Automated Testing of Industrial Control Devices: The Delphi Database

Dan Hoffman, P.Eng.
Department of Computer Science
University of Victoria

Nate Kube and Kevin Yoo
Wurldtech Security Technologies
Networking in Industrial Control Systems

Diagram showing:
- HMI
- PLC
- Data historian
- Sensors & actuators
- Internet

With an air gap between the industrial control system and the business network.
Talk Overview

- Networking: ICS versus IT
- Test harness
- Three test types
- Grammar-based test generation
- Database entries
- Prevention and mitigation strategies
## The Internet versus the Factory Floor

<table>
<thead>
<tr>
<th></th>
<th>Internet</th>
<th>Factory Floor</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Reliability</strong></td>
<td>failures tolerated</td>
<td>failures intolerable</td>
</tr>
<tr>
<td><strong>Risk impact</strong></td>
<td>loss of data</td>
<td>loss of production, equipment, life</td>
</tr>
<tr>
<td><strong>Performance</strong></td>
<td>high throughput</td>
<td>low delay/jitter</td>
</tr>
<tr>
<td><strong>Risk mgt.</strong></td>
<td>recover by reboot</td>
<td>fault tolerance essential</td>
</tr>
<tr>
<td><strong>Security</strong></td>
<td>most sites insecure</td>
<td>tight physical/cybersecurity</td>
</tr>
</tbody>
</table>
Test Harness

DUT

Ethernet

digital output

discrete monitor

forward traffic

Ethernet

HMI

Achilles Satellite
Three Test Types

- **Rate-based (≈ 10)**
  - denial-of-service attacks
  - send packets at precisely controlled rates

- **Known vulnerability (≈ 30)**
  - send packets previously shown to exploit specific device vulnerabilities

- **Grammar-based test generation (≈ 30)**
  - specify tests with context-free grammar
  - focus on illegal packet fields and field combinations
Grammar-based Test Generation

- Grammar fragment
  
  ```
  packet ::= ethernetHdr ethernetData;
  ethernetHdr ::= srcAddr dstAddr protocol;
  ethernetData ::= arpHdr | ipHdr ipData;
  ipHdr ::= version ipHdrLen ToS ipTotalLen ...
  tcpHdr ::= srcPort dstPort seq ack tcpHdrLen ...
  ```

- Bad lengths test: generate packets with correct header values, except that the lengths are inconsistent
  
  - `ipTotalLen = 100` but transmit 117 bytes
  - illegal because the Ethernet header is 18 bytes
Database Contents

- **Raw data**
  1. Test data from 31 devices and approximately 10,000 tests

- **Vulnerabilities:** approximately 500 vulnerabilities stored
  1. Test case id
  2. CVSS score
  3. Monitors impacted
  4. Packet rate
  5. Packet size
  6. Recovery time
  7. Device type
  8. Relevant industries
Operator Mitigation Strategies

- Rate limit network traffic
- Block the TCP/IP LAND attack
- Prevent port scans
- Be wary of fragmented packets
- Block impossible packet header field combinations
Vendor Prevention Methods

- Drop unsolicited ARP replies
- Carefully manage memory/CPU utilization
- Assume the worst about network input
- Properly manage data buffers
- Rate-limit traffic
Conclusions

▶ **Problem**: changes to security policies and networking technologies have made ICS networks too vulnerable to cyber-attack.

▶ **One attack on this problem**:
  ▶ a framework for testing a wide variety of devices thoroughly and at reasonable cost.
  ▶ validated on significant set of devices
  ▶ produced description of specific device vulnerabilities
  ▶ supported recommendations for prevention and mitigation

▶ An opportunity for AST researchers:
  ▶ improve the quality of the software in the “critical infrastructure”