Semantic Description and Semantic Modeling
IoTSec Kick-off meeting Halden

Olaf Owe

Department of Informatics, University of Oslo

Oct. 5, 2015

WP1 Semantic system, application, and attack description

Understanding of

- background. What has been done before?
- focus. What are we interested in?
- applications. What kind of applications we are aiming at?
- attacks. What kind of attacks do we want to handle?
- challenges. What problems do we want to solve?
- industry. What problems are important to industry?

T1.1 Semantic description of infrastructure, attack detection, system view

We should consider

- abstraction. We need a general semantic model. We need to find suitable abstractions, not to low-level and not too high-level.
- analysis. How can be analyze the model to check properties.
- attacks. General modeling of attacks.
- detection. How to use our model in order to detect weaknesses wrt. attacks. How smart are the attackers?
- tools. Tools for doing the above tasks.
- understanding of components and communication

T1.2 Measurable: security, privacy and dependability, metrics

Objective: This task will establish the Multi-Metrics Model for the Smart Grid use cases. The task includes:

- adaptation to real world infrastructure
- analysis of most relevant sub-systems
- application-specific goals for security, privacy and dependability
- What metrics are suitable
- What security and privacy issues should be considered.
- How to evaluate these?
- Feedback from industry partners

Expected results T1.1

From our proposal:
- a non-trivial case study (M12),
- a minimum of 3 papers, including one journal paper (M12-36),
- the completion of a PhD candidate within the project period (M48).

The *Case Study* is the most urgent starting point:

- involving several partners
- should be relevant to our industry partners
- what is realistic in 12 month?
- should serve as a basis for further work and research
- should serve as a basis for papers

The case study should serve as unifying activity between the partners.
The problem question should come from industry.

Expected results T1.2

From our proposal:
- System analysis for main sub-systems on current infrastructure (M12),
- Identification of 3-5 use cases, to be further elaborated in T3.1 (M12),
- Feedback from industry on applicability of system analysis (M12),
- Extension of the Smart Grid system to 2+ new functionalities (M24),
- Identification of challenges for industrial applicability (M24).

3 first points most urgent. Should connect to the *Case Study* of T1.1.
Need to find

- main security issues in the case study
- main privacy issues in the case study
- main dependability issues in the case study
- suitable metrics to use in case study

All issues should be of interest to industry.

A possible modeling framework

The next foils present a possible framework for modeling for modeling and with state-of-the-art tools for advanced analysis.
Note:

- executable modeling , useful for experimentation and simulation.
- analysis of properties, useful for detection of attacks, for finding weaknesses of a model.
- probabilistic modeling possible.

The modeling framework of Rewriting Logic

High-level general language and tool
- for modeling, prototyping and analysis
- for formalizing new (or old) paradigms in computer science
- developed at SRI (Menlo Park), UIUC (Illinois), USA
- Real-Time extension by Peter Ölveczky (PMA)

Supporting

- concurrency/parallelism, distribution,
- message passing, OO, actors,
- deterministic/non-deterministic behavior
- open/dynamic and mobile systems, software upgrades
- security issues
- cyber physical systems

Executable modeling/programming through the language *Maude*

Main Elements of Maude

- pattern matching, rule based
- functional programming by equations (=)
- state changes by rules (=>)
- async. as well as sync. communication
- extension to real time
- extension to probabilistic behavior
- model checking and model exploration

Small Example: Broadcasting Protocol

```
subsort String ⟨Oid Msg .
msg broadcast : Msg Oid → Msg .

class Node|neighbors : OidSet, msgRead : Configuration .

vars O O' : Oid . var OS : OidSet . var M : Msg .

rl [startBroadcast] :
broadcast(M, O)
⟨O : Node|neighbors : OS, msgRead : none⟩ ⟶
⟨O : Node|msgRead : M⟩
multimsg M from O to OS .

rl [readAndForward] :
(msg M from O to O')
⟨O' : Node|neighbors : O ; OS, msgRead : none⟩ ⟶
⟨O' : Node|msgRead : M⟩
multimsg M from O' to OS .

rl [readSeenMsg] :
(msg M from O to O')
⟨O' : Node|neighbors : OS, msgRead : M⟩ ⟶
⟨O' : Node|⟩ .

...
```

Broadcasting Protocol (2)

```
op msg_from_to_ : Msg Oid Oid → Msg [ctor] .
op multimsg_from_to_ : Msg Oid OidSet → Msg [ctor] .
var M : Msg . vars SENDER ARECEIVER : Oid .
var OTHER-RECEIVERS : OidSet .

eq multimsg M from SENDER to none = none .
eq multimsg M from SENDER to ARECEIVER ; OTHER-RECEIVERS =
  (msg M from SENDER to ARECEIVER)
  (multimsg M from SENDER to OTHER-RECEIVERS) .

op initState : → Configuration .
eq initState =
broadcast("eksempel-melding", "b")
⟨"a" : Node|neighbors : "b" ; "e", msgRead : none⟩
⟨"b" : Node|neighbors : "a" ; "d", msgRead : none⟩
⟨"c" : Node|neighbors : "d", msgRead : none⟩
⟨"d" : Node|neighbors : "b" ; "c" ; "e", msgRead : none⟩
⟨"e" : Node|neighbors : "a" ; "d", msgRead : none⟩ .

(rew initState .)
(search initState ⟶! C: Configuration .)
```

Example

Slightly more complex protocol from US used in industry.
Found errors with Maude analysis (search)
because in Maude one may explore *all* possible executions and search for certain patterns, possibly specifying certain properties.

Similar experiences with

- Internet Explorer (US)
- Car software (Cruise control systems) (Japan)
- wireless sensor systems (US/Europe),
- security protocols (US/Europe)

Conclusion

Maude seems promising as a framework for IoTSec descriptions

- semantic modeling
- new paradigms easily defined
- model checking
- intrusion detection
- quick model design, prototyping and analysis
- probabilistic modeling and analysis