Transparent Botnet Command and Control for Smartphones over Text Messages

Georgia Weidman

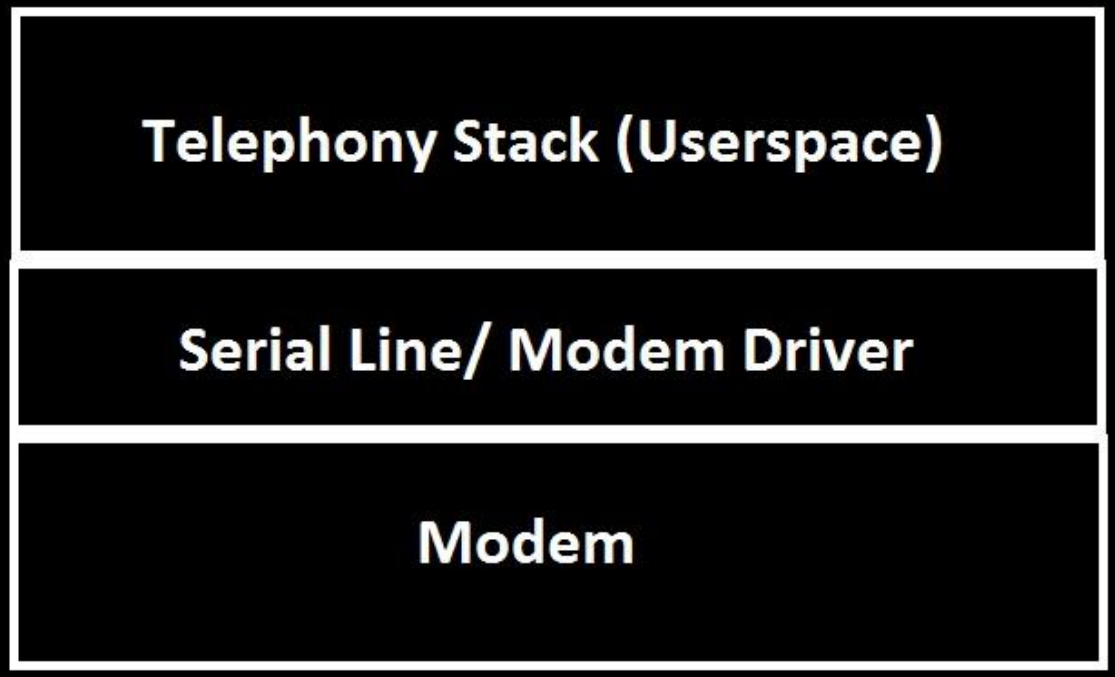
Why Smartphone Botnets

- Ubiquitous smartphones
- Common development platforms
- Strong technical specs

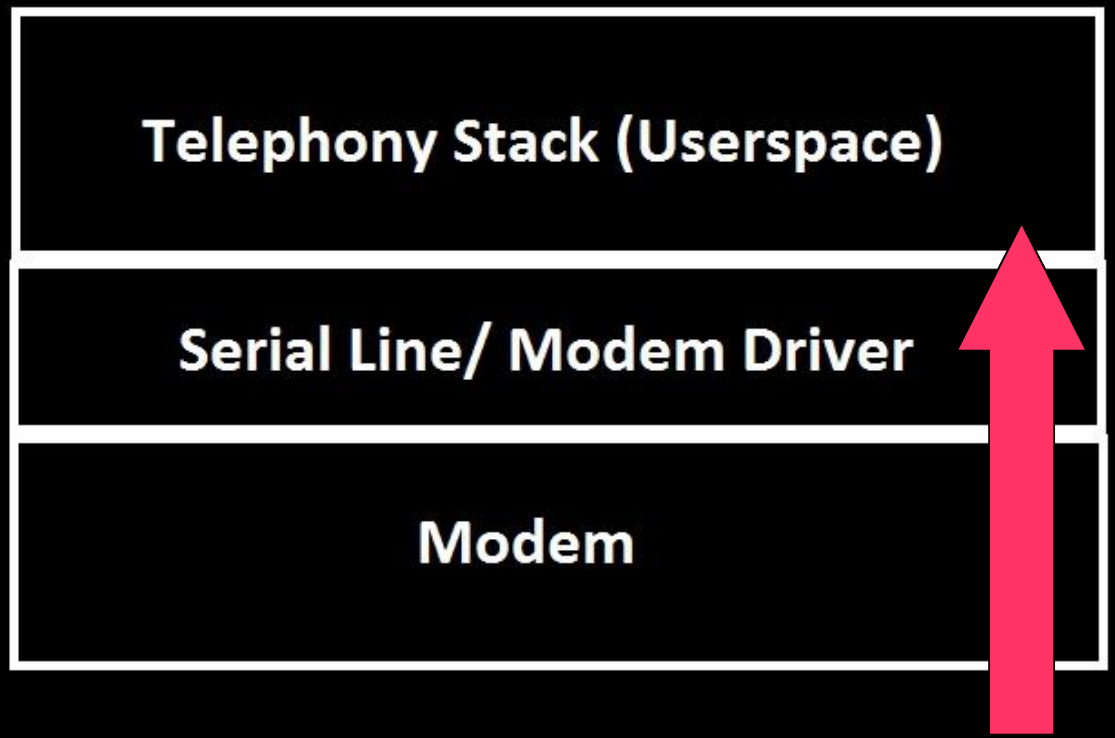
Why Text Messages?

- Battery managements
- Difficult to monitor
- Fault Tolerant

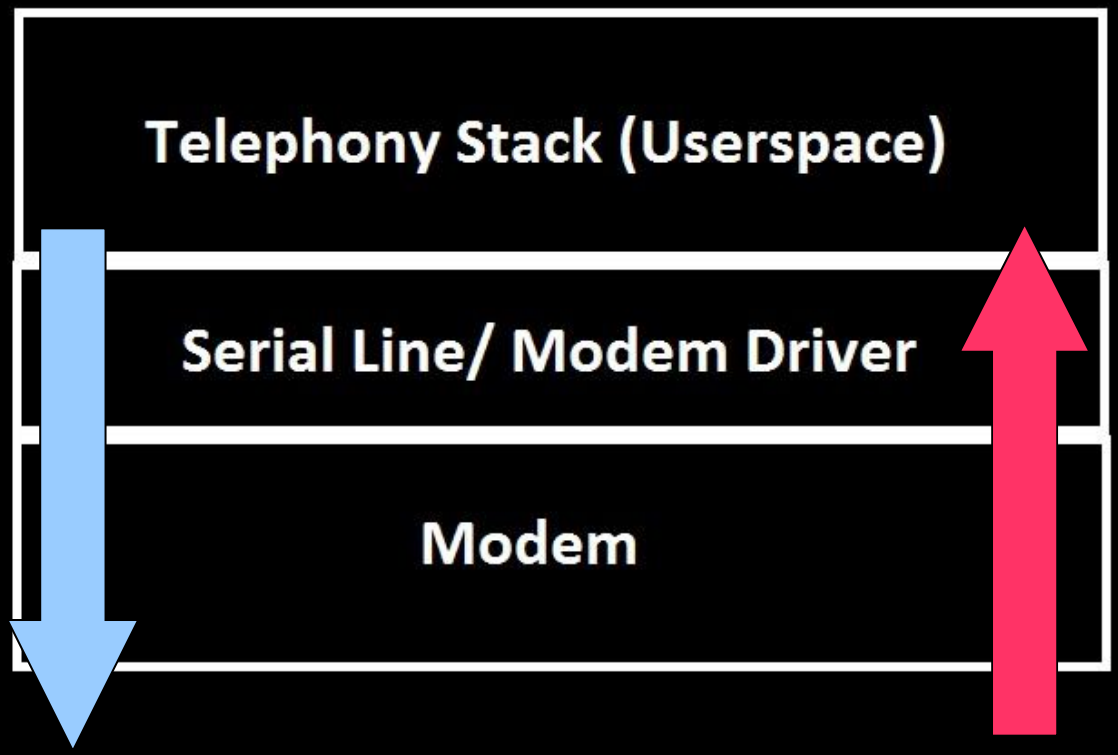
How an SMS is sent and received



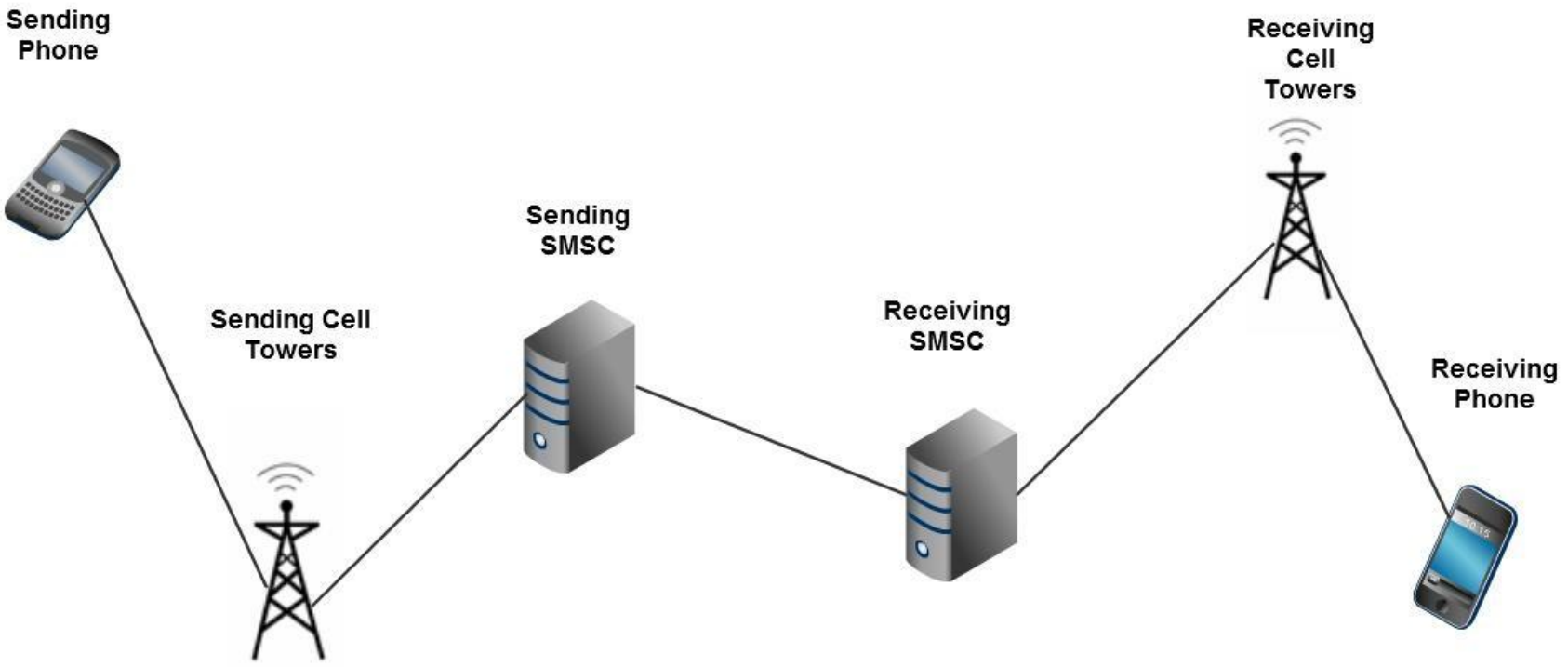
How an SMS is sent and received



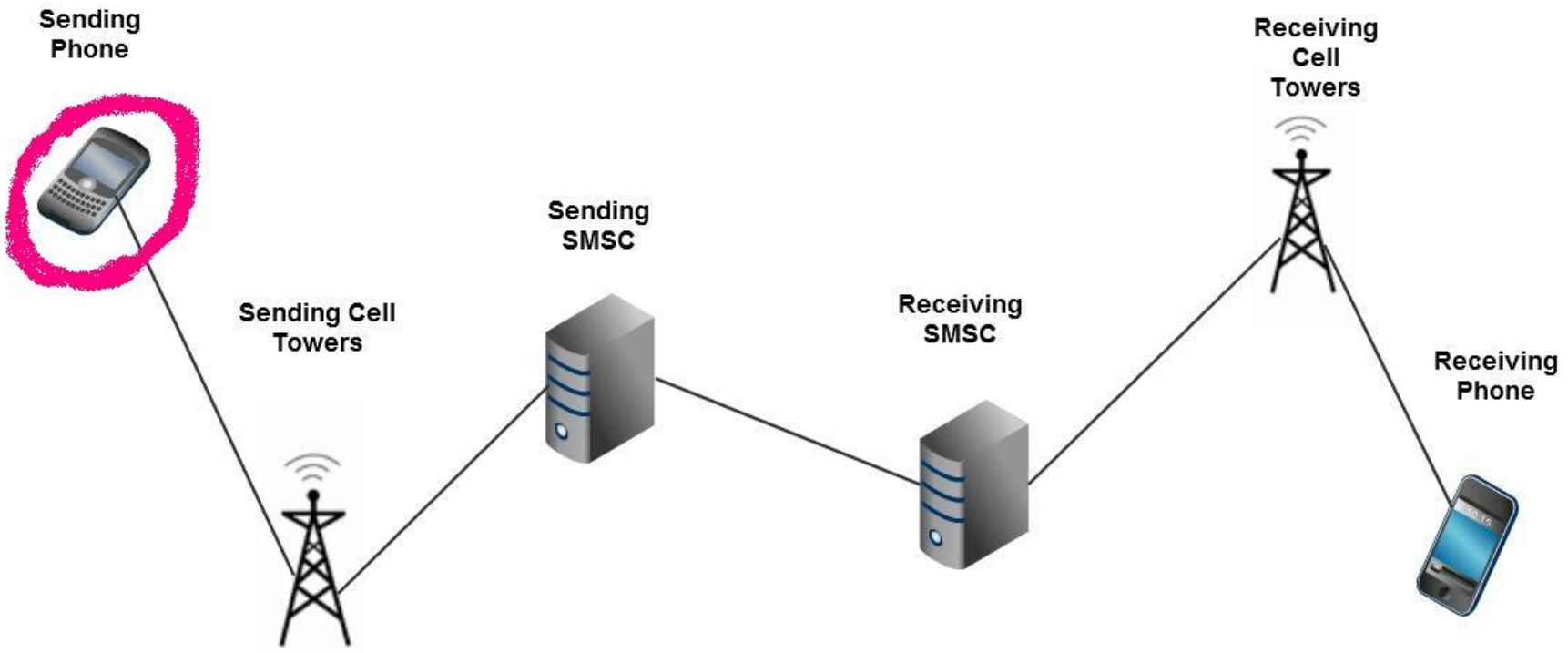
How an SMS is sent and received



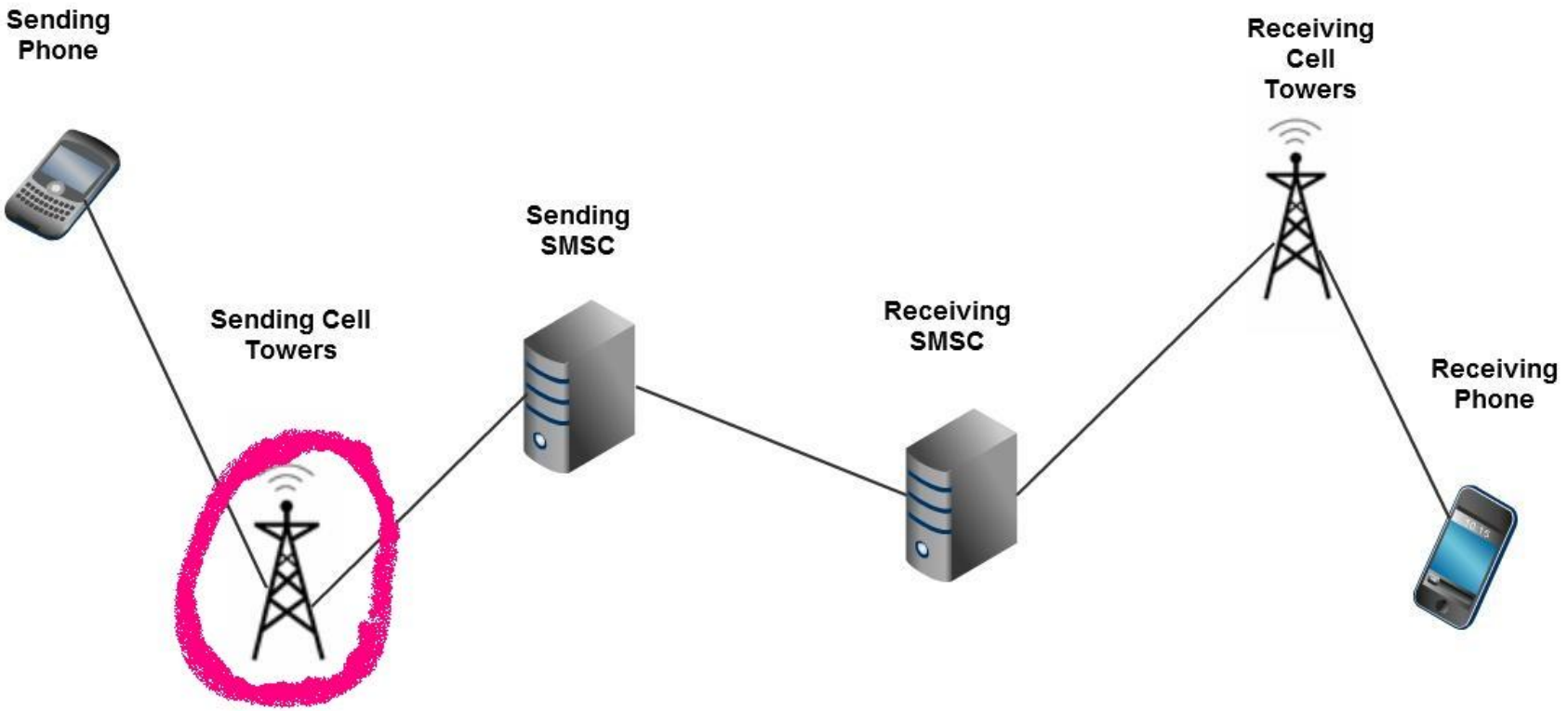
How an SMS is sent and received



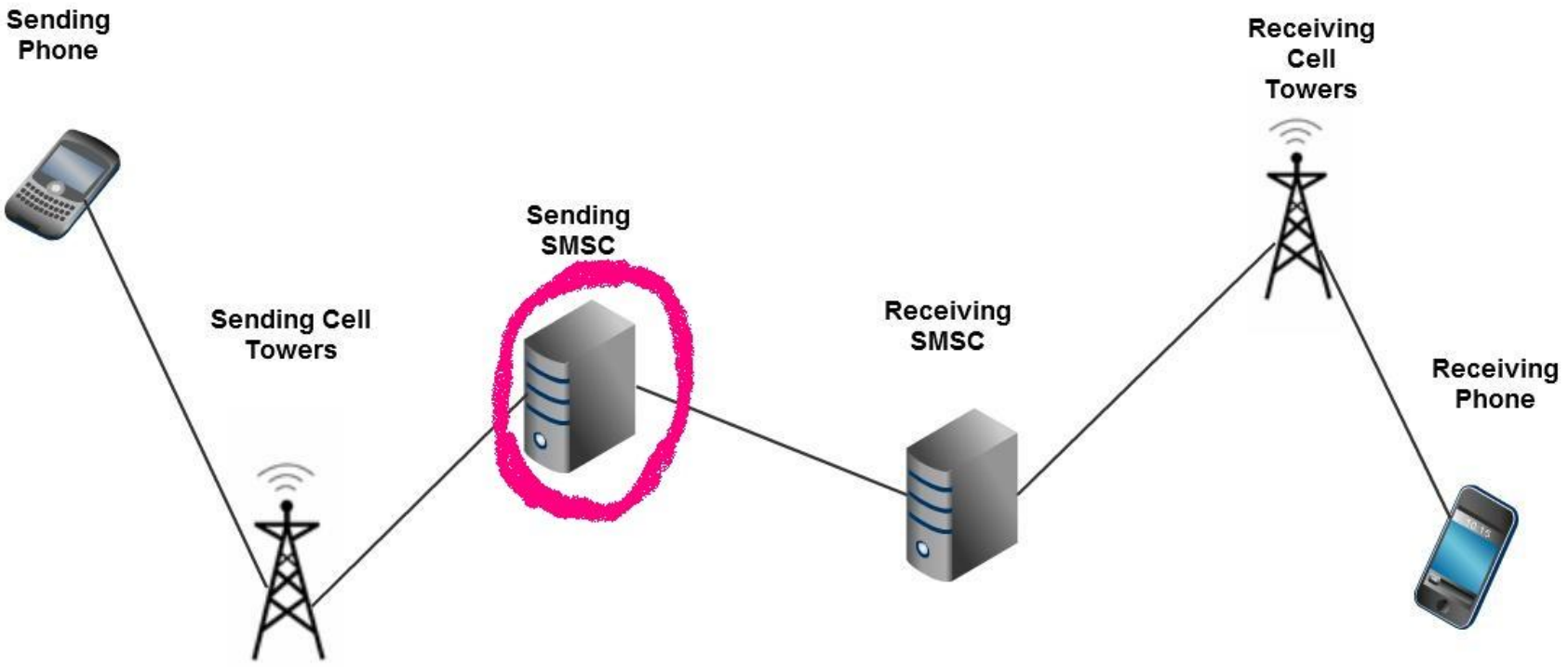
How an SMS is sent and received



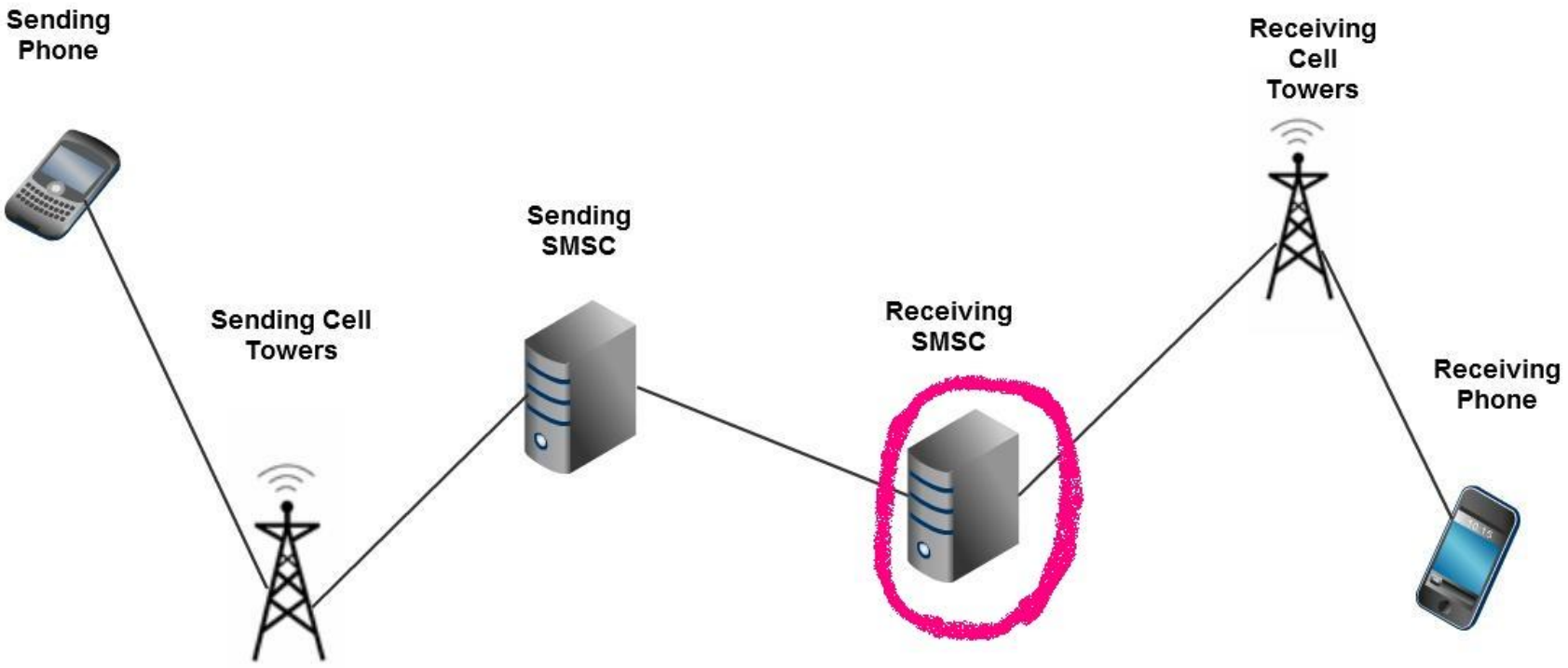
How an SMS is sent and received



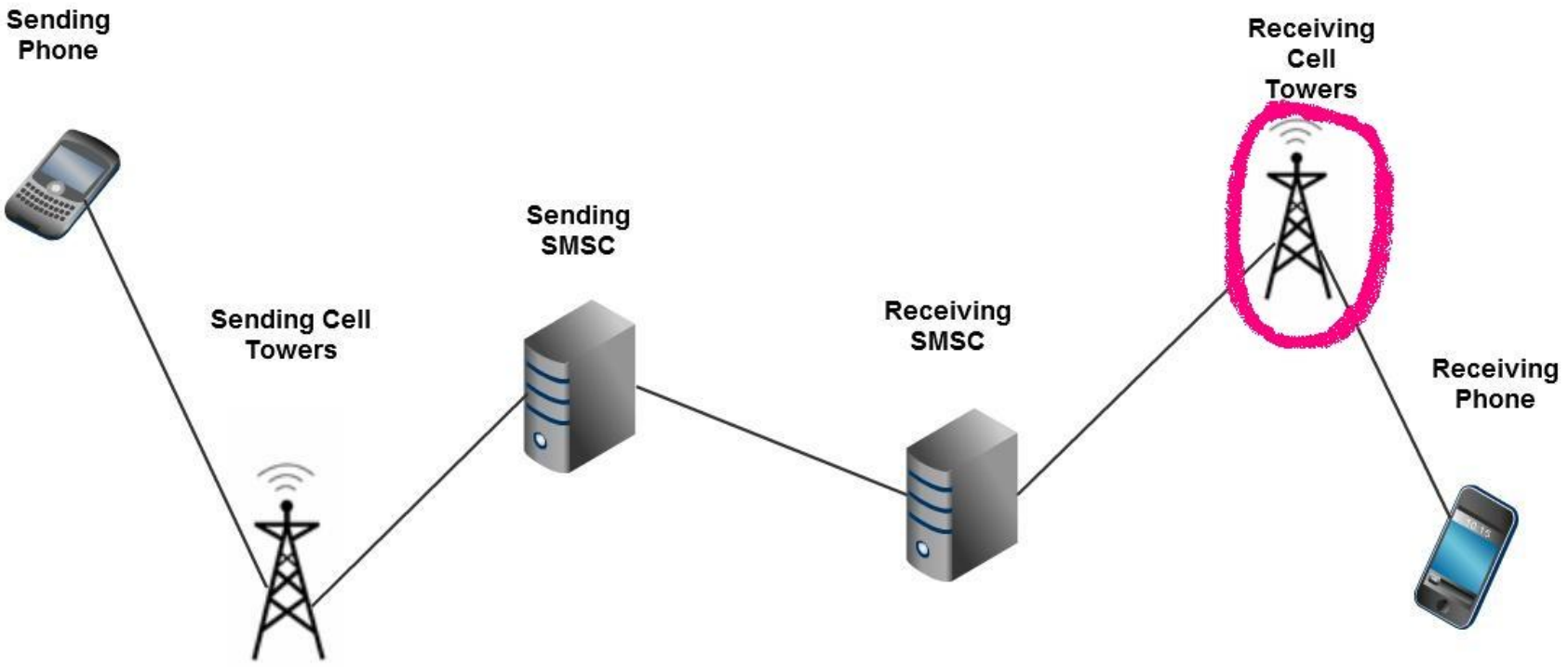
How an SMS is sent and received



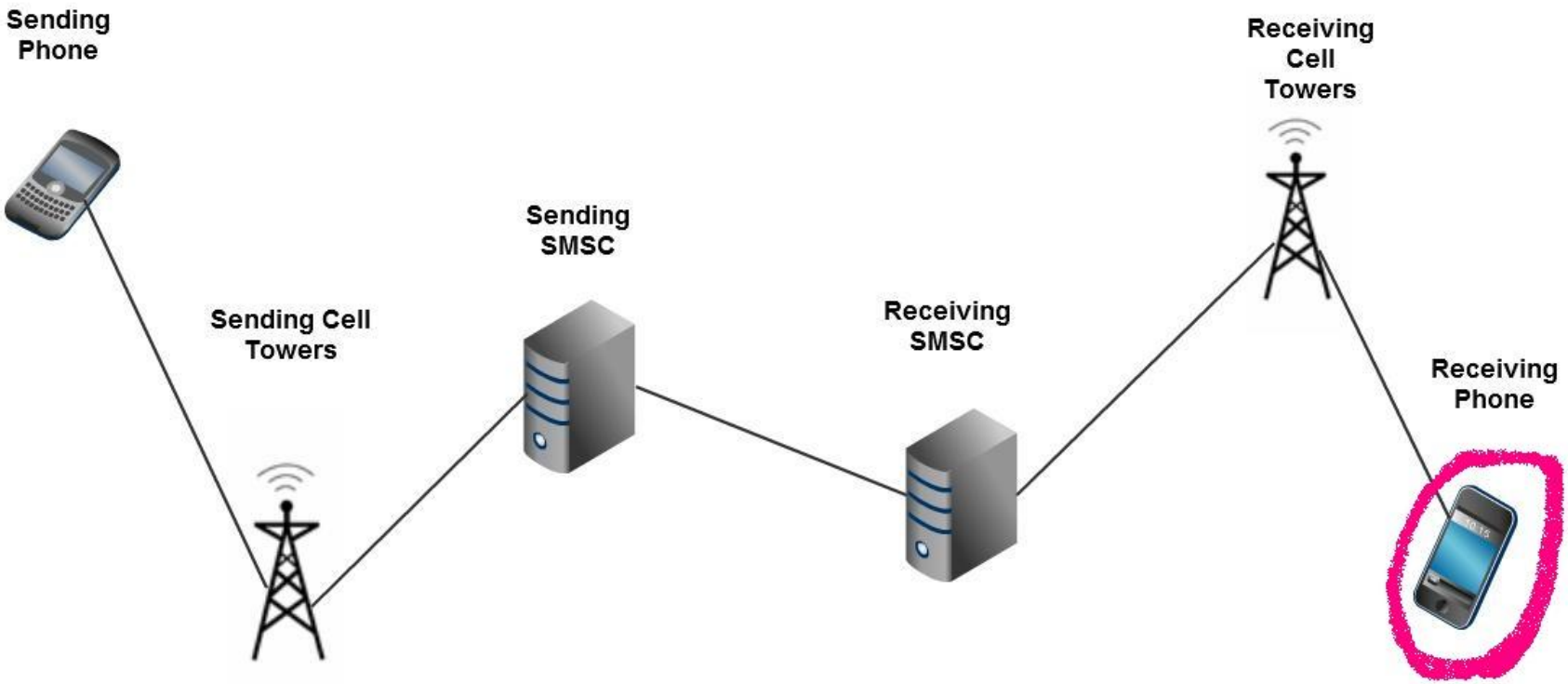
How an SMS is sent and received



How an SMS is sent and received



How an SMS is sent and received

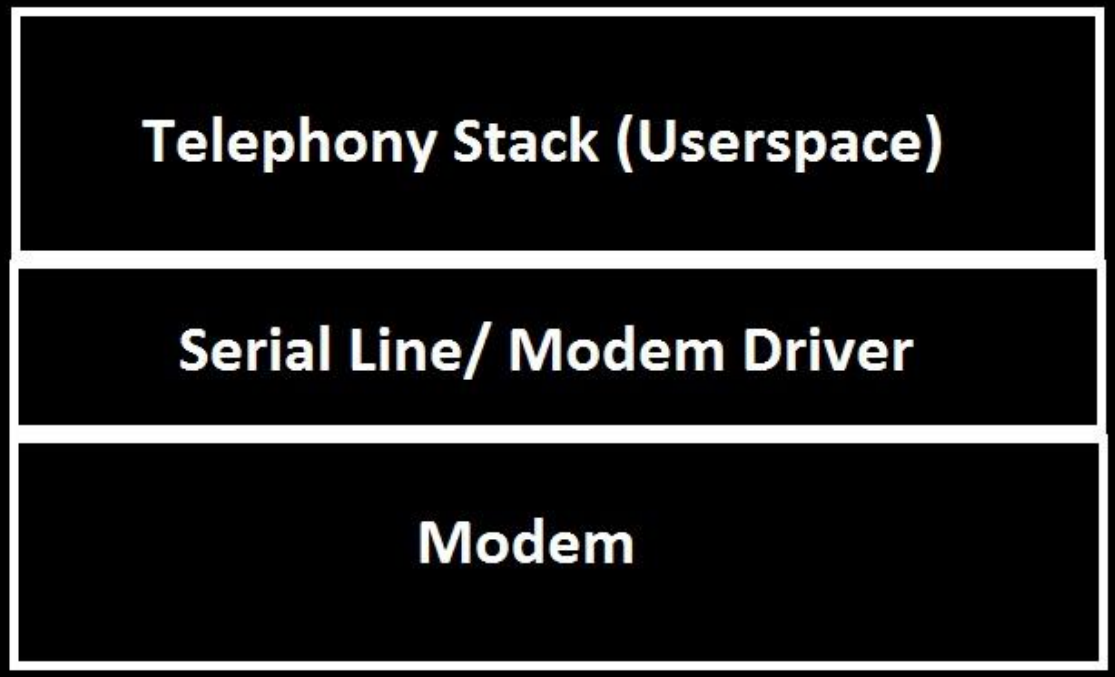


Previous Work: SMS Fuzzing

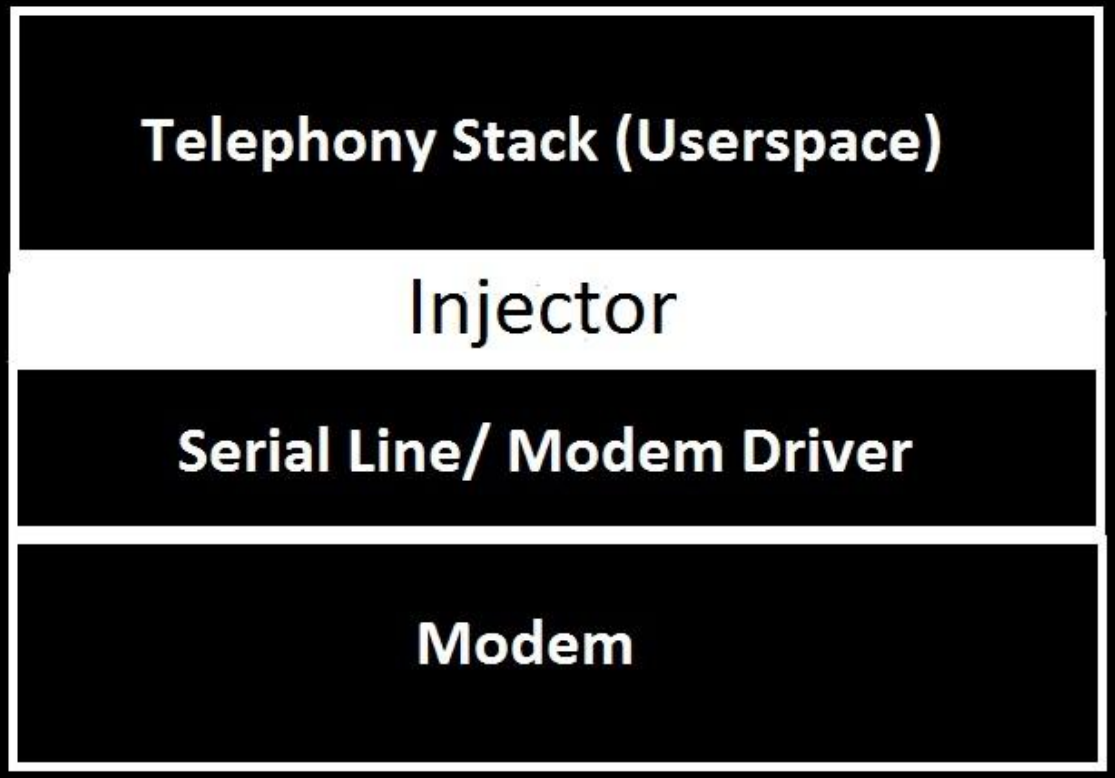
At Blackhat 2009, Charlie Miller & Collin Mulliner proxied the application layer and modem to crash smartphones with SMS.

http://www.blackhat.com/presentations/bh-usa-09/MILLER/BHUSA09-Miller-FuzzingPhone-PAPER.pdf

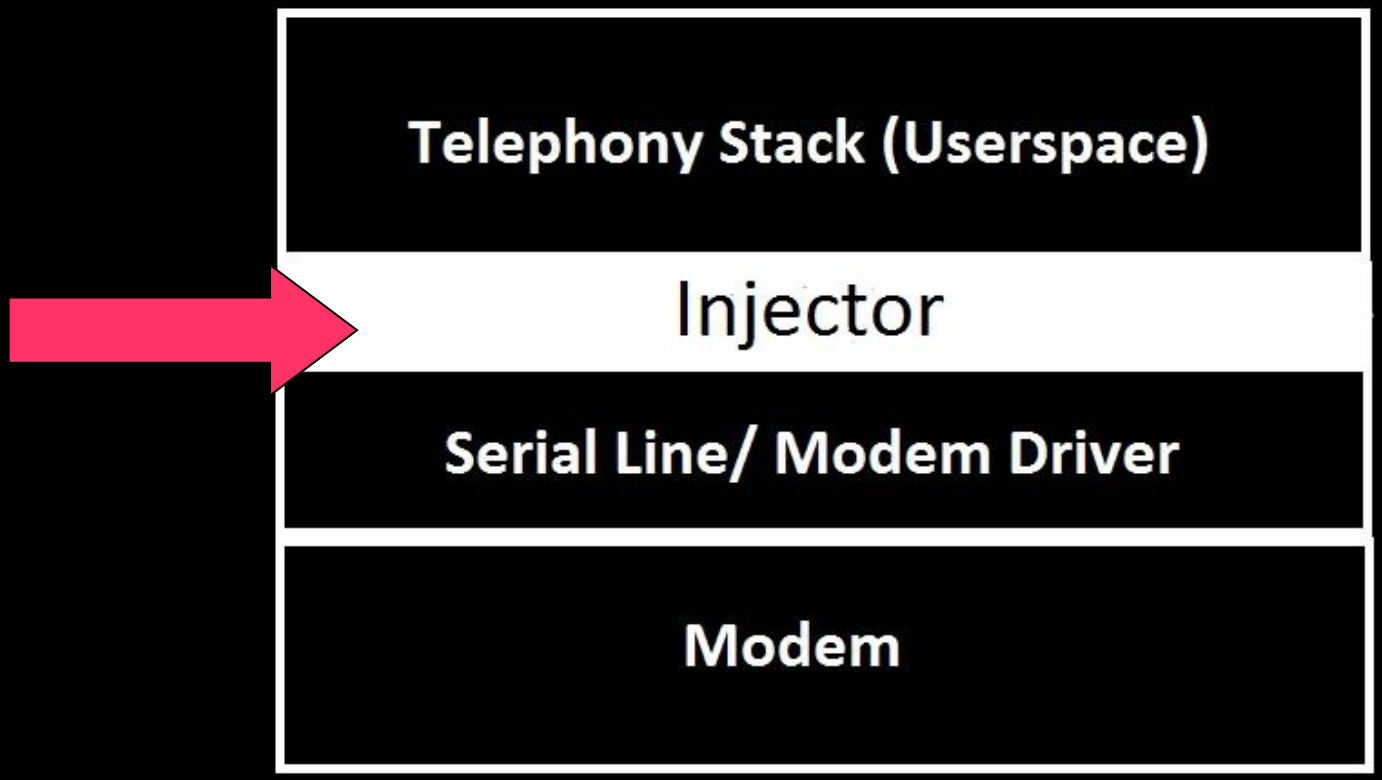
Previous Work: SMS Fuzzing



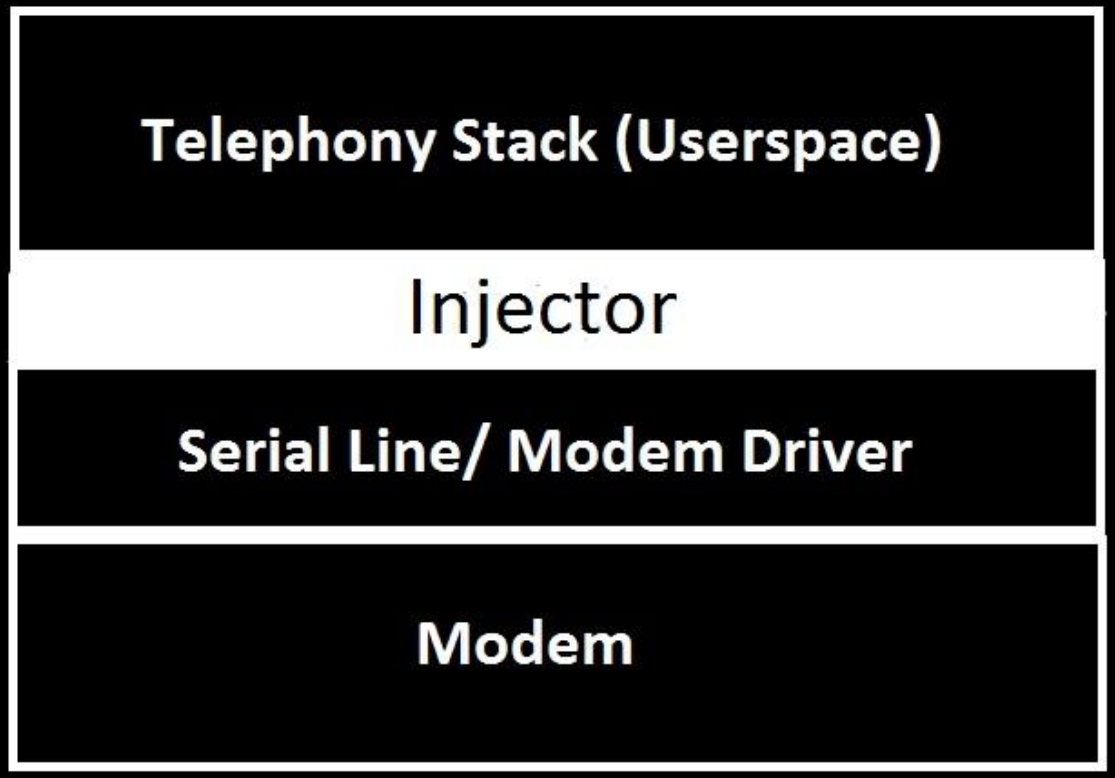
Previous Work: SMS Fuzzing



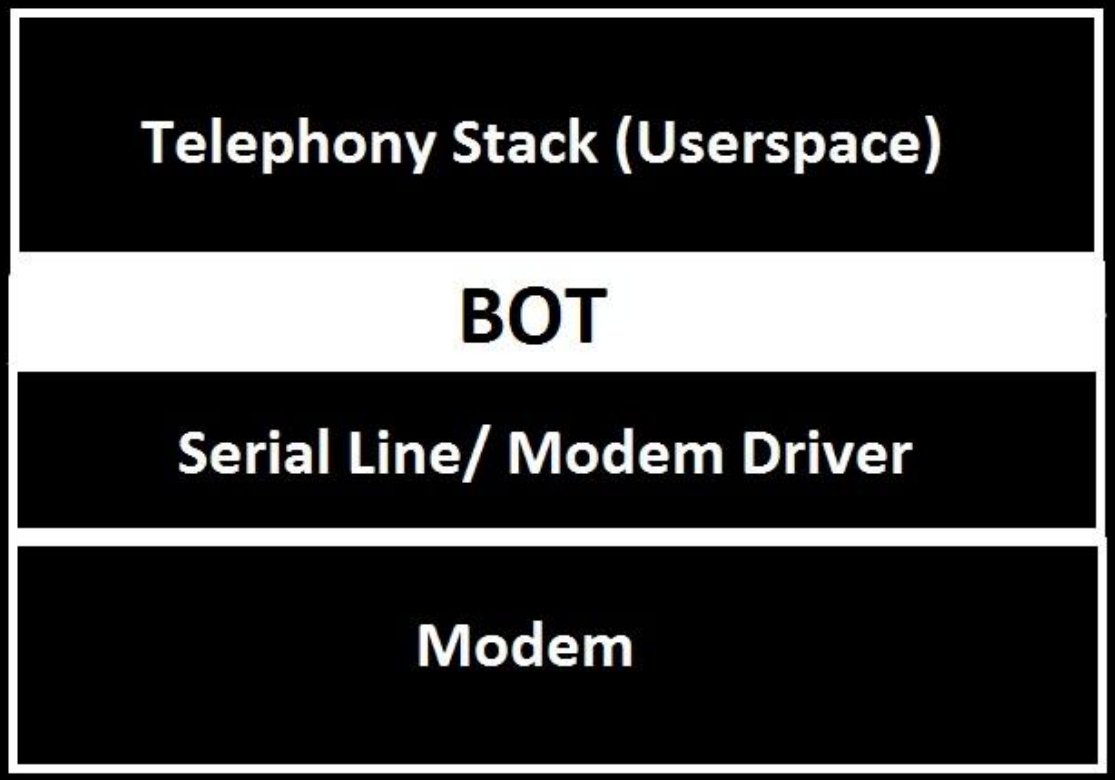
Previous Work: SMS Fuzzing



My Work: SMS Botnet C&C



My Work: SMS Botnet C&C



SMS-Deliver PDU

0791414054051 0F1040B916117345476F1000001210371400 44A0A E8329BFD4697D9EC37

Field	Value
Length of SMSC	07
Type of Address (SMSC)	91
Service Center Address (SMSC)	41 40 54 05 10 F1
SMS Deliver Info	04
Length of Sender Number	0B
Type of Sender Number	91
Sender Number	51 17 34 45 88 F1
Protocol Identifier	00
Data Coding Scheme	00
Time Stamp	01 21 03 71 40 04 4A
User Data Length	0A
User Data	E8 32 9B FD 46 97 D9 EC 37

SMS-Deliver PDU

07914140540510F1040B916117345476F10000012103714004 4A0A
E8329BFD4697D9EC37

Field	Value
Length of SMSC	07
Type of Address (SMSC)	91
Service Center Address (SMSC)	41 40 54 05 10 F1
SMS Deliver Info	04
Length of Sender Number	0B
Type of Sender Number	91
Sender Number	61 17 34 54 76 F1
Protocol Identifier	00
Data Coding Scheme	00
Time Stamp	01 21 03 71 40 04 4A
User Data Length	0A
User Data	**E8 32 9B FD 46 97 D9 EC 37**

How the Botnet Works

1. Bot Receives Message

2. Bot Decodes User Data

3. Bot Checks for Bot Key

4. Bot Performs Payload Functionality

How the Botnet Works

1. **Bot Receives Message**

2. Bot Decodes User Data

3. Bot Checks for Bot Key

4. Bot Performs Payload Functionality

How the Botnet Works

1. Bot Receives Message

2. **Bot Decodes User Data**

3. Bot Checks for Bot Key

4. Bot Performs Payload Functionality

How the Botnet Works

1. Bot Receives Message

2. Bot Decodes User Data

3. **Bot Checks for Bot Key**

4. Bot Performs Payload Functionality

How the Botnet Works

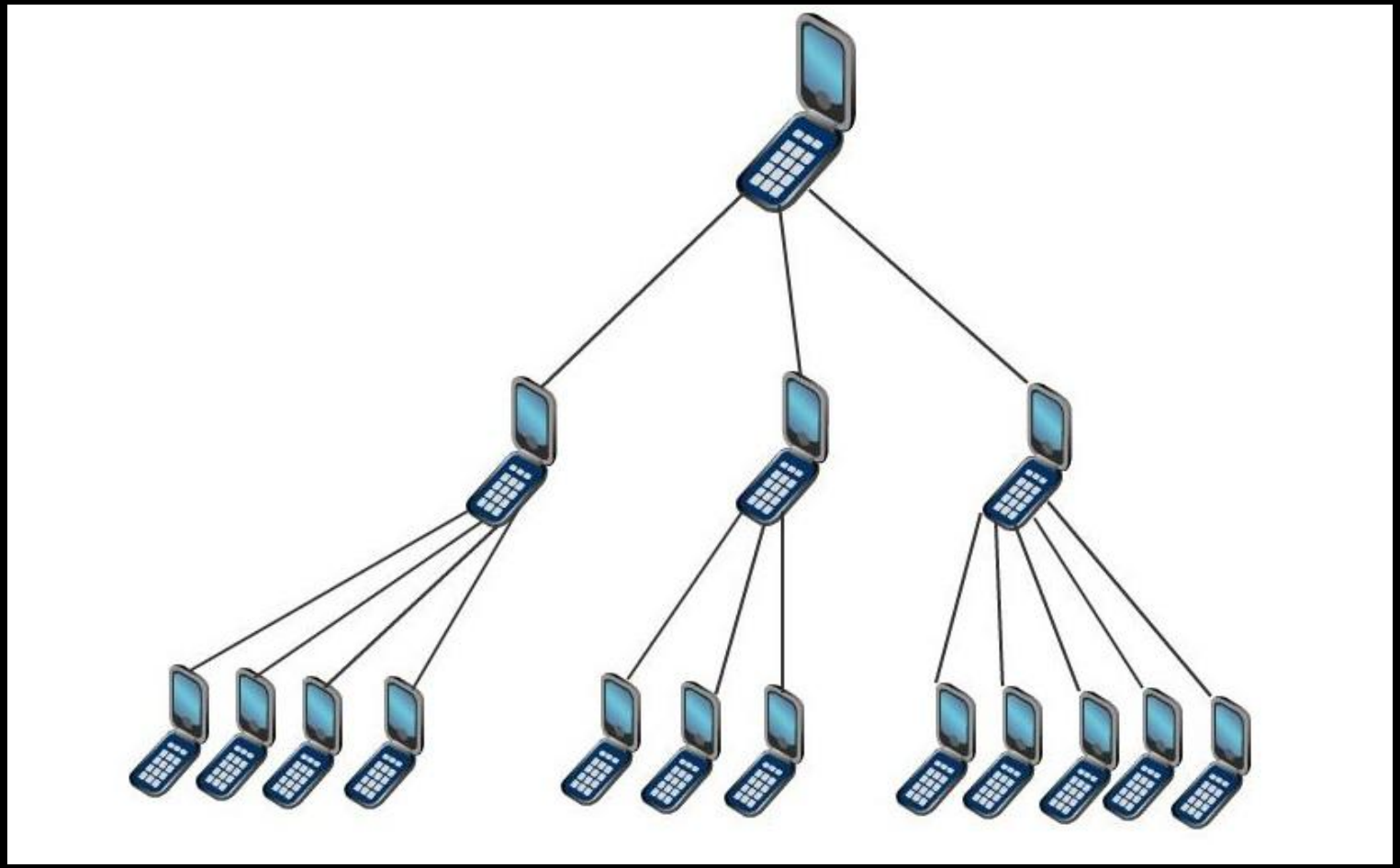
1. Bot Receives Message

2. Bot Decodes User Data

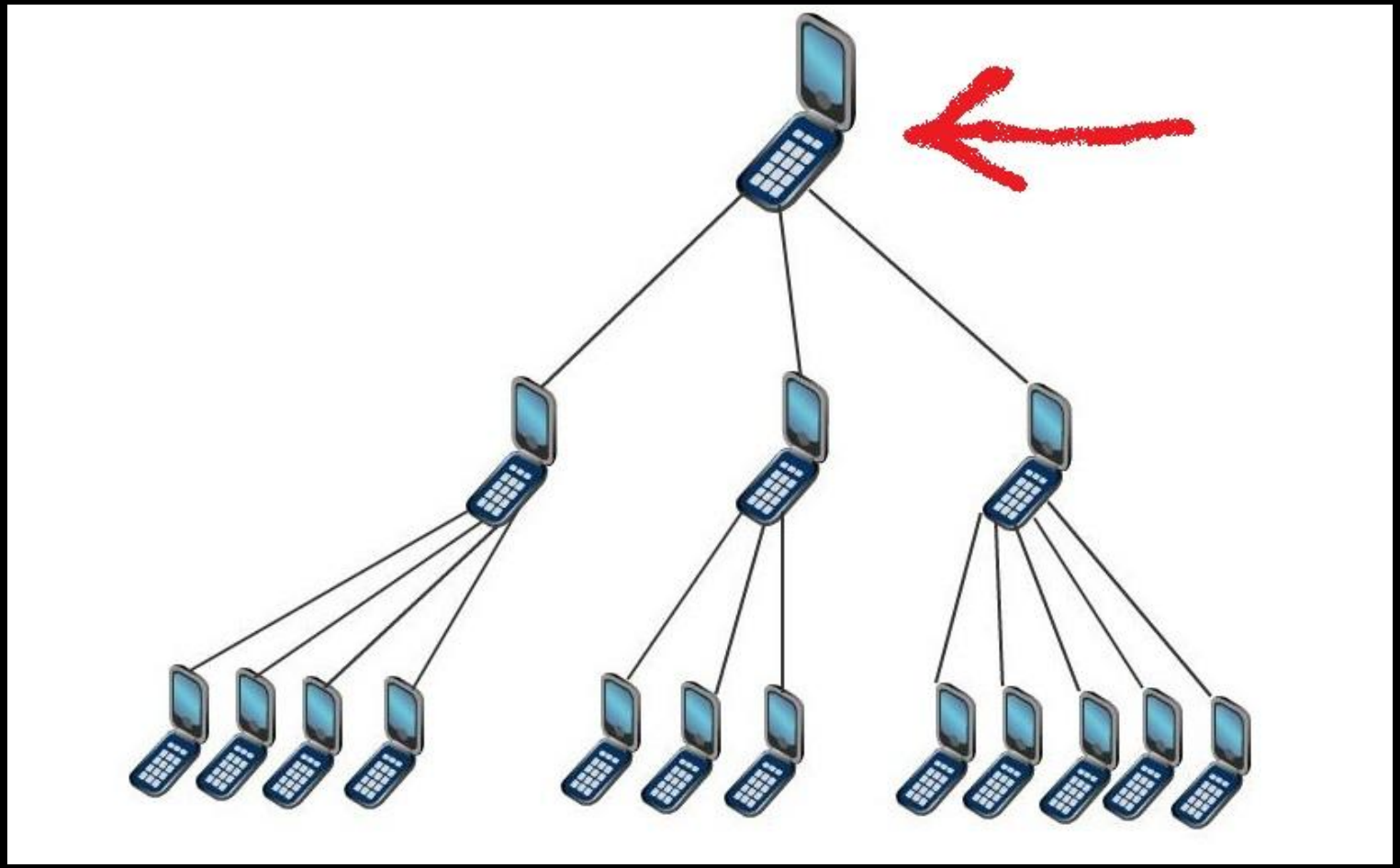
3. Bot Checks for Bot Key

4. **Bot Performs Payload Functionality**

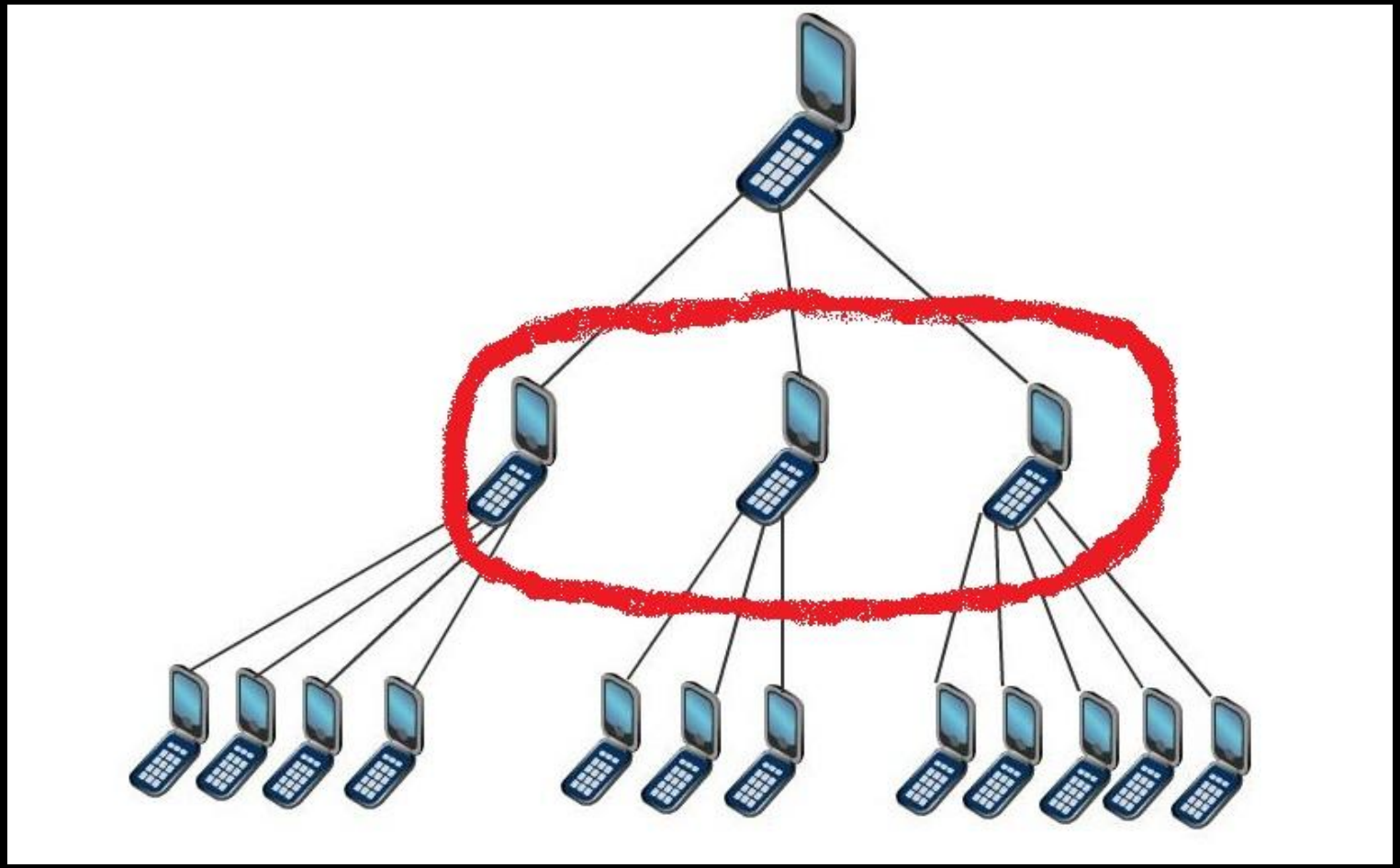
Botnet Structure



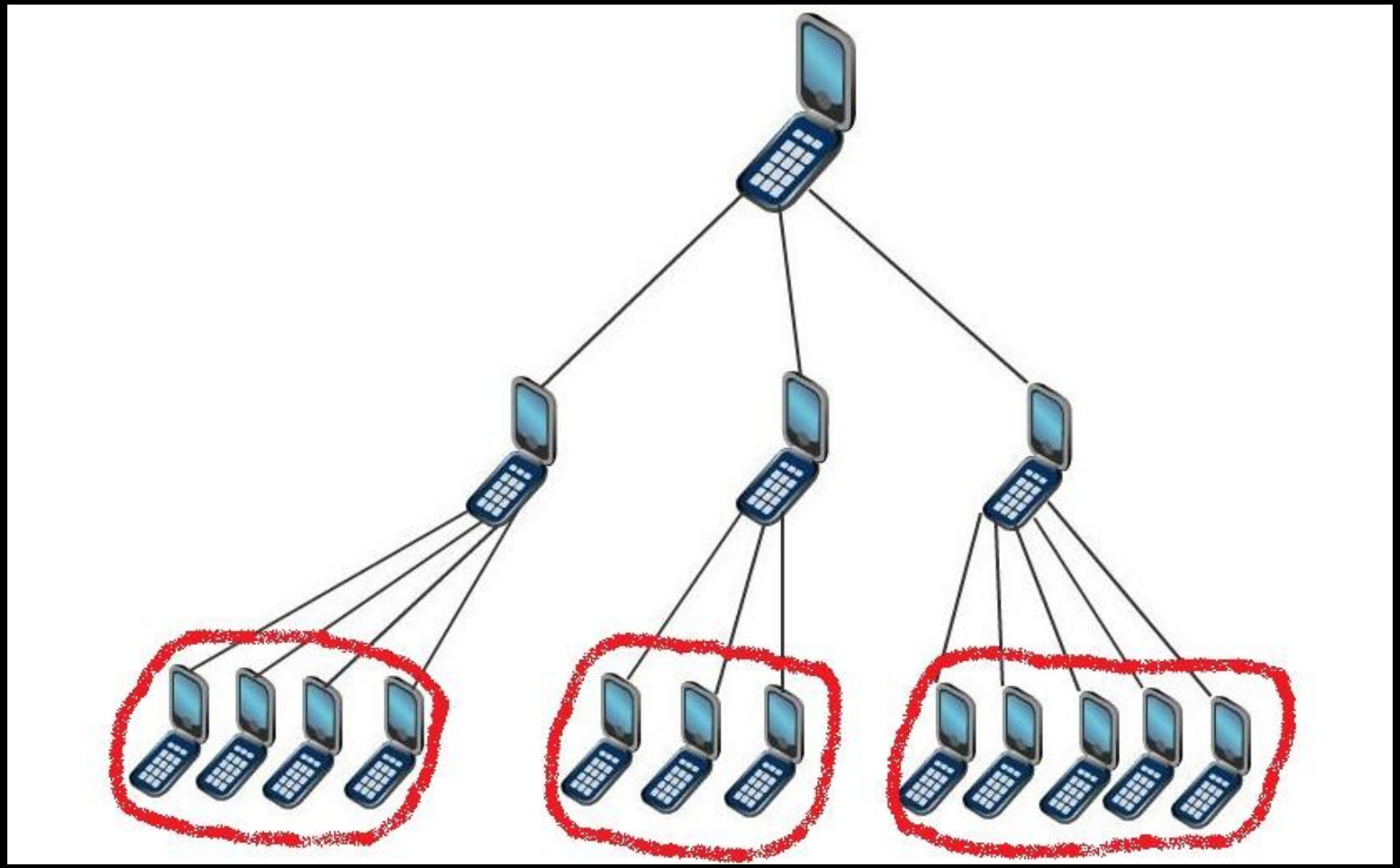
Master Bot



Sentinel Bots



Slave Bots



Security Concerns

- Impersonation
- Replay
- Cryptographic solutions

Limitations

- Possible detection methods
- User data length

Getting the Bot Installed

- Regular Users
- Rooted/Jailbroken Users
- Remote

Example Payloads

- Spam
- Denial of service
- Load new functionality
- Degrading cell service

What This Really Means

- If attackers can get the bot installed they can remotely control a user's phone without giving any sign of compromise to the user.

Mitigations

- Integrity checks
- Liability for smartphone applications
- User awareness

Demo

- Android Bot with Spam Payload

Contact

- Georgia Weidman
- Company: Neohapsis Inc.
- Email: Georgia@grmn00bs.com
  Georgia.weidman@neohapsis.com
- Website: http://www.grmn00bs.com
- Twitter: vincentkadmon

Selected Bibliography

- SMS fuzzing: http://www.blackhat.com/presentations/bh-usa-09/MILLER/BHUSA09-Miller-FuzzingPhone-PAPER.pdf
- Cell bots attack GSM core: http://www.patrickmcdaniel.org/pubs/ccs09b.pdf
- Twilight botnet: http://jon.oberheide.org/files/summercon10-androidhax-jonoberheide.pdf
- SMS/P2P iPhone bots: http://mulliner.org/collin/academic/publications/ibots_malware10_mulliner_seifert.pdf