Malware Detection and Prevention on Mobile Devices
Liang Xie, Sencun Zhu (collaboration with Samsung)

- **Cell phone Malware/Viruses**
  - Malicious programs that exploit vulnerabilities in cell-phone software and spread via MMS, Bluetooth, WiFi, ...

- **Attacking Strategies**
  - **Attack I**: Malware creates malicious process in a phone device and launch attacks, or
  - **Attack II**: Malware exploits internal software vulnerability (e.g., buffer over-flow) and launch attacks within current software framework
  - Both attacks cause leakage of private user information, unauthorized messaging, abnormal consumption of system resources ...

- **Real Cases**
  - more than 200 cell phone malware: *Cabir, Mabir, CommWarrior, ...*

---

**Demo Scenarios**

- **Attack I (without defense)**
  - Malware creates a malicious process which discloses content of addressbook to an external server. Meanwhile, it automatically generates unauthorized messages and randomly delivers the messages to users in addressbook.

- **Attack I (with SELinux defense)**
  - SELinux protection is launched to OMAP-5912 board. When malware creates a malicious process and accesses addressbook or other key system resources (e.g., socket, modem), SELinux denies such access and prevents the phone from being compromised.

- **Attack II**
  - Malware hijacks an existing user process (qtmail) in the phone to cause information leakage and unauthorized messaging.

---

**Demo of Cell-phone Malware Attack/Defense on OMAP-5912**

- **OMAP5912 Platform** *(a generic development platform for Windows CE, Linux, Symbian smart phones)*
  - **Hardware features**
    - Texas Instruments TMS320C55xx DSP core operating at 192 MHZ.
    - ARM926TEJ core operating at 192 MHZ, 32 Mbyte mobile DDR RAM, 32 Mbyte Flash ROM
  - **Software features**
    - OS: embedded Linux (customized kernel 2.6.20.4), u-boot-1.1.6, supporting QVLM module, USB
    - Trolltech Qtokia 4.2 Phone Edition, supporting messaging through email, SMS/MMS, Bluetooth

- **Demo Environment**

  ![Diagram of Demo Environment](image)

  - **Phones**
    - Serial port
    - Phone monitor
    - Malicious server
    - Victims

---

**Worms Like Wireless Phones, Too**

- **T. J. BURNHAM**
- [10:11 PM ET Tuesday, May 3, 2005]

  The malware is spreading like wildfire, spreading into many other platforms to exploit vulnerabilities in the software. The worm is able to spread from phone to phone, infecting other phones and causing damage. Once infected, the worm retrieves the address book and sends a malicious message to all the contacts listed in the address book. The worm spreads rapidly, infecting thousands of phones within a short period of time. The damage caused by the worm includes the loss of personal information, unauthorized access to the address book, and possible financial loss due to unauthorized transactions. The worm poses a significant threat to the security of wireless networks and the information stored on mobile devices.