Combining Performance Modeling and Risk Analysis: A Homeland Security Case Study

Bojan Cukic, Jesse Mussgrove

Lane Department of CSEE
West Virginia University

IV&V Annual Workshop,
September 2012
Motivation

- At the system level, performance analysis is an essential part of verification and validation.
  - Recent use of IV&V on complex networks and ECTP.

- Performance and security are always interrelated.
  - Performance implications of security risk minimization are essential.
  - Combined modeling approaches are rare.
    - Cortellessa et al.: Component interaction analysis.
    - Petriu et al.: Aspect oriented approach, primary and secondary models.

- Complex methodology developed for a DHS study.
  - Modeling principles applicable to IV&V practice.
Proposed Framework

UML Model with performance annotations

Risk Model

Performance Model

Performance/risk feedback
Domain: Border Management

Legend
- = Required Signal
- = Optional Signal
- = Movement
- - = Optional Movement

Acceptance, modality, quality?

Modality, quality, scalability, update, access?

Traveler Queues

Public Key Directory

Local, distributed, or central?

Modality, FMR, vulnerability, exceptions, throughput?

False Non-Match Rate, Inconvenience.

Border Access

Inspection Stations (w/ biometric)

Watch Lists / Identity DB

Modality, FMR, vulnerability, exceptions, throughput?
An Airport Inspection System

Traveler Queue

Inspection Facility

Traveler

MRTD Card

MRTD Reader

PKD

TNS (Name lookup)

TBS (Biometric lookup)

POE Officer

Digital Camera

Fingerprint Reader
Approach

• **System architecture is nontrivial**
  – Static and dynamic architectural aspects using UML.
  – Creation and evaluation of quantitative performance models using LQN.

• **Risk analysis**
  – Border security systems rely on identity verification.
  – Validity of traveler’s biometric information.
  – Checks through *watch lists*.
  – *Cost Curve modeling*. 
Performance Analysis

• UML mapping to LQN performance model
LQN Model: Traveler Examination
Experiments Match rates & watch lists
Performance Analysis

• Performance models are derived from specifications.
  – Tedious, semi-automatic, but well justified analysis steps.
  – Performance analysis exposes architectural limitations.

• Watch-list size affects the system performance.
  – Knowing the limits early helps plan for contingencies.
  – “Rapid” screening not a goal by itself.
Risk function

Legend
- Required Signal
- Optional Signal
- Movement
- Optional Movement

Acceptance, modality, quality?

Modality, FMR, vulnerability, exceptions, throughput?

Local, distributed, or central?

False Non-Match Rate, Inconvenience acceptance?

Risk in Border Management

Watch Lists / Identity DB

Inspection Stations (w/ biometric)

Public Key Directory

Secondary Inspection / Detainment

Border Access

Traveler Queues

Modality, quality, scalability, update, access?
Why biometric systems err?

FMR – Security Risk

FNMR – Performance Burden
Cost Curve Modeling

- A methodology for classification evaluation based on expected cost of misclassification.
  - \( C(+)\) denotes the cost of incorrectly classifying a genuine user (as an impostor)
    → Secondary inspection (False Non Match, FNMR).
  - \( C(-)\) denotes the cost of misclassifying an impostor as a genuine user.
    → Security breach (False Match, FMR).
  - \( p(+)\) probability of a user being an impostor.
  - \( p(-)\) probability of a user being a genuine.
Parameters considered

• Which biometric modality (or algorithm) best meets the following operational conditions?
  – Impostor arrival rate varies
    • One in thousand passengers \((10^{-3})\)
    • One in hundred thousand passengers \((10^{-5})\)
    • One in ten million passengers \((10^{-7})\)
  – Misclassification cost ratio \(\mu = C(+|-):C(-|+)\)
    • It is 100 times more costly to miss an impostor \((10^{-2})\)
    • 10,000 times more costly to miss an impostor \((10^{-4})\)
    • 1,000,000 times more costly to miss an impostor \((10^{-6})\)
    • 100,000,000 times more costly to miss an impostor \((10^{-8})\)
Face Recognition for Border Inspections

2006 Face Recognition Vendor Test (FRVT)
**Analysis Results**

Table 3. Combined performance and risk modeling assuming the use of face biometrics

<table>
<thead>
<tr>
<th>$p(+) \mu$</th>
<th>PC</th>
<th>FNMR</th>
<th>FMR</th>
<th>Algorithm</th>
<th>$\text{Norm}(E[\text{Cost}])$</th>
<th>Total waiting time (min)</th>
</tr>
</thead>
<tbody>
<tr>
<td>$10^{-3}$</td>
<td>0.0909918111</td>
<td>0.00152</td>
<td>0.322</td>
<td>V-norm</td>
<td>0.030681056</td>
<td>31.87054</td>
</tr>
<tr>
<td>$10^{-4}$</td>
<td>0.909173561</td>
<td>0.367</td>
<td>0.003</td>
<td>Ts2-norm</td>
<td>0.036060824</td>
<td>∞</td>
</tr>
<tr>
<td>$10^{-6}$</td>
<td>0.999001997</td>
<td>0.451</td>
<td>0.048</td>
<td>V-norm</td>
<td>0.0884</td>
<td>∞</td>
</tr>
<tr>
<td>$10^{-8}$</td>
<td>0.999999001</td>
<td>0.451</td>
<td>0</td>
<td>NV1-norm</td>
<td>0.0884</td>
<td>∞</td>
</tr>
<tr>
<td>$10^{-2}$</td>
<td>0.000999011</td>
<td>0.00152</td>
<td>0.322</td>
<td>V-norm</td>
<td>0.001840163</td>
<td>27.93481</td>
</tr>
<tr>
<td>$10^{-4}$</td>
<td>0.090909917</td>
<td>0.00152</td>
<td>0.322</td>
<td>V-norm</td>
<td>0.03605481</td>
<td>27.93481</td>
</tr>
<tr>
<td>$10^{-6}$</td>
<td>0.909091736</td>
<td>0.367</td>
<td>0.003</td>
<td>Ts2-norm</td>
<td>0.036090608</td>
<td>∞</td>
</tr>
<tr>
<td>$10^{-8}$</td>
<td>0.999001009</td>
<td>0.451</td>
<td>0</td>
<td>NV1-norm</td>
<td>0.0884</td>
<td>∞</td>
</tr>
<tr>
<td>$10^{-7}$</td>
<td>9.9999E-06</td>
<td>0.00152</td>
<td>0.322</td>
<td>V-norm</td>
<td>0.001523205</td>
<td>27.89579</td>
</tr>
<tr>
<td>$10^{-8}$</td>
<td>0.000999001</td>
<td>0.00152</td>
<td>0.322</td>
<td>V-norm</td>
<td>0.00184016</td>
<td>27.89579</td>
</tr>
<tr>
<td>$10^{-8}$</td>
<td>0.909090999</td>
<td>0.367</td>
<td>0.003</td>
<td>V-norm</td>
<td>0.036090906</td>
<td>∞</td>
</tr>
</tbody>
</table>

In feasible implementations, FMR is NOT ACCEPTABLE!
• ECTP – Emergency Communication Transformation Program, revamped NYC 911 phone system.
Complex Network (PSAP) Model

Dotted lines show Simulink model elements
Analysis

Wait Time in Queue for English Call Taker

- The average wait time surpasses 10 seconds at a call rate of 12620 calls/hour.
- Below 12115 calls/hour the wait time is less than one second.
- Below 10200 calls/hour there is never any wait time.
• **With respect to utilization, wait time increases very late.**
  – Analysis scenario represents 321 English call takers.
  – Because it’s such a high number, even around 95% average utilization it’s rare to have a call come in when every call taker is busy.
Summary

- **Analytical performance models are very suitable for early system verification.**
  - Possible to create performance models from UML specs.

- **Queueing network models and tools are versatile.**
  - Reasonably quick learning curve.
  - Possible to build multi-level models in LQN.
  - Offer simulation capabilities for distributions that cannot be analytically solved.

- **Currently**
  - Updating the ECTP model, assessing its fidelity.
  - Enhancing simulation analysis (LQN-Sim, Simulink).
  - More detailed complex networks presentation tomorrow!