NR Norsk Regnesentral
NORWEGIAN COMPUTING CENTER

Adaptive Security Model for IoTSec

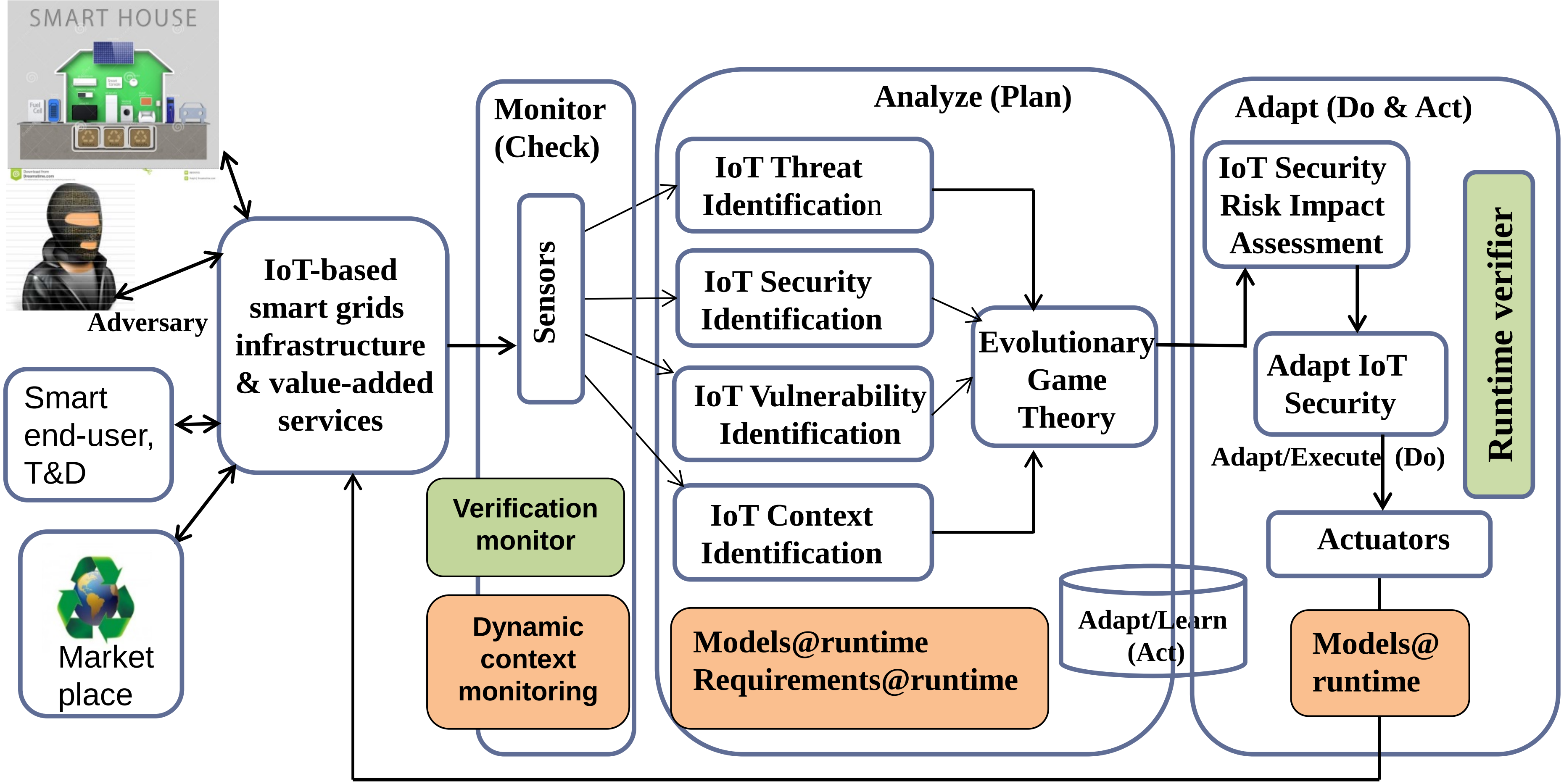
IoTSec Project 248113/O70 General Meeting

Habtamu Abie, Norwegian Computing Center

Oslo/NR

02-12-2015

Anticipatory adaptive security + semantic provability


SMART HOUSE
Adversary
Smart end-user, T&D
Market place
IoT-based smart grids infrastructure & value-added services
Monitor (Check)
Sensors
Verification monitor
Dynamic context monitoring
Analyze (Plan)
IoT Threat Identification
IoT Security Identification
IoT Vulnerability Identification
IoT Context Identification
Evolutionary Game Theory
Models@runtime Requirements@runtime
Adapt/Learn (Act)
Adapt (Do & Act)
IoT Security Risk Impact Assessment
Adapt IoT Security
Adapt/Execute (Do)
Actuators
Models@ runtime
Runtime verifier

Later this will be integrated with machine learning for Integrated analysis and decision making, and optimized adaptation

Feedback control loops: Monitor-Analyze-Adapt (PDCA)

- Monitor (Check)
  - Application requirements
  - Environment sensors
  - Network environment
  - User context
- Analyze (Plan)
  - Inference
  - Uncertain reasoning
  - Economic models
  - Rules and policies
  - Game theory
  - Risk analysis
- Adapt (Do & Act)
  - Risk analysis
  - Decision theory
  - Hypothesis generation
  - Managed things
  - Record strategies
  - Inform users or sys admin

Monitor

- Collects relevant data that reflect the current state of the system
  - environmental sensors
  - other sources
- Questions
  - What is the required sample rate
  - How reliable is the sensor data
  - Is there a common event format across sensors
  - What is granularity of self-monitoring

Analyze

- Analyzes the collected data
- Questions
  - How is the current state of the system inferred?
  - How much past state may be needed in the future?
  - What data need to be archived for validation and verification?
  - How faithful is the model to the real world?
  - Can an adequate model be derived from the available sensor data?

Adapt

- Makes decisions about how to adapt in order to reach a desirable state and implements the decisions via available actuators and effectors
  - **Decide**: Risk analysis, Decision theory, Hypothesis generation
  - **Act**: Managed things, Record strategies, Inform users or sys admin
- Questions
  - How is the future state of the system inferred?
  - How is a decision reached (e.g., with off-line simulation or utility/goal functions)?
  - What are the priorities for adaptation across multiple control loops and within a single control loop?

Adapt …

- More questions?
  - When should the adaptation be safely performed?
  - How do adjustments of different control loops interfere with each other?
  - Does centralized or decentralized controls help achieve the global goal?
  - Does the control system have sufficient command authority over the process — i.e., can the action be implemented using the available actuators and effectors?
- Caveat: Adaptors
  - Cannot blindly apply adaptations since it might have a negative impact on functionality or even worse it could create new faults altogether

Adaptive
Human-Computer Interaction

- Analyzing feedback types from
  - human-computer interaction, collected information and how this is used in the adaptation
- Devising novel mechanisms for
  - exposing the control loops to the users, keeping the users of self-adapting systems “in the loop” to ensure their trust
- Visual feedback of the adaptation
- Give the users the option to
  - disable the self-adaptive features and
  - the system should not contradict this

To measure human behavior in a security context

- Taken verbatim from " Socio-Technical Security Metrics" seminar: http://drops.dagstuhl.de/opus/volltexte/2015/4974/pdf/dagrep_v004_i012_p001_s14491.pdf
  - what behaviors we can expect to see;
  - what triggers behaviors;
  - what the range of behaviors is;
  - what behaviors we want to encourage or discourage;
  - what the differences between individual and group behaviors are;
  - what triggers for sharing are;
  - what attitudes lead to what behaviors.

Getting reliable data [Socio-Technical Security Metrics Seminar]

- They formulated the following problems and recommendations:
  - Use metrics that are as explicit as possible;
  - People collecting data need hands-on experience of risk analysis – this is currently often confused with requirements analysis;
  - Predict risk level after changes have been implemented;
  - Combine risk analysis with other techniques to check risk model;
  - Use two risk models – before and after;
  - Combine with other measures, e.g. vulnerability scans, to check predictions – program and functional testing.

Methodologies and methods

- Risk analysis (basis for security decision)
- Evolutionary theory (conflicting incentives)
- Control theory (attack strategies seeds)
- Distributed behavioral analysis (computational capabilities)
- Adaptive Systems and Interaction (Contextual intelligence) http://research.microsoft.com/en-us/groups/adapt/
- Machine learning (optimization), reinforcement learning and/or Inverse reinforcement learning (learning the reward function)
- Prosa (security protocol specification)

Evolutionary game theory

- bridges concepts from
  - biology
  - evolution
  - non-linear dynamics, and
  - game theory
- populations of players
  - different strategies
  - a process similar to natural selection is used to determine how the population evolves
- allows us to deal with evolutionary threats

Control theory

- The control loop
  - a central element of control theory
- control theory provides
  - well established mathematical models, tools, and techniques to analyze system performance, stability, sensitivity, or correctness
  - Instruction how to compute plans (sequences of actions) that are optimal with respect to maximizing an objective
- interactions of control loops
  - explicit and expose how these interactions are handled

The Prosa Process

Scope

Review documentation
Perform interviews
Identify critical sections

Deliveries:
System overview
Critical sections
Scope recommendation

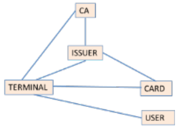
Critical sections identified

Modeling

Detailed documentation review:
- System modeling
- Review with key personnel to Identify:
  1. Model updates
  2. Documentation errors
  3. Design errors

Deliveries:
Precise PROSA model providing:
- System overview
- Detailed system behavior
- Complete, uniform documentation
- Implementation errors identified

Detailed design documented in precise PROSA model

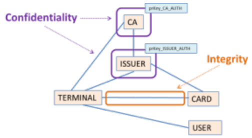


Security require-ments

Identify and validate information assets (critical information elements)
Model requirements

Deliveries:
Model with complete requirements including :
- Confidentiality goals
- Integrity goals

Complete, precise security requirements documentation

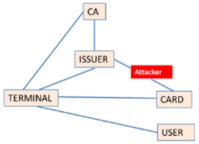


Threats

Perform eavesdropper simulation
Attack landscaping
Impersonation patterns

Deliveries:
Documentation of possible threats (potential attacks) with description of attack behavior

Issue descriptions for Library of attacks

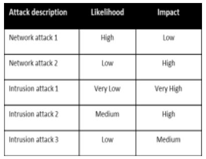


Risk Analysis

Threats overview
Decision making priorities

Deliveries:
Risk documentation for each potential threat

Risk documentation for threats

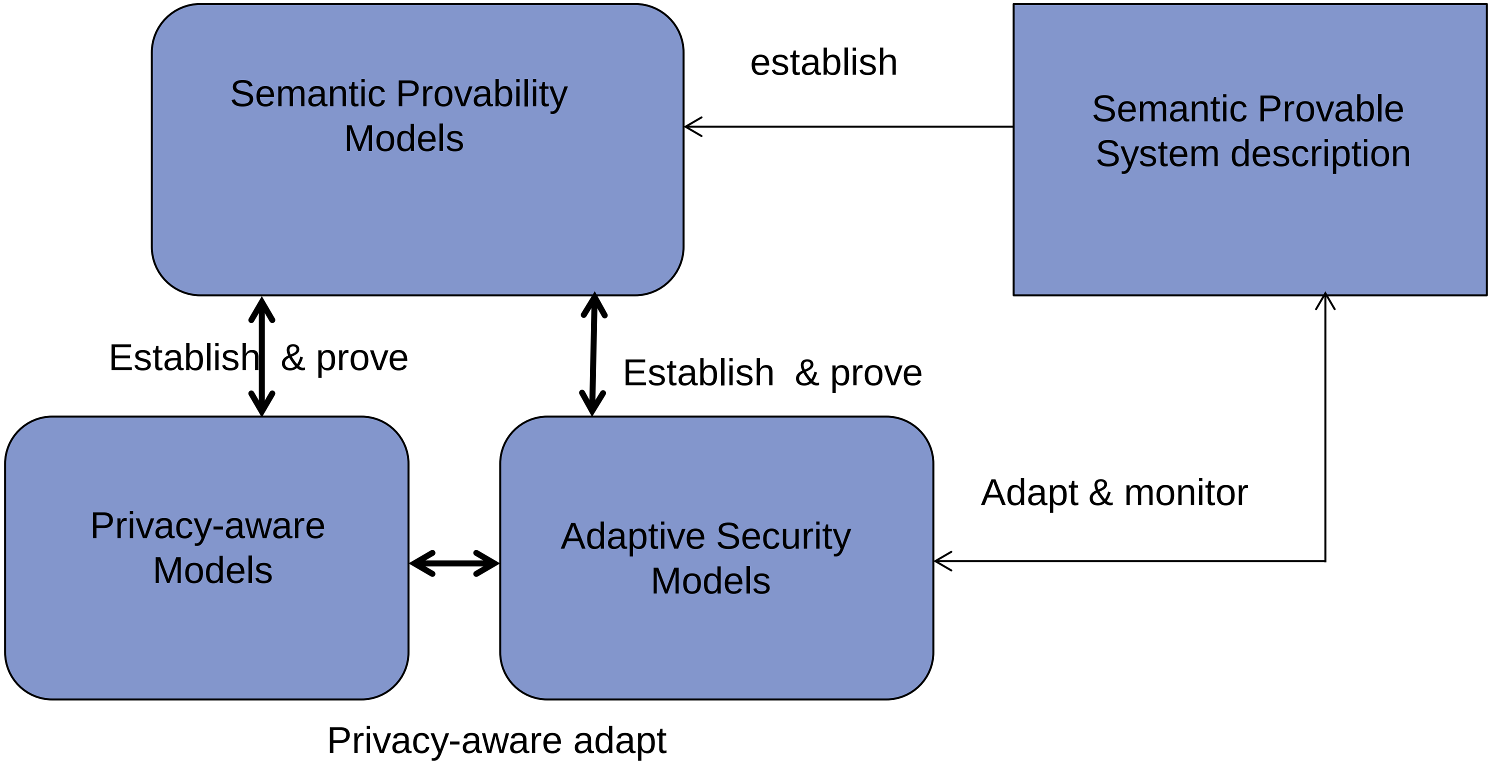


Attack description	Likelihood	Impact
Network attack 1	High	Low
Network attack 2	Low	High
Intrusion attack 1	Very Low	Very High
Intrusion attack 2	Medium	High
Intrusion attack 3	Low	Medium

Discussions

- How should integrate with other activities
- Should we make our feedback control loops and their features explicit
- What activities and methods should we use in each loops
- Can you help us answer questions we have raised and for how many of them you can answer

WP2 – Inter-tasks research integration


Semantic Provability Models
establish
Semantic Provable System description
Establish & prove
Establish & prove
Privacy-aware Models
Adaptive Security Models
Adapt & monitor
Privacy-aware adapt