Virusability of Modern Mobile Environments

Dr. Vesselin Bontchev, anti–virus researcher
FRISK Software International
Thverholt 18, IS–105 Reykjavik, Iceland

National Laboratory of Computer Virology
Bulgarian Academy of Sciences
Acad. G. Bontchev Str., bl. 2, BG–1113 Sofia, Bulgaria

E–mail: bontchev@complex.is

Outline

- Introduction
- Symbian S60 R3
- Windows Mobile 6.0
- J2ME
- Other Devices
- Conclusion

Symbian S60 R3

- Let's look at S60 R2 first
  - The most widespread mobile environment
  - Malware for it is becoming "a problem"
- Improvements in R3
  - Binary incompatible with R2
  - Symbian-signed packages only
    - Alas, this can be turned off
  - Cryptographically enforced policies
  - R2 is being aggressively phased out

Symbian S60 R3 – Continued

- The situation:
  - Spyware for R3 already exists. No viruses, though
  - Viruses for R3 are not impossible
    - A virus author might manage to get his virus signed
    - Vulnerabilities might be discovered
  - But *viruses* will not become a *problem* for R3
    - Didn't say that malware won't be
    - Cryptographic policy can't protect from social engineering tricks
    - The biggest security hole is between the chair and the keyboard

Windows Mobile 6.0

- Older versions are most vulnerable
  - Common vulnerabilities with desktop Windows
  - More difficult to patch
- Improvements in 6.0
  - Code signing
    - One-tier devices: signed applications can do anything, unsigned ones prompt the user once
    - Two-tier devices: cryptographic manifests, “dangerous” APIs not available to unsigned applications
    - But even unsigned applications can send SMS/MMS!

Windows Mobile 6.0 - Continued

- Other improvements:
  - safe SEH
  - secure C run-time libraries
  - separation of kernel and user space
  - WPA2 WiFi support
  - IPv6
  - improved process isolation
  - secure boot loader
  - hardware-supported security

Windows Mobile 6.0 - Conclusion

- This is the mobile platform, for which I am the least certain that viruses won't become a problem
- Security holes are easier to find
- Code signing enforcement is weaker
- Patches are difficult to distribute
- We'll have to wait and see

J2ME

- Very widespread – available even on devices with proprietary OSes
- Very powerful – file access, SMS/MMS, Bluetooth support, etc.
- Based on a very secure model
  - Every “dangerous” operation generates user prompt
  - Even users who make mistakes don’t like to be annoyed. ☺

J2ME - Conclusion

- Viruses are not impossible
  - Social engineering tricks tend to work (e.g., `RedBrowser`)
  - Server-based IM viruses are possible
  - Vulnerabilities in the security could be discovered
- But viruses are unlikely to become a *real* problem for this environment, ever
  - Non-replicating malware is much more likely

BlackBerry

- Uses the J2ME security model
- Uses code signing and cryptographically-enforced policies
  - But signatures are much easier to obtain than for Symbian
- "Dangerous" actions not available to unsigned applications
  - But TCP/IP and HTTP/WAP are
- The applications cannot be accessed through file system – i.e., parasitic infection is impossible

BlackBerry - Continued

- File transfer is possible only between paired devices – i.e., Bluetooth worms are possible but unlikely to become successful
- Phone calls cannot be made programmatically
- E-mail attachments do not support executable content
- Viruses (e.g., server-based IM worms) are not impossible but are unlikely to become a serious problem
  - Non-viral malware is more likely to be successful

Other Devices

- PalmOS
  - Covered elsewhere
- Sony PSP
  - Too small population
  - No significant software exchange
  - Proof-of-concept excluded, viruses are unlikely to become a problem for this environment
- iPod
  - Same as above, except the population is much bigger

Other Devices - Continued

- iPhone
  - Runs only Apple-authorized software
  - Only hobbyists who remove the built-in protection and/or install other OSes on it are at risk – and even that is minimal
  - Vulnerabilities could be discovered
  - Spim and Smishing are much more likely to be a problem than malware, let alone viruses

Conclusion

- *Viruses* are unlikely to become a *serious problem* for the modern mobile operating systems
- I didn't say that viruses for them are *impossible* – only that they won't become a problem. See the modern Office macro virus world
- I didn't say that *malware* for these environments won't be a problem, either – only that self-replicating malware won't be.

Questions?