An Evaluation Methodology for Protocol Analysis Systems

Chris W. Hoffmeister
academic.hoffmeister.c.w@gmail.com
Acknowledgement

- This project was Master’s thesis work done under Prof. Dinolt and Prof. Herzog. at the Naval Postgraduate School.
Disclaimer

The views discussed and presented herein are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.
Agenda

- Project Overview
- Criteria
- Next Steps
Project Overview: Why

- Why the need for an evaluation methodology?
  - Single tool assessments
  - Broad survey of tools
  - Address user needs
Project Overview: What

- Formal evaluation methodology
  - Is detailed
  - Able to be tailored
  - Produces comparable results
  - Adaptable
Project Overview: Components

- Criteria
- Methods
- Ratings and weightings
Project Overview: Functional

Set of Protocol Analysis Systems

A X Z Y B

Evaluation Methodology

Scope Testing
- Type Support
- Operation Support

Correctness Testing
- Theoretical Correctness
- Observed Correctness

Performance Testing
- Execution Time
- Main Memory Requirement

Usability Testing
- Automation
- Syntax Errors

Overall Weighting Function

Evaluation Results

A Best
B
Z Worst
Agenda

- Project Overview
- Criteria
- Next Steps
Criteria: Scope

- Capture tool capability
- Characterize tool
- Core criteria
Criteria: Scope

- **Type Support**
  - Message, principal, nonce, keys, ...
  - Derived from Clark and Jacob 1997
  - Native, non-native, unable

- **Operation Support**
  - Cryptography, hashing, concatenation, ...
  - Derived from Clark and Jacob 1997
  - Native, non-native, unable
Criteria: Scope

- **Session Type**
  - Protocol states
  - Fixed, bounded, infinite

- **Theoretical Testable Protocol Characteristics**
  - CIAA, non-repudiation, round efficiency
  - Derived from survey of literature
Criteria: Correctness

- Input x Output
  - Protocol: Insecure or Secure
  - Tool: Insecure w/ Information, Insecure w/o Information, Secure, or Inconclusive

<table>
<thead>
<tr>
<th>Protocol Analysis System Results</th>
<th>Testable Protocol Characteristic</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Insecure</td>
</tr>
<tr>
<td>Insecure with Information</td>
<td>IW-I</td>
</tr>
<tr>
<td>Insecure without Information</td>
<td>IO-I</td>
</tr>
<tr>
<td>Secure</td>
<td>S-I</td>
</tr>
<tr>
<td>Inconclusive</td>
<td>N-I</td>
</tr>
</tbody>
</table>

Table 1: Protocol Analysis System Results x Protocol Possibilities
Criteria: Correctness

- Theoretical Correctness
  - Evaluation for each testable characteristic
  - Research based

- Observed Correctness
  - Evaluation for each testable characteristic
  - Experiment based
Criteria: Performance

- **Execution Time**
  - Length of time tool analyzes protocol

- **Main Memory Requirement**
  - Amount of RAM tool uses

- **Secondary Memory Requirement**
  - Amount of disk space tool uses
Criteria: Usability

- Objective vs. Subjective
- Automation
  - Automated, automatable, non-automatable
- Specification Comments
  - Smart, flat, unable
Criteria: Usability

- Syntax Errors During Protocol Specification
  - Syntax error count

- Structural Errors During Protocol Specification
  - Structural error count
Criteria: Usability

- **Specification Time**
  - Length of time user specifies protocol

- **Results Analysis Time**
  - Length of time user analyzes tool results
Criteria: Usability

- Participant Feedback
- Experimenter Feedback
Agenda

- Project Overview
- Criteria
- Next Steps
Next Steps

- Definitions of CIAA
  - Currently use general definition
  - Expand to include tools definition
- Subjective usability criteria
  - Define testing methods and rating schemes
- Define sets of protocols
Next Steps

- Use the evaluation methodology
Questions?
References


References
