ATtention Spanned: Comprehensive Vulnerability Analysis of AT Commands Within the Android Ecosystem

Dave (Jing) Tian*, Grant Hernandez*, Joseph Choi*, Vanessa Frost*, Christie Ruales*,
Patrick Traynor*, Hayawardh Vijayakumar**, Lee Harrison**,
Amir Rahmati**^, Michael Grace**, Kevin Butler*

*University of Florida, Gainesville, FL
**Samsung Research America (SRA), Mountain View, CA
^Stony Brook University, Stony Brook, NY

USENIX Security '18, Baltimore, MD
Aug 15, 2018

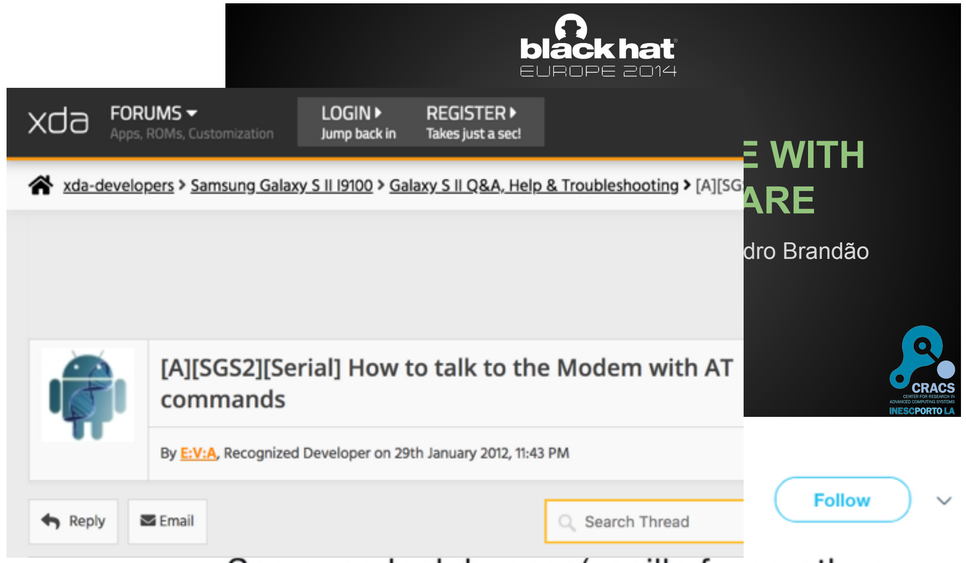
Those BBS Days…

Modem A	Modem B
ATDT15551234	
	RING
	ATA
CONNECT	*CONNECT*
abcdef	*abcdef*
	+++
	OK
	ATH
NO CARRIER	*OK*

Motivation

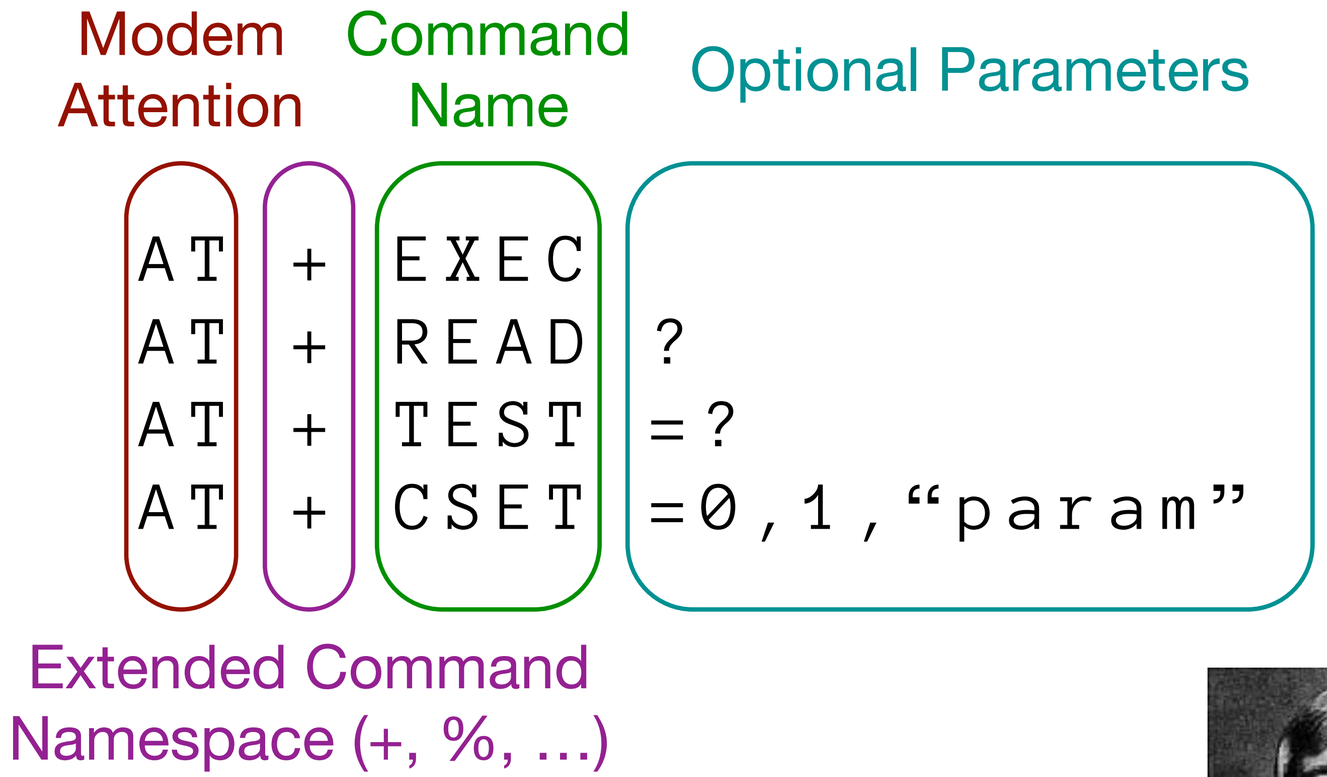
- **AT commands are not new…**
  - The prevalence is unclear
  - The functionality is unclear
  - The security impact is unclear

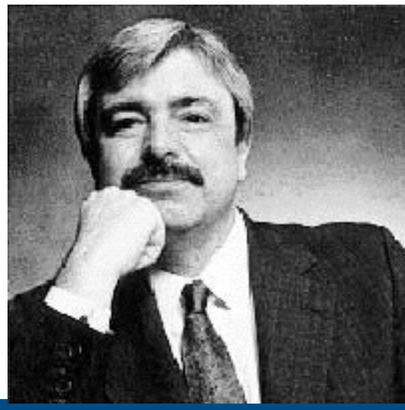
- **A systematic study of AT commands within the Android ecosystem**
  - How to find them?
  - How to test them?
  - How to abuse them?



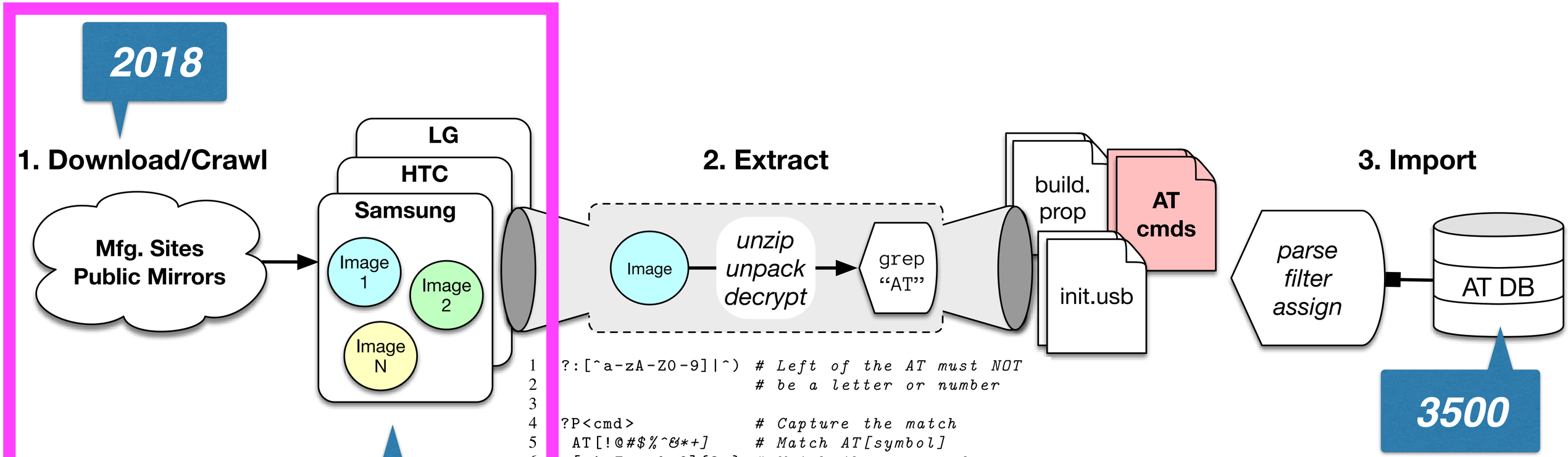
AT Commands

- **Hayes**
  - ATD
- **ITU-T/ETSI**
  - AT+CMGS
- **Android Ecosystem**
  - AT+USBDEBUG





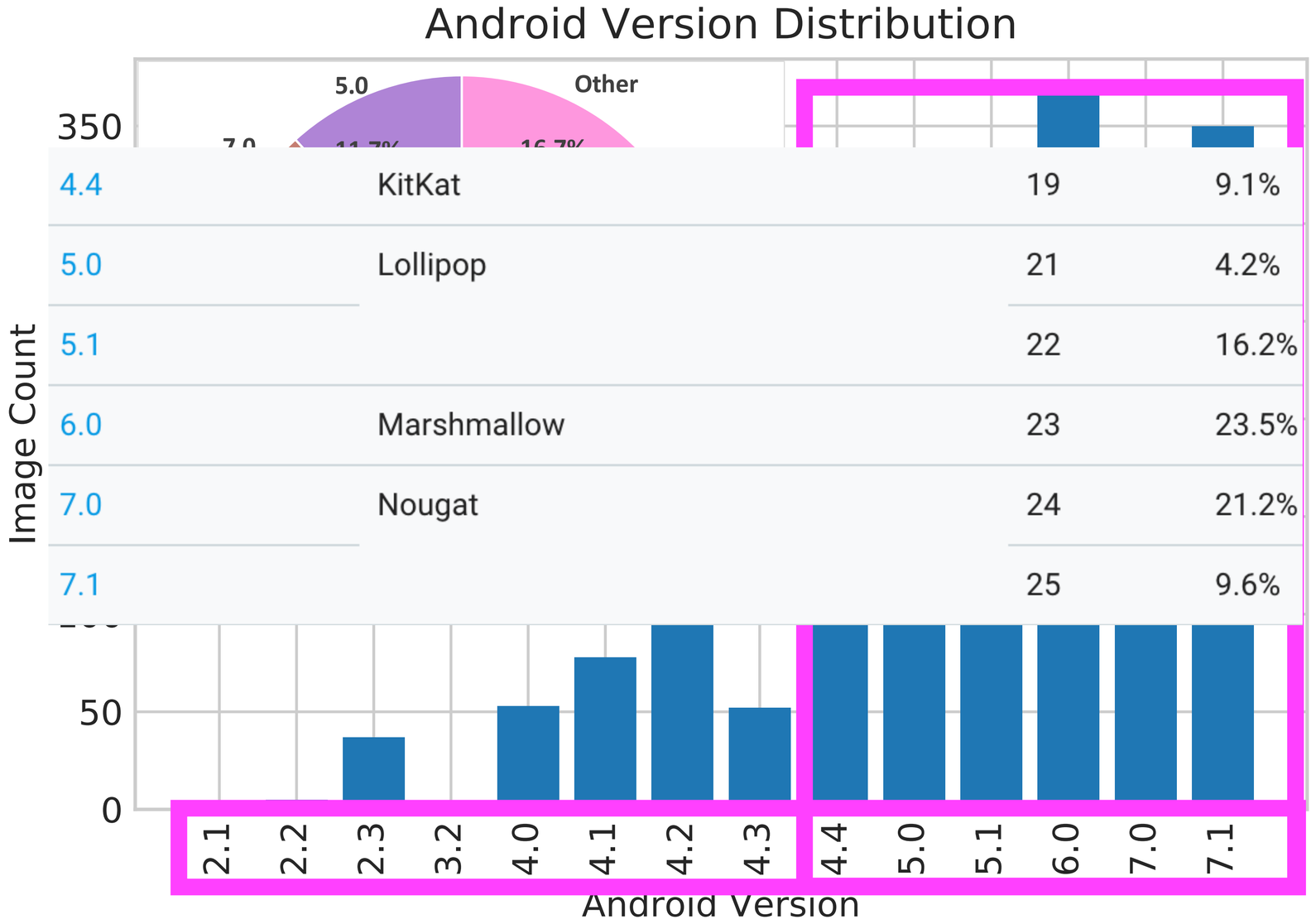
How to find them?



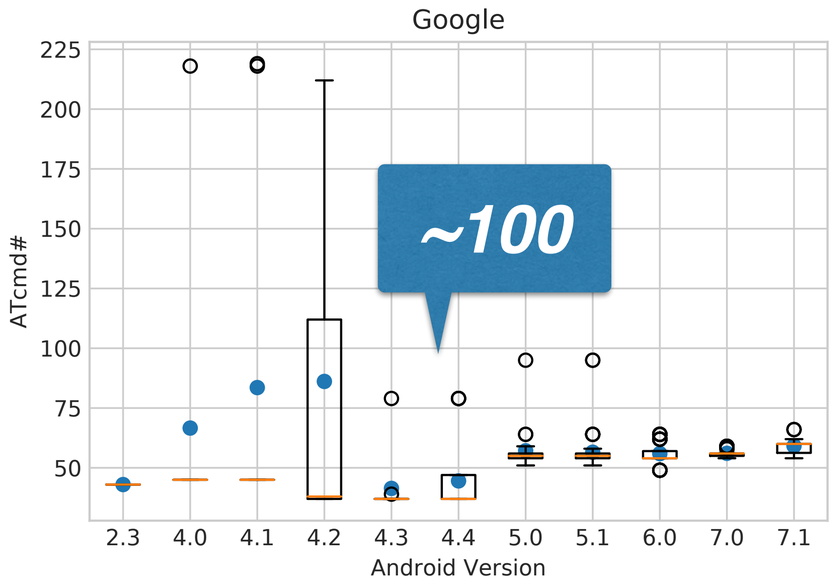

```
1  ?:[^a-zA-Z0-9]|^)  # Left of the AT must NOT
2                     # be a letter or number
3
4  ?P<cmd>            # Capture the match
5   AT[!@#$%^&*+]     # Match AT[symbol]
6   [_A-Za-z0-9]{3,}  # Match the name and
7
8
9  ?P<arg>            # Capture the match
10  \?   |            # Match AT+READ?
11                    # Match AT+CSET=0,1,"param"
12  =["'+=;%,?A-Za-z0-9]+ |
13  =\? |             # Match AT+TEST=?
14  =                 # Match a blank parameter
15 )?                 # Match AT+EXEC
```

Specification	Usage	# of AT Commands
Hayes [16, 17]	Basic	46
ITU-T V.250 [35]	Application	61
ETSI GSM 07.05 [25]	SMS	20
ETSI TS 100 916 [26]	GSM	95
Total (unique)		222

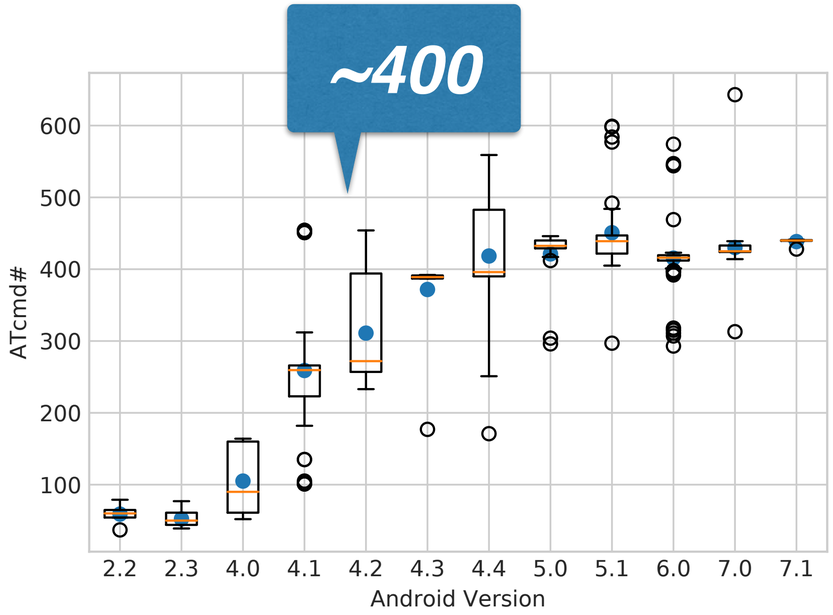
Android Version Distribution



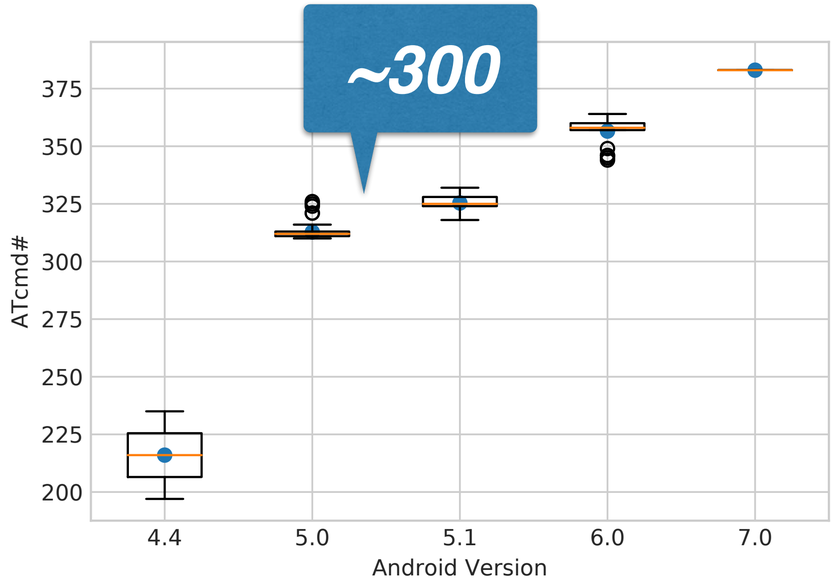
ATcmd Distribution Per Vendor



Google



Samsung



LG

How to test them?

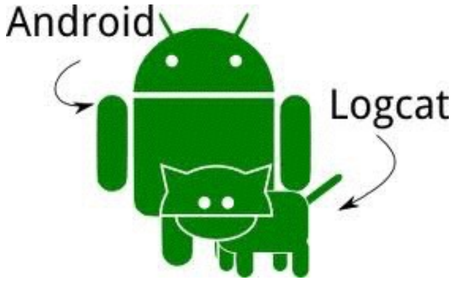
- **Setup**
  - A USB connection
- **Requirement**
  - A USB CDC ACM interface

Android Devices Tested

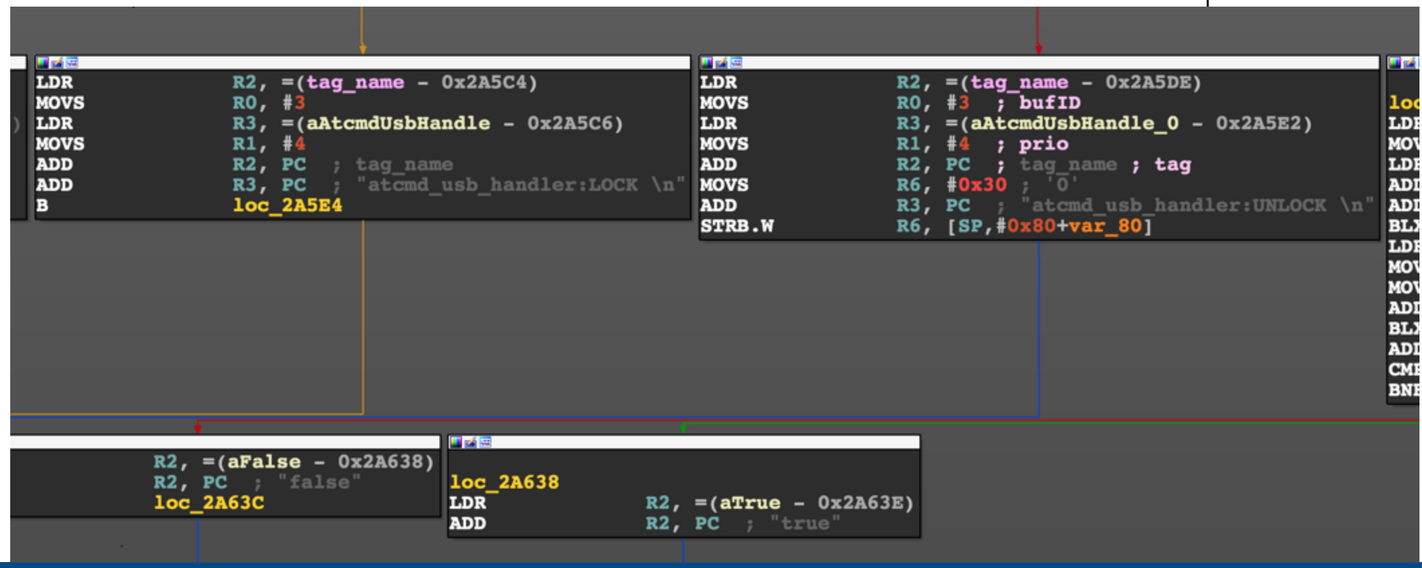
Device	Android Ver#	Modem Exposed
Samsung Galaxy Note 2	4.4.2	Y
Samsung Galaxy S7 Edge	7.0	Y
Samsung Galaxy S8 Plus	7.0	Y
LG G3	6.0	Y
LG G4	6.0	Y
HTC One	4.4.2	Y*
HTC Desire 626	5.1	N
Asus ZenPhone 2	5.0	Y (root)
Asus ZenPad	5.0.2	Y (root)
Google Nexus 5	5.1.1	Y (root)
Google Nexus 5X	6.0	Y (root)
Google Nexus 6P	7.1.1	N*
Google Pixel	7.1.1	N
Motorola Moto X	5.1	N*

How to abuse them?

- **When the reply is "OK"…**
  - Dynamic Analysis
  - Static Analysis



Google	ATcmd#
/vendor/lib/libsec-ril_lte.so	183
/lib/libxgold-ril.so	73
/lib/libreference-ril.so	37
/lib/hw/bluetooth.default.so	23
/lib/bluez-plugin/audio.so	19
Samsung	
/bin/at_distributor	331
/app/FactoryTest_CAM.apk	145
/bin/sec_atd	142

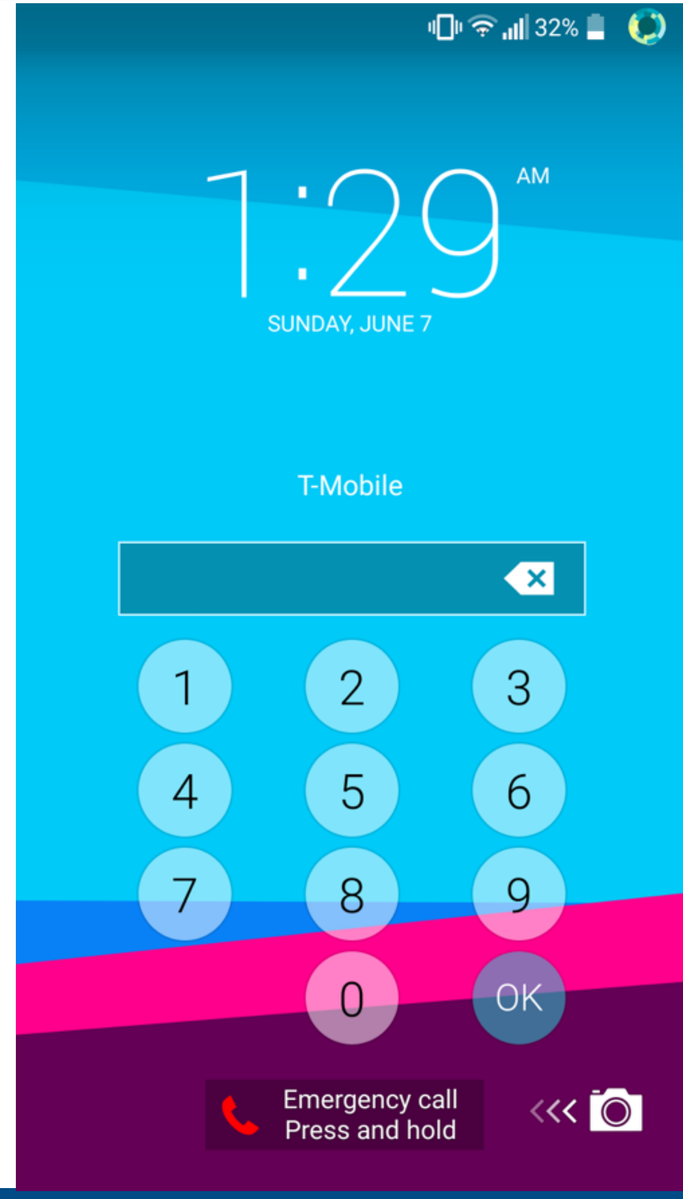


Firmware Flashing

- AT%DLOAD
- AT+SUDDLMOD=0,0
- AT+FUS?
- AT%FRST
- AT+CRST=FS
- AT+FACTORST=0,0
- AT%MODEMRESET
- AT%RESTART

Android Security Bypassing

- ATD
- ATH
- ATA
- AT%IMEI=[param]
- AT%USB=adb
- AT%KEYLOCK=0
- AT+CKPD
- AT+CMGS
- AT+CGDATA



Sensitive Information Leaking

- **34 AT commands**
- AT+DEVCONINFO
- AT+IMEINUM
- AT+SIZECHECK
- AT+CLAC
- AT$QCCLAC
- AT%PROCCAT
- AT%SYSCAT

```
[['AT+DEVCONINFO\r+DEVCONINFO:
MN(SM-G955U);BASE(SM-N900);VER(G955USQU1AQD9/
G955UOYN1AQD9/G955USQU1AQD9/G955USQU1AQD9);
HIDVER(G955USQU1AQD9/G955UOYN1AQD9/G955USQU1AQD9/
G955USQU1AQD9);MNC();MCC();PRD(VZW);;OMCCODE();
SN(R38HC09NWMR);IMEI(354003080061555);
UN(9887BC45395656444F);PN();CON(AT,MTP);LOCK(NONE);
LIMIT(FALSE);SDP(RUNTIME);HVID(Data:196609,
Cache:262145,System:327681);USER(OWNER)\r',
'#OK#\r', 'OK\r']]
```

AT%PROCCAT=../arbitrary/file

Modem AT Proxy

- AT+TRACE
- AT+XDBGCONF
- AT+XABBTRACE
- AT+XSYSTRACE
- AT+XLOG=95,1

- https://forum.xda-developers.com/galaxy-s2/help/how-to-talk-to-modem-commands-t1471241
- https://software.intel.com/en-us/blogs/2015/04/30/new-intel-usb-driver-version-190-for-android-devices-available-for-download

Hidden Menus

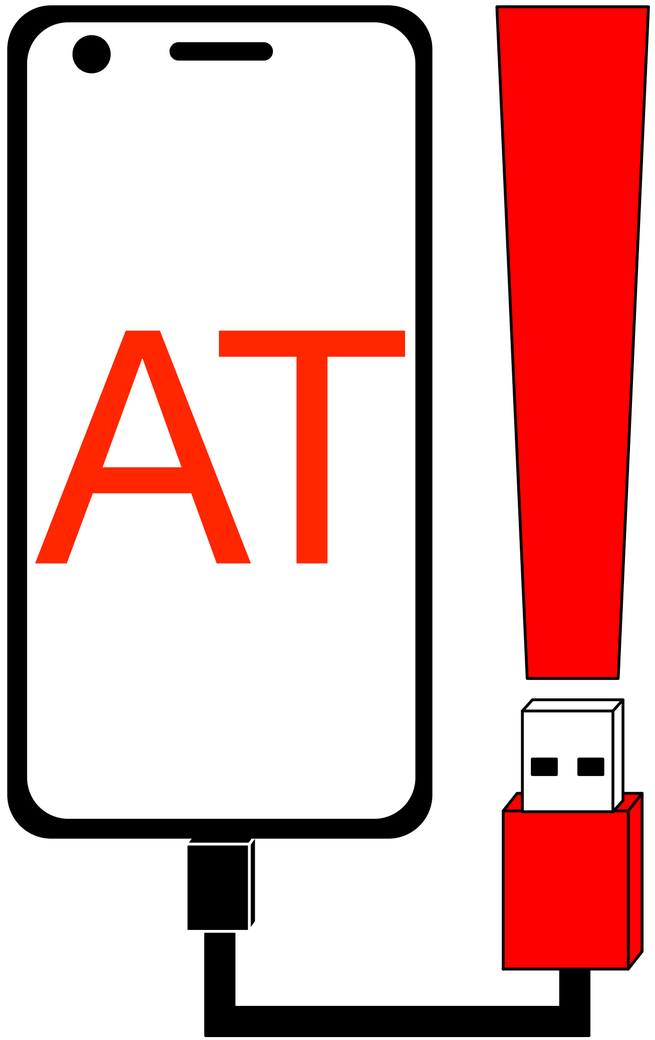
- AT+VZWAPNE
- AT$SPDEBUG
- AT%MINIOS
- AT%VZWHM
- AT%VZWIOTHM
- AT%AUTOUITEST

LG G4 Touch Injection to Enable Developer Options

Mitigations & Fixes

- Remove the USB Modem interface
- Restrict the USB Modem interface
- Use whitelist for command filtering
- **Samsung and LG have issued security updates**

- **LVE-SMP-180001**
- Severity : **High**
- Date reported : **February 02, 2018**
- Affected device information : Android devices with OS 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2, **8.0, 8.1**
- Description : Vulnerability of AT CMD(Command) in smartphones.



Now What?

Home About

By Vendor By Version

https://atcommands.org

AT+DATABASE

AT+USB

AT+USBCHANG
AT+USBDEBUG
AT+USBMODEC
AT+USBMODEM
AT+USBSWITCH
AT+USBTTEST
AT+USBTYPEC

Q&A

https://davejingtian.org

Thanks!