Internet of Things 2015

Verifiable Security for the Internet of Things

Dave Hughes, CEO HCC Embedded
Why is Security A Problem for IoT?

GNU security library GnuTLS fails on cert checks: Patch now

Many eyes missed bug for many years

By Richard Chirgwin, 6 Mar 2014

Toyotas killer firmware: Bad design and its consequences

Michael Dunn – October 28, 2013
Security in a Connected World

Security is about connectivity & ensuring three things:

1. Data is not modified
2. You are talking to the correct person
3. Data is secure from eavesdroppers

Context may change but the logic is always the same
## Identifying the Source of Problems

<table>
<thead>
<tr>
<th>Software Security Issue</th>
<th>Contributing Factors</th>
</tr>
</thead>
<tbody>
<tr>
<td>OpenSSL</td>
<td>No software design</td>
</tr>
<tr>
<td></td>
<td>No traceable test cases</td>
</tr>
<tr>
<td></td>
<td>No boundary case analysis</td>
</tr>
<tr>
<td></td>
<td>No software life cycle</td>
</tr>
<tr>
<td>Apple SSL</td>
<td>Static analysis</td>
</tr>
<tr>
<td></td>
<td>Code structure</td>
</tr>
<tr>
<td>GCC SSL</td>
<td>No design</td>
</tr>
<tr>
<td></td>
<td>No traceable test cases</td>
</tr>
<tr>
<td></td>
<td>No boundary case analysis</td>
</tr>
<tr>
<td></td>
<td>In short – no software lifecycle</td>
</tr>
<tr>
<td>BASH</td>
<td>System too complex;</td>
</tr>
<tr>
<td></td>
<td>Too easy for application to get security access. Too many possible applications that could have holes.</td>
</tr>
<tr>
<td>US POS (Point of Sale)</td>
<td>Badly structured System</td>
</tr>
</tbody>
</table>
The Anatomy of Heartbleed Bug

• Code is released to control the security of at least 500,000 servers - difficult to know how many people that affects.

  1. change request (heartbeat enhancement)
  2. change made
  3. change reviewed

• Is defect the fault of OpenSSL?

• Announcement that OpenSSL will be re-written
  – deleting code
  – rewriting code
  – testing code

• What will really make things better? Process, change management?
Risks of Freestyle Software

• OpenSSL is free – how much did it cost industry?
  – Most orgs had to re-issue all certificates at significant financial cost without fixing the fundamental Heartbleed problem. What happens next time?
  – Huge costs to reputation, corporate brand and customer trust.

• Obvious risks....
  – So why do corporations risk exposing their customers valuable assets and their reputation?
  – Why risk having executives stand in court and defend poor development methods?
Specification and RFCs

- It is "normal" to have a specification for ALL software.
- RFCs are not software specifications!
- Checking the validity of headers not obviously in either TLS (rfc5246) or Heartbleed RFC (rfc6520).
- Now this issue is fixed ...
- Where are the specifications?
Safety v Security Disconnect

• Security software has never had the rigors of safety software applied to it.

• For all the literature and education on embedded software quality is defined by vertical markets.

• Security is another “orthogonal” component – needs some logical thinking.
## Security Design Issues

<table>
<thead>
<tr>
<th>System Design Issue</th>
<th>Mitigation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Software Authentication</td>
<td>Ensure the hardware only operates with authenticated software and ensure that new releases of software will only work with authentic hardware.</td>
</tr>
<tr>
<td>Software Integrity</td>
<td>Ensure the software has not been modified by any external party.</td>
</tr>
<tr>
<td>Software Secure</td>
<td>Ensure the software cannot be read by a third party (this makes constructing attacks more difficult).</td>
</tr>
<tr>
<td>System Complexity</td>
<td>Minimize risk of back doors and unforeseen consequences by having the security component do security – no more or less than it needs to. Also minimize the effort required to develop secure software to the required level</td>
</tr>
</tbody>
</table>
How to Develop Reliable Security

• There is no mystery surrounding development of reliable software

• IEC 61508 - reformulated in 26262, 62304, FDA510K, DO178B etc

• ‘V’ model with requirements, design, implementation, static and dynamic analysis

• Traceable back to requirements with full software life-cycle maintenance

• What may be the cost of implementing SSL using well defined process....

It could be as much as $1-2 USD for every server running OpenSSL?
Applying V Model; TLS & Encryption

• Approach the problems systematically

• How have HCC addressed TLS and Encryption?
  – Requirements
  – Specification
  – Coding Standard (MISRA – portability)
  – Static and Dynamic Analysis
  – Test Suite (MC/DC - portability)

• Why will this make a difference?

• What are the potential benefits?
Taking Control of IoT Security

1. Assess the risk your product poses to your company & customers.

2. Can you demonstrate you took all possible steps to protect your products and reputation or will you just gamble?

3. Move the odds in your favour: use products and methods fit for purpose.