Common Criteria in a Global Consumer Market

David MacFarlane
Director of Security Certifications
Research In Motion Limited
Agenda

- Industry and Trends
- Challenges and Security Risks
- Common Criteria
Industry and Trends
Global Shipments

Source: IDC, Canalys

- **Smartphones**
- **All PCs**
Source: IDC
Growth in Capabilities

2004

2011
Evolution of Interaction
Mobility of Assets
Convergence of Platforms
A personal liable device is owned and paid for by the employee but connected to corporate resources:
- Lower operating budget for enterprises
- Increases choice of technology for employees

More than 60% of corporate mobile devices will be personal liable devices by 2013.

90% of organisations will support corporate applications on personal devices by 2014.

Source: IDC WW Business Use Smartphone 2010-2014 Forecast and Analysis; Gartner as quoted in Wireless Week March 9, 2011
Challenges and Security Risks
Software Complexity

[Source: “Embedded Software: facts, figures and futuro”, (C.Ebert, C Jones, IEEE Computer), April 2009]
Scarcity of Resources
Personal Liable

Employees want mobile device choice and flexibility

IT wants ease of use, transparent control and manageability

Executives want business-critical data protected wherever it resides
## Mobile Malware

<table>
<thead>
<tr>
<th>August 2006</th>
<th>December 2010</th>
</tr>
</thead>
<tbody>
<tr>
<td>31 families, 170 variants</td>
<td>153 families, 1000+ variants</td>
</tr>
<tr>
<td>Spread via Bluetooth, MMS</td>
<td>Spread via Bluetooth, MMS, removable media</td>
</tr>
<tr>
<td>• Remote control of smartphone</td>
<td>In addition to 2006:</td>
</tr>
<tr>
<td>• Steal data</td>
<td>• Damage user/enterprise data</td>
</tr>
<tr>
<td>• Send premium SMS messages</td>
<td>• Disable OS security mechanisms</td>
</tr>
<tr>
<td>• Lock memory cards</td>
<td>• Download other files from Internet</td>
</tr>
<tr>
<td></td>
<td>• Call paid services</td>
</tr>
<tr>
<td></td>
<td>• Polymorphism</td>
</tr>
</tbody>
</table>

Basic economics – Follow the money!

Source: Securelist.com
Security Threats Are Real…

➢ 11.3% of data leaks are due to lost smartphones
  Source: Forrester Consulting Though Leadership Paper, November 2009

➢ 30,000+ mobile devices left in New York taxicabs every 6 months
  Source: Credant Technologies, 2009

➢ 17% of [European] companies have experienced mobile security breach
  Source: Continental Research & Fox Parrack Singapour, 2009
Security Threats Are Costly…

$6.75 million
Total organisational cost of a data breach in United States in 2009

$2.0 million
Total organisational cost of a data breach in Australia in 2010

Source: Ponemon Institute LLC, April 2010
But Perfect Security Does Not Exist!

Security is about balance!
4 Steps to Controlling Risk

1. Vendor selection process
   - Secure development process?
   - Security updates?
   - Accreditation activities?

2. Technology selection process
   - Device boot integrity?
   - Runtime protections?
   - Non-bypassable policy enforcement?
   - Accreditation of security functionality and cryptography?
3. Develop a mobile security policy
   - Password – length, complexity
   - Data encryption – data in transit, data at rest
   - Connections – network, peripherals
   - Applications – white/black list, business value
   - Auditing – text messages, phone logs, regulatory requirements
   - Device life cycle – disposal, trade
   - Always consider the impact to the end user!

4. Educate users
Common Criteria
Intersection of the Industries
BlackBerry Evaluation Experience: Challenge #1 – Evaluation Scope

- No smartphone protection profile available
  - Customers unable to articulate desired scope
  - Simply ask for “CC certification”

- Smartphone usability, risks, and challenges
  - A delicate balancing act!

- BlackBerry approach:
  - Lead rather than follow
  - Focus on key security mechanisms
  - Data protection, remote management, policy enforcement, application management
BlackBerry Evaluation Experience: Challenge #2 – Educating Stakeholders

- Customers understand smartphones…
  - But do not understand the application or benefit of CC!

- Certification bodies understand the CC…
  - But they cannot master every technology!

- BlackBerry approach:
  - Ongoing communication with all stakeholders
  - Again, focus on key security mechanisms
BlackBerry Evaluation Experience:
Challenge #3 – CCRA

- Common Criteria Recognition Arrangement is a great brand and concept but...

recognition of certifications ≠ acceptance of certified products
Opportunities for the Future

- How do you effectively evaluate a smartphone?
  - Mobile Device protection profile in progress!

- What is considered a secure mobile payment?

- What defines the strength of the CCRA?

- How does the CC community remain focused?
Thank you for your time!

David MacFarlane  
Director, Certifications and Approvals  
BlackBerry Security

damacfarlane@rim.com