Mobile security in real life
Janne Uusilehto, Nokia
Director, Head of Nokia Product Security
How does this sound:

Mobile security in real life
--------------------------------
This presentation discusses topics like: the megatrends in the global mobile security industry. How is the mobile industry thinking about the situation in the marketplace, and what kind of counter-measures has the mobile industry taken towards mobile security? What is the basic nature of mobile security, and what are the weak points in mobile security? Can hardware security be standardized, why should it be standardized, what are the leading HW security standardization forums offering at the moment, what is available already, and what is missing? And what are the challenges and possibilities."

Best Regards,
/Jmu
Nature of Security
There are many definitions already existing for product security

- A product does what it is designed to.
- Security is a process, not a product.
- Product Security is the incorporation into anything that is productized via security-related design, architecture, process, development, testing, release and maintenance.
- Product Security requires extra robustness and resistance from attacks against all parts of the architecture and functionality.

What security are you?

- Corporate Security – corporate physical assets & people
- IT Security – corporate information assets and IT systems
- Product & Services security – products, services & engineering
- Security response – incident management & response
The Key of security

- Perfect HW security?
- Application security?
- Full data encryption?
- Trusted User Interface?
- State-of-the-art usability?
- Operating system security?
- Access control systems?
- Connection (transport layer) security?
- Bug-free software?
- Perfect maintenance & service processes?
- Excellent user instructions?
- Reactive processes for vulnerabilities?
- SW update capability?
Matching security levels with product life cycle - the business case

How the competition works in the consumer product industry

Security, Time & Money

Product/SW/Service life cycle

Maximum level

Ideal level

Here is the “right” competition, based on skills and knowledge.

Never goes back to “zero” again.

The needed security level (effort) during the product lifecycle
• What is good usability? Is it ease of use? User engagement?
• Is usability about user awareness and education?
• If the user is involved in all security decisions, what is the impact?
• If the user is not involved in any security decisions, what is the impact then?

Who is in control? You? Or your system designer? The integrator?
Mobile malware status - Year 2009

The TOTAL CUMULATIVE AMOUNT over the last 10 years of mobile malware for all mobile platforms is around 500.

Note: According to F-Secure, they receive about 200,000 malware samples every day, out of which 500-6000 of them are real malware and a few thousand are completely new ones.

http://www.tietokone.fi/uutiset/hypponen_rikolliset_alkavat_iskea_windows_7_aan

What about year 2015? What about Android, Windows Phone or iOS?
• Many times, discussion points to the manufacturer or vendor of the system when there are challenges with security.
• Most ICT systems are designed for a great variety of uses.
• In many cases, a system integrator will manage system configuration, including the security policies.
• Or then, it is all just left for the end-user/user.
• Dedicated ("turnkey") systems are designed and configured for a specific purpose only.
• Many IT projects fail when systems are not specified for the correct purpose.

So, what actually is the weakest link?

Configuration and security ...
USA
Cyber Security, executive order, BYOD, ...

Europe
Certification, WP29 Opinion, ENISA, ...

China
Certification(s), law changes, standards

Where else?

What is going on...?
1. 3GPP (Telecomm & network security)
2. BSIMM (Security engineering management maturity)
3. CCSA (China Communications Standards Association)
4. Common Assurance Maturity Mode
5. DIGITALEUROPE Mobile SIG (Industry-level issues in mobile)
6. FIRST (Incident response)
7. Global Platform (Secure elements, smart cards)
8. GSMA SG (MNO security focused group)
9. ICASI (Protect the Internet)
10. Independent CERTs (Incident response)
11. ISF (IT Security focused forum)
12. ISO (International Organization for Standardization)
13. Mobey Forum (Mobile banking security)
14. NFC (Wireless Payments Security)
15. OMA (Content protection related security)
16. OpenGroup - Security Forum
17. OWASP (Internet application security)
18. PCI Forum (Payment industry compliance group)
19. SAFECode (SW Security)
20. TC260 (National Information Security Standards Association)
21. Trusted Computing Group (HW & Systems security)
22. VSIE (Information exchange)
23. W3C (XML security)
24. WAC (Application security)
25. ...

Why it is good to standardize security?
* How to ensure reasonable expectations towards SW security
* Fair and reasonable liability sharing between players
* Reasonable global harmonization of SW security (US, China, EU, …)
* Global harmonization of lawful interception-related issues
* Freedom of speech vs. control & protection of information assets
* How to limit the risk of "over-regulation" and keep the global markets functioning
* ...

"Security creates controls, controls create politics ..."
What do you sell if you sell product security?

* There is a variety of business opportunities depending on what approach one takes for the security. Do you want to give all of the control to the end-user, or do you want to keep all of the control to yourself, or something of both?

* Security is game of freedom of choice and responsibility. You cannot have one without the other. Also in real life ;-)
Interesting "reading":
http://www.bsimm.com
http://www.globalplatform.org
http://www.owasp.org
http://www.safecode.org
http://www.trustefcomputinggroup.org

Discussion

janne.uusilehto@nokia.com
Director, Head of Nokia Product Security