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

ATD123456789;

Dial 123456789

Call 123456789
AT Comand Interface

AT+CFUN
/dev/ttyACM*

AT+CFUN
Rfcomm socket

USB Interface

Bluetooth Interface
Prior Works on AT Comand

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

Dave (Jing) Tian*1, Grant Hernandez1, Joseph I. Choi1, Vanessa Frost1, Christie Rual es1, Patrick Traynor1, Hayawardh Vijayakumar2, Lee Harrison2, Amir Rahmati2,3, 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
Challenges of Systematic Analysis

- Firmware rarely available
- Vendor specific firmware
- Binary Instrumentation
ATFuzzer

FUZZING TESTING!
ATFuzzer – Challenges

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

- No of Argument
- Type of Arguments
- Conditions & Context

Feedback of Test Input
Challenges

ATFuzzer Design

Findings

Impact & Mitigation

Conclusion & Future Work
ATFuzzer Design
Main Components of ATFuzzzer

Evolution Module

Evaluation Module
ATFuzzer – Design

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

HUAWEI
Telit
SAMSUNG
3GPP
A GLOBAL INITIATIVE
ATFuzzer – Design

Diverse sets of invalid AT commands AT grammars

Evolution Module  Evaluation Module
ATFuzzer – Design

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

Evolution Module

Evaluation Module

AT command Injector

Smartphone Under Test

AT
ATFuzzer – Design

- Precise timing loose indicator for coverage
- Detection of disruption
Uncover **classes** of incorrect inputs compared to **single** inputs
Grammar Crossover

\[ +\text{CFUN} = \text{CFUNarg}_1, \text{CFUNarg}_2 \]

\[ +\text{CTFR} = \text{number}, \text{type}, \text{subaddr}, \text{satype} \]
Grammar Mutation

$$+CTFR = \text{number, type, subaddr, satype}$$

$$+CTFR = \text{type, subaddr, satype}$$

$$+CTFR = \text{- number, type, subaddr, satype}$$

$$+CTFR = \text{number, satype, type, subaddr, satype}$$
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) dumpsys
3) tombstone
Findings
# Devices

<table>
<thead>
<tr>
<th>Device</th>
<th>Android Version</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>Samsung Note2</td>
<td>4.3</td>
<td></td>
</tr>
<tr>
<td>Samsung Galaxy S3</td>
<td>4.3</td>
<td></td>
</tr>
<tr>
<td>LG G3</td>
<td>6.0</td>
<td></td>
</tr>
<tr>
<td>HTC Desire 10</td>
<td>6.0.1</td>
<td></td>
</tr>
<tr>
<td>Lifestyle</td>
<td></td>
<td></td>
</tr>
<tr>
<td>LG Nexus 5</td>
<td>5.1.1</td>
<td></td>
</tr>
<tr>
<td>Motorola Nexus 6</td>
<td>6.0.1</td>
<td></td>
</tr>
<tr>
<td>Huwaei Nexus 6P</td>
<td>6.0</td>
<td></td>
</tr>
<tr>
<td>Galaxy S8+</td>
<td>8.0.0</td>
<td></td>
</tr>
<tr>
<td>Huwaei P8 Lite</td>
<td>5.0.1</td>
<td></td>
</tr>
<tr>
<td>Pixel 2</td>
<td>8.0.0</td>
<td></td>
</tr>
</tbody>
</table>
Findings

4 invalid AT grammars

11 invalid AT grammars
Attack Scenario
IMSI, IMEI Catching

+CIMI;;;abc

Invalid AT Command

3102601234

LTE

PRIVATE
DEMO

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

Google

Google Search
## Comparison

<table>
<thead>
<tr>
<th>Fuzzing Approach</th>
<th>Problematic Grammars</th>
</tr>
</thead>
<tbody>
<tr>
<td>ATFuzzer</td>
<td>9</td>
</tr>
<tr>
<td>ATFuzzer w/o Feedback</td>
<td>5</td>
</tr>
<tr>
<td>ATFuzzer w/o Crossover</td>
<td>3</td>
</tr>
<tr>
<td>ATFuzzer w/o Mutation</td>
<td>2</td>
</tr>
<tr>
<td>Modified AFL</td>
<td>2</td>
</tr>
</tbody>
</table>
Impact
Impact

- Blocked USB and Bluetooth Modem interface
- Patch released on November 5, 2019
Impact

• Blocked AT interface

• Released patch on September 5, 2019
Impact

- Re
- AT
- Standard!!
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