Advantages of Firmware Over the Air (FOTA) for Mobile Security

Gene Wang
Chairman, OTA Flash Forum
CEO, Bitfone Corporation
First, a Quiz:

Q: What are paraskevidekatriaphobics?
A: People afflicted with a morbid, irrational fear of Friday the 13th

Q: What percent of Americans suffer from this condition?
A: 8%

Q: What do these notorious killers have in common?
   Jack the Ripper, Charles Manson, Jeffrey Dahmer, Theodore Bundy and Albert De Salvo
A: 13 characters in their names
What is OTAFF?

- A “safe” acronym for a 13-letter name!
- Special Interest Group focused on OTA device management
- Founded in June 2003, now 32 members
- Submits recommendations to OMA
  - Firmware Update Mgmt Object (FUMO)
- Publishes “best practice” white papers:
  - FOTA Interoperability
  - End-to-end FOTA Security
- FOTA Security & Mobile Security are 2 of the 4 Top Priorities in 2005
- www.otaflashforum.org
Reviewing Intruder Capabilities

- **Eavesdropping** - intruder picks up signals and data connections associated with other users; requires a *modified MS*

- **Impersonation of a user** - intruder sends signal and/or user data to the network, which interprets data as originating from a target user; requires a *modified MS*

- **Impersonation of the network** - intruder sends signal and/or user data to a target user, who interprets the data as originating from a genuine network; requires a modified *BS*.

- **Man-in-the-middle** - intruder places itself in between a target user and a genuine network and has the ability to eavesdrop, modify, delete, re-order, replay, and spoof signals and user data messages exchanged between the two parties; requires modified *BS in conjunction with a modified MS*.

- **Compromised authentication vectors in the network** - intruder possesses a *compromised authentication vector*, which may include challenge/response pairs, cipher keys and integrity keys. This data may have been obtained by compromising network nodes or by intercepting signal messages on network links.

  Ref: *3G TR 33.900 V1.2.0 (2000-01) 8 3G TR 33.900 version 1.2.0*
Types of Device Threats

- **Viruses**
  - Self replicating and causing damage, but requires some user action to be triggered (e.g. executable email attachment)

- **Worms**
  - Virus variant that infects without any user interaction

- **Trojans**
  - Malicious code hidden within innocuous code or data; can be distributed with viruses

- **Spyware / adware**
  - Program that secretly gathers information and relays it to other interested parties

- **Dialers**
  - Program that dials / establishes connections without user’s permission

- **Blended threats**
  - Hybrids combining the characteristics of the above
How can FOTA Help?

Restrictions Today:
• Updating core software - OS, menus, drivers, or flex files - requires special, cable-based equipment
• No way to identify rogue software or enforce a predefined software configuration
• No way to identify devices that have been compromised or are at risk (vulnerable)
• No easy way to proliferate security updates to appropriate devices in bulk

FOTA allows operators to:
• Wirelessly update core firmware: radio/sw stacks, menus, gaming platforms, etc.
• Manage sensitive system files: device credentials, security policies, virus signature files, etc
• Identify devices with particular software/hardware configurations for mass updating
FOTA Process

1. Create Update Packages
   - Firmware Version 1
   - Firmware Version 2
   - Update Package Generator (OEM)

2. Upload to repository
   - Update Package
   - FOTA mgmt server (Operator)
   - FOTA delivery server (Operator)

3. Operator “Push” to device(s) or Subscriber “Pull” via handset or self-care portal
   - Embedded OMA-DM agent (download)
   - Embedded FOTA agent (update)
   - Subscriber’s device

4. Verify Update
5. Install, Reflash
6. Report Status
FOTA Security Framework

- Update package is encrypted and/or signed: SHA-X, public key infrastructure (PKI), or other algorithms
- Transport Layer and DRM can be leveraged
FOTA Security Framework

- Update package generator runs in OEM’s environment
- Update package embeds credentials for authentication by device
- Device update agent is part of core firmware and runs in protected mode
- Framework allow additional, customizable levels of authentication:
  - Prevent update package replay
  - Leverage device unique credentials to bind it to a unique device (e.g. IMEI, CPU key, etc.)
  - Leverage user unique credentials to bind it to a specific subscriber (e.g. SIM stored key)
Device Integrity through FOTA

- OEM / Operators can provide software updates and upgrades with complete security
- Users, particularly corporate users, can securely receive update of sensitive system files such as core application parameters, virus signature updates, etc.
- Service providers can encompass network and service security changes transparently to end users (e.g. manage credentials and security policies)
- If device is corrupted, device software can be reset to a known state (file system & firmware update)
Threat Detection Scenario

1) Remote virus detection through OTA profiling and virus scanning

2) Unresolved issues are "flagged" and exported for expert analysis.

3) Analysis to identify new threat. Create anti-virus update to protect from new threat.

External sources of threat intelligence

Customer Care DB

Rule Engine detects outdated virus definition files and suspicious files or programs.

Virus Analysis System

Profiling Agent

Security Agent

Device Data
Example – CSR Interface

### Device Details

<table>
<thead>
<tr>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SmartCare Agent</td>
<td>9.1.0</td>
</tr>
<tr>
<td>Version</td>
<td></td>
</tr>
<tr>
<td>SmartCare Agent UID</td>
<td>0x101FF52F</td>
</tr>
<tr>
<td>Platform</td>
<td>Symbian UIQ v7.0</td>
</tr>
<tr>
<td>Manufacturer</td>
<td>SONY ERICSSON</td>
</tr>
<tr>
<td>Model</td>
<td>1021011-CN</td>
</tr>
<tr>
<td>Device Revision</td>
<td>R3C006 CXC162022</td>
</tr>
<tr>
<td>OEM Info</td>
<td>270512814</td>
</tr>
<tr>
<td>Device Family</td>
<td>Quartz</td>
</tr>
<tr>
<td>CPU Speed</td>
<td>152 MHz</td>
</tr>
<tr>
<td>Processor Level</td>
<td>THUMB</td>
</tr>
<tr>
<td>Processor Revision</td>
<td>1</td>
</tr>
<tr>
<td>IMEI</td>
<td>350433-02-312333-6</td>
</tr>
<tr>
<td>Backlight Enabled</td>
<td>No</td>
</tr>
<tr>
<td>Backlight State</td>
<td>Off</td>
</tr>
<tr>
<td>Horizontal Resolution</td>
<td>208 lines</td>
</tr>
<tr>
<td>Resolution</td>
<td>320 lines</td>
</tr>
<tr>
<td>Number of Colors</td>
<td>65536 colors</td>
</tr>
<tr>
<td>OS Major Version</td>
<td>1</td>
</tr>
</tbody>
</table>

### Device Settings

<table>
<thead>
<tr>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Software List</td>
<td></td>
</tr>
<tr>
<td>Dictionary</td>
<td></td>
</tr>
<tr>
<td>Application Status</td>
<td>Not Running</td>
</tr>
<tr>
<td>Viewer</td>
<td></td>
</tr>
<tr>
<td>Application Status</td>
<td>Not Running</td>
</tr>
<tr>
<td>Contacts</td>
<td></td>
</tr>
<tr>
<td>Application Status</td>
<td>Not Running</td>
</tr>
<tr>
<td>Cabir</td>
<td></td>
</tr>
<tr>
<td>Application Status</td>
<td>Running</td>
</tr>
</tbody>
</table>

*Microsoft Internet Explorer*

Application Name:
Actual: [Cabir]
Expected: [Cabir]

Msg: Virus Alert - Bluetooth Virus Cabir found

OK
Threat Resolution Scenario

1) New virus file is uploaded to authoring tool

2) New rules added to Customer Care DB to detect new virus symptoms and check latest anti-virus versions.

3) Critical updates can be pushed to many devices using DM Server; may include FOTA operation

4) DM server redirects to anti-virus authoring tool for download of anti-virus updates.

External sources of threat intelligence

Customer Care DB

Update Notification

Anti-virus version info and new rule

Virus Analysis System

New Virus File

Anti-virus authoring tool and DB

Update Download

DM Server

DM Agent

FOTA Agent

Security Agent

OTAFlashForum
Refresh the Mobile World

13
Summary

- FOTA is a proven and commercialized technology
  - Fault-tolerant and efficient
  - Standardized & interoperable; backed by OMA, OTA Flash Forum
  - Customizable security framework based on proven security standards and technologies
- FOTA enables “down-to-the-metal” threat resolution
  - Low-level security holes plugged via FOTA reflash
  - Integration with DM server enables proactive scans and scheduled virus updates
- Manage threats for targeted subscriber groups
  - Bulk push enables high volume updates
  - DM database enables selective push updates for “premium service” subscribers
About Bitfone

- Domain Expertise:
  - Pioneered Firmware Over-the-Air (FOTA)
  - Handset architectures and OMA-DM Interoperability
  - Automated customer care and remote diagnostics
  - Carrier-grade systems and analytics engine development
- Customers: Motorola, LG, QUALCOMM, Sony Ericsson, SK Telecom, UTStarcom (CDMA)
- Key Partners: IBM, HP, LogicaCMG, Gemplus, PalmSource, WDSGlobal, McAfee
- Solutions: mProve, MVP, SmartCare

Find it. Fix it. Enhance it.