Thwarting Smartphone SMS Attacks at the Radio Interface Layer

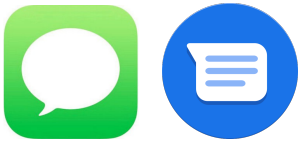
Haohuang Wen[1], Phillip Porras[2], Vinod Yegneswaran[2], and Zhiqiang Lin[1]

[1]The Ohio State University, [2]SRI International

Feb 28th, 2023

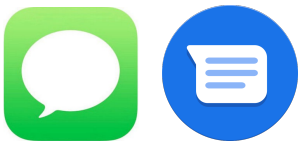
In Proceedings of the 30th ISOC Network and Distributed System Security Symposium (NDSS'23), San Diego, CA, February 2023

Short Message Service (SMS)



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

Short Message Service (SMS)

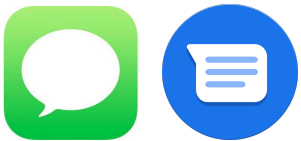


- Introduced since December, 1992
- Defined in 3GPP TS 23.040 [3gp]

Applications

- Text-based messaging

Short Message Service (SMS)

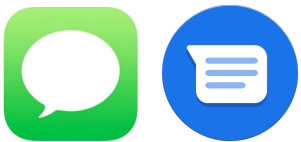


- Introduced since December, 1992
- Defined in 3GPP TS 23.040 [3gp]

Applications

- Text-based messaging
- Two-factor authentication

Short Message Service (SMS)

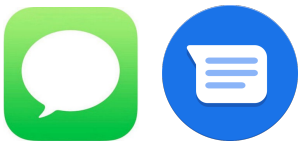


- Introduced since December, 1992
- Defined in 3GPP TS 23.040 [3gp]

Applications

- Text-based messaging
- Two-factor authentication
- Alerts & notifications

Short Message Service (SMS)

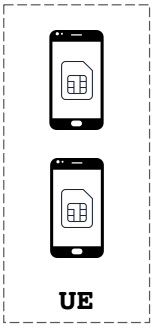


- Introduced since December, 1992
- Defined in 3GPP TS 23.040 [3gp]

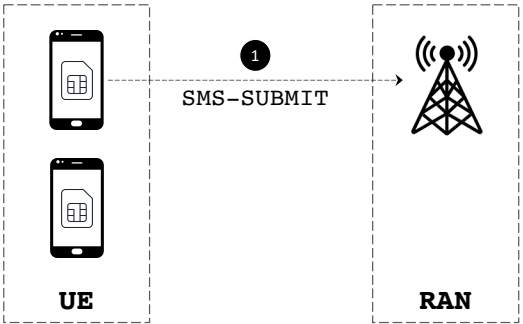
Applications

- Text-based messaging
- Two-factor authentication
- Alerts & notifications
- Marketing & advertising
- .....

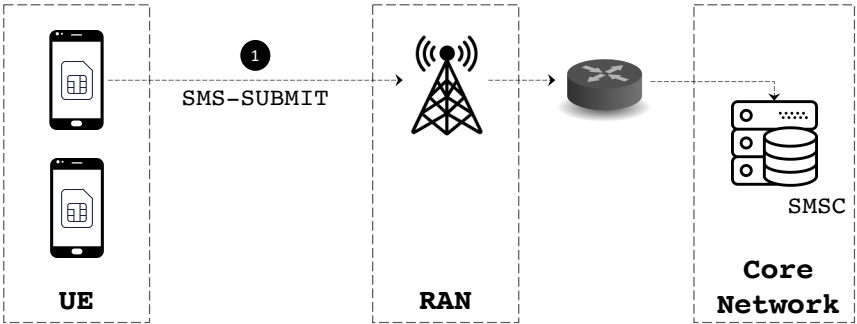
SMS Transmission Path in Cellular Network



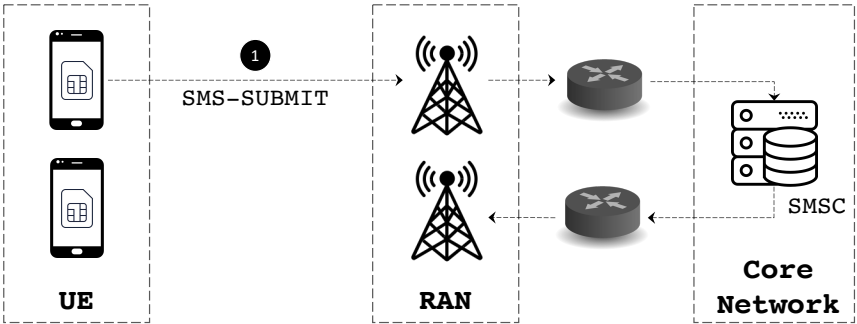
SMS Transmission Path in Cellular Network



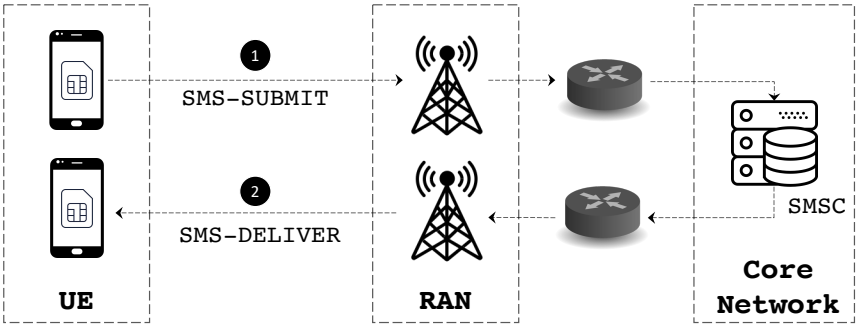
SMS Transmission Path in Cellular Network



SMS Transmission Path in Cellular Network

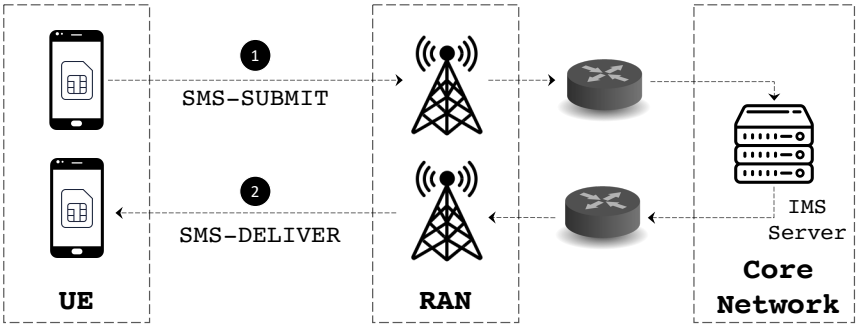


SMS Transmission Path in Cellular Network



SMSC-Based SMS (2G/3G)

SMS Transmission Path in Cellular Network



IMS-Based SMS (4G+)

Exploiting SMS

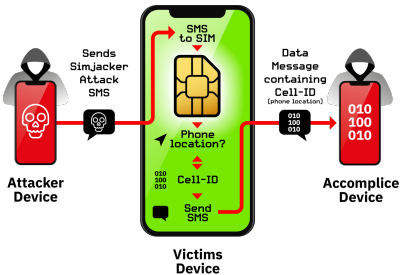
- SMS is **not** just a *text-based service*

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

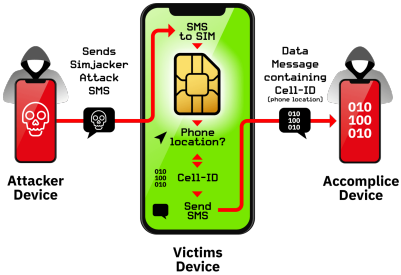
- SMS is **not** just a *text-based service*
- Zero-click exploits exist in various ways to compromise security, privacy and availability without the user's knowledge and consent



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



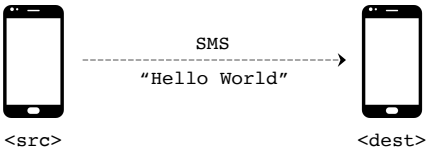
SimJacker Attack [sim]

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

Exploiting SMS

SMS PDU Payload

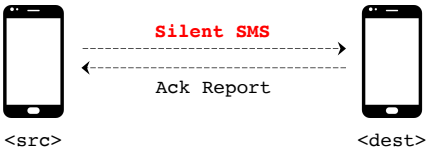
Field	SCA	FO	OA/DA	PID	DCS	...	UDL	UD
Value	-	01	<dest>	00	00		0C	C8329BF...



Exploiting SMS

SMS PDU Payload

Field	SCA	FO	OA/DA	PID	DCS	...	UDL	UD
Value	-	01	<dest>	40	00		0C	C8329BF...

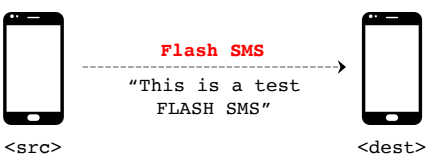


UE will not display silent SMS to user

Exploiting SMS

SMS PDU Payload

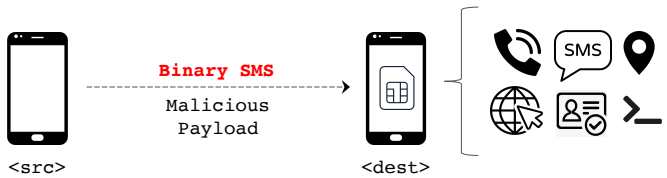
Field	SCA	FO	OA/DA	PID	DCS	...	UDL	UD
Value	-	01	<dest>	00	18		0C	C8329BF...



Exploiting SMS

SMS PDU Payload

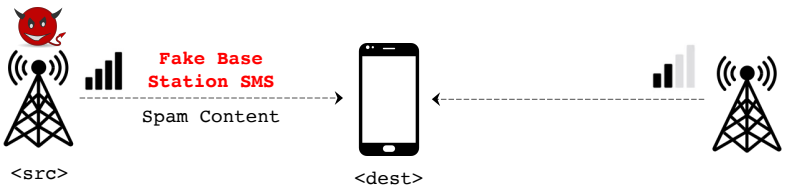
Field	SCA	FO	OA/DA	PID	DCS	...	UDL	UD
Value	-	01	<dest>	7F	F6		0C	<Payload>



Exploiting SMS

SMS PDU Payload

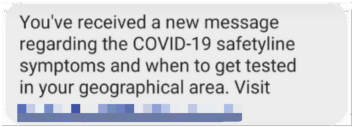
Field	SCA	FO	OA/DA	PID	DCS	...	UDL	UD
Value	-	01	<dest>	00	00		0C	Spam Content



Exploiting SMS

SMS PDU Payload

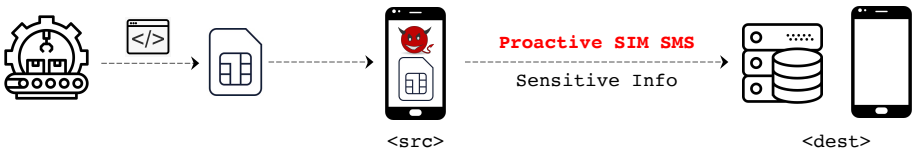
Field	SCA	FO	OA/DA	PID	DCS	...	UDL	UD
Value	-	01	<dest>	00	00		0C	Spam Content



Exploiting SMS

SMS PDU Payload

Field	SCA	FO	OA/DA	PID	DCS	...	UDL	UD
Value	-	01	<dest>	00	00		0C	Sensitive Info



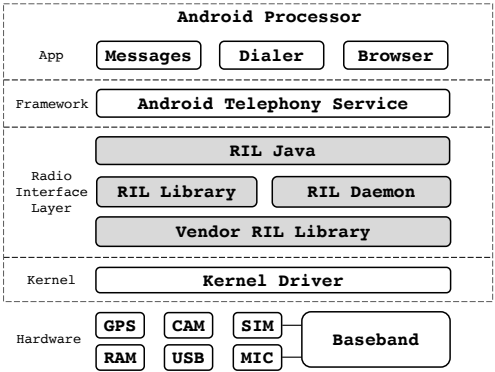
Exploitation Cost

Pre-paid SIM: $5

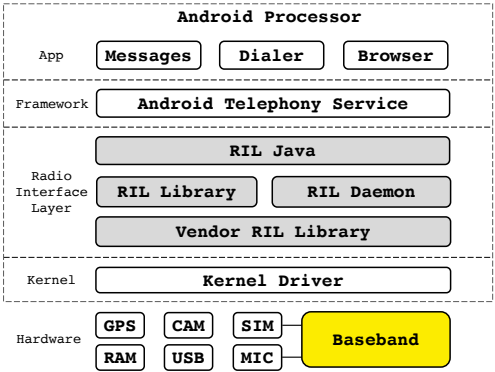
GSM USB Modem: $15

Total Cost: As low as $20!

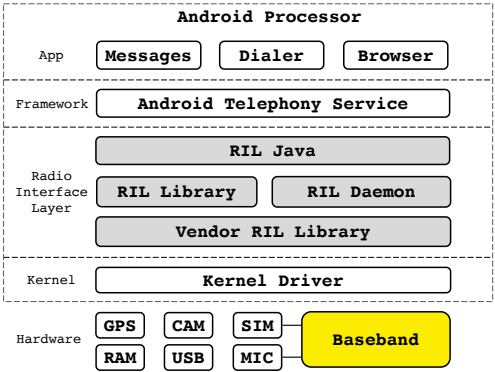
Defending Against SMS Attacks



Defending Against SMS Attacks



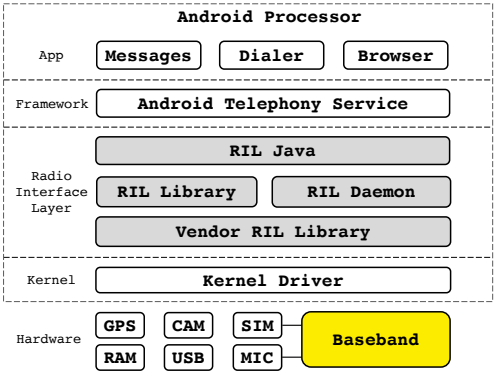
Defending Against SMS Attacks



Baseband-Layer Defenses

- FBS Detection in Qualcomm chips [qua]

Defending Against SMS Attacks



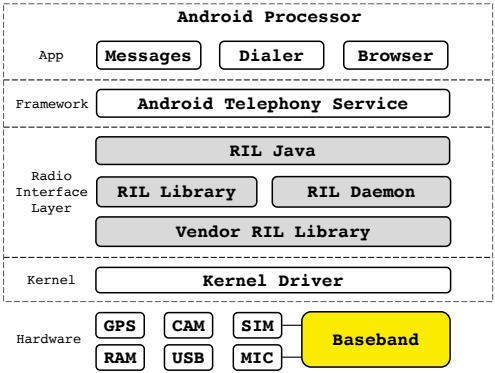
Baseband-Layer Defenses

- FBS Detection in Qualcomm chips [qua]

Pros

+ High visibility
+ Mitigation capability

Defending Against SMS Attacks



Baseband-Layer Defenses

- FBS Detection in Qualcomm chips [qua]

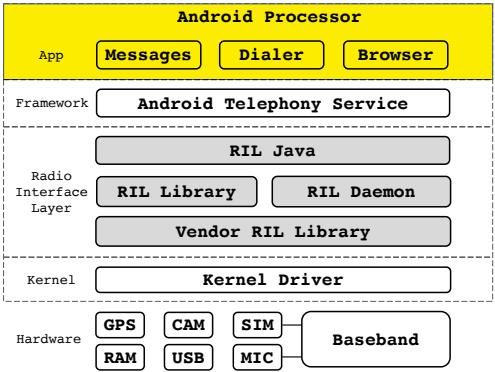
Pros

+ High visibility
+ Mitigation capability

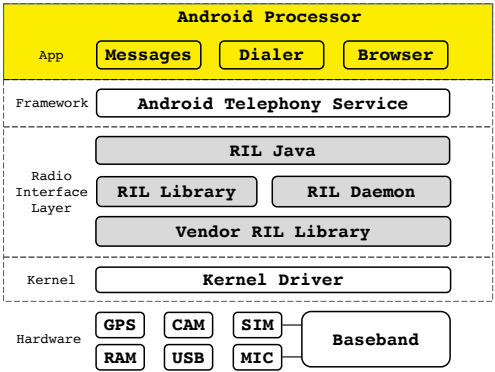
Cons

– Closed-source
– Integrity-protected
– Highly customized implementation

Defending Against SMS Attacks



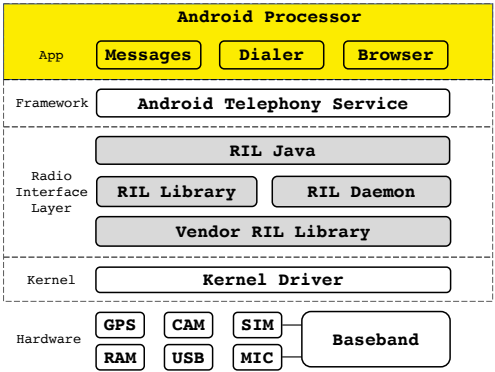
Defending Against SMS Attacks



App-Layer Defenses

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

Defending Against SMS Attacks



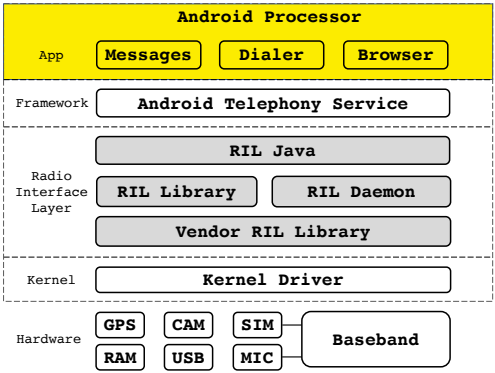
App-Layer Defenses

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

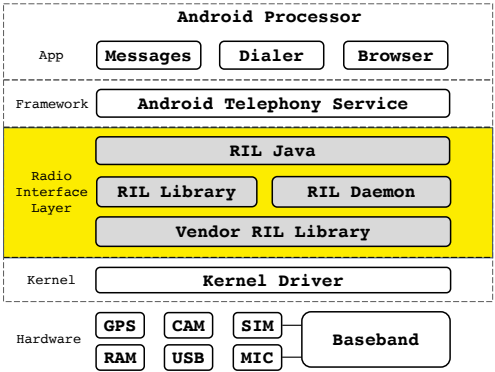
Pros

+ Low deployment cost

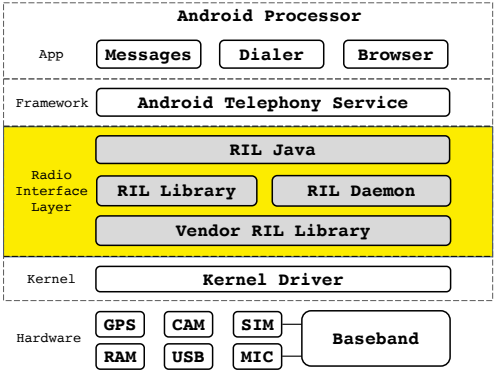
Cons

– Low visibility
– Passive detection only
– Root required

RILDefender Overview



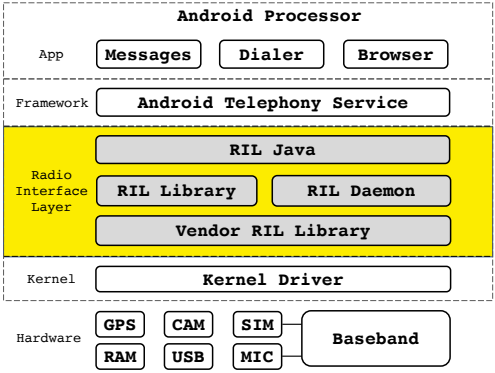
RILDefender Overview



RIL-layer Defenses

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

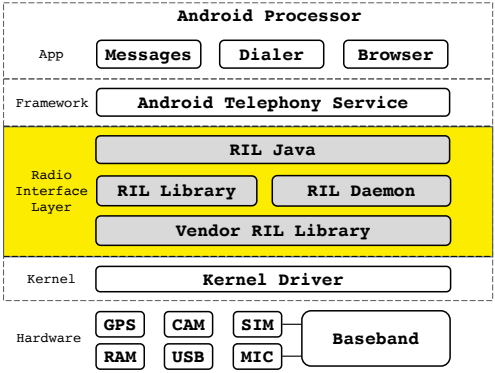
RILDefender Overview



RIL-layer Defenses

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

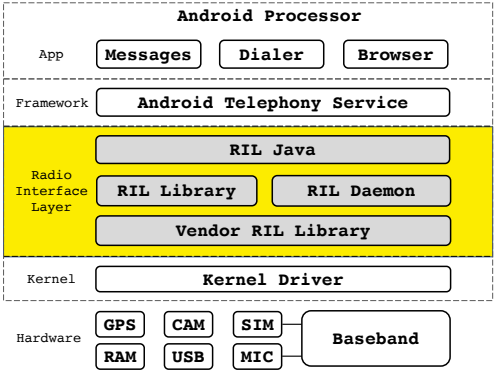
RILDefender Overview



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



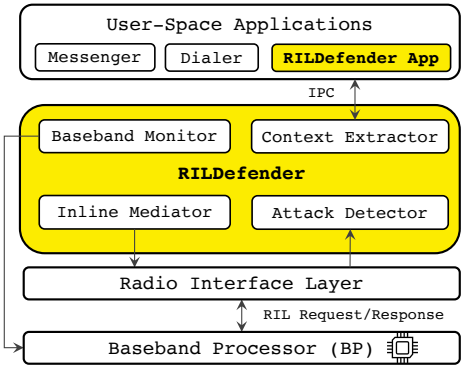
RIL-layer Defenses

- 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

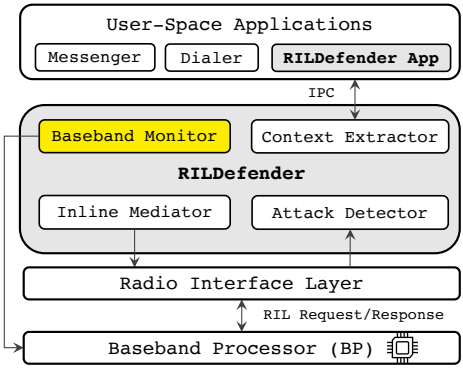
RILDefender At the Radio Interface Layer



RILDefender Architecture

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

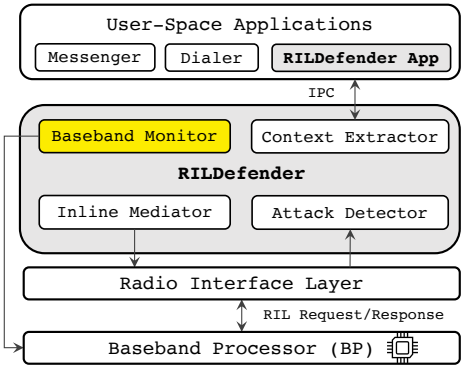
RILDefender At the Radio Interface Layer



Baseband Monitor

- Monitor baseband-only SMS attacks (one exception)

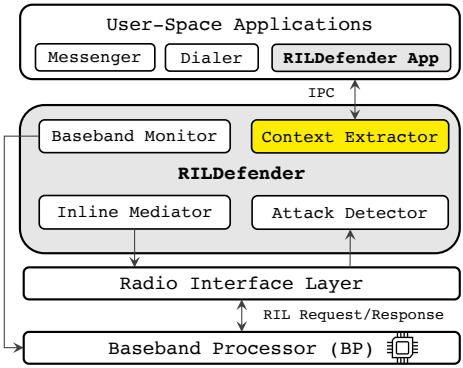
RILDefender At the Radio Interface Layer



Baseband Monitor

- Monitor baseband-only SMS attacks (one exception)
- Interpret baseband traffic from diagnostic interfaces (e.g., `/dev/diag`)
- Adapted from existing libraries [sno]

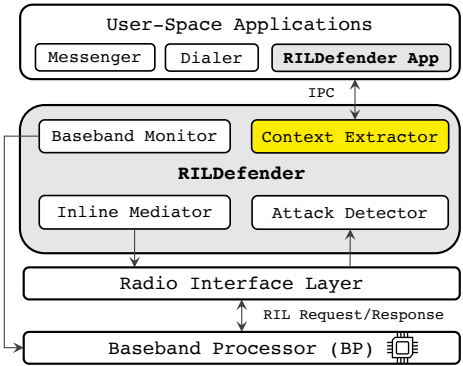
RILDefender At the Radio Interface Layer



Context Extractor

- Track context of user-space applications (e.g., SMS sender PID)

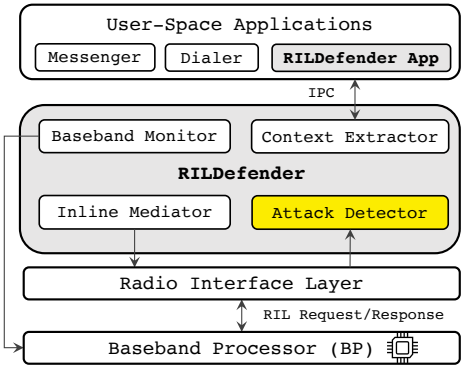
RILDefender At the Radio Interface Layer



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

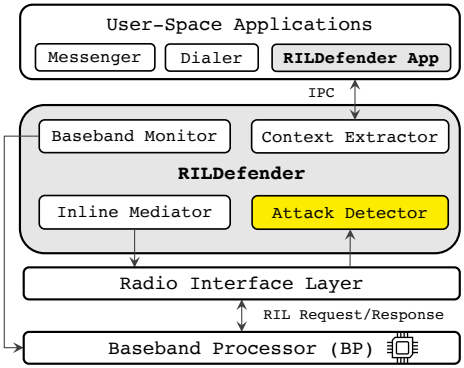
RILDefender At the Radio Interface Layer



Attack Detector

- Instrument the main RIL handler

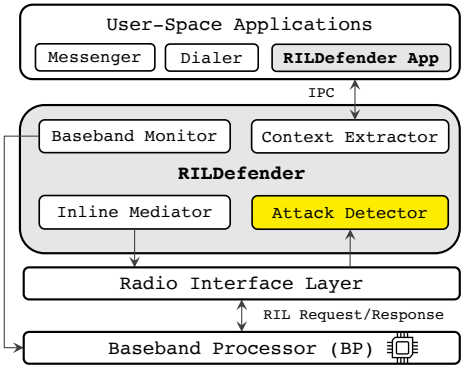
RILDefender At the Radio Interface Layer



Attack Detector

- Instrument the main RIL handler
- Synthesize SMS payload and information from other component

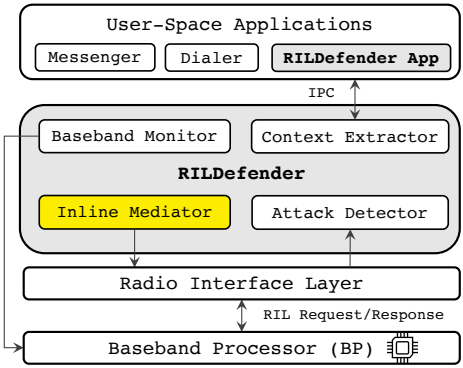
RILDefender At the Radio Interface Layer



Attack Detector

- Instrument the main RIL handler
- Synthesize SMS payload and information from other component
- Load user-defined attack signature set

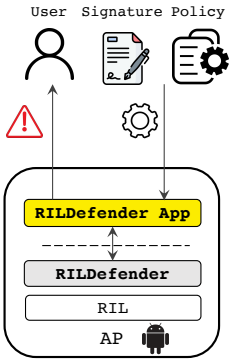
RILDefender At the Radio Interface Layer



Inline Mediator

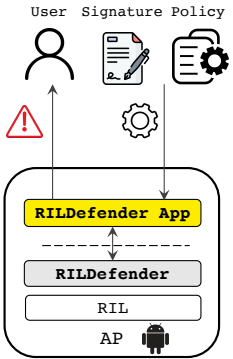
- Instrument the RIL logic for attack prevention
- Interact through specific RIL commands

RILDefender at the Application Layer



RILDefender App

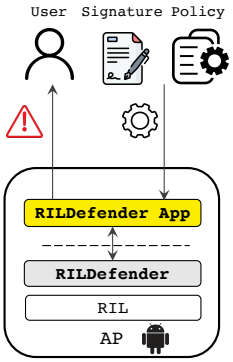
RILDefender at the Application Layer



RILDefender App

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

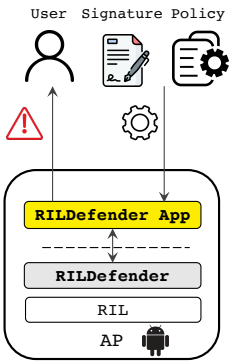
RILDefender at the Application Layer



RILDefender App

- Configure security level for each attack
  - Block and Notify
  - Block without Notify
  - Notify only
  - Allow
- Receive real-time alerts for attack events

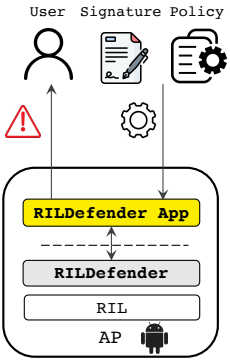
RILDefender at the Application Layer

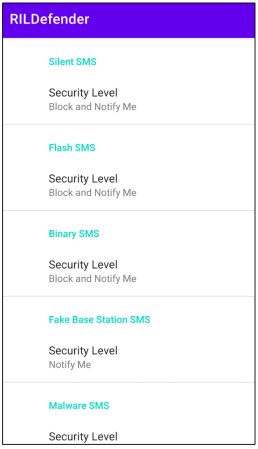


RILDefender App

- 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

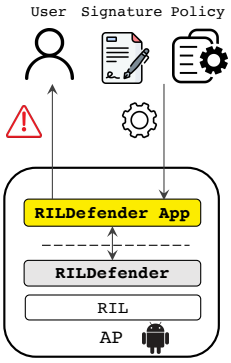
RILDefender at the Application Layer

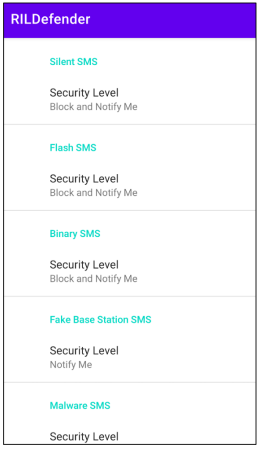




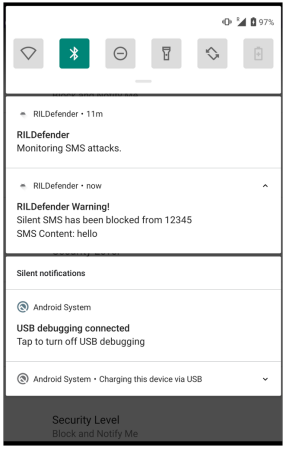
Configuration UI

RILDefender at the Application Layer





Configuration UI



Alert UI

RILDefender at the Application Layer

Category	SMS Feature
SMS Fields	$sms.mti$
	$sms.smsc$
	$sms.oa$
	$sms.da$
	$sms.scts$
	$sms.pid$
	$sms.dcs$
	$sms.udl$
	$sms.ud$
	$sms.proactiveCmd$
SMS Context	$sms.src$
	$sms.ts$
	$bs.\overline{ss}$
	$bs.mcc$
	$bs.mnc$
	$bs.cid$
	$bs.lac$
	$bs.arfcn$
	$bs.rat$
SMS Events	$evnetCount$
	$\{sms_1, ..., sms_n\}$

RILDefender at the Application Layer

Category	SMS Feature
SMS Fields	$sms.mti$
	$sms.smsc$
	$sms.oa$
	$sms.da$
	$sms.scts$
	$sms.pid$
	$sms.dcs$
	$sms.udl$
	$sms.ud$
	$sms.proactiveCmd$
SMS Context	$sms.src$
	$sms.ts$
	$bs.\overline{ss}$
	$bs.mcc$
	$bs.mnc$
	$bs.cid$
	$bs.lac$
	$bs.arfcn$
	$bs.rat$
SMS Events	$evnetCount$
	$\{sms_1, ..., sms_n\}$

```
<Rule>    → <RuleName>: <Expr>
<Expr>    → { lvalue: <Value>
              opCode: <Op>
              condition: <Cond>
              rvalue: <Value> }
<Value>   → <Feature> | <Const> | <Expr> | List(<Expr>)
<OpCode>  → + | - | * | / | & | | | ^ | && | || | << | >>
<Cond>    → == | != | > | < | >= | <=
<Feature> → sms.mti | sms.smsc | 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>
```

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

Implementation and Experiment Setup

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

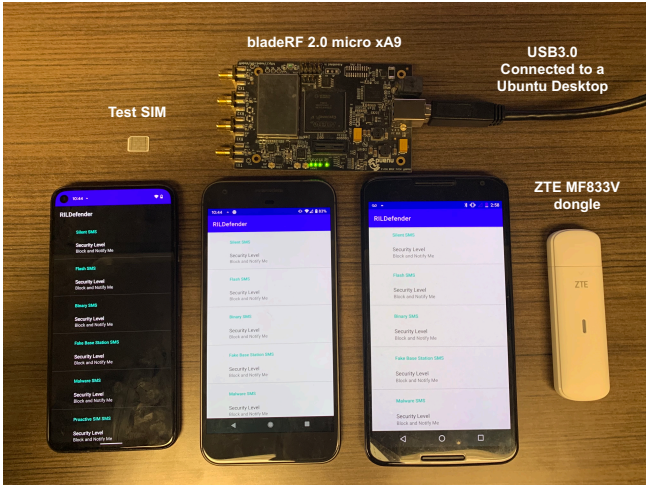
Smartphone UEs and AOSP versions that RILDefender has been implemented on and evaluated

Implementation and Experiment Setup

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

Smartphone UEs and AOSP versions that RILDefender has been implemented on and evaluated

Implementation and Experiment Setup



Effectiveness Evaluation

Attack	SMS Payload			Cellular Network Params.			D	B
	PID	DCS	Proactive CMD	TxPower	MNC	MCC		
Binary SMS (Interactive)	0x7F	0xF6	DISPLAY_TEXT	-	-	-	✓	✓
	0x7F	0xF6	SET_UP_CALL	-	-	-	✓	✓
	0x7F	0xF6	LAUNCH_BROWSER	-	-	-	✓	✓
	0x7F	0xF6	PLAY_TONE	-	-	-	✓	✓
	0x7F	0xF6	GET_INPUT	-	-	-	✓	✓
	0x7F	0xF6	SELECT_ITEM	-	-	-	✓	✓
	0x7F	0xF6	SET_UP_MENU	-	-	-	✓	✓
	0x7F	0xF6	GET_INKEY	-	-	-	✓	✓
Binary SMS (Non-interactive)	0x7F	0xF6	SEND_SMS	-	-	-	✓	✗
	0x7F	0xF6	RUN_AT_CMD	-	-	-	✓	✗
Silent SMS	0x40	0x00	-	-	-	-	✓	✓
Flash SMS	0x00	0x18	-	-	-	-	✓	✓
FBS SMS	0x00	0x00	-	>-40dBm	MNC	MCC	✓	✓
	0x00	0x00	-	<-40dBm	MNC*	MCC*	✓	✓
	0x00	0x00	-	>-40dBm	MNC*	MCC*	✓	✓
	0x40	0x00	-	>-40dBm	MNC*	MCC*	✓	✓
	0x00	0x18	-	>-40dBm	MNC*	MCC*	✓	✓
	0x7F	0xF6	DISPLAY_TEXT	>-40dBm	MNC*	MCC*	✓	✓
Proactive SIM SMS	0x00	0x00	-	-	-	-	✓	✓

SMS test cases (D: Detected, B: Blocked)

Effectiveness Evaluation

Attack	SMS Payload			Cellular Network Params.			D	B
	PID	DCS	Proactive CMD	TxPower	MNC	MCC		
Binary SMS (Interactive)	0x7F	0xF6	DISPLAY_TEXT	-	-	-	✓	✓
	0x7F	0xF6	SET_UP_CALL	-	-	-	✓	✓
	0x7F	0xF6	LAUNCH_BROWSER	-	-	-	✓	✓
	0x7F	0xF6	PLAY_TONE	-	-	-	✓	✓
	0x7F	0xF6	GET_INPUT	-	-	-	✓	✓
	0x7F	0xF6	SELECT_ITEM	-	-	-	✓	✓
	0x7F	0xF6	SET_UP_MENU	-	-	-	✓	✓
	0x7F	0xF6	GET_INKEY	-	-	-	✓	✓
Binary SMS (Non-interactive)	0x7F	0xF6	SEND_SMS	-	-	-	✓	✗
	0x7F	0xF6	RUN_AT_CMD	-	-	-	✓	✗
Silent SMS	0x40	0x00	-	-	-	-	✓	✓
Flash SMS	0x00	0x18	-	-	-	-	✓	✓
FBS SMS	0x00	0x00	-	>-40dBm	MNC	MCC	✓	✓
	0x00	0x00	-	<-40dBm	MNC*	MCC*	✓	✓
	0x00	0x00	-	>-40dBm	MNC*	MCC*	✓	✓
	0x40	0x00	-	>-40dBm	MNC*	MCC*	✓	✓
	0x00	0x18	-	>-40dBm	MNC*	MCC*	✓	✓
	0x7F	0xF6	DISPLAY_TEXT	>-40dBm	MNC*	MCC*	✓	✓
Proactive SIM SMS	0x00	0x00	-	-	-	-	✓	✓

SMS test cases (D: Detected, B: Blocked)

Effectiveness Evaluation

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

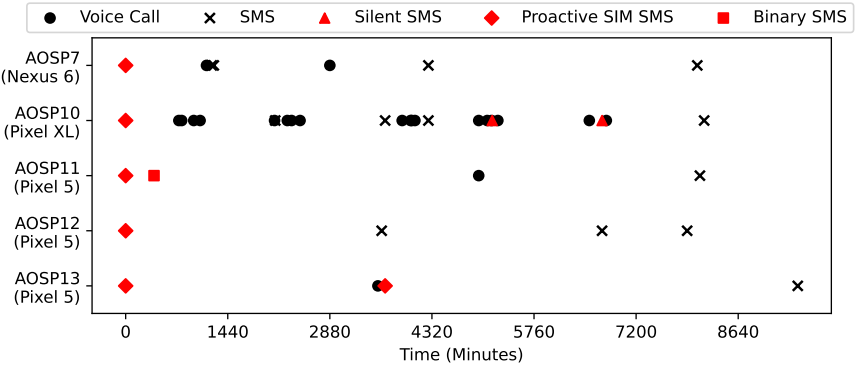
Malware SMS test cases (D: Detected, B: Blocked)

Effectiveness Evaluation

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

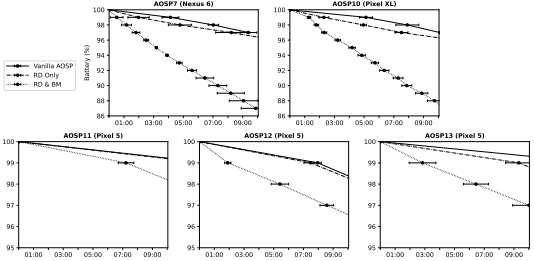
Malware SMS test cases (D: Detected, B: Blocked)

Effectiveness Evaluation

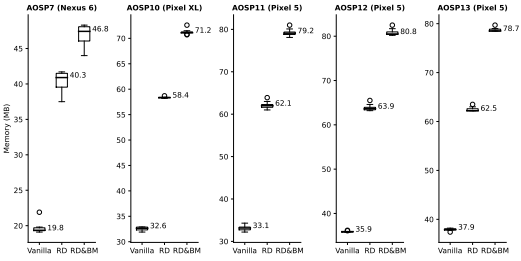


Real-world SMS events in 7 days collected by RILDefender on the five AOSP implementations

Overhead Evaluation



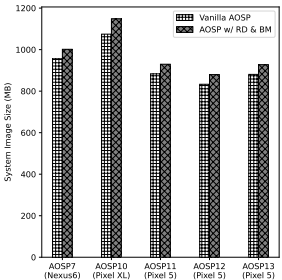
(a) Power.



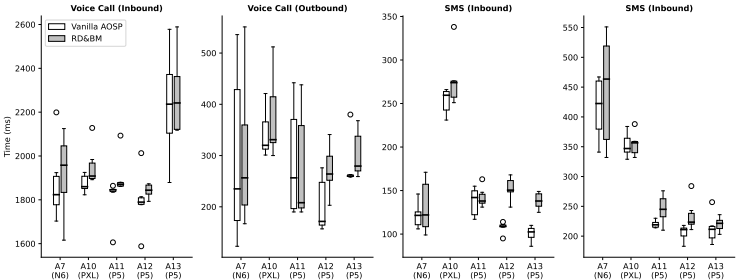
(b) Memory.

Overhead of RILDefender (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

Future Work

- Distinguish SMS attacks from benign use cases (law-enforcement tracking via silent SMS)

Future Work

Future Work

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

Future Work

Future Work

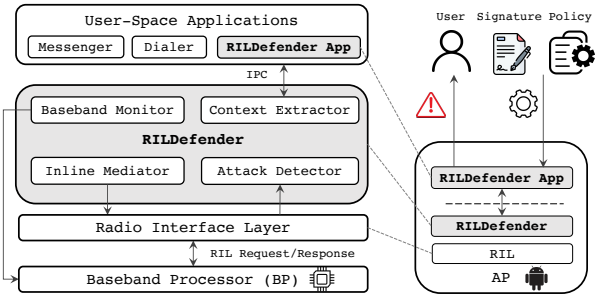
- Distinguish SMS attacks from benign use cases (law-enforcement tracking via silent SMS)
- Automatic prevention of baseband-only SMS attacks
- Extension to IMS-based SMS and Multimedia Messaging Service (MMS)

Future Work

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

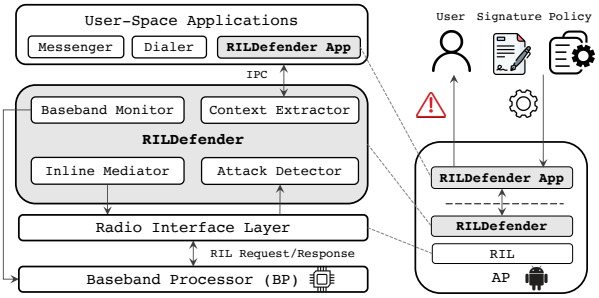
Takeaway



RILDefender

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

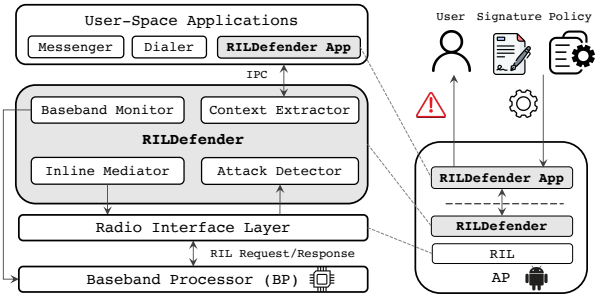
Takeaway



RILDefender

- 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.

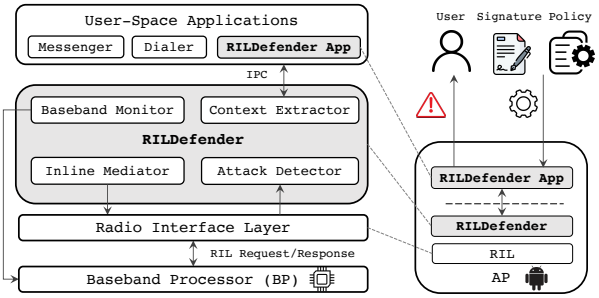
Takeaway



RILDefender

- 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.

Takeaway



RILDefender

- 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

Sec.Com

The Ohio State University

SRI International

RILDefender Source Code: *github.com/OSUSecLab/RILDefender*

RILDefender Video: *5GSec.com/distro/RILDefender.mp4*

References I

Etsi ts 123 040 v12.2.0, https://www.etsi.org/deliver/etsi_ts/123000_123099/123040/12.02.00_60/ts_123040v120200p.pdf.

Android imsi-catcher detector, https://cellularprivacy.github.io/Android-IMSI-Catcher-Detector.

Remote access tool trojan list - android, https://github.com/wishihab/Android-RATList.

Mitziu Echeverria, Zeeshan Ahmed, Bincheng Wang, M Fareed Arif, Syed Rafiul Hussain, and Omar Chowdhury, *Phoenix: Device-centric cellular network protocol monitoring using runtime verification*, Network and Distributed Systems Security (NDSS) Symposium, 2021.

Fakespy android malware spread via 'postal-service' apps, https://threatpost.com/fakespy-android-malware-spread-via-postal-service-apps/157102/.

Byeongdo Hong, Shinjo Park, Hongil Kim, Dongkwan Kim, Hyunwook Hong, Hyunwoo Choi, Jean-Pierre Seifert, Sung-Ju Lee, and Yongdae Kim, *Peeking over the cellular walled gardens-a method for closed network diagnosis*, IEEE Transactions on Mobile Computing **17** (2018), no. 10, 2366–2380.

Yuanjie Li, Chunyi Peng, Zengwen Yuan, Jiayao Li, Haotian Deng, and Tao Wang, *Mobileinsight: Extracting and analyzing cellular network information on smartphones*, Proceedings of the 22nd Annual International Conference on Mobile Computing and Networking, 2016, pp. 202–215.

Qualcomm reveals demo to prevent smartphones from being hacked by connecting to fake base stations, https://iphonewired.com/news/259588/.

Simjacker, https://simjacker.com.

References II


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


Snoopsnitch, https://opensource.srlabs.de/projects/snoopsnitch.