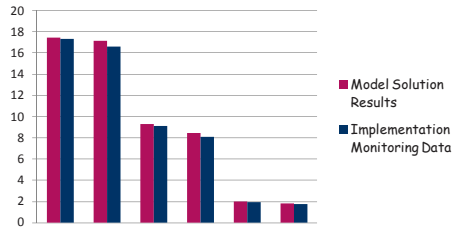
19

» Experimental results (1/2)

**System Configuration $SC_1$**

| | KeySize (byte) | Model Solution Results (tags/sec) | Implementation Monitoring Data (tags/sec) | Model Prediction Error (%) |
|---|---|---|---|---|
| Platform 1 | 1024 | 17.45 | 17.3 | *0.86* |
| | 2048 | 9.32 | 9.11 | *2.25* |
| | 4096 | 1.98 | 1.92 | *3.03* |
| Platform 2 | 1024 | 17.13 | 16.61 | *3.03* |
| | 2048 | 8.45 | 8.11 | *4.02* |
| | 4096 | 1.85 | 1.78 | *3.78* |

**Platform 1** - Intel(R) Core2, 2.0GHz with 2GB RAM, Windows Vista
**Platform 2** - Intel Pentium4, 3.4Ghz with 2GB RAM, Windows XP






## Validation of the case study

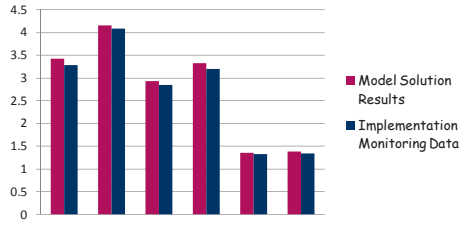
20

» Experimental results (2/2)

**System Configuration $SC_2$**

| | KeySize (byte) | Model Solution Results (tags/sec) | Implementation Monitoring Data (tags/sec) | Model Prediction Error (%) |
|---|---|---|---|---|
| Platform 1 | 1024 | 3.43 | 3.29 | *4.08* |
| | 2048 | 2.93 | 2.85 | *2.73* |
| | 4096 | 1.35 | 1.33 | *1.48* |
| Platform 2 | 1024 | 4.16 | 4.09 | *1.68* |
| | 2048 | 3.33 | 3.2 | *3.90* |
| | 4096 | 1.38 | 1.34 | *2.90* |

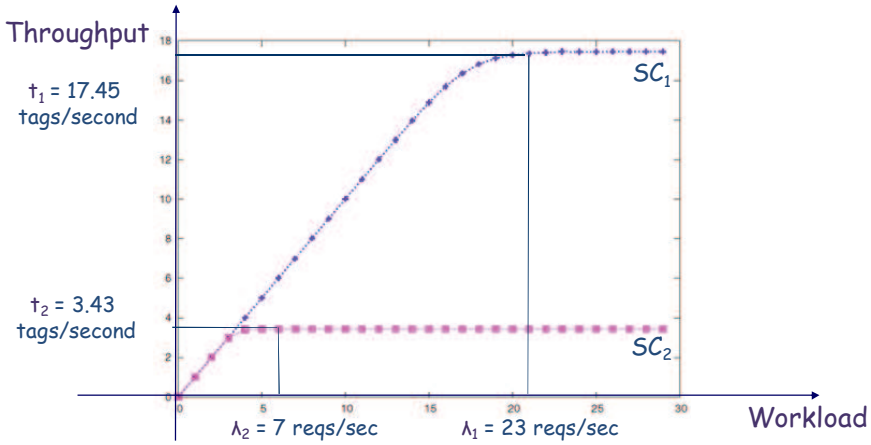
**Platform 1** - Intel(R) Core2, 2.0GHz with 2GB RAM, Windows Vista
**Platform 2** - Intel Pentium4, 3.4Ghz with 2GB RAM, Windows XP



## A broader analysis



» What happens while varying the system workload across the $SC_1$ and $SC_2$ configurations?






## Afterthougths



» Experimentation:

- Our models provide promising results (i.e. the worst model prediction error is 4.08%)
- The analysis of the workload provides interesting insights

» Limitations:

- Security Mechanisms: encryption and digital signature
- Enabling security implies the usage of the mechanisms at the application level, thus they can be influenced by application-dependent characteristics

## Conclusions



» Contributions:

- A framework to support the analysis of software architecture (i.e., performance degradation while varying security solutions)
- Introduction of models for basic security mechanisms

» Future works:

- Introduction of costs for security solutions
- Trade-off analysis between security and other non-functional attributes, e.g. availability





# Thank you!