Configuration Security (ConSec)

Mr. Jacob I. Torrey

Proposers Day

November 17, 2017
Develop a system to automatically generate, deploy, and enforce secure configurations of components and subsystems for use in military platforms.
Configuration complexity is a major source of vulnerabilities

M1 Garand

Partial representation of weapons platform network

Source: https://www.flickr.com/photos/dcoetzee/6271688256/

Source: https://www.flickr.com/photos/145317968@N02/32207891206/
Configuration complexity is a major source of vulnerabilities.

Example configuration settings:

<table>
<thead>
<tr>
<th>Configuration Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>RTS Threshold:</strong></td>
</tr>
<tr>
<td>2347</td>
</tr>
<tr>
<td><strong>Telnet</strong></td>
</tr>
<tr>
<td>Enable</td>
</tr>
<tr>
<td>Disable</td>
</tr>
<tr>
<td><strong>NAT Firewall</strong></td>
</tr>
<tr>
<td>Enable</td>
</tr>
<tr>
<td>Disable</td>
</tr>
</tbody>
</table>

Failure scenarios of power grid:

- **Configuration-based** 61%
- **Other** 39%

Electric Power Research Institute classification of power grid failure scenarios.

Real-world IT penetration-test findings:

- **Entirely configuration-based** 27%
- **Partially configuration-based** 40%
- **Other** 33%

Cobalt.io pen-test metrics report of 1500 vulnerability findings, 2016.

Source: Screenshot of Verizon home router.
• Develop a system to
  • Explore configuration state space, deploy secured settings, and monitor for deviation

TA1: Understand composed system
  • Build model of functionality and operational contexts

TA2: Generate secure configuration optimized for operational contexts

TA3: Voice of the offense
  • Challenge TA1/TA2 system with configuration and composition vulnerabilities

TA4: Evaluation and integration
  • Target platform provider and integrator
TA1: Understand composed system

- Represent the operational context of a composed system in a model
- Rapid ingest of human-readable system documentation
- Automated generation of configuration-aware functional specifications
- Reducing dimensionality of configuration parameters
- Deployment and monitoring of configuration sets on target system
TA1 challenges

- Semantic extraction to produce a model of configuration parameter functionality relative to system behavior

- Principled reduction of the configuration space for each component

- Semi-automated modeling of operational context(s) of the target system from human-readable documentation

- Automatically generate a specification of each component’s functionality based on its software, firmware and configuration parameters

- Develop a vendor-agnostic representation for communicating these models and specifications to the TA2 system

- Develop a capability to access and modify the configuration parameters on diverse devices
• Rapidly generate mission-optimized configurations
• Support authority-to-operate approval of configuration sets with formalized arguments
• Enable large scale context-sensitive reasoning with incomplete specifications
• Discover hidden behaviors in composed systems
TA2 challenges

- Performing compositional analysis of the TA1-provided system models and specifications to determine an optimal configuration set for the target in each operational context.

- Automatically generating human-readable evidence supporting the selected configuration set in order to allow authorization approval.

- Communicating the configuration state of the system with the TA1-developed monitoring subsystem to detect indicators of compromise or assist in changing between operational contexts.
• Challenge TA1/TA2 system with configuration and composition vulnerabilities

• TA3 proposals should address the following challenges
  • Develop tools, techniques, and procedures to exploit composed systems solely via configuration- or composition-enabled vulnerabilities
  • Use TA1-provided models and specifications to guide the generation of attack paths, minimizing human-in-the-loop effort
TA4: Evaluation and integration

• Technical progress assessment
  • Conduct functional, regression, performance, and scalability testing
  • Provide specific, constructive feedback to all performers developing code

• Evaluations
  • Develop relevant test cases for integrated TA1/TA2 systems and measure performance against system-specific metrics
  • Conduct evaluations in advance of PI meetings to inform the technical discussion

• Exercises
  • Plan, develop and coordinate program exercises
  • Exercises will increase in complexity and duration over the period of performance

• TA4 proposals should address the following challenges
  • Facilitation of common data formats between TA1 and TA2
  • Coordination of exercises on limited physical target systems
  • Metrics evaluation and novel metrics to measure the progress and success of the ConSec system
## ConSec program metrics

<table>
<thead>
<tr>
<th></th>
<th>Phase 1 (scaffolding)</th>
<th>Phase 2 (initial deployment)</th>
<th>Phase 3 (Highly-complex system)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>TA1: Model Fidelity</strong></td>
<td>80% of static space</td>
<td>80% of static space</td>
<td>90% of static</td>
</tr>
<tr>
<td><strong>TA1: Documentation Ingest</strong></td>
<td>10x manual, 60% accuracy</td>
<td>10x manual, 70% accuracy</td>
<td>10x manual, 80% accuracy</td>
</tr>
<tr>
<td><strong>TA1: Deployment time</strong></td>
<td>1.5x faster than manual</td>
<td>5x faster than manual</td>
<td>15x faster than manual</td>
</tr>
<tr>
<td><strong>TA2: Configuration-space coverage</strong></td>
<td>60% coverage</td>
<td>60% coverage</td>
<td>75% coverage</td>
</tr>
<tr>
<td><strong>TA2: Risk reduction</strong></td>
<td>85% reduction</td>
<td>85% reduction</td>
<td>85% reduction</td>
</tr>
<tr>
<td><strong>TA2: Correctness guarantee</strong></td>
<td>None</td>
<td>Basic</td>
<td>Formal</td>
</tr>
</tbody>
</table>
## ConSec schedule

<table>
<thead>
<tr>
<th>Phase 1</th>
<th>Phase 2</th>
<th>Phase 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>15 months</td>
<td>15 months</td>
<td>12 months</td>
</tr>
<tr>
<td>Scaffolding on simple system</td>
<td>Whole-system test on commercial system</td>
<td>Maturing ConSec for two DoD systems</td>
</tr>
</tbody>
</table>

**Demonstrations**
- Demonstration of capability on simulated system

**Exercises**
- Time-limited exercises on high-fidelity system
Program funding

- Total program funding available for award is $45m over 3 1/2 years

- Proposals may address only one Technical Area

- Organizations can submit proposals to all Technical Areas
  - Which to consider for award is at the discretion of the Government
  - TA-4 performer may perform on other TAs subject to an acceptable OCI Mitigation Plan
To summarize

- Read the BAA, carefully and more than once
  - “Specifically excluded is research that primarily results in evolutionary improvements…”
  - DARPA does not acquire commercial products

- The goal of ConSec is to automatically generate, deploy, and enforce secure configurations of embedded COTS/GOTS devices for use in military platforms