

# Mobile Phone Messaging Anti-Forensics

BlackHat USA 2008



• Presented by:

Zane Lackey ([zane@isecpartners.com](mailto:zane@isecpartners.com))

Luis Miras ([luis@ringzero.net](mailto:luis@ringzero.net))

iSEC Partners

<https://www.isecpartners.com>

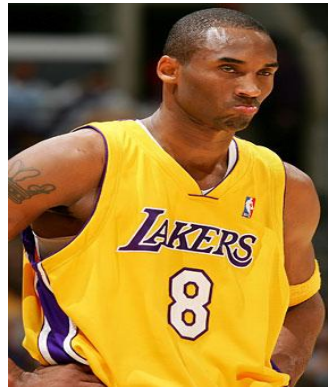
iSEC  
PARTNERS

# Agenda

- **Introduction**
- **SMS Background**
- **Evasion Attacks**
- **Attacking Mobile Forensics Software**
- **Demo**
- **Tools**
- **Q&A**

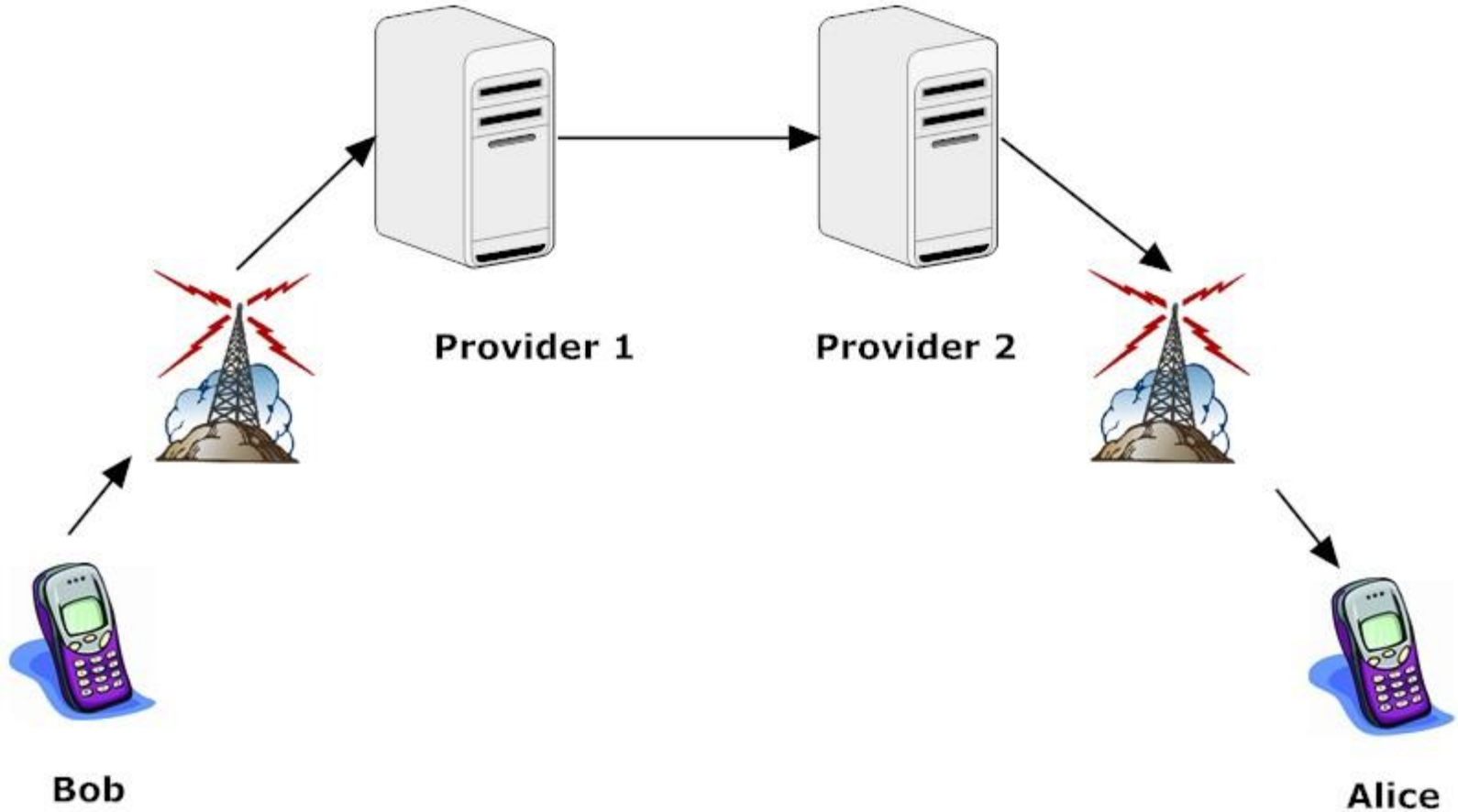
# Introduction

- **Why listen to this talk?**
  - SMS messages are increasing being used as evidence<sup>1</sup> in investigations:



- Rapidly emerging field
- Security issues largely unexplored

# SMS Background



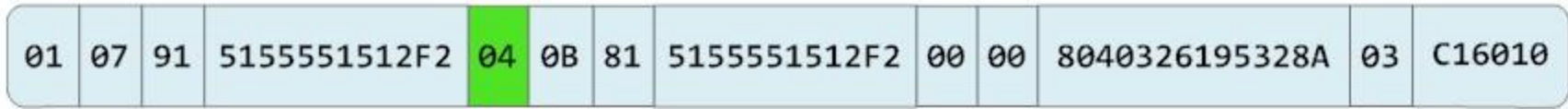
# SMS Background

- **SMS messages stored on SIM or phone**
  - Interested in SIM
- **SMS as umbrella term that can mean one of several types of messages**
  - SMS
  - MMS
  - EMS
  - Others

# SMS Background

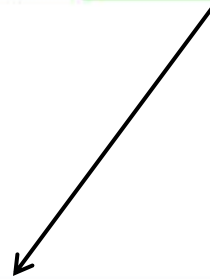
|    |    |    |              |    |    |    |              |    |    |                |    |        |
|----|----|----|--------------|----|----|----|--------------|----|----|----------------|----|--------|
| 01 | 07 | 91 | 5155551512F2 | 04 | 0B | 81 | 5155551512F2 | 00 | 00 | 8040326195328A | 03 | C16010 |
|----|----|----|--------------|----|----|----|--------------|----|----|----------------|----|--------|

# SMS Background



# SMS Background

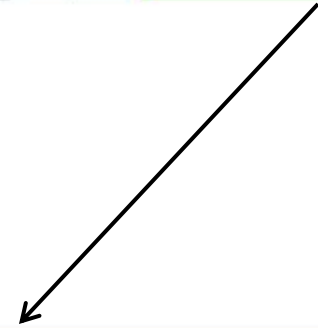
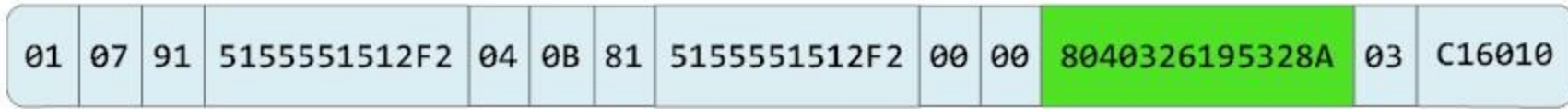
|    |    |    |              |    |    |    |              |    |    |                |    |        |
|----|----|----|--------------|----|----|----|--------------|----|----|----------------|----|--------|
| 01 | 07 | 91 | 5155551512F2 | 04 | 0B | 81 | 5155551512F2 | 00 | 00 | 8040326195328A | 03 | C16010 |
|----|----|----|--------------|----|----|----|--------------|----|----|----------------|----|--------|



5155551512F2

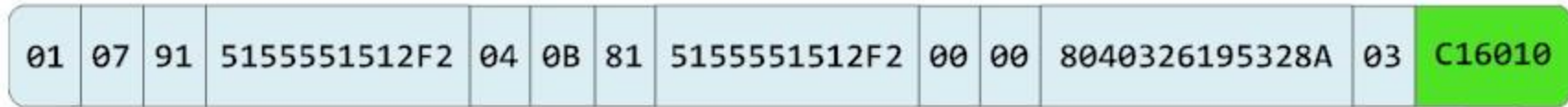


# SMS Background



8040326195328A

# SMS Background



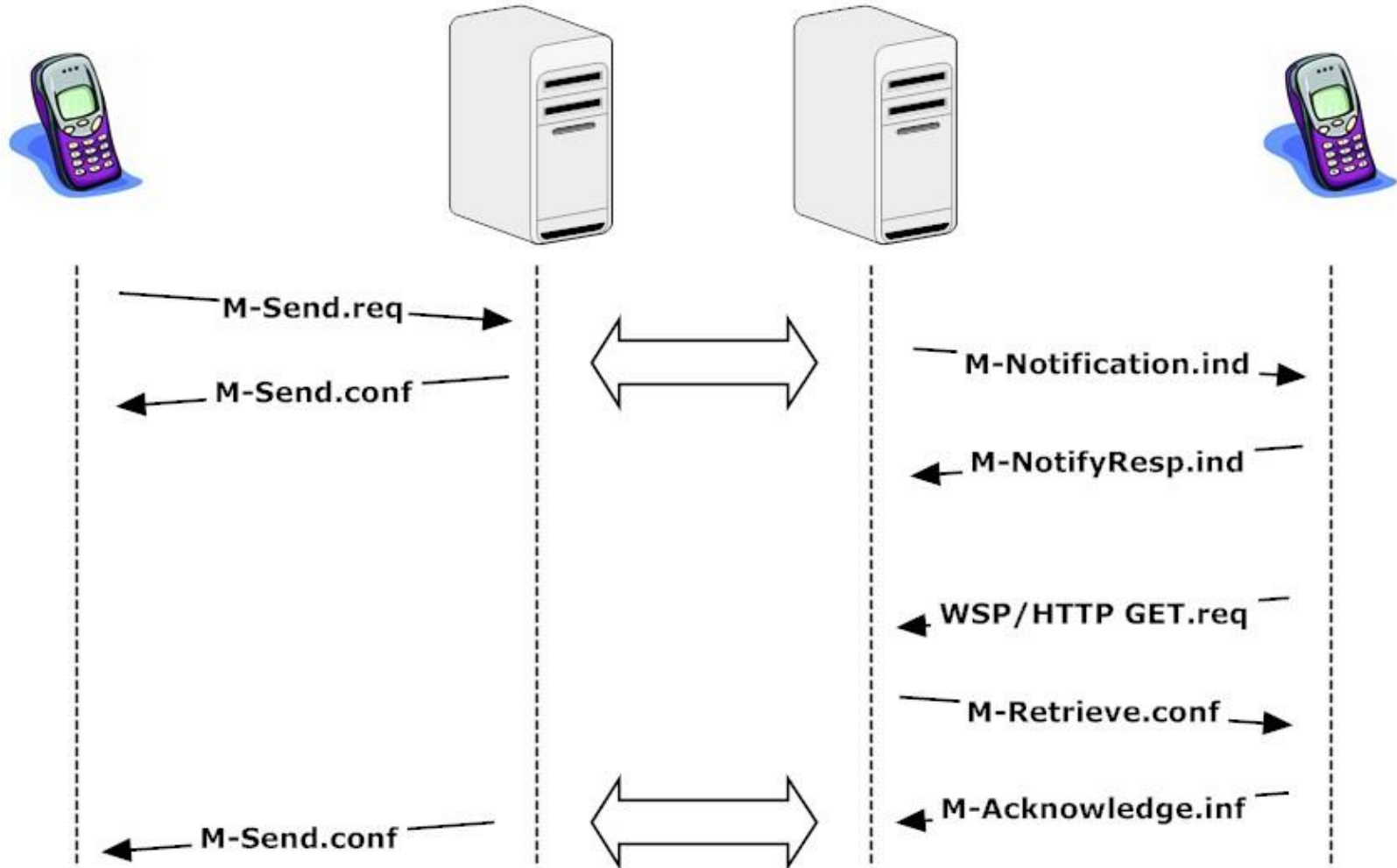
# Messages We're Discussing Today

- **Basic messages**
  - DELIVER
  - SUBMIT
- **Multimedia Messages (MMS)**
- **Network Originated Messages**
  
- **What we're not covering:**
  - EMS
    - Ringtones
    - Simple Pictures (backgrounds)
  - Concatenated Messages

# Evasion Attacks

- **Focus on ways to make forensics tools miss messages during acquisition of SIM/phone**
- **Why not just encrypt?**
  - Attackers will likely do that too!
  - Why not hide the message as well?
  - Why not hide parts of encrypted message?
- **Two methods we'll discuss today:**
  - Network originated messages
  - UCS-2 Byte Order Mark

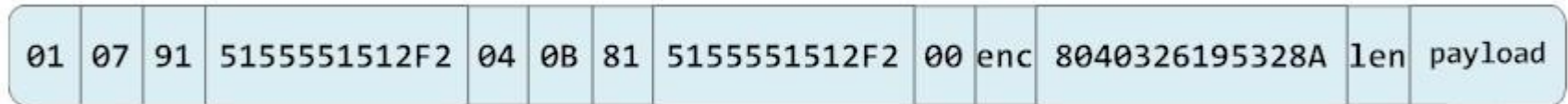
# Evasion Attacks – Network originated messages



# Evasion Attacks – Network originated messages

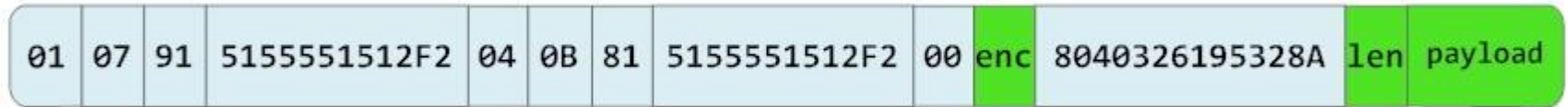
- **Messages designed to be generated from MMS proxy**
  - MMS proxy controlled by network provider
- **Initial research shows handsets can send these messages**
- **These messages can still contain a normal payload worth of data**
- **Tested forensics software ignores these messages**
  - Either displays a blank message body or no message at all

# Evasion Attacks - Encoding



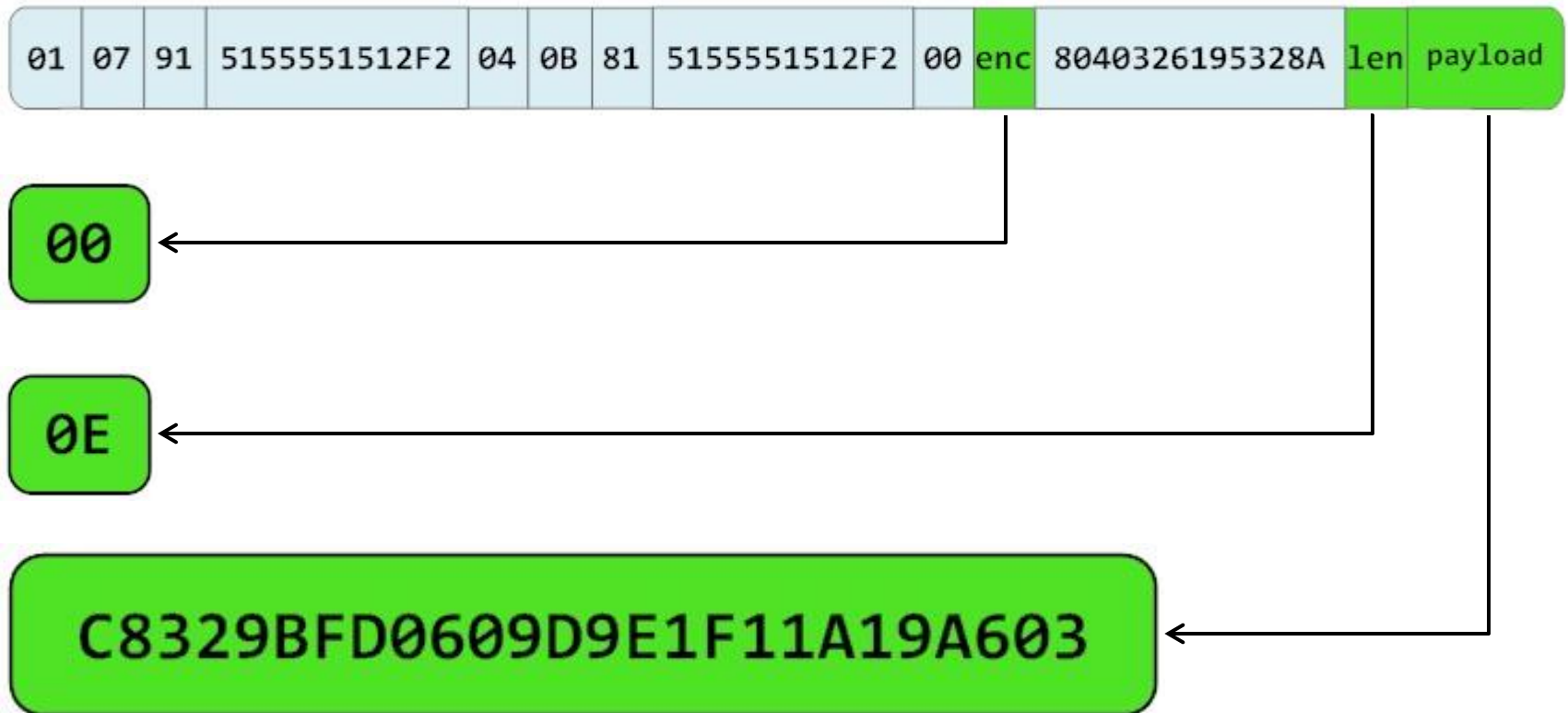
- **Three normal types of encoding:**
  - GSM 7bit
  - ASCII 8bit
  - UCS-2 16bit

# Encoding



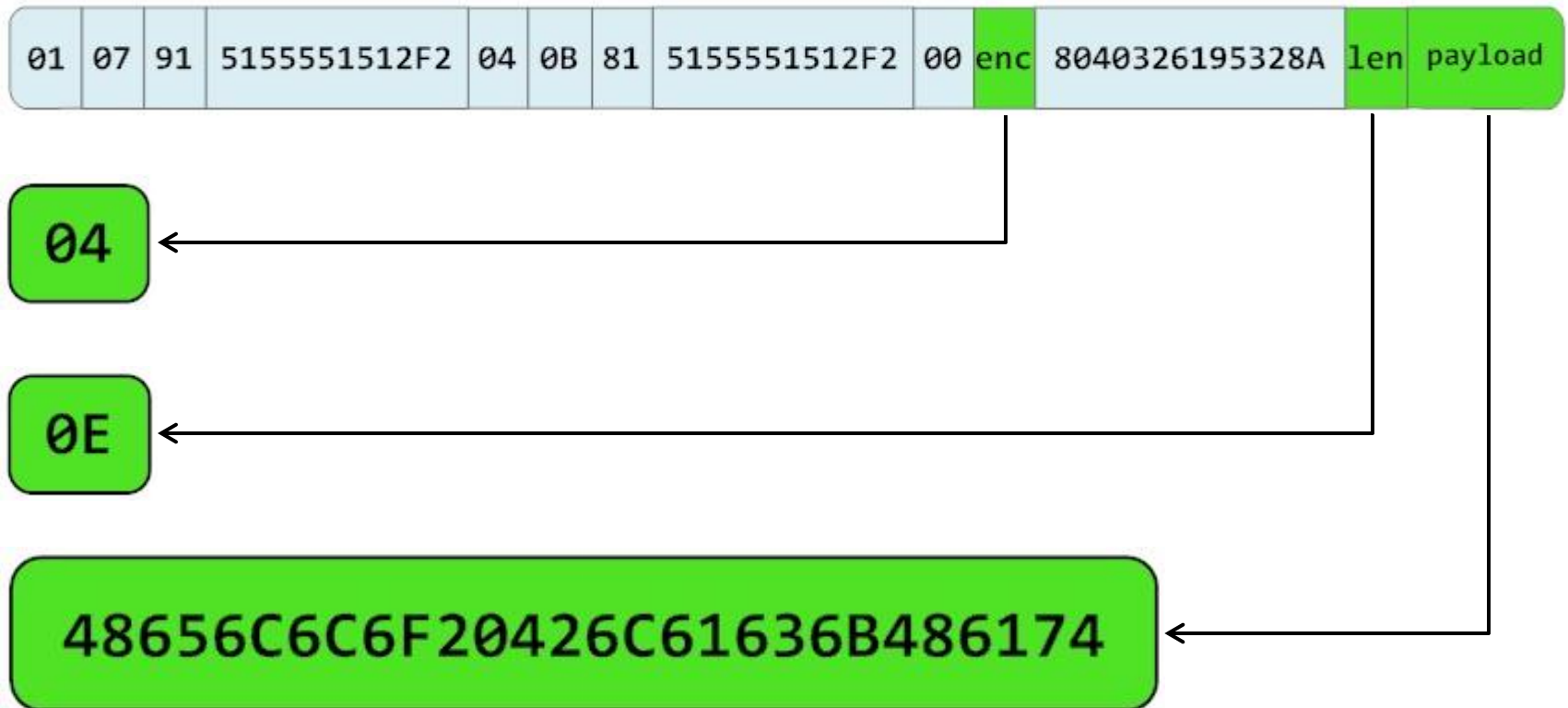


# Encoding – GSM 7 bit



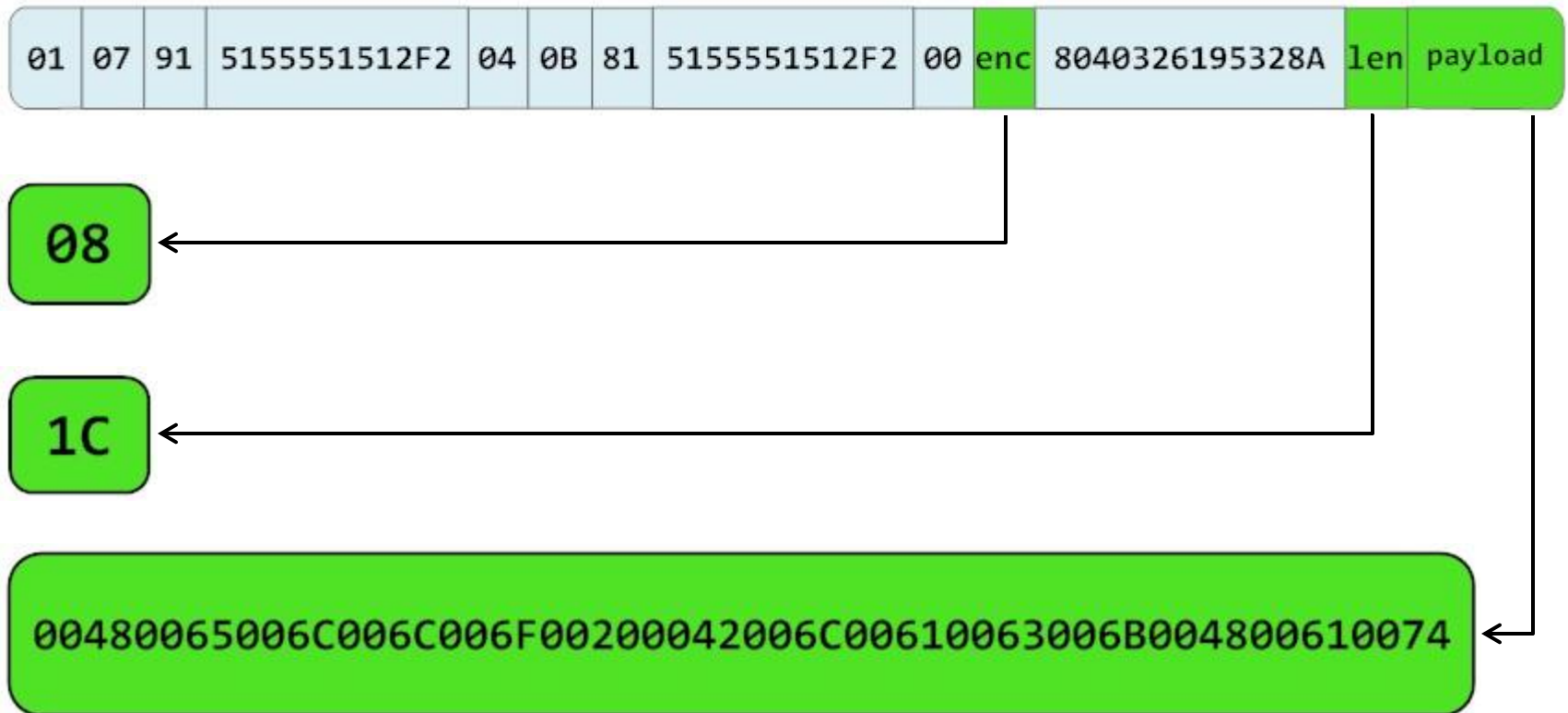
“Hello BlackHat”

# Encoding – ASCII 8 bit



“Hello BlackHat”

# Encoding – UCS2 16 bit



“Hello BlackHat”

# Evasion Attacks - Encoding

- **UCS-2 similar to UTF-16**
- **UCS-2 and UTF-16 allow definition of endianness**
  - Via Byte Order Mark (BOM)<sup>2</sup>
- **All observed traffic follows big endianness**
  - Tested forensics software assumes big endianness
  - Flipping endianness results in improperly interpreted messages

# Attacking Forensics Software

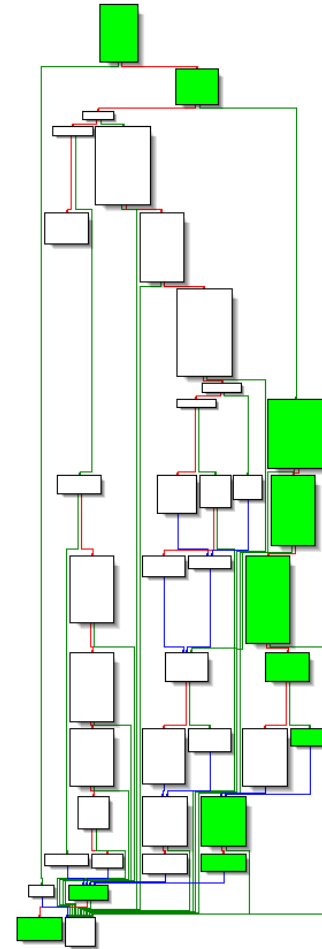
- **As with any software doing complex parsing, implementation flaws will exist**
- **Focus on attacking the forensics tools themselves to make them crash or execute arbitrary code when performing an acquisition of a hostile SIM/phone**

# Attacking Forensics Software

- **Similar to auditing for file format vulnerabilities**
  - Length fields
  - Encoding/decoding problems
  - Flags/bitmasks
  - Signed/unsigned issues
- **Messaging specific**
  - Bitmask header values
  - Length fields
  - UDH fields

# Attacking Forensics Software

- **Parser runtime analysis**
- **Many options available**
  - Paimei/pydbg
  - IDA code coverage plugin
  - Custom scripts
- **Using python scripts**
  - Idapython
  - Immunity Debugger



# Attacking Forensics Software

- **Challenges**
  - Rudimentary tools on phones
  - Fuzzing on SIM is impractical
  - Sending raw SMS data requires custom hardware/software
    - “raw socket”
  - Vendor inconsistencies
    - Data stores
    - Interfaces
  - Error detection
    - Point of failure
  - Data hiding requires manual verification



# DEMO

# Testing Environment



# Testing Environment

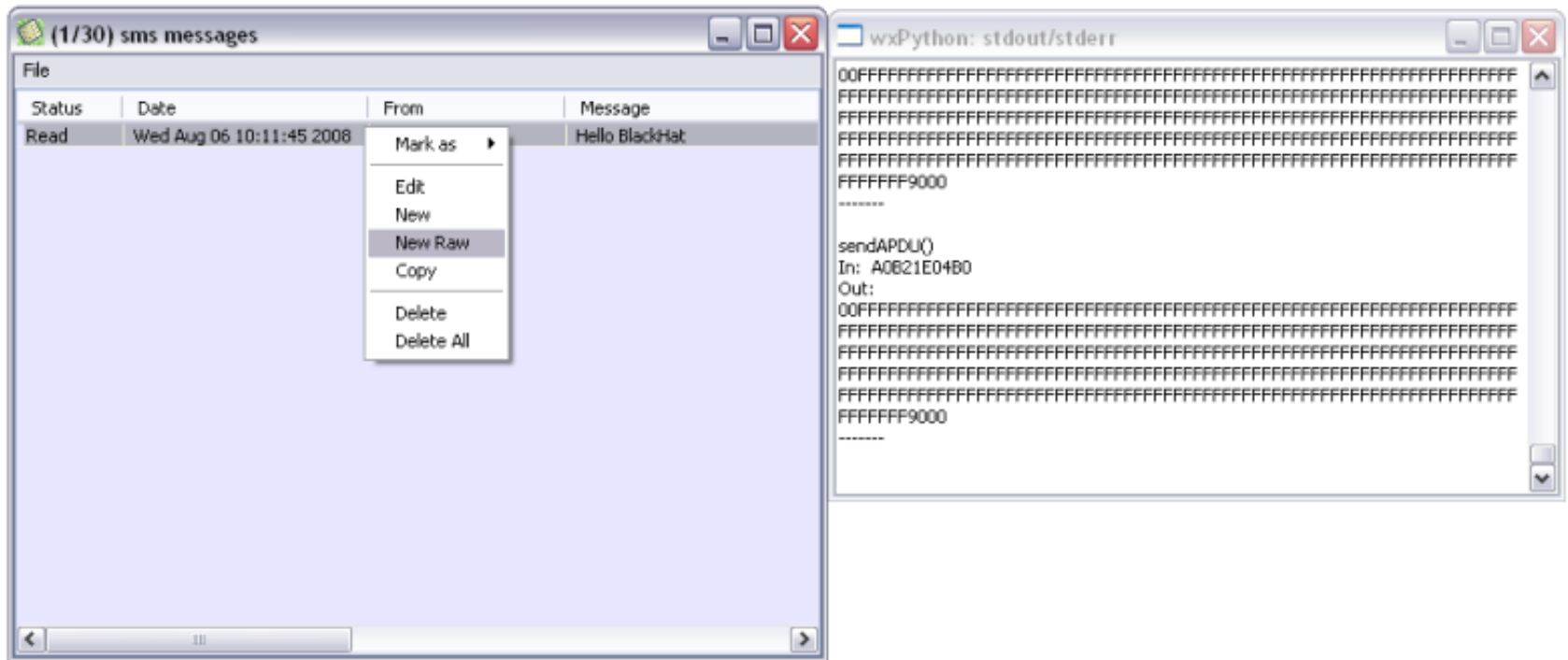


ACS ACR38T ~\$30 <http://www.txsystems.com/acs.html>

# Testing Environment



# Testing Environment



<http://www.isecpartners.com/tools.html>

# Q&A

- **Thanks for coming!**
  
- **We are always looking for a few good geeks!**

[careers@isecpartners.com](mailto:careers@isecpartners.com)

# 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

- **SMS fuzzing tools**

- Are (unfortunately) essentially useless when doing the sort of testing discussed in this talk, due to:
  - Small capacity of SIMs (usually ~30 messages)
  - Necessity of human involvement when looking for errors
- Early in testing we developed a basic SMS fuzzer with the Peach framework, discarded it in favor of targeted test cases with PySimReader

- **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](http://mobileforensics.files.wordpress.com/2007/06/understanding_sms.pdf)

- **Prior Research:**

- [http://www.mulliner.org/pocketpc/feed/CollinMulliner\\_syscan07\\_pocketpcmms.pdf](http://www.mulliner.org/pocketpc/feed/CollinMulliner_syscan07_pocketpcmms.pdf)