

Opening Pandora's Box through ATFuzzer: Dynamic Analysis of AT interface for Android Smartphones

Imtiaz Karim^{*}, Fabrizio Cicala^{*}, Syed Rafiul Hussain^{*},

Omar Chowdhury[†], Elisa Bertino^{*}

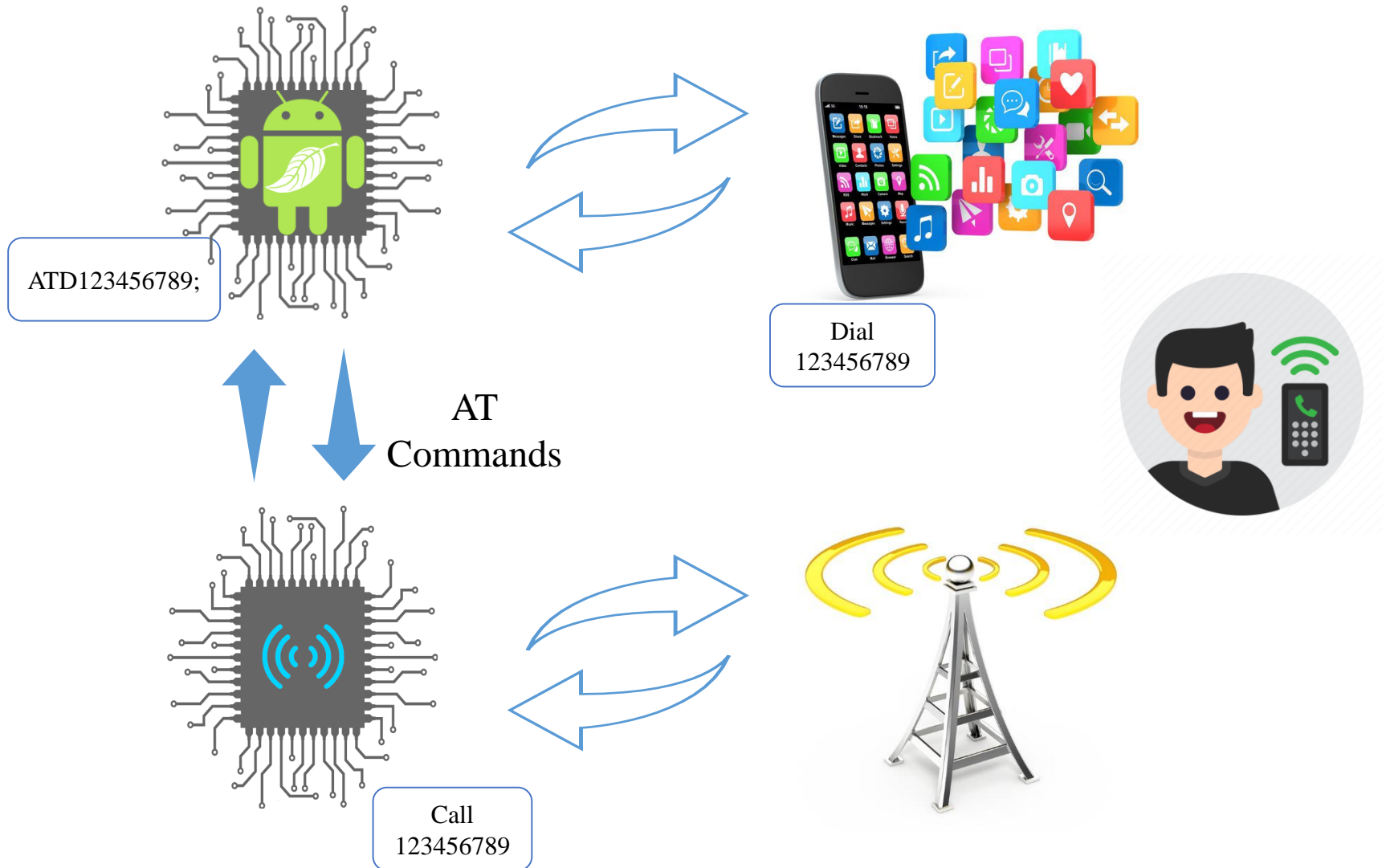
PURDUE UNIVERSITY, UNIVERSITY OF IOWA



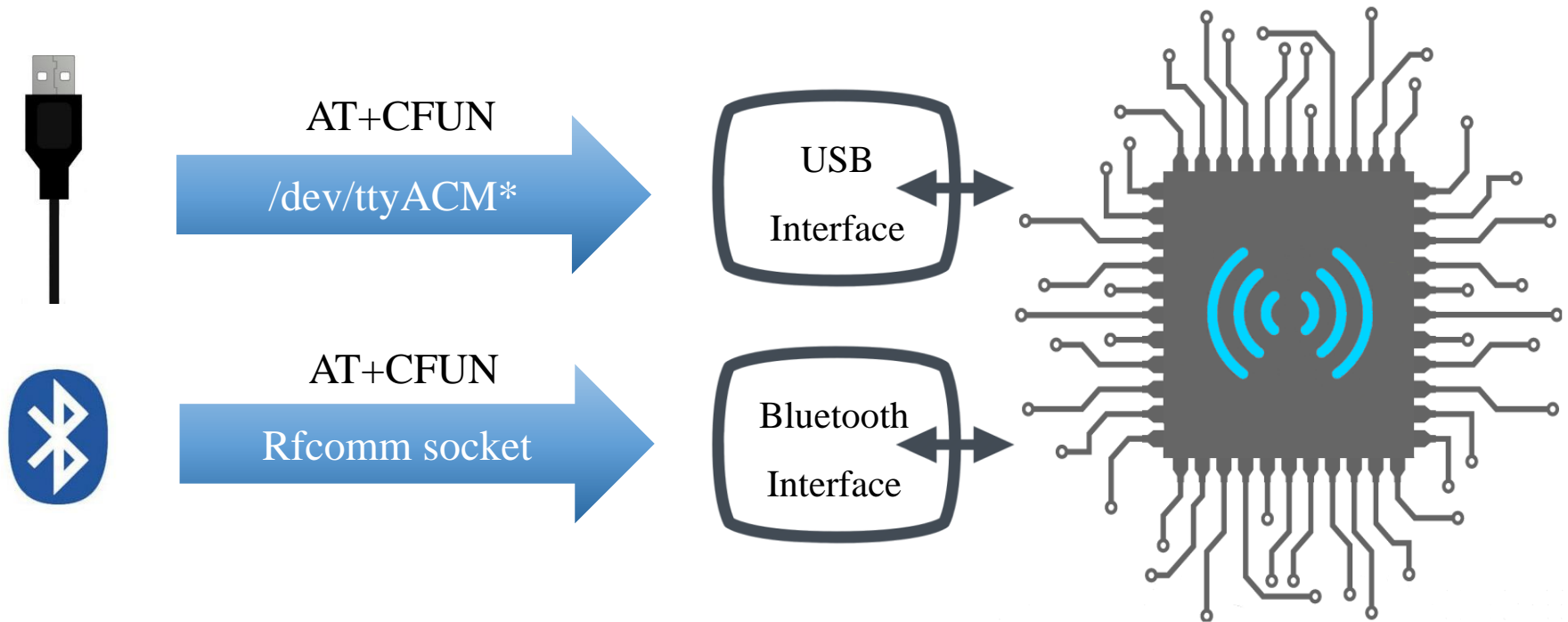
Smartphones



ATtention (AT) Commands



AT Command Interface



Prior Works on AT Command

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

Dave (Jing) Tian^{*1}, Grant Hernandez¹, Joseph I. Choi¹, Vanessa Frost¹, Christie Ruales¹, Patrick Traynor¹, Haywardh Vijayakumar², Lee Harrison², Amir Rahmati^{2,3}, Michael Grace², and Kevin R. B. Butler¹



Misuse & Abuse of valid AT
Commands over USB!

**CHARGE YOUR DEVICE WITH
THE LATEST MALWARE**

André Pereira, Manuel E. Correia and Pedro Brandão

Perils of invalid AT Commands



Is it possible to systematically analyze the **correctness** and **robustness** of the baseband-related AT command execution process?





Challenges



ATFuzzer
Design



Findings



Impact



Conclusion
& Future
Work



Challenges

Challenges of Systematic Analysis



Static Analysis



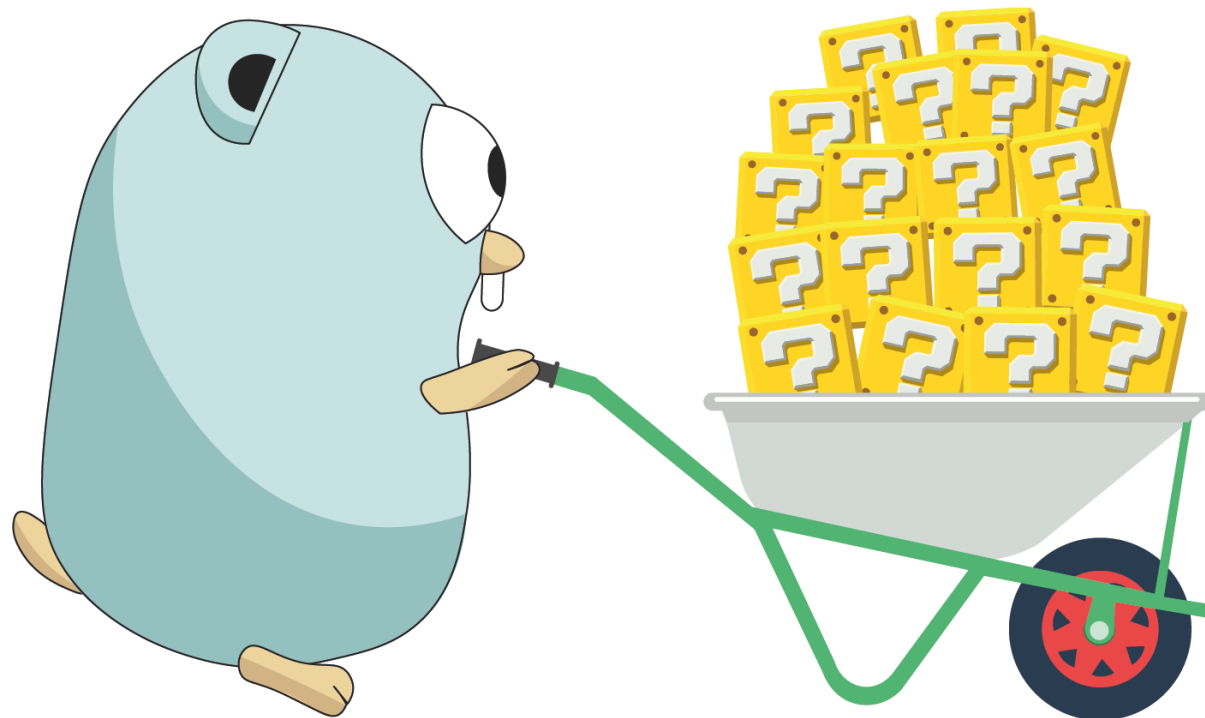
Dynamic Analysis

- Firmware rarely available
- Vendor specific firmware
- Binary Instrumentation



ATFuzzer

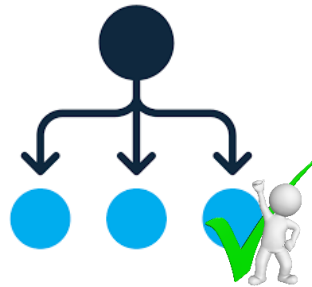
FUZZING TESTING!



ATFuzzer – Challenges



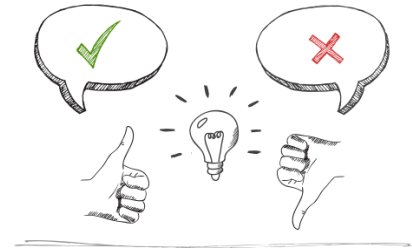
Input Representation



Syntactic Correctness

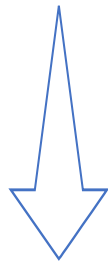


Semantic Correctness

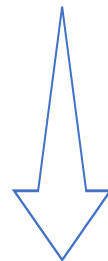


Feedback of Test Input

ATD ATDATD (phone no) ATD (phone no) [length]
+4632048030 +765409204



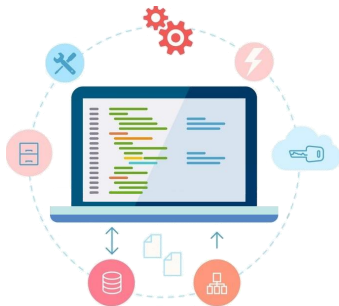
No of Argument
type of Arguments



Conditions
& Context



Challenges



ATFuzzer
Design



Findings



Impact &
Mitigation

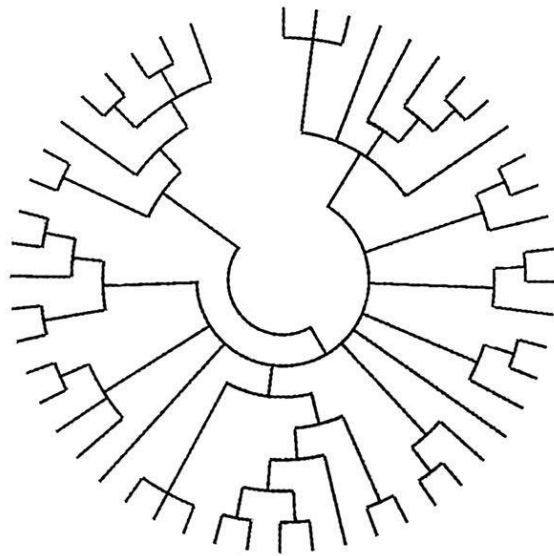


Conclusion
& Future
Work



ATFuzzer Design

Main Components of ATFuzzer

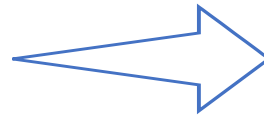
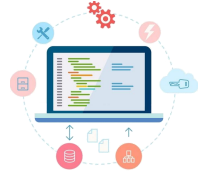


**Evolution
Module**



**Evaluation
Module**

ATFuzzer – Design



command → AT.cmd
cmd → cmd.cmd
cmd → €
cmd → D.Dnum.Darg;cmd
cmd →...



ATFuzzer – Design

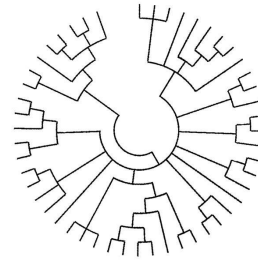
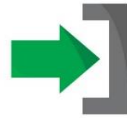
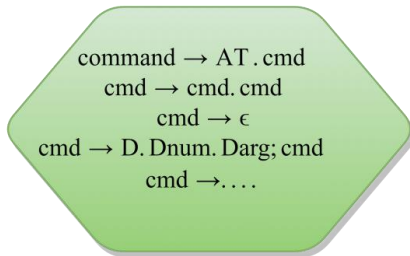


Diverse sets of invalid **AT commands** AT grammars

Evolution
Module

Evaluation Module

ATFuzzer – Design



**Evolution
Module**



Evaluation Module

AT



**AT command
Injector**



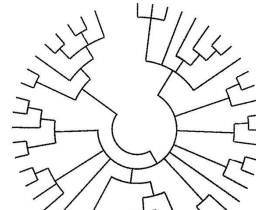
**Smartphone
Under Test**

ATFuzzer – Design



Score

command → AT . cmd
cmd → cmd. cmd
cmd → ε
cmd → D. Dnum. Darg; cmd



- **Precise timing loose indicator for coverage**
- **Detection of disruption**

OK/Error

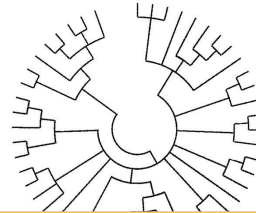


Smartphone
Under Test

ATFuzzer – Design Score

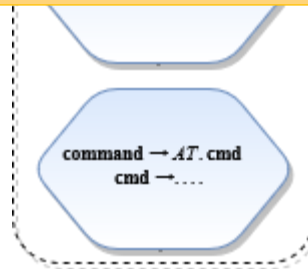
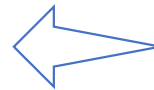
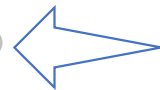


command → AT . cmd
cmd → cmd . cmd
cmd → ε
cmd → D. Dnum. Darg; cmd



Uncover **classes** of incorrect inputs compared to **single** inputs

command → AT . cmd
cmd → cmd . cmd
cmd → ε
cmd → D. Dnum. Darg; cmd
cmd →

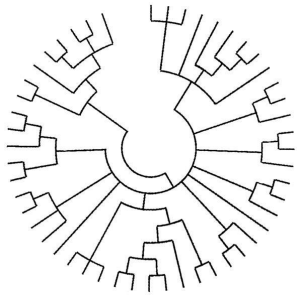


Population of Invalid AT Grammars

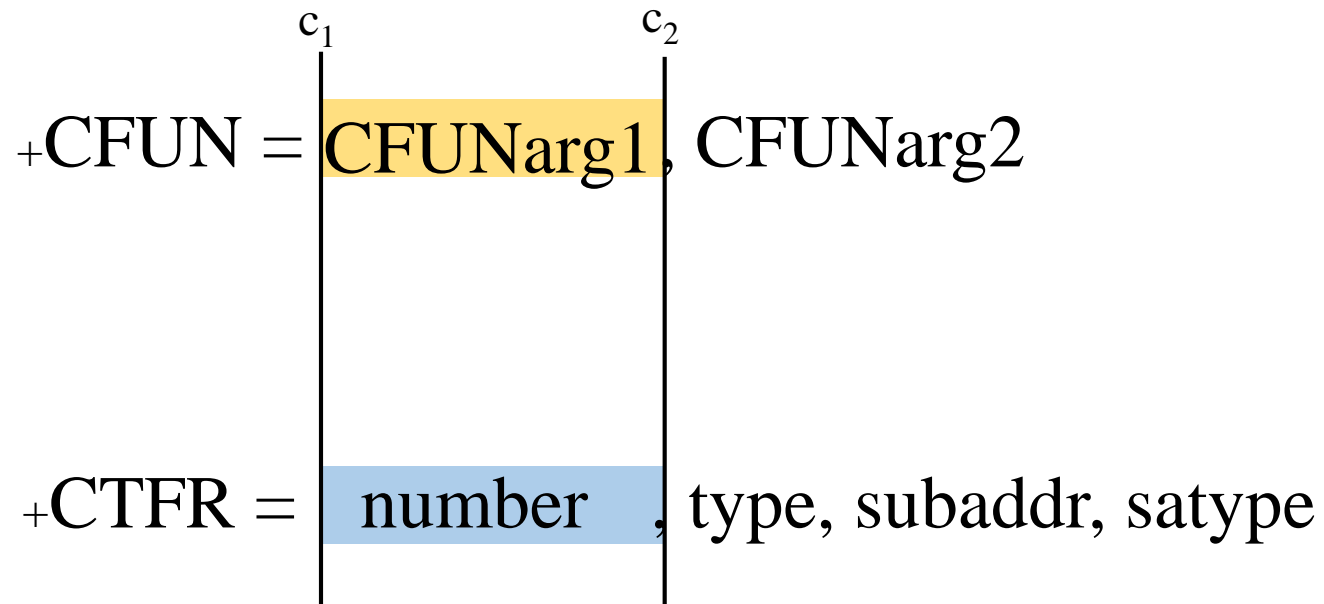
Crossover
+
Mutation

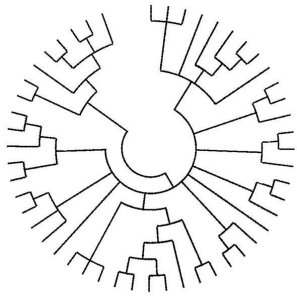
Parent Selection

Smartphone Under Test



Grammar Crossover





Grammar Mutation



+CTFR = number, type, subaddr, satype

+CTFR = type, subaddr, satype

+CTFR = - number, type, subaddr, satype

+CTFR = number, type, subaddr, satype



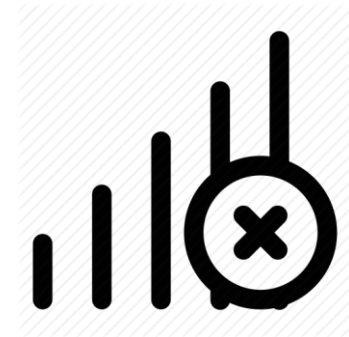
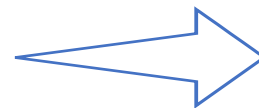
Fitness Evaluation



$$\text{fitness} = \alpha \text{ timing}_{\text{score}} + (1 - \alpha) \text{ disruption}_{\text{score}}$$

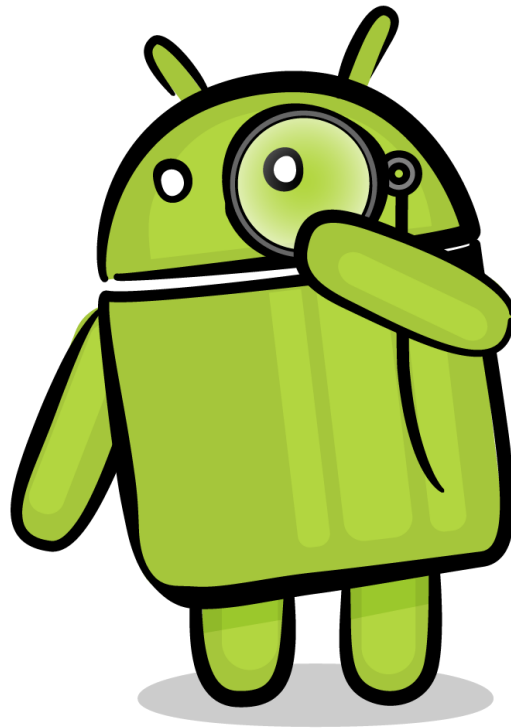
: hyperparameter to controls impact of both scores!

$$= \frac{\text{time for an AT command}}{\text{total time}}$$





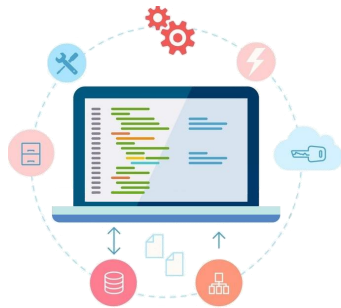
Fitness Evaluation



- 1) logcat
- 2) dumphsys
- 3) tombstone



Challenges



ATFuzzer
Design



Findings



Impact





















Conclusion
& Future
Work



Findings

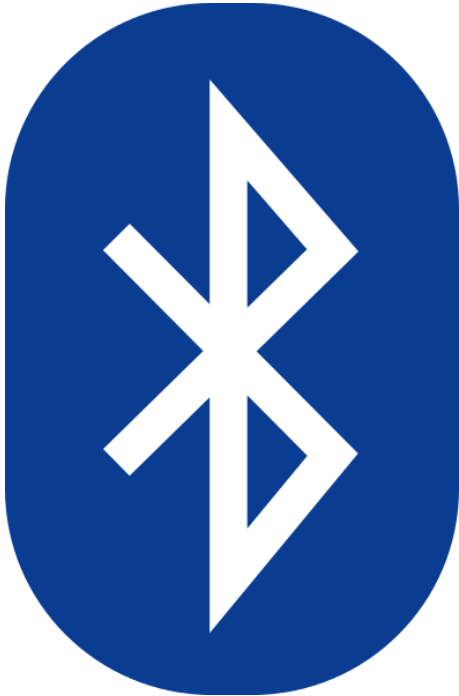


Devices

Device	Android Version	Interface
Samsung Note2	4.3	 
Samsung Galaxy S3	4.3	 
LG G3	6.0	 
HTC Desire 10 lifestyle	6.0.1	 
LG Nexus 5	5.1.1	 
Motorola Nexus 6	6.0.1	 
Huawei Nexus 6P	6.0	 
Galaxy S8+	8.0.0	 
Huawei P8 Lite	5.0.1	
Pixel 2	8.0.0	



Findings



4 invalid AT
grammars

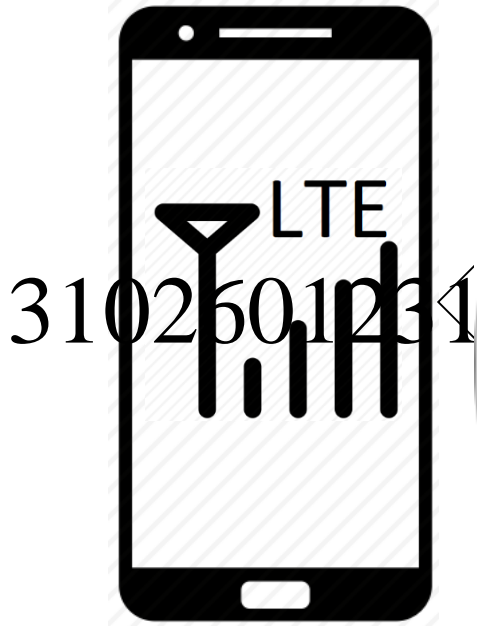


11 invalid AT
grammars

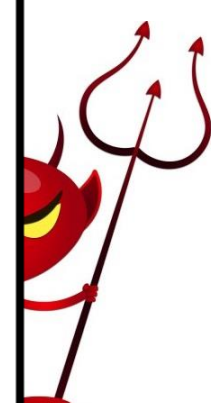
Attack Scenario



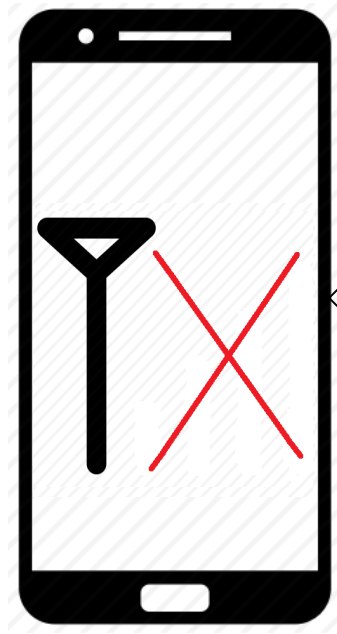
IMSI, IMEI Catching



+CIMI;;;abc
lid AT Command



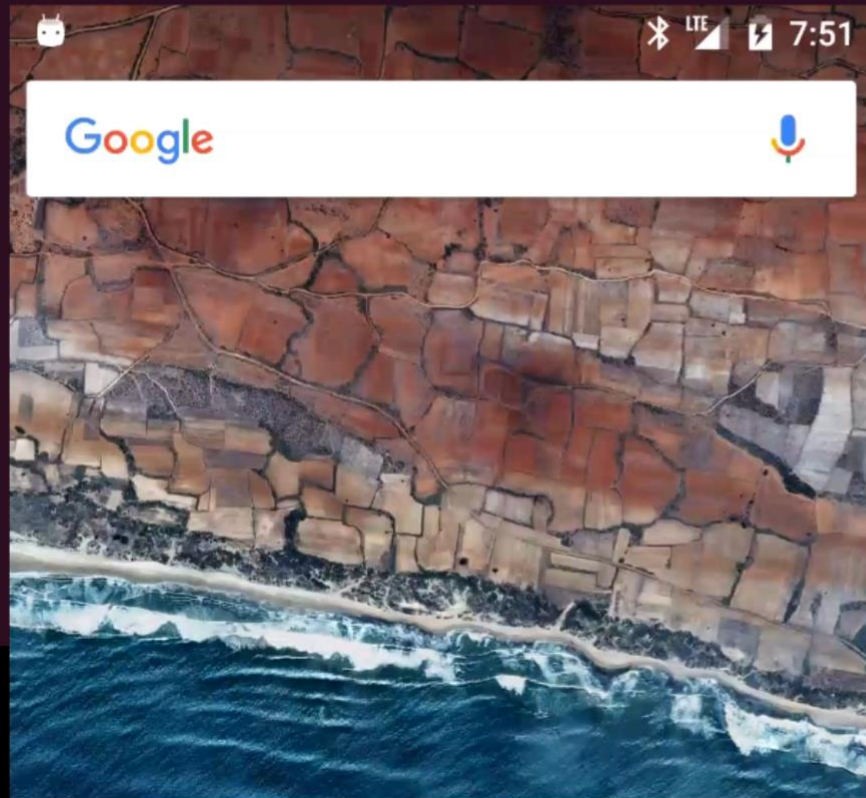
DB;A;B
AT Command



DEMO



```
(base) cyber2slab@cyber2slab-ThinkPad-T480:~/Desktop/report/Nexus 5 6 6P/Nexus Demos$ python2.7 atsend.py
```



Comparison

Fuzzing Approach	Problematic Grammars
ATFuzzer	9
ATFuzzer w/o Feedback	5
ATFuzzer w/o Crossover	3
ATFuzzer w/o Mutation	2
Modified AFL	2



Challenges



ATFuzzer
Design



Findings



Impact



Conclusion
& Future
Work



Impact



Impact

- Blocked USB and Bluetooth Modem interface
- Patch released on November 5, 2019
- CVE-2019-16400, CVE-2019-16401

SAMSUNG



Impact

- Blocked AT interface
- Released patch on September 5, 2019

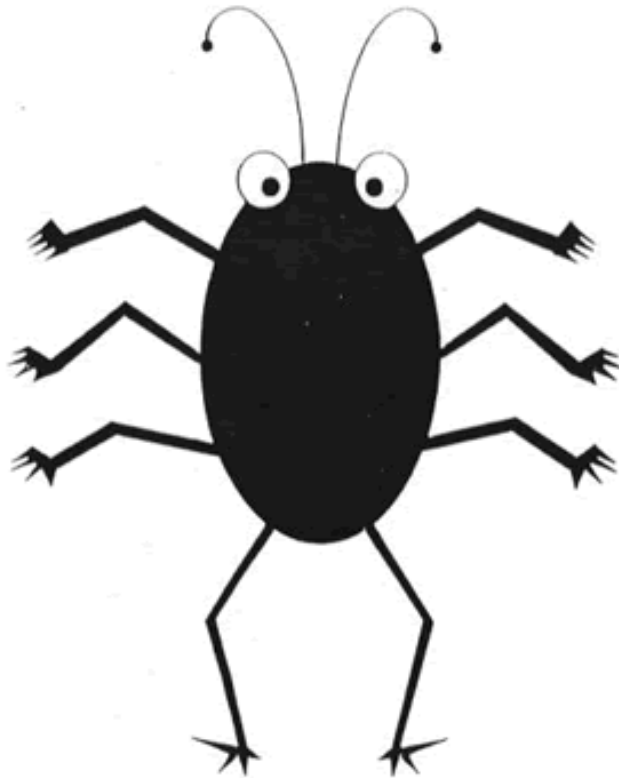




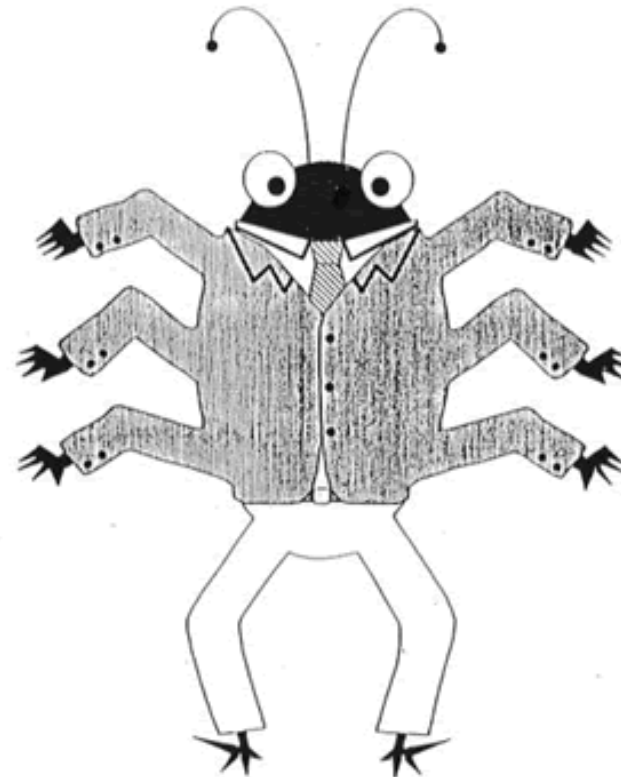
Impact

- Re

- AT
Sta



BUG



FEATURE





Challenges



ATFuzzer
Design



Findings



Impact



Conclusion
& Future
Work



Conclusion &
Future Work



Future work

- Applying the fuzzing technique to other parsers with complex input patterns
- Analyzing baseband processor



Conclusion

- Proposed ATFuzzer with a novel grammar guided evolutionary fuzzing approach
- Reported 4 incorrect AT grammars over Bluetooth and 11 over USB
- Vulnerabilities recognized by major vendors
- Patches released to mitigate them

Thank you!
Questions!

<https://github.com/Imtiazkarimik23/ATFuzzer>