SECURITY MODELING IN AUTOMOTIVE INDUSTRY

SHAHANAS CHOLAYIL MAYANKUTTY

AGENDA

Motivation

Workflow

Results

Lessons Learnt

MOTIVATION

- Academic Motivation

  Build confidence in security modeling notations by validating them with industrial case studies

- Industrial Motivation

  Visualizing security properties in system models at design level

  - Documentation of security design decisions
  - Analyisis of secuirty properties early on
  - Support for Model Driven/Model Based security engineering

WORKFLOW

STEP 1: Literature review to understand state-of-art in academics

STEP 2: Stakeholder interviews to extract selection criteria for filtering of modeling notations

STEP 3: Decide scenarios for implementation of selected modeling notations

STEP 4: Discussion and selection of evaluation criteria for comparison of notations

STEP 5: Comparison of models produced and documentation of results

STEP 2: SELECTION OF NOTATIONS

- From a total of 30 notations, 11 addressed more than one security concern and 6 had tool support

  UMLsec, SysML-Sec, SecureSOA, Hoisl-SOA (notion to shift to SOA) and Secure Tropos.

- Filtered 5 candidates through a decision matrix to conclude with two notations for comparison – UMLSec and SysML-sec

  Research question: “What criteria do companies consider important when assessing/adopting a security modeling notation? ”

STEP 3: SCENARIOS FOR MODELING

Select scenarios that have good coverage of security properties-

Confidentiality, Integrity, Authentication, Authorization, Auditabiltiy, Freshness and Privacy

Case 1: OTA – Over The Air Software Download

Case 2: RVDC – Remote Vehicle Data Collection

STEP 4: EVALUATION CRITERIA

Ease of Use

- Documentation to support learnability
- Range of Diagrams that can be annotated using the notation
- Dependencies or constraints that guide the use of symbols in the notations

Expressive Capability

- Extend to which the notation can express security concerns and other secuirty related information
- Does the notation convey its intended meaning without confusing the user
- How obvious is the role of a symbol in the notation

STEP 5: COMPARISON

Ease of Use

- Documentation to support learnability

  UMLsec has a book and several papers describing the notation

  SysML-sec has only papers (Not enough to get full understanding)

- Range of Diagrams that can be annotated using the notation

  The entire profile of UML can be used for UMLsec

  Only block diagrams can be annotated in SysML-sec

STEP 5: COMPARISON

- Dependencies or constraints that guide the use of symbols in the notation

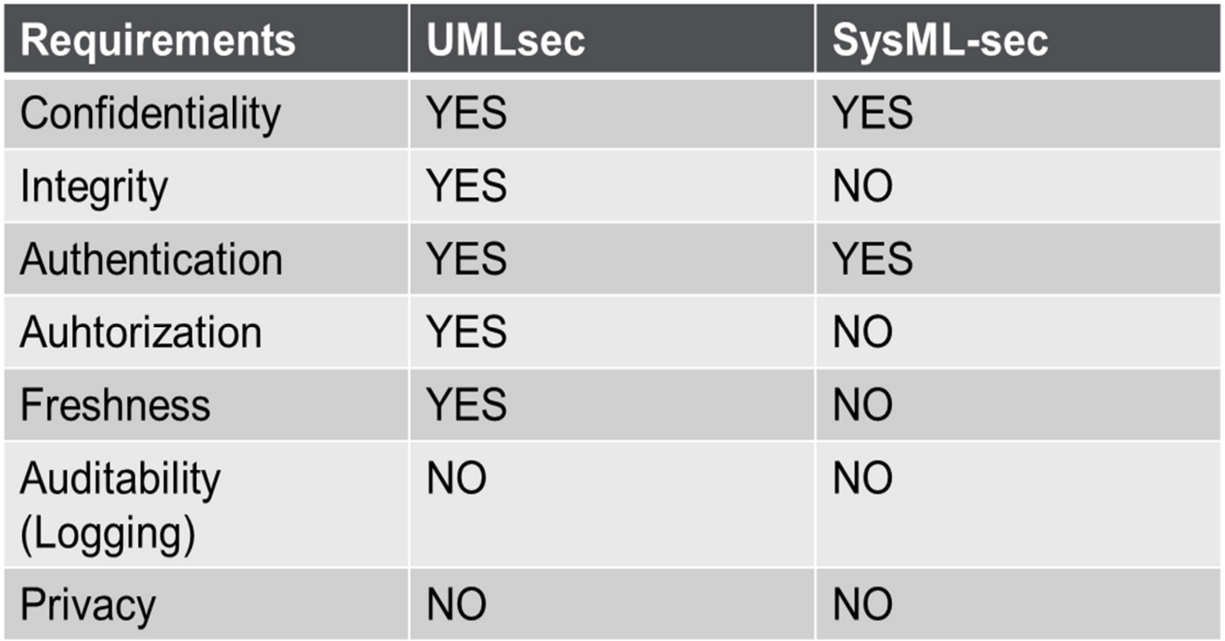
  UMLsec profile consists of stereotypes and tag that are connected to each other

  In SysML-sec each *pragma* should have a corresponding state diagram.

STEP 5: COMPARISON

Expressive Capability

- Coverage of Security Concerns



Requirements	UMLsec	SysML-sec
Confidentiality	YES	YES
Integrity	YES	NO
Authentication	YES	YES
Auhtorization	YES	NO
Freshness	YES	NO
Auditability (Logging)	NO	NO
Privacy	NO	NO

STEP 5: COMPARISON

Investigate whether operational properties can be represented:

- SysML-sec has predefined functions within the cryptoblock to show encryption to achieve confidentiality
- Well defined stereotypes depicting authorization through Role Based Access Control (RBAC) for UMLsec
- None of the other properties (Integrity, Authentication, Freshness, Auditability, Privacy) are addressed to an operational level

Additional Capabilities

- Security of physical infrastructure
- Security of Data
- Labelling of Assets
- Capabilties of Adversaries

STEP 5: COMPARISON

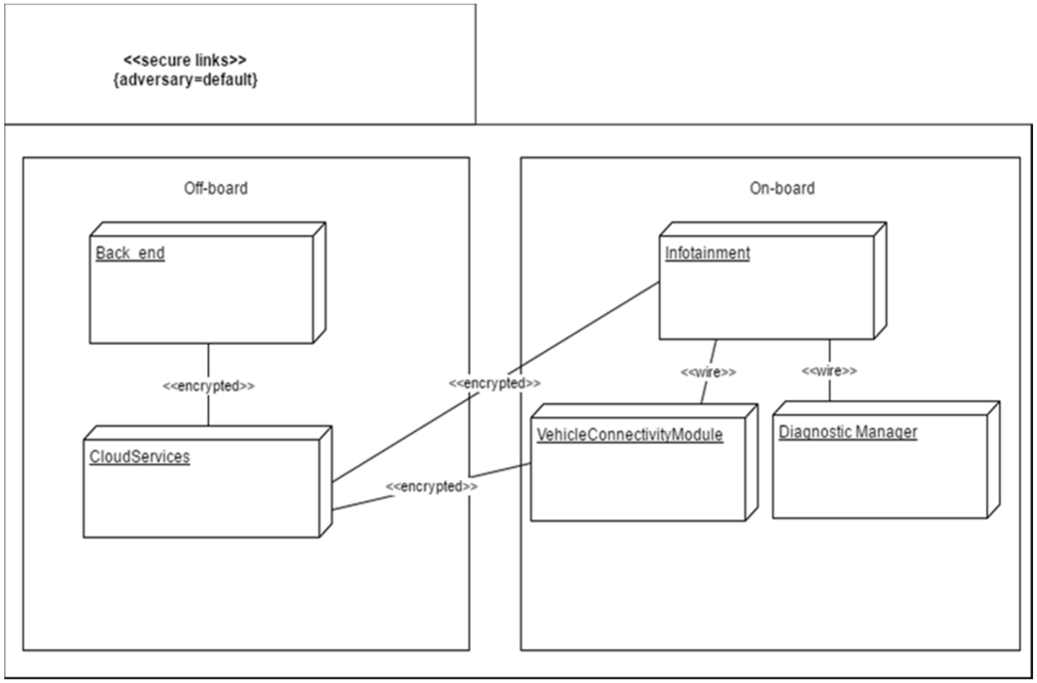
Does it convey the intended information without confusing the user

- UMLsec was more easily understood

How obvious is the role of a symbol used in the notation

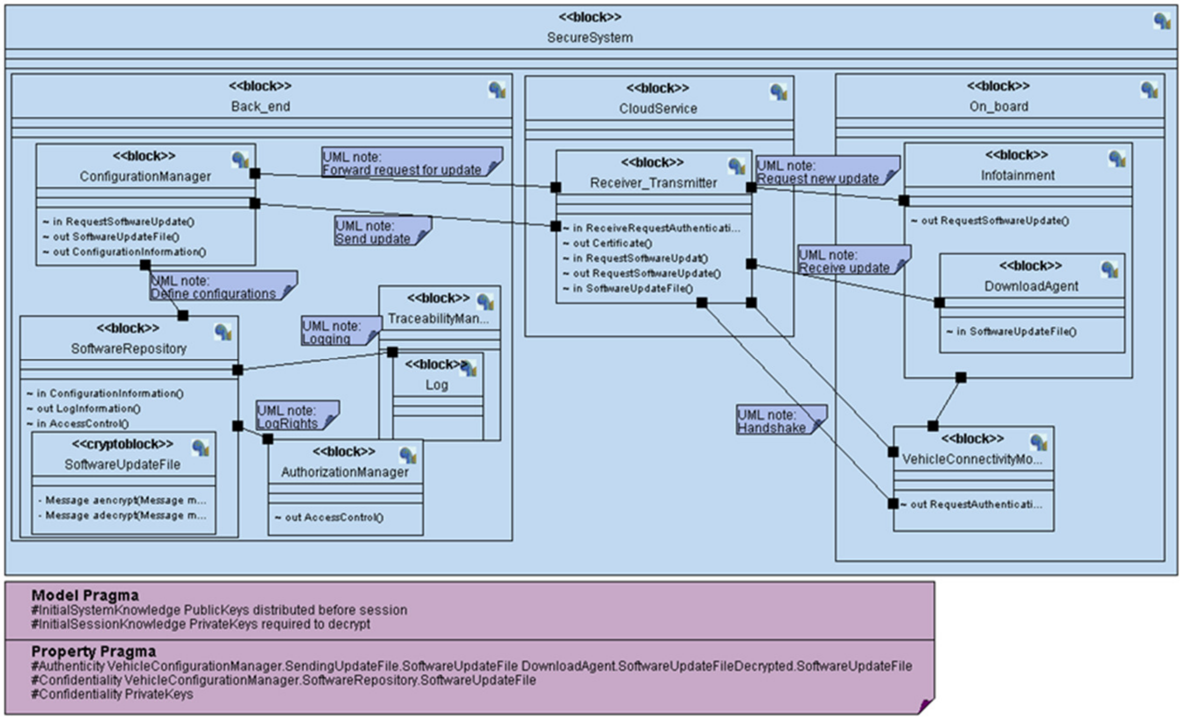
- UMLsec stereotypes annotating a package were often ignored
- Private type of communication in SysMLsec was ignored

EXAMPLE:



<<secure links>>
{adversary=default}
Off-board
Back_end
<<encrypted>>
CloudServices
<<encrypted>>
<<encrypted>>
On-board
Infotainment
<<wire>>
<<wire>>
VehicleConnectivityModule
Diagnostic Manager

EXAMPLE:



Model Pragma
#InitialSystemKnowledge PublicKeys distributed before session
#InitialSessionKnowledge PrivateKeys required to decrypt

Property Pragma
#Authenticity VehicleConfigurationManager.SendingUpdateFile.SoftwareUpdateFile DownloadAgent.SoftwareUpdateFileDecrypted.SoftwareUpdateFile
#Confidentiality VehicleConfigurationManager.SoftwareRepository.SoftwareUpdateFile
#Confidentiality PrivateKeys

RESULTS

What criteria do companies consider important when assessing/adopting a security modeling notation?

- Out of 14 criterias extracted at Step 2, 9 were Volvo specific.
- Availability of tool support
- Number of security concerns covered
- Current modeling knowledge within the company
- Detailed documentation
- Support for annotating wide range of diagrams

Evaluated two notations (UMLsec and SysML-sec) in terms of:

- Ease of Use
- Expressive Capability
- UMLSec was better

LESSONS LEARNT

- Most notations immature for industrial application
  - Lacking with respect to tool support, documentation, coverage of security concerns.
- UMLsec is closer to becoming the notation that provides complete solutions to security modeling concerns.
- SysML-sec has a long way to reach the maturity offered by UMLsec
- Researchers should focus on improving not only the notations but also documentation and tool support.

THANK YOU…

Questions???

shahanas.cholayil.mayankutty@volvocars.com