ADAPTIVE SECURITY
A Requirements-Driven Approach

Mazeiar Salehie
EASSY, Japan
September 2013
Adaptive Security

Saturn model
Adaptive security: Our Focus

• Protecting valuable assets as the main goal of security
  • Changes in assets should be monitored

  • Security goals should be adequately satisfied all the time with considering other goals

• Proactive adaptive security
  • Asset variability, threat variation, risk fluctuation, changing context without harms to assets
Adaptive Security Framework

- Requirements at runtime
- Causal reasoning for
  - Analyzing
  - Planning (Decision making)
Trio: Asset Model
Trio: Threat Model
Security Fuzzy Causal Network (SFNet)

- Asset → Asset
- Asset → Threat
- Threat → Attack
- Attack → PR
- Asset → Partial Risk (PR)
- Risk → Utility
- SC → Goal
- SC → Vulnerability
- Goal → Utility
- Utility

Symbols:
- Asset
- Threat
- Attack
- PR
- Risk
- Goal
- SC
- Utility
SFNet for Mobile Security (partial model)
Building SFNet

- Transforming Trio to SFNet
  - e.g., Asset containment and association to positive causality
- SFNet structure validation
  - e.g., Holding properties for primary assets, security controls and partial risks
Aggregation Functions

<table>
<thead>
<tr>
<th>Causal Link</th>
<th>Aggregation</th>
</tr>
</thead>
<tbody>
<tr>
<td>{as} → as</td>
<td>TC0Norm</td>
</tr>
<tr>
<td>{as} → th</td>
<td>TC0Norm</td>
</tr>
<tr>
<td>{th} → at</td>
<td>TC0Norm</td>
</tr>
<tr>
<td>{v} → at</td>
<td>TC0Norm</td>
</tr>
<tr>
<td>{th}, {v} → at</td>
<td>TC0Norm</td>
</tr>
<tr>
<td>{as} → sgp</td>
<td>TC0Norm</td>
</tr>
<tr>
<td>{sg} → sgp</td>
<td>No aggregation (only one goal)</td>
</tr>
<tr>
<td>{as} {sg} → sgp</td>
<td>TC0Norm</td>
</tr>
<tr>
<td>{sc} → sg</td>
<td>TC0Norm</td>
</tr>
<tr>
<td>{sg} → sg</td>
<td>TC0Norm</td>
</tr>
<tr>
<td>{sc} → v</td>
<td>TC0Norm</td>
</tr>
<tr>
<td>{sc} → nsg</td>
<td>Average</td>
</tr>
<tr>
<td>{as} → pr</td>
<td>TC0Norm</td>
</tr>
<tr>
<td>at → pr</td>
<td>No aggregation (only one attack)</td>
</tr>
<tr>
<td>{as}, at → pr</td>
<td>TC0Norm</td>
</tr>
<tr>
<td>{pr} → R</td>
<td>TC0Norm</td>
</tr>
<tr>
<td>R, {sg}, {nsg} → U</td>
<td>Average</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Aggregation</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>TNorm</td>
<td>Minimum</td>
</tr>
<tr>
<td></td>
<td>Product</td>
</tr>
<tr>
<td></td>
<td>Lukasiewicz</td>
</tr>
<tr>
<td></td>
<td>Maximum</td>
</tr>
<tr>
<td>TCoNorm</td>
<td>BoundedSum</td>
</tr>
<tr>
<td></td>
<td>ProbabilisticSum</td>
</tr>
<tr>
<td>Average</td>
<td>Average</td>
</tr>
</tbody>
</table>
Building SFNet

Validity of the trio model
Decreasing the building effort

The trio model
- Translating the structure to SFNet
- Assigning causal influences
- Structure validation

Risk assessment report

Example security configurations

Security experts
Stakeholders

Weight & aggregation function assignment
Evaluation & sensitivity analysis

Generating SFNet
Tuning SFNet

Selecting aggregation functions
Tuning weights

SFNet model
Fuzzy Causal Reasoning

- Propagate changes in source nodes (e.g., assets) through causal links and aggregation functions

- Search for a security configuration
  - For each specific utility solve a satisfaction problem (Using Z3 SMT solver)
  - Perform a binary search between utility [0,1] with a precision
Mobile Phone Security: Asset variability

- Security variation for different asset values
- Priorities: Security=1, Performance=0.75, Usability=0.75

- Utility variation for different asset values
- Priorities: Security=1, Performance=0.75, Usability=0.75
Deployment Architecture

- SFNet
- Monitoring
- Organizational knowledge-base & contextual data
- Valuable Assets
- Executing
- Monitoring
- Sensors
- Effectors
- Valuable Assets

Organization
Adaptive Access Control

- Asset-based physical access control
- Cyber and physical assets may move in/out areas
- People may move in/out areas
- Authentication, authorization, logging and surveillance mechanisms as security controls
- Adaptive security can be realized as single or two different controllers
Exp: Asset variability in access control

- Utility variation for different asset values
- Priorities: Security=1, Performance=0.75, Usability=0.75

- Security variation for different asset values
- Priorities: Security=1, Performance=0.75, Usability=0.75
Adaptive Emergency Response Service

• Protecting valuable assets in an area after occurring an incident with possible security impacts
• Dynamically generating SFNet from a template model
Summary & Next Steps

• Focusing on assets to achieve the ultimate goal of security: “Protecting valuable assets”
• Linking assets, goals and threats in the trio model
  • Can be useful for other security analyses as well
• Turning the configuration search to solving several satisfaction problems

• Validating the trio model
• Automated weight & aggregation function tuning
• Generating SFNet from a template
• Alternative search algorithms