Anil Dhawan, Program Manager Rich Internet Applications – Windows Mobile
[anild@microsoft.com]

Geir Olsen, Program Manager – Security for Windows Mobile
[geiro@microsoft.com]
Microsoft Corp

SECURITY CHALLENGES FOR INTERNET TECHNOLOGIES ON MOBILE DEVICES

Windows Mobile

Key Questions

1. How are Web page scripts and Widgets different from “native” applications?
   - Deployment model
   - Programming model
   - Security model

Key Questions

2. What are the criteria for assessing trust?

Risk Factor	High Risk	Low Risk	Comment
Identity	Unverifiable	Verifiable	
Intent (publisher)	Undiscoverable	Discoverable	
Intent Discovery and Response (device)	Broad Access	Custom Sandbox	The risk is lower if device architecture can act on discoverable intent
Publisher Reputation	Low	High	
Publisher Title Reliability	Low	High	A publisher can distribute many solutions. While previous "reputability" measure is related to publisher directly. This measure is related to a particular title or solution.
Isolation	No Isolation	Isolated	This relates to the device's ability to isolate one publisher's solution from another
Revocation/ Blocking	No revocation/ blocking capabilities	Revocation and Blocking capabilities	

Key Questions

3. What are the key elements of risk management and mitigation?
4. How should code identity be securely issued, managed and verified?
5. How should intent of code be disclosed and discovered?
   - Declarative vs. run-time models

Key Questions

6. What does it mean to act on intent, reputation and reliability information?
   - Prompt based models
   - Least privilege environments
7. How should device capabilities be defined and discovered?
   - Verifiable Disclosure

Opportunities for Standards

1. Code Identity
2. Declarative Self-Disclosure of Security Capability Needs
3. Disclosure and Discovery of device capabilities
4. Risk assessment criteria
5. Risk level definitions and symbols
6. Risk Mitigation Approaches & Quality Standards