Malicious Threats on Handheld Operating Systems

Eric Chien
Symantec Security Response
Europe, Middle East, Africa

Agenda

- Background on handheld device operating systems
- Vectors of delivery
- Exploitable architecture
- Trojans, Viruses, Worms, Blended Threats
- Future Threat Potential
- Solutions

Background

- **Palm OS**
  - PDAs (Palm, Handspring)
  - PDA Phones (Kyocera, Palm)
- **Windows CE**
  - Windows CE Palmtops
  - Pocket PC PDAs
  - SmartPhone
  - Other Embedded Devices
- **Symbian OS**
  - PDAs (Psion)
  - Smartphones
  - UIQ

Vectors of Delivery

- **Syncing with a PC**
- **Peer to Peer Connectivity**
  - Bluetooth
  - Infrared
- **Telephony**
  - GSM
  - GPRS
  - UTMS
- **Network Connectivity**
  - WLAN (802.11)
  - PCMCIA Network Cards

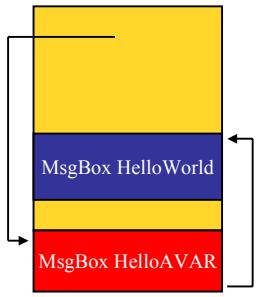
Exploitable Architecture – Access Control

- **Turn-on password**
- **Poorly implemented**
  - Password modifiable without knowledge of previous password
  - Password program replaceable
- **Demonstration**

Exploitable Architecture – File System

- **No or only rudimentary access control lists or attributes**
- **No multi-user support**
- **Files can be opened, read, and written to**
- **Classic virus is possible**
- **ROM protects system files from being infected**

Code Injection - Demonstration



Exploitable Architecture - Memory

- **Depends on operating system**
  - Single space (Palm OS)
  - Separate process space (virtual memory), but accessible via APIs (Windows CE)
  - Protected virtual memory (Symbian OS)
- **Modify other processes' memory**
- **Kill other processes**
- **No 'CreateRemoteThread' support**
- **Can extract ROM files**
- **Demonstration**

Programmability

- **Possible to redirect or substitute ROM system applications**
  - Demonstration
- **Hook system events**
  - Demonstration
- **Programmable Internet-enabled applications**
  - Email worms
  - Demonstration
- **Programmable Telephony applications**
  - Initiate and hook telephone calls
  - Indirect SMS worms
  - SMS backdoor trojans
  - Demonstration

Middleware Platforms

- **Java support**
  - J2ME
  - MIDP
- **Additional developer APIs and languages**
  - UIQ
  - Smartphone SDK
  - OPO
  - .NET/C#
- **OEM modifications**

Trojans, Viruses, Worms, Blended Threats

- **Trojans, viruses, worms, and blended threats are all possible**
- **Trojans**
  - Delete or modify data
  - Change configuration settings
  - Provide remote access via networking and telephony support
- **Viruses**
  - Programs modifiable
  - Resident or direct infectors
- **Worms**
  - Internet and telephony applications programmable
- **Blended Threats**
  - Exploits that cause denial of service (Nokia/SMS)

Trojans, Viruses, Worms, Blended Threats

- **Very few threats today**
  - Palm.Liberty.A, Palm.Vapor.A, Palm.MTXII.A
  - Palm.Phage.A
  - Symbian Joke programs

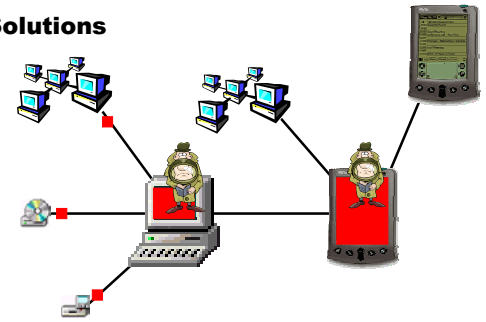
Potential Threat

- **Factors affecting current low threat danger**
  - Diversity
  - Low adoption rate (relative to PCs or 'dumb'-phones)
  - Lack of unsecure default functionality (listening services)
  - Hardware knowledge
- **Future threat**
  - Technology standardization (Microsoft?)
  - Adoption as a standard device (home and corporations)
  - Increased exchange of data (asymmetric -> symmetric)
  - Increased network and telephony connectivity (3G, WLAN)

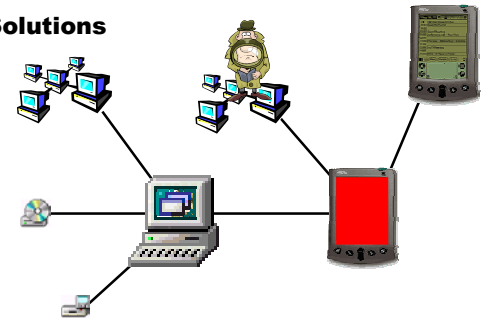
Solutions

- **On-device solutions**
- **Associated device solutions**
- **Signed code model**
- **Gateway solutions**

Solutions



Solutions



Summary

- **Devices are far from secure**
- **Low adoption rate and diversity make them low threat potential**
- **Threats are possible**
- **Only takes one infected device**
- **Corporations should standardize and employ policies**

Questions ?