Case Study:
Treating Challenges in Software Trustability

Ian Bryant
Technical Director SSDRI

ACSA Conference 2012 (ACSAC)
Orlando FL US
7 December 2011
Software Defects

• Software problems are high cost to economy:
  – US Government National Institute of Standards & Technology (NIST) ~$60 billion / year to US alone
  – No definitive figure for UK / worldwide

• Software a major source of IT project failure:
  – ESSU (European Services Strategy Unit) 2007
  – Tata Consultancy 2007
  – Standish Chaos Reports 2004 onwards
  – Rand 2004
Malicious Software

• Malicious Software (MalWare) ecosystem

• Ever increasing number of MalWare strains has challenges for reactive mitigation approaches (analysis workload and host performance)

• ICT marketplace is evolving in ways that will seem a proliferation of new types of platforms and software, increasing potential attack surface

• Software supply base broadening to those with little knowledge of good development practices
Software Composition

<table>
<thead>
<tr>
<th>Segment</th>
<th>Embedded Systems</th>
<th>SCADA Systems</th>
<th>Communications Systems</th>
<th>IT Infrastructure</th>
<th>IT Applications</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reuse</td>
<td>Limited</td>
<td>Libraries</td>
<td>Libraries; Mobile Code</td>
<td>Libraries; Mobile Code; Cloud Services</td>
<td>Libraries; Mobile Code; Cloud Services; Mashups</td>
</tr>
</tbody>
</table>

**Trusted Supply Chain Required**
Context: Effort Imbalance

- **Ideal**: The expected balanced effort across different stages.
- **Current**: The actual effort distribution currently being applied.
- **Probable**: A likely scenario for future effort distribution.

Legend:
- **Operate**
- **Validate**
- **Implement**
- **Build**
- **Design**

SSDR1: UK’s public-private partnership for Making Software Better
Software Development

• Underlying assumption software will be developed under engineering-style “waterfall” model, under single organisational control

• Challenges to these assumptions include:
  – Agile Development
  – Open Source
  – Untrusted platforms (incl. counterfeit hardware)
  – Software / hardware boundary (e.g. VHDL)
  – Multicore Processors
  – Use of structured data (e.g. XML) to control behaviour
Emerging Challenges

Top 10 Strategic Technology Trends for 2012

– Media Tablets and Beyond
– Mobile-Centric Applications and Interfaces
– Contextual and Social User Experience
– Internet of Things
– App Stores and Marketplaces
– Next-Generation Analytics
– Big Data
– In-Memory Computing
– Extreme Low-Energy Servers
– Cloud Computing

Source: Gartner, Inc. (18 October 2011)
Current SDR Drivers

• 2010 UK National Security Strategy has Cyber-attack and deficiencies as one of the 4 “Tier One” Risks

• New Technological / Societal challenges:
  – Distributed application platforms and services (“Cloud’’)
  – Mobile Devices and Lightweight operating systems
  – Consumerisation / Bring-Your-Own-Device (BYOD)
  – Commoditisation in previously closed architectures
  – Consolidation for energy efficiency (Low Carbon / Green)

• These are likely to present Disruptive Challenges, fundamentally deepening dependence on Software
Software Faults

• Mitre’s Common Weakness Enumeration (CWE) is a community developed, formal list of software weakness types created to:
  – Serve as a common language for describing software weaknesses in architecture, design, or code
  – Serve as a standard measuring stick for software tools targeting these weaknesses
  – Provide a common baseline standard for weakness identification, mitigation, and prevention efforts

• Currently 810 distinct CWE entries identified
<table>
<thead>
<tr>
<th>Rank</th>
<th>ID</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>CWE-79</td>
<td>Failure to Preserve Web Page Structure ('Cross-site Scripting')</td>
</tr>
<tr>
<td>2</td>
<td>CWE-89</td>
<td>Improper Sanitization of Special Elements used in an SQL Command</td>
</tr>
<tr>
<td></td>
<td></td>
<td>('SQL Injection')</td>
</tr>
<tr>
<td>3</td>
<td>CWE-120</td>
<td>Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')</td>
</tr>
<tr>
<td>4</td>
<td>CWE-352</td>
<td>Cross-Site Request Forgery (CSRF)</td>
</tr>
<tr>
<td>5</td>
<td>CWE-285</td>
<td>Improper Access Control (Authorization)</td>
</tr>
<tr>
<td>6</td>
<td>CWE-807</td>
<td>Reliance on Untrusted Inputs in a Security Decision</td>
</tr>
<tr>
<td>7</td>
<td>CWE-22</td>
<td>Improper Limitation of a Pathname to a Restricted Directory</td>
</tr>
<tr>
<td></td>
<td></td>
<td>('Path Traversal')</td>
</tr>
<tr>
<td>8</td>
<td>CWE-434</td>
<td>Unrestricted Upload of File with Dangerous Type</td>
</tr>
<tr>
<td>9</td>
<td>CWE-78</td>
<td>Improper Sanitization of Special Elements used in an OS Command</td>
</tr>
<tr>
<td></td>
<td></td>
<td>('OS Command Injection')</td>
</tr>
<tr>
<td>10</td>
<td>CWE-311</td>
<td>Missing Encryption of Sensitive Data</td>
</tr>
<tr>
<td>11</td>
<td>CWE-798</td>
<td>Use of Hard-coded Credentials</td>
</tr>
<tr>
<td>12</td>
<td>CWE-805</td>
<td>Buffer Access with Incorrect Length Value</td>
</tr>
<tr>
<td>13</td>
<td>CWE-98</td>
<td>Improper Control of Filename for Include/Require Statement in PHP</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Program ('PHP File Inclusion')</td>
</tr>
</tbody>
</table>
## Mitre/SANS CWE Top 25 (2)

<table>
<thead>
<tr>
<th>Rank</th>
<th>ID</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>14</td>
<td>CWE-129</td>
<td>Improper Validation of Array Index</td>
</tr>
<tr>
<td>15</td>
<td>CWE-754</td>
<td>Improper Check for Unusual or Exceptional Conditions</td>
</tr>
<tr>
<td>16</td>
<td>CWE-209</td>
<td>Information Exposure Through an Error Message</td>
</tr>
<tr>
<td>17</td>
<td>CWE-190</td>
<td>Integer Overflow or Wraparound</td>
</tr>
<tr>
<td>18</td>
<td>CWE-131</td>
<td>Incorrect Calculation of Buffer Size</td>
</tr>
<tr>
<td>19</td>
<td>CWE-306</td>
<td>Missing Authentication for Critical Function</td>
</tr>
<tr>
<td>20</td>
<td>CWE-494</td>
<td>Download of Code Without Integrity Check</td>
</tr>
<tr>
<td>21</td>
<td>CWE-732</td>
<td>Incorrect Permission Assignment for Critical Resource</td>
</tr>
<tr>
<td>22</td>
<td>CWE-770</td>
<td>Allocation of Resources Without Limits or Throttling</td>
</tr>
<tr>
<td>23</td>
<td>CWE-601</td>
<td>URL Redirection to Untrusted Site ('Open Redirect')</td>
</tr>
<tr>
<td>24</td>
<td>CWE-327</td>
<td>Use of a Broken or Risky Cryptographic Algorithm</td>
</tr>
<tr>
<td>25</td>
<td>CWE-362</td>
<td>Race Condition</td>
</tr>
</tbody>
</table>
Risk Segmentation

Potential Flaw Impact

Market Size

Niche

Mainstream

Disbursed

Collateral

SSDRI: UK’s public-private partnership for Making Software Better
Software Security, Dependability and Resilience Initiative (S S D R I)

In response to previous work, the 2010 UK National Security Strategy, and emergent challenges, on 1st July 2011 UK formed SSDRI:

“A public-private platform for enhancing the overall software and systems culture, with the objective that all software should become designed, implemented and maintained in a secure, dependable and resilient manner”
SSDRI Scope

• Goal is to improve Software
  – Security (mainly protection of Confidentiality)
  – Dependability (mainly protection of Integrity)
  – Resilience (mainly protection of Availability)

• Importantly, this applies to both:
  – Specific software and systems developed for specialist markets where Security, Dependability and Resilience (SDR) are Functional Requirements, typically with Medium/High assurance needs
  – And to all other software and systems for which Security, Dependability and Resilience (SDR) are Non Functional Requirements (NFR), typically with Due Diligence needs
UK Potential Audiences

Not forgetting that 60m+ Citizens would also benefit from more trustable ICT

S S D R I: UK's public-private partnership for Making Software Better
The International Dimension

Internet Users

Source: National IA Forum (2010)
SSDRI Context: Lifecycle and Dependencies

SSDRI Focus Areas

Info Security Arch Risk Mgt

Acquisition
- Stakeholder Requirements Definition
- Requirements Analysis

Supply
- Architectural Design

Development
- Implementation
- Integration and Validation
- Transition and Verification

Operation
- Operation

Maintenance
- Organisational Awareness, Training and Verification
- Practitioner Education, Training and Verification
- Component / System Verification and Testing

Static Body of Knowledge
- Architectural Reference Model
- Architectural Reference Case
- Architectural Specification Case
- Design & Effect Classes

Assurance Case
- Assets, Adversity & Vulnerability Catalogue
- Risk Analysis
- Control Catalogue
- Assurance Case

Patching
- Dynamic Information Sharing

© Copyright 2003-2011

SSDRI: UK’s public-private partnership for Making Software Better
SSDRI Work Packages and Effort Clusters

- **Standards Contribution (WP6)**
- **Research**
- **Tools and Services**
- **Independent Verification (WP4)**
- **Environmental Shaping (WP1)**
- **Conceptual Evolution (WP2)**
- **Practice Development (WP3)**
- **TEA (Training, Education and Awareness)**
- **International Collaboration (WP5)**

SSDRI: UK’s public-private partnership for Making Software Better
SSDRI Approach

• Many of concepts and practices needed for software Security / Dependability / Resilience have existed in specialist domains for many years
• Challenge is to “bake in” to all software, recognising that implementations may vary with Audiences and Functional / Assurance Requirements
• Focus of SSDRI on Pareto (“80:20”) approaches to Making Software Better, iteratively using learnings from specialists domains and interpreting them for the common good
  – c.f. “Public Health”: Prevention now avoids Treatment later
SSDRI WP1: Environmental Shaping
SSDRI WP3: Practice Development

• In “mature” industries (e.g. Aviation Engineering), **all** practitioners intrinsically responsible for producing trustable outputs.

• We need SSDR embedded at all levels so it becomes “part of the Culture”:
  – **T**raining of current workforce
  – **E**ducation of future workforce
  – **A**wareness of all producers and consumers
SSDRI WP2: Conceptual Evolution

• Software SDR requires research and innovation in:
  – Situational Awareness – Horizon Scanning
  – Governance (e.g. Metrics, Trusted Information Sharing)
  – Human Factors (e.g. Stakeholder Behaviours)
  – Technical (e.g. New Technologies and Attacks, Trustable Failure Modes, Composability and Traceability, Multicore Technologies)

• A particular challenge is Composability and Traceability
SSDRI: Composability and Traceability Challenge

- Assertions (↑) & Assumptions (↓):
  - Can be Positive (+ve) and/or Negative (-ve)
  - How should this be modelled?
  - Who should be responsible?
  - How should this be documented?

- Updates to Standards
- Artefacts need to be in both System and IA terms

- Become Bidirectional Assertions (↕) & Assumptions (↕) for Composed System linking to Cloud

- An area for further study
SSDRI WP4: Independent Verification

• Product and Service Assurance splits (roughly) into 2 segments
  – “Due Diligence” by Independent Black Box testing
  – “High assurance” with preference for Formal Methods

• Also Maturity Model(s) needed for Supply Chain Assurance

• This Work Package is currently in abeyance whilst new schemes for Information Security Products and Services evolved by CESG
SSDRI WP5: International Collaboration

- Software SDR is not a “UK plc” problem
- International Collaboration is therefore an essential element of efforts
  - Multinational involvement was intrinsically part of the precursor “Paris Workshop”
- Initial International Collaboration options
  - International Standardisation through BSI IST/033
  - Bilateral collaboration with US peer organisation, the Software Assurance (SwA)
SSDRI WP6: International Standardisation

• No standardisation of Standards Development Organisations (SDO)!
• Leading UK recognised SDO in SSDR area would be ISO/IEC JTC1, with multiple active projects in SC7 / SC22 / SC27 / SC38
• Some work in ITU-T
• Also need to keep eye on de facto standardisation through other bodies, such as Mitre and OWASP
SSDRI and UK Cyber Security Strategy

• 2010 UK National Security Strategy (NSS) gives “Cyber” (attacks and shortcomings) as one of 4 “Tier One” Risks
• Amplified by UK Cyber Security Strategy (UKCSS) in 2011, which include Actions for:
  – Raising awareness of needs for protection, including supply chain dependencies (UKCSS 1.23; 4.11 ➔ SSDRI WP1)
  – Anticipating technological, procedural and societal behaviour developments that affect cyberspace, identifying Centres of Excellence in research (UKCSS 4.1; 4.10 ➔ SSDRI WP2)
  ➢ Improving education at all levels, including higher and postgraduate level (UKCSS 4.3 ➔ SSDRI WP3)
  – Working closely with the European Commission to encourage greater coherence within the EU on cyber issues (UKCSS 3.10 ➔ SSDRI WP5)
  – Stimulating the development of international, regional and national standards that are readily used and understood (UKCSS 1.13; 1.24; 3.6 ➔ SSDRI WP6)
Any Questions?
Contact Details

Ian Bryant
Technical Director S S D R I

SSDRI Office
Gateway House pp4.30
De Montfort University - Cyber Security Centre
The Gateway, Leicester, LE1 9BH, England

ian.bryant@ssdri.org.uk
+44 79 7312 1924

secretariat@ssdri.org.uk
+44 33 0001 0479

www.ssdri.org.uk
(Twitter: @ssdriuk)

© Copyright 2003-2011