KNOWN VULNERABILITIES
What you can find with your current security tests.

Anton von Troyer

UNKNOWN VULNERABILITIES
What Codenomicon can help you reveal.
About Codenomicon

Founded in Autumn 2001
Commercialized the academic approach built since 1996
Technology leader in security test automation
  – Model-based, intelligent, targeted tests
  – Software-based, with subscription licensing
  – Horizontal market, supports 150+ technologies
  – 200+ customers globally
State-of-the art Network Analysis and Security assessment services
Highly successful, constantly growing
  – 2009 was 9th subsequent growth year!
  – Profitable year 2009! §
Glossary of Terms: Product Security Terminology

**Vulnerability** – a weakness in software, a bug. Most software has bugs

**Threat/Attack** – exploit/worm/virus against a specific vulnerability

**Protocol Modeling** – Technique for explaining interface message sequences and message structures

**Anomaly** – abnormal or unexpected input

**Failure** – crash, busy-loop, memory corruption, or other indication of a bug in software
Robustness Testing

Discover unknown vulnerabilities with Testing & QA
Fuzzing is a technique for
  – intelligently and
  – automatically
generating and passing into a target system
  – valid and
  – invalid
message sequences to see if the system breaks, and if it does, what it is that makes it break.
Model Based Fuzzing Techniques

Specification Based Fuzzing
- Full test coverage
- Always repeatable
- Short test cycle, more optimized tests
- Easy to edit and add tests

Template Based Fuzzing
- Base test cases on a sample
- Quality of tests is based on the used seed and modeling technique
- Very quick to develop
- No need for protocol specification
Fuzzing = Security Testing

1990 Random fuzzing becomes popular. Hackers use Fuzzing for zero day discovery;
1999 Model-based fuzzing becomes popular. 100% of zero-days found with fuzzing;
2001 Network equipment manufacturers start using Fuzzing for protection against hackers
2006 Telcos integrate Fuzzing into acceptance testing and test for zero-day threats
2010 Large-scale propagation of Fuzzing at
  • Finance
  • Government
  • SCADA
2015-> Fuzzing as a purchase criteria and requirement by GOV
Fuzzing means crash testing... ANY TYPE OF DEVICE!
Fuzzing a popular method also among hackers
Fuzzing mimics the ways attackers search for security holes
Most exploits/zero days nowadays found by fuzzing
Modern security testing is about finding unknown zero-day vulnerabilities in devices and software before and after release.

Provides a quick technique for security assurance for any device or software.

www.codenomicon.com/unknown/
Benefits of fuzzing

“All software has undetected exploitable vulnerabilities”
- Security Vendor 2009

“You would be a fool not to Fuzz.”
– Forrester 2011

“All our zero-day vulnerabilities were found with Fuzzing.”
– Software Vendor 2010
Benefits of fuzzing

• "The Codenomicon tools are *amazing*. Using them is like being attacked by the most relentless adversary who uses every possible method to find flaws in your code.

We fixed subtle crash bugs that had been in our code for over ten years. We would *never* have found those bugs without the Codenomicon tools.

If you're serious about implementing protocols correctly, you need the Codenomicon tools."
### Test Case Selection

<table>
<thead>
<tr>
<th>Test Case</th>
<th>Description</th>
<th>Anomaly</th>
</tr>
</thead>
<tbody>
<tr>
<td>51</td>
<td>regular-payload.valid</td>
<td>none</td>
</tr>
<tr>
<td>614454</td>
<td>chunked-payload.valid</td>
<td>none</td>
</tr>
</tbody>
</table>

**Basic Operation**

- Run valid test case
- Configure
- Select valid
- Start the test