Thwarting Smartphone SMS Attacks at the Radio Interface Layer

Haohuang Wen\textsuperscript{1}, Phillip Porras\textsuperscript{2}, Vinod Yegneswaran\textsuperscript{2}, and Zhiqiang Lin\textsuperscript{1}

\textsuperscript{1}The Ohio State University, \textsuperscript{2}SRI International

Feb 28th, 2023
Short Message Service (SMS)

- Introduced since December, 1992
- Defined in 3GPP TS 23.040 [3gp]
Short Message Service (SMS)

Applications

- Text-based messaging

- Introduced since December, 1992

- Defined in 3GPP TS 23.040 [3gp]
Short Message Service (SMS)

- Introduced since December, 1992
- Defined in 3GPP TS 23.040 [3gp]

Applications

- Text-based messaging
- Two-factor authentication
Short Message Service (SMS)

Introduction

- Introduced since December, 1992
- Defined in 3GPP TS 23.040 [3gp]

Applications

- Text-based messaging
- Two-factor authentication
- Alerts & notifications
Short Message Service (SMS)

- Introduced since December, 1992
- Defined in 3GPP TS 23.040 [3gp]

Applications
- Text-based messaging
- Two-factor authentication
- Alerts & notifications
- Marketing & advertising
- ......
SMS Transmission Path in Cellular Network
SMS Transmission Path in Cellular Network

1. UE (User Equipment) submits a SMS message to SMSC (Short Message Service Center).

2. SMSC forwards the message to the RAN (Radio Access Network).

This diagram illustrates the process of SMS transmission in a cellular network.
SMS Transmission Path in Cellular Network

1. SMS-SUBMIT

UE → RAN → Core Network

SMSC

SMSC-Based SMS (2G/3G)
SMS Transmission Path in Cellular Network

1. SMS-SUBMIT

UE → RAN → Core Network

SMSC-based SMS (2G/3G)
SMS Transmission Path in Cellular Network

SMSC-Based SMS (2G/3G)
SMS Transmission Path in Cellular Network

IMS-Based SMS (4G+)
Exploiting SMS

- SMS is **not** just a *text-based service*
Exploiting SMS

- SMS is **not** just a *text-based service*
- Zero-click exploits exist in various ways to compromise security, privacy and availability without the user’s knowledge and consent
Exploiting SMS

- SMS is **not** just a *text-based service*
- Zero-click exploits exist in various ways to compromise security, privacy and availability without the user’s knowledge and consent

SimJacker Attack [*sim*]
Exploiting SMS

- SMS is **not** just a *text-based service*
- Zero-click exploits exist in various ways to compromise security, privacy and availability without the user’s knowledge and consent

Contemporary UE operating systems cannot see these SMS attacks, let alone stop them

SimJacker Attack [sim]
Exploiting SMS

**SMS PDU Payload**

<table>
<thead>
<tr>
<th>Field</th>
<th>SCA</th>
<th>FO</th>
<th>OA/DA</th>
<th>PID</th>
<th>DCS</th>
<th>...</th>
<th>UDL</th>
<th>UD</th>
</tr>
</thead>
<tbody>
<tr>
<td>Value</td>
<td>-</td>
<td>01</td>
<td>&lt;dest&gt;</td>
<td>00</td>
<td>00</td>
<td>0C</td>
<td>C8329BF</td>
<td>...</td>
</tr>
</tbody>
</table>

**SMS**

```
<dest> 0000 0CC8329BF...

"Hello World"
```

**Diagram**

```
<src> --- SMS "Hello World" --- <dest>
```
Exploiting SMS

SMS PDU Payload

<table>
<thead>
<tr>
<th>Field</th>
<th>SCA</th>
<th>FO</th>
<th>OA/DA</th>
<th>PID</th>
<th>DCS</th>
<th>...</th>
<th>UDL</th>
<th>UD</th>
</tr>
</thead>
<tbody>
<tr>
<td>Value</td>
<td>-</td>
<td>01</td>
<td>&lt;dest&gt;</td>
<td>40</td>
<td>00</td>
<td></td>
<td>0C</td>
<td>C8329BF</td>
</tr>
</tbody>
</table>

Silent SMS

UE will not display silent SMS to user
Exploiting SMS

SMS PDU Payload

<table>
<thead>
<tr>
<th>Field</th>
<th>SCA</th>
<th>FO</th>
<th>OA/DA</th>
<th>PID</th>
<th>DCS</th>
<th>...</th>
<th>UDL</th>
<th>UD</th>
</tr>
</thead>
<tbody>
<tr>
<td>Value</td>
<td>-</td>
<td>01</td>
<td>&lt;dest&gt;</td>
<td>00</td>
<td>18</td>
<td></td>
<td>0C</td>
<td>C8329BF...</td>
</tr>
</tbody>
</table>

Flash SMS

“This is a test FLASH SMS”

Class 0 message

This is a test FLASH SMS.
Exploiting SMS

SMS PDU Payload

<table>
<thead>
<tr>
<th>Field</th>
<th>SCA</th>
<th>FO</th>
<th>OA/DA</th>
<th>PID</th>
<th>DCS</th>
<th>...</th>
<th>UDL</th>
<th>UD</th>
</tr>
</thead>
<tbody>
<tr>
<td>Value</td>
<td>-</td>
<td>01</td>
<td>&lt;dest&gt;</td>
<td>7F</td>
<td>F6</td>
<td>0C</td>
<td></td>
<td>&lt;Payload&gt;</td>
</tr>
</tbody>
</table>

Binary SMS
Malicious Payload

<src>

<dest>
Exploiting SMS

SMS PDU Payload

<table>
<thead>
<tr>
<th>Field</th>
<th>SCA</th>
<th>FO</th>
<th>OA/DA</th>
<th>PID</th>
<th>DCS</th>
<th>...</th>
<th>UDL</th>
<th>UD</th>
</tr>
</thead>
<tbody>
<tr>
<td>Value</td>
<td>-</td>
<td>01</td>
<td>&lt;dest&gt;</td>
<td>00</td>
<td>00</td>
<td></td>
<td>0C</td>
<td>Spam Content</td>
</tr>
</tbody>
</table>

Fake Base Station SMS

Spam Content
Exploiting SMS

SMS PDU Payload

<table>
<thead>
<tr>
<th>Field</th>
<th>SCA</th>
<th>FO</th>
<th>OA/DA</th>
<th>PID</th>
<th>DCS</th>
<th>...</th>
<th>UDL</th>
<th>UD</th>
</tr>
</thead>
<tbody>
<tr>
<td>Value</td>
<td>-</td>
<td>01</td>
<td>&lt;dest&gt;</td>
<td>00</td>
<td>00</td>
<td></td>
<td>0C</td>
<td>Spam Content</td>
</tr>
</tbody>
</table>

Malware SMS

Spam Content

You've received a new message regarding the COVID-19 safetyline symptoms and when to get tested in your geographical area. Visit
# Exploiting SMS

## Proactive SIM SMS

### SMS PDU Payload

<table>
<thead>
<tr>
<th>Field</th>
<th>SCA</th>
<th>FO</th>
<th>OA/DA</th>
<th>PID</th>
<th>DCS</th>
<th>...</th>
<th>UDL</th>
<th>UD</th>
</tr>
</thead>
<tbody>
<tr>
<td>Value</td>
<td>-</td>
<td>01</td>
<td>&lt;dest&gt;</td>
<td>00</td>
<td>00</td>
<td>0C</td>
<td>Sensitive Info</td>
<td></td>
</tr>
</tbody>
</table>

### Diagram

- **<src>**
- **Proactive SIM SMS**
- **Sensitive Info**
- **<dest>**
Exploitation Cost

Pre-paid SIM: $5
GSM USB Modem: $15

Total Cost: As low as $20!
Defending Against SMS Attacks
Defending Against SMS Attacks

Android Processor

App
- Messages
- Dialer
- Browser

Framework
- Android Telephony Service

Radio Interface Layer
- RIL Java
- RIL Library
- RIL Daemon
- Vendor RIL Library

Kernel
- Kernel Driver

Hardware
- GPS
- CAM
- SIM
- Baseband
- RAM
- USB
- MIC
Defending Against SMS Attacks

### Baseband-Layer Defenses

- **FBS Detection in Qualcomm chips** [qua]
Defending Against SMS Attacks

<table>
<thead>
<tr>
<th>Android Processor</th>
<th>RADIO Interface Layer</th>
<th>Framework</th>
<th>App</th>
</tr>
</thead>
<tbody>
<tr>
<td>App</td>
<td>Messages</td>
<td>Android Telephony Service</td>
<td>Dialer</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RIL Java</td>
<td>Browser</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RIL Library</td>
<td>RIL Daemon</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Vendor RIL Library</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Kernel Driver</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Kernel</td>
<td></td>
</tr>
<tr>
<td>Hardware</td>
<td>GPS</td>
<td>CAM</td>
<td>SIM</td>
</tr>
<tr>
<td></td>
<td>RAM</td>
<td>USB</td>
<td>MIC</td>
</tr>
</tbody>
</table>

Baseband-Layer Defenses

- FBS Detection in Qualcomm chips [qua]

Pros

- High visibility
- Mitigation capability
# Defending Against SMS Attacks

## Baseband-Layer Defenses

- FBS Detection in Qualcomm chips [qua]

## Pros

- High visibility
- Mitigation capability

## Cons

- Closed-source
- Integrity-protected
- Highly customized implementation
Defending Against SMS Attacks

![Diagram of Android Architecture]

---

**Android Processor**

- **App**
  - Messages
  - Dialer
  - Browser

- **Framework**
  - Android Telephony Service

- **Radio Interface Layer**
  - RIL Java
  - RIL Library
  - RIL Daemon
  - Vendor RIL Library

- **Kernel**
  - Kernel Driver

- **Hardware**
  - GPS
  - CAM
  - SIM
  - RAM
  - USB
  - MIC
  - Baseband

---

**Defending Against SMS Attacks**

- **RIL Java**
- **Android Telephony Service**
- **RIL Daemon**
- **RIL Library**
- **Vendor RIL Library**
- **Kernel Driver**
- **Baseband**

---

**Integrating External Libraries and Services**

- **Defensive Strategies**
  - AIMSIC [AIM], SnoopSnitch [sno]
  - MobileInsight [LPY]
  - SCAT [HPK]
  - Phoenix [EAW]

**Pros**
- Low deployment cost

**Cons**
- Low visibility
- Passive detection only
- Root required
Defending Against SMS Attacks

### App-Layer Defenses

- AIMSICD [AIM], SnoopSnitch [sno]
- MobileInsight [LPY+16], SCAT [HPK+18], Phoenix [EAW+21]
Defending Against SMS Attacks

**App-Layer Defenses**

- AIMSICD [AIM], SnoopSnitch [sno]
- MobileInsight [LPY\textsuperscript{+16}], SCAT [HPK\textsuperscript{+18}], Phoenix [EAW\textsuperscript{+21}]

**Pros**

+ Low deployment cost
Defending Against SMS Attacks

App-Layer Defenses
- AIMSICD [AIM], SnoopSnitch [sno]
- MobileInsight [LPY+16], SCAT [HPK+18], Phoenix [EAW+21]

Pros
- Low deployment cost

Cons
- Low visibility
- Passive detection only
- Root required
**RILDefender Overview**

The first defense, RILDefender, is deployed at the Radio Interface Layer (RIL) in Android UEs, generally intercepting all BP-AP traffic.

**Key Distinctions over Existing Defenses**

- Detection & Prevention capability
- Vendor-agnostic
- Extensibility

---

**Diagram:**

- **Android Processor**
  - App: Messages, Dialer, Browser
- **Framework**
  - Android Telephony Service
- **Radio Interface Layer**
  - RIL Java
  - RIL Library
  - RIL Daemon
  - Vendor RIL Library
- **Kernel**
  - Kernel Driver
- **Hardware**
  - GPS, CAM, SIM, Baseband, USB, MIC, RAM, SIM, MIC, Baseband
RILDefender Overview

Android Processor

- App: Messages, Dialer, Browser

Framework: Android Telephony Service

Radio Interface Layer:
- RIL Java
- RIL Library, RIL Daemon
- Vendor RIL Library

Kernel:
- Kernel Driver

Hardware:
- GPS, CAM, SIM, Baseband
- RAM, USB, MIC

RIL-layer Defenses

- The first defense RILDefender
- Deployed at the Radio Interface Layer (RIL)
**RILDefender Overview**

### RIL-layer Defenses

- **The first defense** RILDefender
- Deployed at the *Radio Interface Layer* (RIL)
  - Generally exists in Android UEs
RILDefender Overview

RIL-layer Defenses

- The first defense RILDefender
- Deployed at the Radio Interface Layer (RIL)
  - Generally exists in Android UEs
  - Intercept all BP-AP traffic
RILDefender Overview

RIL-layer Defenses

- The first defense RILDefender
- Deployed at the Radio Interface Layer (RIL)
  - Generally exists in Android UEs
  - Intercept all BP-AP traffic

Key Distinctions over Existing Defenses

+ Detection & Prevention capability
+ Vendor-agnostic
+ Extensibility
**RILDefender** At the Radio Interface Layer

**RILDefender Architecture**
- Radio Interface Layer
  - Four logical components
- Application Layer
  - The RILDefender app

---

**User-Space Applications**
- Messenger
- Dialer
- **RILDefender App**

**RILDefender**
- Baseband Monitor
- Context Extractor
- Inline Mediator
- Attack Detector

**Radio Interface Layer**
- RIL Request/Response

**Baseband Processor (BP)**
RILDefender At the Radio Interface Layer

User-Space Applications

Dialer

RILDefender App

Baseband Monitor

Context Extractor

Inline Mediator

Attack Detector

Radio Interface Layer

Baseband Processor (BP)

IPC

Baseband Monitor

- Monitor baseband-only SMS attacks (one exception)
RILDefender At the Radio Interface Layer

User-Space Applications
- Messenger
- Dialer
- RILDefender App

RILDefender
- Baseband Monitor
- Context Extractor
- Inline Mediator
- Attack Detector

Radio Interface Layer
- RIL Request/Response
- Baseband Processor (BP)

Baseband Monitor
- Monitor baseband-only SMS attacks (one exception)
- Interpret baseband traffic from diagnostic interfaces (e.g., /dev/diag)
- Adapted from existing libraries [sno]
**RILD Defender** At the Radio Interface Layer

**Context Extractor**
- Track context of user-space applications (e.g., SMS sender PID)
RILDefender: At the Radio Interface Layer

- **Context Extractor**
  - Track context of user-space applications (e.g., SMS sender PID)
  - Track context of system-level parameters (e.g., signal strengths)
  - Interact through IPC calls

User-Space Applications
- Messenger
- Dialer
- RILDefender App

Radio Interface Layer
- Baseband Monitor
- Inline Mediator
- Attack Detector

Baseband Processor (BP)

IPC

RIL Request/Response
**RILDefender** At the Radio Interface Layer

**Attack Detector**
- Instrument the main RIL handler
RILDefender At the Radio Interface Layer

User-Space Applications
- Messenger
- Dialer
- RILDefender App

RILDefender
- Baseband Monitor
- Context Extractor
- Inline Mediator
- Attack Detector

Radio Interface Layer
- RIL Request/Response
- Baseband Processor (BP)

IPC

Attack Detector
- Instrument the main RIL handler
- Synthesize SMS payload and information from other component
**RILDefender** At the Radio Interface Layer

---

**User-Space Applications**
- Messenger
- Dialer
- RILDefender App

**RILDefender**
- Baseband Monitor
- Context Extractor
- Inline Mediator
- Attack Detector

**Radio Interface Layer**
- RIL Request/Response

**Baseband Processor (BP)**

---

**Attack Detector**
- Instrument the main RIL handler
- Synthesize SMS payload and information from other component
- Load user-defined attack signature set
RILDefender At the Radio Interface Layer

User-Space Applications
- Messenger
- Dialer
- RILDefender App

Baseband Monitor
Context Extractor

RILDefender
- Inline Mediator
- Attack Detector

Radio Interface Layer

RIL Request/Response

Baseband Processor (BP)

']),

"Inline Mediator"
- Instrument the RIL logic for attack prevention
- Interact through specific RIL commands
RILDefender at the Application Layer

- Configure security level for each attack
- Block and Notify
- Block without Notify
- Notify only
- Allow
- Receive real-time alerts for attack events
- Configure user-defined attack signatures
RILDefender at the Application Layer

RILDefender App
- Configure security level for each attack
  - Block and Notify
  - Block without Notify
  - Notify only
  - Allow

User Signature Policy

RILDefender

AP

RIL
RILDefender at the Application Layer

RILDefender App

- Configure security level for each attack
  - Block and Notify
  - Block without Notify
  - Notify only
  - Allow
- Receive real-time alerts for attack events
RILDefender at the Application Layer

RILDefender App
- Configure security level for each attack
  - Block and Notify
  - Block without Notify
  - Notify only
  - Allow
- Receive real-time alerts for attack events
- Configure user-defined attack signatures
**RILDefender at the Application Layer**

RILDefender App

- User
- Signature Policy

Configuration UI

- Silent SMS
  - Security Level
  - Block and Notify Me

- Flash SMS
  - Security Level
  - Block and Notify Me

- Binary SMS
  - Security Level
  - Block and Notify Me

- Fake Base Station SMS
  - Security Level
  - Notify Me

- Malware SMS
  - Security Level
RILDefender at the Application Layer

**RILDefender**

- **User**
- **Signature Policy**

**Configuration UI**

**Alert UI**

- **RILDefender App**
- **RILDefender**
- **RIL**
- **AP**

**RILDefender**

- Silent SMS
- Security Level: Block and Notify Me
- Flash SMS
- Security Level: Block and Notify Me
- Binary SMS
- Security Level: Block and Notify Me
- Fake Base Station SMS
- Security Level: Notify Me
- Malware SMS
- Security Level

- **RILDefender Warning!**
  - Silent SMS has been blocked from 12345
  - SMS Content: hello

- **Silent notifications**
- Android System
- USB debugging connected
  - Tap to turn off USB debugging
- Android System • Charging this device via USB

- **Security Level**
  - Block and Notify Me
# RILD Defender at the Application Layer

<table>
<thead>
<tr>
<th>Category</th>
<th>SMS Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMS Fields</td>
<td><code>sms.mti</code> <code>sms.smsc</code> <code>sms.ua</code> <code>sms.da</code> <code>sms.scts</code> <code>sms.pid</code> <code>sms.dcs</code> <code>sms.udl</code> <code>sms.ud</code> <code>sms.proactiveCmd</code></td>
</tr>
<tr>
<td>SMS Context</td>
<td><code>sms.src</code> <code>sms.ts</code> <code>bs.mcc</code> <code>bs.mnc</code> <code>bs.cid</code> <code>bs.lac</code> <code>bs.arfcn</code> <code>bs.rat</code></td>
</tr>
<tr>
<td>SMS Events</td>
<td><code>eventCount</code> <code>{sms1, ..., smsn}</code></td>
</tr>
</tbody>
</table>
RILDefender at the Application Layer

<table>
<thead>
<tr>
<th>Category</th>
<th>SMS Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>sms.mti</td>
</tr>
<tr>
<td></td>
<td>sms.smsec</td>
</tr>
<tr>
<td></td>
<td>sms.oa</td>
</tr>
<tr>
<td></td>
<td>sms.da</td>
</tr>
<tr>
<td></td>
<td>sms.scts</td>
</tr>
<tr>
<td></td>
<td>sms.pid</td>
</tr>
<tr>
<td></td>
<td>sms.dcs</td>
</tr>
<tr>
<td></td>
<td>sms.ud</td>
</tr>
<tr>
<td></td>
<td>sms.proactiveCmd</td>
</tr>
</tbody>
</table>

**SMS Fields**

- sms.src
- sms.ts
- bs.ss
- bs.mcc
- bs.mnc
- bs.cid
- bs.lac
- bs.arfcn
- bs.rat

**SMS Events**

- eventCount
- {sms<sub>1</sub>, ..., sms<sub>n</sub>}

---

**YAML-based language to describe SMS attack signatures as propositional logic**

```yaml
<Rule> → <RuleName>: <Expr>
<Expr> → { lvalue: <Value> }
<OpCode> → + | - | * | / | & | | ^ | && | || | << | >>
<Cond> → == | != | > | < | >= | <=
<Feature> → sms.mti | sms.smsec | sms.oa | sms.da | sms.ud |
            | sms.pid | sms.scts | sms.dcs | sms.udl |
            | sms.src | sms.ts | sms.proactiveCmd |
            | bs.ss | bs.mcc | bs.mnc | bs.cid | bs.lac |
            | bs.arfcn | bs.rat | eventCount | sms_n |
<Const> → <Integer> | <Float> | <String>
```
## Implementation and Experiment Setup

<table>
<thead>
<tr>
<th>Device</th>
<th>Chipset</th>
<th>OS Ver.</th>
<th>AOSP Build</th>
<th>LoC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nexus 6</td>
<td>QCOM Snapdragon 805</td>
<td>7.1.1</td>
<td>N6F26Q</td>
<td>3,342</td>
</tr>
<tr>
<td>Pixel XL</td>
<td>QCOM Snapdragon 821</td>
<td>10.0.0</td>
<td>QP1A.190711.019</td>
<td>3,462</td>
</tr>
<tr>
<td>Pixel 5</td>
<td>QCOM Snapdragon 765G</td>
<td>11.0.0</td>
<td>RQ3A.211001.001</td>
<td>3,476</td>
</tr>
<tr>
<td>Pixel 5</td>
<td>QCOM Snapdragon 765G</td>
<td>12.0.0</td>
<td>SQ1A.220205.002</td>
<td>3,476</td>
</tr>
<tr>
<td>Pixel 5</td>
<td>QCOM Snapdragon 765G</td>
<td>13.0.0</td>
<td>TP1A.221005.002</td>
<td>3,482</td>
</tr>
</tbody>
</table>

Smartphone UEs and AOSP versions that RILD\text{DEFENDER} has been implemented on and evaluated.
Implementation and Experiment Setup

<table>
<thead>
<tr>
<th>Device</th>
<th>Chipset</th>
<th>OS Ver.</th>
<th>AOSP Build</th>
<th>LoC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nexus 6</td>
<td>QCOM Snapdragon 805</td>
<td>7.1.1</td>
<td>N6F26Q</td>
<td>3,342</td>
</tr>
<tr>
<td>Pixel XL</td>
<td>QCOM Snapdragon 821</td>
<td>10.0.0</td>
<td>QP1A.190711.019</td>
<td>3,462</td>
</tr>
<tr>
<td>Pixel 5</td>
<td>QCOM Snapdragon 765G</td>
<td>11.0.0</td>
<td>RQ3A.211001.001</td>
<td>3,476</td>
</tr>
<tr>
<td>Pixel 5</td>
<td>QCOM Snapdragon 765G</td>
<td>12.0.0</td>
<td>SQ1A.220205.002</td>
<td>3,476</td>
</tr>
<tr>
<td>Pixel 5</td>
<td>QCOM Snapdragon 765G</td>
<td>13.0.0</td>
<td>TP1A.221005.002</td>
<td>3,482</td>
</tr>
</tbody>
</table>

Smartphone UEs and AOSP versions that RILDEFENDER has been implemented on and evaluated.
Implementation and Experiment Setup
## Effectiveness Evaluation

<table>
<thead>
<tr>
<th>Attack</th>
<th>SMS Payload</th>
<th>Cellular Network Params</th>
<th>D</th>
<th>B</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>PID</td>
<td>DCS</td>
<td>Proactive CMD</td>
<td>TxPower</td>
</tr>
<tr>
<td>Binary SMS</td>
<td>0x7F</td>
<td>0xF6</td>
<td>DISPLAY_TEXT</td>
<td>-</td>
</tr>
<tr>
<td>(Interactive)</td>
<td>0x7F</td>
<td>0xF6</td>
<td>SET_UP_CALL</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>0x7F</td>
<td>0xF6</td>
<td>LAUNCH_BROWSER</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>0x7F</td>
<td>0xF6</td>
<td>PLAY_TONE</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>0x7F</td>
<td>0xF6</td>
<td>GET_INPUT</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>0x7F</td>
<td>0xF6</td>
<td>SELECT_ITEM</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>0x7F</td>
<td>0xF6</td>
<td>SET_UP_MENU</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>0x7F</td>
<td>0xF6</td>
<td>GET_INKEY</td>
<td>-</td>
</tr>
<tr>
<td>Binary SMS</td>
<td>0x7F</td>
<td>0xF6</td>
<td>SEND_SMS</td>
<td>-</td>
</tr>
<tr>
<td>(Non-interactive)</td>
<td>0x7F</td>
<td>0xF6</td>
<td>RUN_AT_CMD</td>
<td>-</td>
</tr>
<tr>
<td>Silent SMS</td>
<td>0x40</td>
<td>0x00</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Flash SMS</td>
<td>0x00</td>
<td>0x18</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>FBS SMS</td>
<td>0x00</td>
<td>0x00</td>
<td>-</td>
<td>&gt;-40dBm</td>
</tr>
<tr>
<td></td>
<td>0x00</td>
<td>0x00</td>
<td>-</td>
<td>&lt;-40dBm</td>
</tr>
<tr>
<td></td>
<td>0x00</td>
<td>0x00</td>
<td>-</td>
<td>&gt;-40dBm</td>
</tr>
<tr>
<td></td>
<td>0x40</td>
<td>0x00</td>
<td>-</td>
<td>&gt;-40dBm</td>
</tr>
<tr>
<td></td>
<td>0x00</td>
<td>0x18</td>
<td>-</td>
<td>&gt;-40dBm</td>
</tr>
<tr>
<td></td>
<td>0x7F</td>
<td>0xF6</td>
<td>DISPLAY_TEXT</td>
<td>&gt;-40dBm</td>
</tr>
<tr>
<td>Proactive SIM SMS</td>
<td>0x00</td>
<td>0x00</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

SMS test cases (D: Detected, B: Blocked)
### Effectiveness Evaluation

<table>
<thead>
<tr>
<th>Attack</th>
<th>SMS Payload</th>
<th>Cellular Network Params.</th>
<th>D</th>
<th>B</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Binary SMS</strong> (Interactive)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0x7F 0xF6 DISPLAY_TEXT</td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>0x7F 0xF6 SET_UP_CALL</td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>0x7F 0xF6 LAUNCH_BROWSER</td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>0x7F 0xF6 PLAY_TONE</td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>0x7F 0xF6 GET_INPUT</td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>0x7F 0xF6 SELECT_ITEM</td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>0x7F 0xF6 SET_UP_MENU</td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>0x7F 0xF6 GET_INKEY</td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td><strong>Binary SMS</strong> (Non-interactive)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0x7F 0xF6 SEND_SMS</td>
<td></td>
<td></td>
<td>✓</td>
<td>X</td>
</tr>
<tr>
<td>0x7F 0xF6 RUN_AT_CMD</td>
<td></td>
<td></td>
<td>✓</td>
<td>X</td>
</tr>
<tr>
<td><strong>Silent SMS</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0x40 0x00</td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td><strong>Flash SMS</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0x00 0x18</td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td><strong>FBS SMS</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0x00 0x00</td>
<td>&gt;-40dBm MNC MCC</td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>0x00 0x00</td>
<td>&lt;40dBm MNC MCC*</td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>0x00 0x00</td>
<td>&gt;-40dBm MNC* MCC*</td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>0x40 0x00</td>
<td>&gt;-40dBm MNC* MCC*</td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>0x00 0x18</td>
<td>&gt;-40dBm MNC* MCC*</td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>0x7F 0xF6 DISPLAY_TEXT</td>
<td>&gt;-40dBm MNC* MCC*</td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td><strong>Proactive SIM SMS</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0x00 0x00</td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

SMS test cases (D: Detected, B: Blocked)
## Effectiveness Evaluation

<table>
<thead>
<tr>
<th>Attack</th>
<th>SMS Payload</th>
<th>Malware Type</th>
<th>Malware Name</th>
<th>D</th>
<th>B</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>PID</td>
<td>DCS</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Malware SMS</td>
<td>0x00</td>
<td>0x00</td>
<td>Open-source RAT</td>
<td>AndroRAT [and]</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>0x00</td>
<td>0x00</td>
<td>Open-source RAT</td>
<td>AhMyth [and]</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>0x00</td>
<td>0x00</td>
<td>Open-source RAT</td>
<td>BetterAndroidRAT [and]</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>0x00</td>
<td>0x00</td>
<td>Open-source RAT</td>
<td>Android Trojan [and]</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>0x00</td>
<td>0x00</td>
<td>Real-world malware</td>
<td>FakeSpy [fak]</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>0x00</td>
<td>0x00</td>
<td>Real-world malware</td>
<td>Corona Updates [sms]</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>0x00</td>
<td>0x00</td>
<td>Real-world malware</td>
<td>Anubis [sms]</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>0x00</td>
<td>0x00</td>
<td>Real-world malware</td>
<td>Dendroid [sms]</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>0x00</td>
<td>0x00</td>
<td>Real-world malware</td>
<td>Ginp [sms]</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>0x00</td>
<td>0x00</td>
<td>Real-world malware</td>
<td>Golden Eagle [sms]</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>0x00</td>
<td>0x00</td>
<td>Real-world malware</td>
<td>SilkBean [sms]</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>0x00</td>
<td>0x00</td>
<td>Real-world malware</td>
<td>WolfRAT [sms]</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>0x00</td>
<td>0x00</td>
<td>Real-world malware</td>
<td>BlackRock [sms]</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>0x00</td>
<td>0x00</td>
<td>Real-world malware</td>
<td>Cerberus [sms]</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>0x00</td>
<td>0x00</td>
<td>Real-world malware</td>
<td>Mandrake [sms]</td>
<td>✓</td>
</tr>
</tbody>
</table>

Malware SMS test cases (D: Detected, B: Blocked)
# Effectiveness Evaluation

<table>
<thead>
<tr>
<th>Attack</th>
<th>SMS Payload</th>
<th>Malware Type</th>
<th>Malware Name</th>
<th>D</th>
<th>B</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>PID DCS</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0x00</td>
<td>0x00</td>
<td>Open-source RAT</td>
<td>AndroRAT [and]</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>0x00</td>
<td>0x00</td>
<td>Open-source RAT</td>
<td>AhMyth [and]</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>0x00</td>
<td>0x00</td>
<td>Open-source RAT</td>
<td>BetterAndroidRAT [and]</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>0x00</td>
<td>0x00</td>
<td>Open-source RAT</td>
<td>Android Trojan [and]</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>0x00</td>
<td>0x00</td>
<td>Real-world malware</td>
<td>FakeSpy [fak]</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>0x00</td>
<td>0x00</td>
<td>Real-world malware</td>
<td>Corona Updates [sms]</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>0x00</td>
<td>0x00</td>
<td>Real-world malware</td>
<td>Anubis [sms]</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>0x00</td>
<td>0x00</td>
<td>Real-world malware</td>
<td>Dendroid [sms]</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>0x00</td>
<td>0x00</td>
<td>Real-world malware</td>
<td>Ginp [sms]</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>0x00</td>
<td>0x00</td>
<td>Real-world malware</td>
<td>Golden Eagle [sms]</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>0x00</td>
<td>0x00</td>
<td>Real-world malware</td>
<td>SilkBean [sms]</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>0x00</td>
<td>0x00</td>
<td>Real-world malware</td>
<td>WolfRAT [sms]</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>0x00</td>
<td>0x00</td>
<td>Real-world malware</td>
<td>BlackRock [sms]</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>0x00</td>
<td>0x00</td>
<td>Real-world malware</td>
<td>Cerberus [sms]</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>0x00</td>
<td>0x00</td>
<td>Real-world malware</td>
<td>Mandrake [sms]</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

Malware SMS test cases (D: Detected, B: Blocked)
Effectiveness Evaluation

Real-world SMS events in 7 days collected by RILDENDE on the five AOSP implementations
Overhead Evaluation

(a) Power.

(b) Memory.

Overhead of RILD\textsc{efender} (A: AOSP, N6: Nexus 6, PXL: Pixel XL, P5: Pixel 5)
Overhead Evaluation

(a) Storage.

(b) Computation.

Overhead of RILDEFENDER (A: AOSP, N6: Nexus 6, PXL: Pixel XL, P5: Pixel 5)
Future Work

- Distinguish SMS attacks from benign use cases (law-enforcement tracking via silent SMS)
- Automatic prevention of baseband-only SMS attacks
- Extension to IMS-based SMS and Multimedia Messaging Service (MMS)
- Exploring vendor-specific RIL libraries and functions
Future Work

- Distinguish SMS attacks from benign use cases (law-enforcement tracking via silent SMS)
- Automatic prevention of baseband-only SMS attacks
Future Work

► Distinguish SMS attacks from benign use cases (law-enforcement tracking via silent SMS)
► Automatic prevention of baseband-only SMS attacks
► Extension to IMS-based SMS and Multimedia Messaging Service (MMS)
Future Work

- Distinguish SMS attacks from benign use cases (law-enforcement tracking via silent SMS)
- Automatic prevention of baseband-only SMS attacks
- Extension to IMS-based SMS and Multimedia Messaging Service (MMS)
- Exploring vendor-specific RIL libraries and functions
We present RILDefender, the first RIL-based defense to automatically detect and mitigate SMS attacks.

RILDefender is implemented as an extension to AOSP and evaluated for its effectiveness and overhead. The source code is available at [https://github.com/OSUSecLab/RILDefender](https://github.com/OSUSecLab/RILDefender).
Takeaway

We present **RILDefender**, the first RIL-based defense to automatically detect and mitigate SMS attacks.

We demonstrate using **RILDefender** to comprehensively defend against six types of SMS attacks.
We present RILDefender, the first RIL-based defense to automatically detect and miti- gated SMS attacks. We demonstrate using RILDefender to comprehensively defend against six types of SMS attacks. We implement RILDefender as an extension to AOSP and evaluate its effectiveness and overhead.
Takeaway

We present RILDefender, the first RIL-based defense to automatically detect and mitigate SMS attacks.
We demonstrate using RILDefender to comprehensively defend against six types of SMS attacks.
We implement RILDefender as an extension to AOSP and evaluate its effectiveness and overhead.

The source code is available at https://github.com/OSUSecLab/RILDefender.
Thank You

**RILDefender Source Code:** [github.com/OSUSecLab/RILDefender](https://github.com/OSUSecLab/RILDefender)

**RILDefender Video:** [5GSec.com/distro/RILDefender.mp4](http://5GSec.com/distro/RILDefender.mp4)
References

---


Sms control, technique t1582 - mobile, https://attack.mitre.org/techniques/T1582/.