Modelling Security of Critical Infrastructures: A Survivability Assessment

Ricardo J. Rodríguez†, José Merseguer†, Simona Bernardi§
{rjrodriguez, jmerse, simonab}@unizar.es

© All wrongs reversed

†Dpto. de Informática e Ingeniería de Sistemas
Universidad de Zaragoza, Zaragoza, Spain

§Centro Universitario de la Defensa
Academia General Militar, Zaragoza, Spain

15 de Junio, 2016
II Jornadas Nacionales de Investigación en Ciberseguridad
Granada, España
Accepted in The Computer Journal. doi: 10.1093/comjnl/BXU096
Introduction (I)

Critical Infrastructures

- Provide **essential services to the society**
  - Power distribution, water treatment, telco, financial services...
- Discontinuity of service may lead to fatalities or injuries
  - Different nature, from unintended acts of nature to intentional attacks (e.g., sabotage, terrorism)
Recent examples

2003 Northeast (U.S.) blackout
- Attributed to downed power line
- 11 deaths and an estimated $6B in economic damages, plus disrupted power over a wide area for two days

2013 Bowman Avenue Dam in NY was compromised, and control of the floodgates was gained
- Attributed to Iranian hackers

2015 Prykarpattyaoblenergo Control Center (PCC) in the Ivano-Frankivsk region of Western Ukraine
- Leaving 230K residents without power for up to 6 hours
- Presumed Russian cyberattacker

Not only safe, but also secure
The game just begun...

- Cyberattacks against SCADA systems doubled in 2014: more than 160K (Dell’s 2015 Annual Security Report)
- Malware targeting SCADA systems identified:
  - Examples: Stuxnet, Havex, and BlackEnergy3
Survivability

- **Capability of a system to fulfill its mission, in a timely manner, in the presence of attacks, failures, or accidents**
- **Usually qualitative in nature; and not precise or detailed enough to facilitate measurable survivability requirements and evaluations**
- **Survivability strategies phases:**
  1. Resistance
  2. Recognition
  3. Recovery
**Survivability**

- **Capability of a system to fulfill its mission, in a timely manner, in the presence of attacks, failures, or accidents**
- Usually qualitative in nature; and not precise or detailed enough to facilitate measurable survivability requirements and evaluations
- Survivability strategies phases:
  1. Resistance
  2. Recognition
  3. Recovery

**Our proposal**

- SecAM (Security Analysis and Modelling) UML profile
  - Enables survivability analysis for critical infrastructures to provide capabilities for assessing defence plans
Advantages

- Specification, in a quantitatively and quantitatively manner, of security and survivability in early stages of development
- Specific models for infrastructures and attack patterns
- Survivability analysis through formal models (in particular, Generalized Stochastic Petri nets)
  - Model-checking techniques
  - Allows steady-state analysis
  - Efficient techniques, as linear algebra and linear programming-based techniques
Introduction (V)

Advantages

- Specification, in a quantitatively and quantitatively manner, of security and survivability in early stages of development
- Specific models for infrastructures and attack patterns
- Survivability analysis through formal models (in particular, Generalized Stochastic Petri nets)
  - Model-checking techniques
  - Allows steady-state analysis
  - Efficient techniques, as linear algebra and linear programming-based techniques

Disadvantages

- Model complexity increased
- Lack of CASE tools with automated translation
Background (I): UML profile

UML profile

- UML tailored for specific purposes: profiling
- Stereotypes and tagged values
  - Extend model semantics
  - Allow to express non-functional properties (e.g., performance, reliability, security) within the model

OMG example

Modelling and Analysis of RT Embedded systems (MARTE)

Provides support for performance and schedulability analysis

Well-defined language to express NFPs (VSL, Value Specification Language)

R. J. Rodríguez, J. Merseguer, S. Bernardi

Modelling Security of CIs: A Survivability Assessment

JNIC 2016
### Background (I): UML profile

#### UML profile
- **UML tailored for specific purposes:** profiling
- **Stereotypes and tagged values**
  - Extend model semantics
  - Allow to express non-functional properties (e.g., performance, reliability, security) within the model

#### OMG example
- *Modelling and Analysis of RT Embedded systems* (MARTE)
  - Provides support for performance and schedulability analysis
  - Well-defined language to express NFPs (*VSL, Value Specification Language*)
UML profiling sounds cool, but…

- Express quantitative properties for analysis
- Transformation to formal models (in particular, Generalized Stochastic Petri nets)
- Good (and mature) analysis framework
Background (II): GSPNs

UML profiling sounds cool, but...

- Express quantitative properties for analysis
  - Transformation to formal models (in particular, Generalized Stochastic Petri nets)
  - Good (and mature) analysis framework

GSPN – explanation simplified

- Underlying Markov-chain
- Places (circles, $p_X$)
- Transitions (white/black bars, $t_X$)
- Time interpretation
  - Immediate transitions ($t = 0$)
  - Timed (allows different probabilistic distributions)
- Tokens (black dots)
SecAM Profile (I): a General Overview (1)

- SecAM relies on two profiles:
  - **MARTE**: analysis capabilities (among other features)
  - Dependability Analysis and Modeling (DAM): concepts shared by the dependability and security fields

- Set of stereotypes; and basic and complex types
SecAM Profile (I): a General Overview

Security

Integrity: √ √ √
Availability: √ √
Confidentiality: √ √ √
Authorisation: √
Non-repudiation: √
Authenticity: √


SecAM Profile (I): a General Overview (2)
## SecAM Profile (II): Cryptography package (1)

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SecAM::Cryptography</strong></td>
<td>Cryptography package definition</td>
</tr>
<tr>
<td><strong>Import</strong></td>
<td>SecAM::SecAM_Library</td>
</tr>
<tr>
<td><strong>Constant</strong></td>
<td>Software, Hardware, Biometric</td>
</tr>
<tr>
<td><strong>Enumeration</strong></td>
<td>KeyType, KeyKind, PaddingScheme, OperationMode, StreamType, Perioricity</td>
</tr>
<tr>
<td><strong>Tuple</strong></td>
<td>SecaStepKind, SecaKey, SecaMessageDigest, SecaMAC</td>
</tr>
<tr>
<td><strong>Stereotype</strong></td>
<td>SecaStep, DAM::DaStep</td>
</tr>
</tbody>
</table>

**Class Diagram**

- **SecAM::Cryptography**
- **SecAM::SecAM_Library**
- **SecaStep**
- **SecaKey**
- **SecaMessageDigest**
- **SecaMAC**
- **SecaBlock**
- **SecaStream**

**Attributes**

- Error Rate: NFP_Real
- Operational Rate: NFP_Real
- Key Kind: CipherKind
- Concrete Algorithm: NFP_String
- Size: NFP_Integer
- Padding: PaddingScheme[0..1]
- Operation Mode: OperationMode
- Key: SecaKey
- Length: NFP_DataSize
- Padding: PaddingScheme[0..1]
- Operation Mode: OperationMode
- Blocks: SecaBlock [1..*]

**Operations**

- DAM::DaStep
- SecaStep

**Enums**

- KeyType: Assymmetric, Symmetric
- KeyKind: Zero, Bit, Byte
- PaddingScheme: ECB, CBC, CFM, OFM, CTR
- OperationMode: Synchronous, Asynchronous
- StreamType: Periodic, NonPeriodic
- Perioricity: vulnerable, intrusion, cryptographic, messageDigest
- CipherKind: Stream, Block

---

R. J. Rodríguez, J. Merseguer, S. Bernardi

Modelling Security of CIs: A Survivability Assessment

JNIC 2016 11 / 27
SecAM Profile (V): AccessControl package

<table>
<thead>
<tr>
<th>Proposal (draft)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Subjects, operations and objects</strong></td>
</tr>
<tr>
<td>Operations: kind and granted/not granted (boolean)</td>
</tr>
<tr>
<td>- Read</td>
</tr>
<tr>
<td>- Write</td>
</tr>
<tr>
<td>- Access</td>
</tr>
<tr>
<td>- Execution?</td>
</tr>
<tr>
<td><strong>Subjects: self-association</strong></td>
</tr>
<tr>
<td>- Delegation of authorisation</td>
</tr>
<tr>
<td>- Separation of duties</td>
</tr>
<tr>
<td><strong>Idea: access control policies specified by OCL (UML constraints)</strong></td>
</tr>
</tbody>
</table>
Model-based Methodology

UML models

CI Flow model (UML Activity diag.)
CI Resource model (UML deployment diag.)
SecAM
Survivability pattern

Annotating security

CI Model

Model to model transformation

CI GSPN Model

Petri net models

GSPN composition

GSPN Model4Analysis

Analysis & Assessment

Qualitative analysis

Quantitative assessment (through sensitivity analysis)

R. J. Rodríguez, J. Merseguer, S. Bernardi
Modelling Security of CIs: A Survivability Assessment
JNIC 2016 15 / 27
Case Study (I)
Saudi Arabia crude-oil pipeline network (1)

Highlights

- World’s largest
  - exporter of petroleum liquids
  - crude oil producer (8-10 mmbbl/day)
- National distribution network
  - > 9,000 miles long
Case Study (1)

Saudi Arabia crude-oil pipeline network (2)

- **Terrorist target**
  - physical attacks (Abqaiq oil facility, 2006)
  - cyberattacks (Shamoon malware, 2012)

---

Case Study (I)
Saudi Arabia crude-oil pipeline network (2)

- **Terrorist target**
  - physical attacks (Abqaiq oil facility, 2006)
  - cyberattacks (Shamoon malware, 2012)

- A 50% reduction of Saudi Arabia crude-oil output would lead to a global recession if the infrastructure could not be repaired within few months\(^a\)

---
Case Study (I)
Saudi Arabia crude-oil pipeline network (2)

- Terrorist target
  - physical attacks (Abqaiq oil facility, 2006)
  - cyberattacks (Shamoon malware, 2012)

- A 50% reduction of Saudi Arabia crude-oil output would lead to a global recession if the infrastructure could not be repaired within few months\(^a\)

- Survivability strategies are a must to quickly recover -hours/days- the infrastructure

---

Case Study (II): Distribution network model

- **Abqaiq**
- **Ras Al-Juaymah**
- **Yanbu**
- **Ras Tanura**
- **Ras Al-Khafji**
- **Jubail**
- **Qadif**

Source plant

Crude-oil seaports

- **Pipe P1**
- **Pipe P3**

**MARTE**: devices & exec. hosts
**SecAM**: security mechs
Case Study (III): Crude-oil system flow model

SecAM annotations to specify
- crude-oil traversal time in pipe, junctions
- routing probabilities
Case Study (IV): Physical Attack (1)

Survivability scenario

SecAM annotations to specify:
- Attack type and concrete target nodes in the network
- Resistance & recognition probabilities
- Time to recovery & repair
Case Study (IV): Physical Attack (2)

Analysis with GSPN

(A1) Oil Distribution Network

Survivability scenario of a physical attack

Network throughput = X(end)

(A2) GSPN transitions

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Value(s)</th>
<th>GSPN transitions</th>
</tr>
</thead>
<tbody>
<tr>
<td>resistance</td>
<td>[0.05-0.95]</td>
<td>recP1OK, recP3OK, recQadifOK</td>
</tr>
<tr>
<td>recognition</td>
<td>1</td>
<td>recP1OK, recP3OK, recQadifOK</td>
</tr>
<tr>
<td>recovery</td>
<td>[72-3] hrs</td>
<td>recoveryP1, recoveryP3,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>recoveryQadif</td>
</tr>
<tr>
<td>MTTR</td>
<td>6 months</td>
<td>repairP1, repairP2, repairQadif</td>
</tr>
</tbody>
</table>
Case Study (IV): Physical Attack (3)

Analysis results

Throughput loss (%)

Mbbl/day loss

- rec < 6hrs → X < 20%, n < 240 Mbbl/day
Case Study (IV): Physical Attack (3)

Analysis results

Throughput loss (%)

- rec < 6hrs → X < 20%, n < 240 Mbbl/day
- res < 50%, rec ∈ [1 – 3]days → X ∈ [40 – 77]%, n ∈ [990K – 1.2M]
Case Study (IV): Physical Attack (3)

Analysis results

**Throughput loss (%)**

- rec < 6hrs → X < 20%, n < 240 Mbbl/day
- res < 50%, rec ∈ [1 – 3]days → X ∈ [40 – 77]%, n ∈ [990K – 1.2M]

**Mbbl/day loss**

- Hard resistance solutions required to maintain X < 50%
  - Example: surveillance combined with external perimeter security
Case Study (V): Cyber Attack (1)

Survivability scenario

- Coordinated attack to two computation nodes
  - DoS to Qadif node & run arbitrary code to P1 node
  - Resistance strategies: IPDS & cryptographic algorithm
Case Study (V): Cyber Attack (2)

Analysis with GSPN

(B1)

network throughput = X(end)

Oil Distribution Network Control System

Survivability scenario of a cyber attack

(B2)

Parameters

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Value(s)</th>
<th>GSPN transitions</th>
</tr>
</thead>
<tbody>
<tr>
<td>filterPb</td>
<td>[0.50;..;0.95]</td>
<td>resQadifOK</td>
</tr>
<tr>
<td>filter</td>
<td>[1.44min;..;14.4min]</td>
<td>filtering</td>
</tr>
<tr>
<td>decipher</td>
<td>2.88 min</td>
<td>deciphering</td>
</tr>
<tr>
<td>recovery</td>
<td>[11min-12hrs]</td>
<td>recoveryQadif</td>
</tr>
</tbody>
</table>

Overhead due filtering solution

- filter and filterPb are in direct proportion
Case Study (V): Cyber Attack (3)

Analysis results

- \( \text{rec} < 3 \text{hrs} \rightarrow \text{Ov} < 16\% \)
Case Study (V): Cyber Attack (3)

Analysis results

- \( \text{rec} < 3\text{hrs} \rightarrow Ov < 16\% \)
- \( \text{rec} \in [6 - 12]\text{hrs} \rightarrow \)

- Overhead (%)
  - Overhead (%)
  - Overhead (%)
  - Overhead (%)
  - Overhead (%)

- Filter (min)
  - Filter (min)
  - Filter (min)
  - Filter (min)
  - Filter (min)

- Recovery (min)
  - Recovery (min)
  - Recovery (min)
  - Recovery (min)
  - Recovery (min)
Analysis results

- \( \text{rec} < 3 \text{hrs} \rightarrow O\nu < 16\% \)
- \( \text{rec} \in [6 – 12] \text{hrs} \rightarrow \)
  - \( O\nu \sim 60\% \) for low quality filters

\[ \begin{array}{c|c|c}
\text{filter (min)} & \text{recovery (min)} & \text{overhead (\%)} \\
\hline
2.5 & 200 & 10 \\
2.0 & 200 & 20 \\
1.5 & 200 & 30 \\
1.0 & 200 & 40 \\
0.5 & 200 & 50 \\
\end{array} \]
Case Study (V): Cyber Attack (3)

Analysis results

- $\text{rec} < 3\text{hrs} \rightarrow Ov < 16\%$
- $\text{rec} \in [6 - 12]\text{hrs} \rightarrow$
  - $Ov \sim 60\%$ for low quality filters
  - $Ov \sim 30\%$ for high quality ones
Conclusions and Future Work

Conclusions

- SecAM enables to express security parameters and requirements
- Formal models to perform survivability analysis
- Evaluate survivability strategies under different scenarios
Conclusions and Future Work

Conclusions

- SecAM enables to express security parameters and requirements
- Formal models to perform survivability analysis
- Evaluate survivability strategies under different scenarios

Future Work

- Automated tool to complete transformation (and feedback!)
- Combine SecAM with other formal methods (e.g., Fault Trees or Bayesian Networks)
Modelling Security of Critical Infrastructures: A Survivability Assessment

Ricardo J. Rodríguez†, José Merseguer†, Simona Bernardi§
{rjrodriguez, jmerse, simonab}@unizar.es

© All wrongs reversed

†Dpto. de Informática e Ingeniería de Sistemas
Universidad de Zaragoza, Zaragoza, Spain

§Centro Universitario de la Defensa
Academia General Militar, Zaragoza, Spain

15 de Junio, 2016

II Jornadas Nacionales de Investigación en Ciberseguridad
Granada, España

Accepted in The Computer Journal. doi: 10.1093/comjnl/BXU096