Malicious Code & wireless networks

By: Brett Neilson
Overview

- Wireless technology, networks & devices
- Defining wireless threats
- Why malicious code will spread on wireless networks
- Economic impact & potential damages
- Protecting against malicious threats
Wireless technology & networks
What is wireless?

• Merriam Webster says:
  – Wireless: adjective
    1: Having no wire or wires

• Basic Components of a wireless system
  – Antenna
    • The conduit of sorts
  – Transmitter
    • Sends the RF
  – Receiver
    • Receives the RF
So who is using it?

- Everybody
  - TV / Radio / Satellite
  - Police / Fire / EMS
  - Cell Phones / Pagers
  - Building access cards
  - Automatic Toll Collection (Toll Tags)
Mobile Data Terminals (MDT)

- Very popular with Police and Fire
- Allows instant access to dispatcher data
- More secure???
  - Up until recently legal to monitor

- New features include
  - Live video monitoring
# Cellular Technologies

<table>
<thead>
<tr>
<th>1G (First Generation)</th>
<th>2G (Second Generation)</th>
</tr>
</thead>
<tbody>
<tr>
<td>- 1983 to present</td>
<td>- 1995 to present</td>
</tr>
<tr>
<td>- Analog cellular service</td>
<td>- Digital / PCS Services</td>
</tr>
<tr>
<td>- Voice only</td>
<td>- Data speeds (9.6 – 19Kbps)</td>
</tr>
<tr>
<td></td>
<td>- Text messaging</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>2.5G (Not quite 3G)</th>
<th>3G (Third Generation)</th>
</tr>
</thead>
<tbody>
<tr>
<td>- 2001 to present</td>
<td>- 2002 and beyond (In progress)</td>
</tr>
<tr>
<td>- Digital / PCS Services</td>
<td>- Data speeds (144+Kbps)</td>
</tr>
<tr>
<td>- Data speeds (56Kbps)</td>
<td>- Video and Audio</td>
</tr>
<tr>
<td>- Email messaging</td>
<td></td>
</tr>
</tbody>
</table>
## 802.11 Networks

<table>
<thead>
<tr>
<th>802.11</th>
<th>802.11a</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 to 2 Mbps</td>
<td>54 Mbps</td>
</tr>
<tr>
<td>2.4 GHz</td>
<td>5.15-5 GHz</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>802.11b</th>
<th>802.11g</th>
</tr>
</thead>
<tbody>
<tr>
<td>11 Mbps</td>
<td>20 Mbps</td>
</tr>
<tr>
<td>2.4 GHz</td>
<td>2.4 Ghz</td>
</tr>
</tbody>
</table>
Wireless Devices

- PDA
  - Palm & iPAQ
  - Strong Growth in 2000
    - Slowly shrinking thereafter
    - Renewed interest due to advances
    - New suppliers entering the market
- Converged Devices
  - PDA & Phone combined into one
  - All the features w/ all the connectivity
  - Designed for size not security
- Wireless (Security) Cameras
- RFID devices
Defining Wireless Threats
Defining the wireless threats

- WarDriving
  - Searching and Logging
- Data Snooping
  - Capturing data
- Jamming
  - Disrupting legitimate signals
- Insertion Attacks
  - Unauthorized clients and APs
Defining the wireless threats

- Malicious Code
  - Virus
    - A piece of code that can replicate itself
      - SMS - URLs & Attachments
  - Worm
    - A program that can copy itself to other disks
      - Masquerades as valid program
  - Trojan
    - A program that launches other programs or code
      - Masquerades as valid program
Emerging threats

- Liberty Trojan (PLAM) - September 2000
  - Deleted applications and was unable to replicate itself
- Timophonica (Spain) - January 2001
  - First automatic dialer
- 911 - April 2001
  - Caused phones to repeatedly dial 911
  - Sent to over 100,000 phones
- Flooder - August 2001
  - Sends unwanted SMS messages
- Phage & Vapor – September 2001
  - Deleted files and hid applications
Why Malicious Code will spread
Why Malicious Code will spread...

• In nature, viruses infect all organisms, even the tiniest bacteria.
  – Small Pox, Plague, SARS

• Likewise, computer viruses infect all platforms that reach a any level of sophistication.
  – Melissa, LoveBug, Klez
Four main factors

1) Protection is poor or non-existent
2) Power of new devices
3) Standardization of networks
4) Increased connection of devices
Protection is poor or non-existent

- Very little built in protection
  - Nokia 9000 series has malicious code protection
- Data transmissions are protected but unchecked
  - Currently no carrier has the ability to scan SMS or MMS delivery servers for malicious code.
  - Current security only offers limited protection and next to no scanning abilities
Power of new devices

- PDAs are now able to run PC like applications
  - Increased power means increased automation
    - Automation is often targeted by virus writers.
- Devices are often synchronized on a regular basis
  - Thus opening a door for the spread of malicious code
- Common language for developing apps
  - Makes it easier to create malicious code
Standardization of networks

- The more standard the easier malicious code will spread
  - Same as in the wired world
- Trend is moving away from proprietary standards and is focusing more on TCP/IP related standards
- Email messaging brought us Melissa and LuvBug
  - Standardized wireless networks are sure to do the same
Increased connection of devices

• More connectivity than ever
  – Bluetooth
  – WiFi 802.11
  – Cellular
• Allows for multiple ways to the internet and email
• Increased SMS/MMS popularity and exposure due to links and attachments
Economic Impact and Potential Damages
Damages

• Users receive unwanted messages
• Some devices send unwanted messages
• Data in devices is erased, deleted or stolen
• Device becomes unusable
• Network slowdowns (congestion)
• Network performance suffers
• Network intrusion
Impact

- Customer complaints
- Higher turnover from unhappy customers
- Cost from unwanted traffic
  - May not be just dollars
- Dropped calls
- Un-infecting or cleaning devices & servers/network
- Purchasing new technology
So what's the financial impact?

![Financial Impact Chart]

- 2003: 43
- 2004: 212
- 2005: 471

Millions
So what needs to be done?
Protecting against malicious threats

• Protection must be implemented at every point possible
  – Devices, Switches, Towers, COs, etc.
• Mobile operators need to start offering scanning services to their clients and need to start scanning their servers and data streams.
• Delivering a solution now rather than latter could save millions of dollars in lost revenue and expenses.
  – AV Vendors need to start step up to the plate
• Mobile operators and device manufactures need to have plans for addressing thousands if not millions of simultaneous infections on their networks.
Conclusion

- Top four reasons malicious code will spread
  1. Current protection of wireless networks/devices is minimal
  2. Increased computing power
  3. Standardization
  4. Growing connectivity

- Not changing security could result in large economic losses
  - $471 Million per 5 Million users estimated for 2005

- Mobile Operators, Administrators, Manufactures and Developers should act now and think proactively in an effort to better protect their systems.
Thank you…

Brett Neilson

defcon@brettneilson.com