Quantification of Security and Survivability

ITI Workshop on Dependability and Security
Urbana, Illinois

Kishor Trivedi
Department of Electrical and Computer Engineering
Duke University
Durham, NC 27708-0291
Email: kst@ee.duke.edu
Home page: www.ee.duke.edu/~kst
Outline

- Quantification of security
- Quantification of survivability
Security Quantification

- Security Attributes
  - Integrity, confidentiality, availability
  - Authentication, non-repudiation

- Threats
  - Design, physical, interaction faults
  - Attacks

- Security Evaluation
  - Qualitative assessment
    - Certain checklists as security evaluation criteria, tiger team
  - Quantitative assessment
    - Based on probabilistic approach
Related work

- Littlewood et al. explored the feasibility of probabilistic quantification on security
- Ortalo et al. used privilege graph to model system operational security
- Jha et al. used attack graph to model attacker behavior
- Singh et al. designed SANs (stochastic activity networks) model for probabilistic validation of security and performance of several intrusion-tolerant architectures
- Chen et al. analyzed vulnerabilities using finite state machine model
- Jonsson et al. conducted experiments and presented a quantitative model of security intrusion based on attacker behavior
- Stevens et al. proposed probabilistic methods to model the DPASA (Designing Protection and Adaptation into a Survivable Architecture) architecture
Probabilistic Security Quantification

Our research publications


Our approach: design state transition diagram of system security states, and use Markov chains, Semi Markov Process, SRN and Attack Response Graph to develop high fidelity models incorporating both attacker and system behavior.
SITAR Overview

- SITAR is an intrusion tolerant architecture developed jointly by MCNC and Duke
- SITAR uses spatial redundancy, diversity and adaptive reconfiguration to achieve intrusion tolerance
- SITAR architecture
  - Proxy modules (PM)
  - Acceptance monitors (AM)
  - Ballot monitors (BM)
  - Audit control module (ACM)
  - Adaptive reconfiguration module (ARM)
  - COTS servers
Security Quantification of SITAR

Threat level 1

Mean time to severe security failure

Mean time to security failure vs. attack rate

Security vs. attack rate
Security Quantification Challenges

- Appropriate modeling of cyber attackers
  - Need to determine appropriate level of detail/abstraction
  - Need different attacker models for different purposes and attack classes

- Comprehensive modeling of system-level security quantification
  - Difficult to model certain security attributes such as confidentiality and integrity using probabilistic techniques
  - Hard to comprehensively quantify high-level security requirement with different security attributes using a single approach

- Measurement techniques for model parameterization and validation
  - Hard, careful work and significant time required for data collection
Survivability Quantification

Threats
- Natural disasters
- Man-made accidents
- Hardware/software faults
- Malicious attacks

Quantitative evaluation
- John Knight
  - A survivability specification is a four-tuple \(\{E, R, P, M\}\), \(E\): operating environment; \(R\): tolerable service; \(P\): pmf on \(R\); \(M\): finite-state machine of state transition (analogous to availability).

- Soung Liew
  - \(r\)-percentile survivability \(N_r\) is the probability that \(N\) is no greater than \(r\) % of the total resource (analogous to performability).

- T1A1.2 working group
  - Survivability depicts the time-varying system performance after a failure occurs
Our Survivability Research

Analysis approach

- Develop, parameterize, and solve Markov and non-Markov models including failure modes, traffic patterns, and resource contention.
- T1A1.2 based survivability measures do NOT depend on the disaster rate; this may be considered good as the disaster rate is hard to quantify in practice.

Our Publications

- Survivability analysis of telephone access network Proc. of 15th IEEE International Symposium on Software Engineering (ISSRE’04)
Availability and performance models

Pure performance model
To compute blocking prob. In each state of the availability model

Pure availability model
Survivability Model and Results

Survivability results – blocking probability

Make this the initial state

Normal operation in this state

Force a failure in the system

\[ P_{bk} = 0.0079366 \]

\[ P_{bk} = 0.0079366 \]

\[ P_{bk} = 1 \]

\[ P_{bk} = 1 \]

\[ P_{bk} = 1 \]

\[ \lambda_f \]

\[ \delta_d \]

\[ \delta_r (1-q) \]

\[ \delta_r (1-c)*q \]

\[ \mu R \]

\[ \delta_s \]

TR: relaxation time

Transient

Steady state

\[ T_R \]
**Excess Loss Due to Failure (ELF)**

ELF: a survivability measure reflecting the total loss before the system is recovered.

\[ P_{bk}(t) = \text{Dropped calls} \times \text{Area in the shadow} + \text{Excess blocked calls} = \text{ELF} \]
Comparison: six proposed architectures of Telephone access network

<table>
<thead>
<tr>
<th></th>
<th>Relaxation time*</th>
<th>Call loss due to failure</th>
<th>Extra call loss due to blocking</th>
<th>ELF</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active/standby</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IIC1</td>
<td>35310 s</td>
<td>9920</td>
<td>19729</td>
<td>29649</td>
</tr>
<tr>
<td>Active/standby</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IIC2</td>
<td>35370 s</td>
<td>9920</td>
<td>25323</td>
<td>35243</td>
</tr>
<tr>
<td>Active/active</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IIB</td>
<td>32940 s</td>
<td>4944</td>
<td>15804</td>
<td>20748</td>
</tr>
<tr>
<td>I, IIA</td>
<td>118 days</td>
<td>9920</td>
<td>9*10^7</td>
<td>9*10^7</td>
</tr>
<tr>
<td>III</td>
<td>0 s</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Survivability Quantification Challenges

- No unified definition
  - Variation due to different metrics
    - Steady state or transient
    - Availability, capacity-oriented availability, or performance
  - Variation due to different systems
    - Wire-line/wireless access networks, optical transport networks, military 3C networks, financial and banking networks, etc.
- Increased system complexity
  - Heterogeneity
    - Components have different capacity, performance, fault tolerance
  - Multiple layer hierarchy
    - Cross layer dependence, fault propagation, resource allocation & optimization
  - Failure scenario and impact
    - Identify potential failures and their impact on services