Project Ideas

Project Ideas

- Cloak and Dagger

- Vulnerabilities and design shortcomings affecting the Android UI (2017)

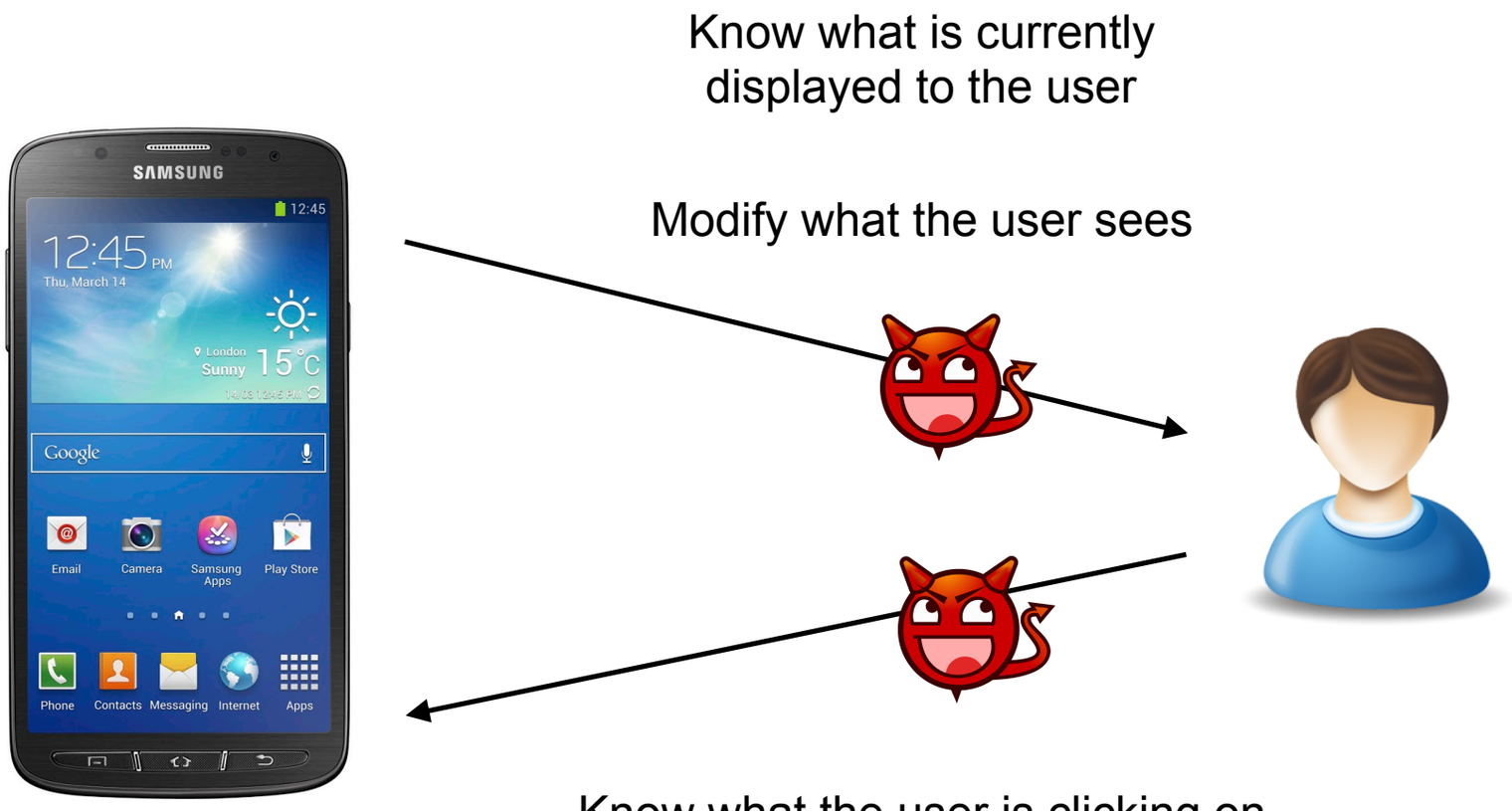
- Android versions < 8 are affected

- Attacks allow a malicious app to completely control the UI feedback loop and take over the device.

- http://cloak-and-dagger.org/

Project Ideas

- Cloak and Dagger



Project Ideas

NGINX servers with PHP-FPM enabled are vulnerable.

Project Ideas

- APACHE STRUTS 2
  CVE-2017-5638

Project Ideas

CVE-2014-0160 (‘Heartbleed’)

OpenSSL was incorporated into a wide variety of software projects and embedded systems.

Project Ideas

CVE-2017-0781, CVE-2017-0782, CVE-2017-0783, CVE-2017-0785

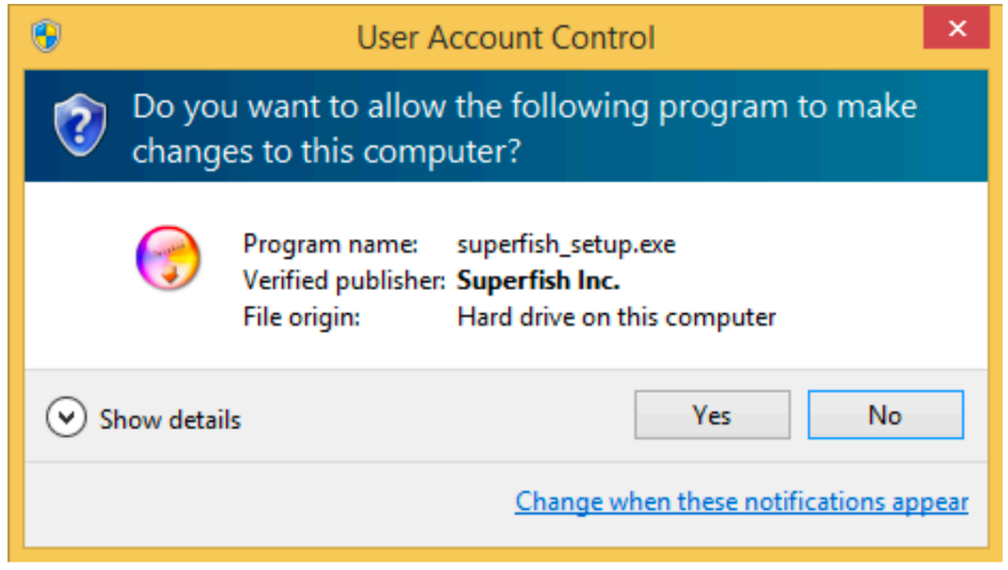
Affects almost every Bluetooth enabled devices

Project Ideas

Lenovo installed “SuperFish” on its laptops between December 2014 and February 2015

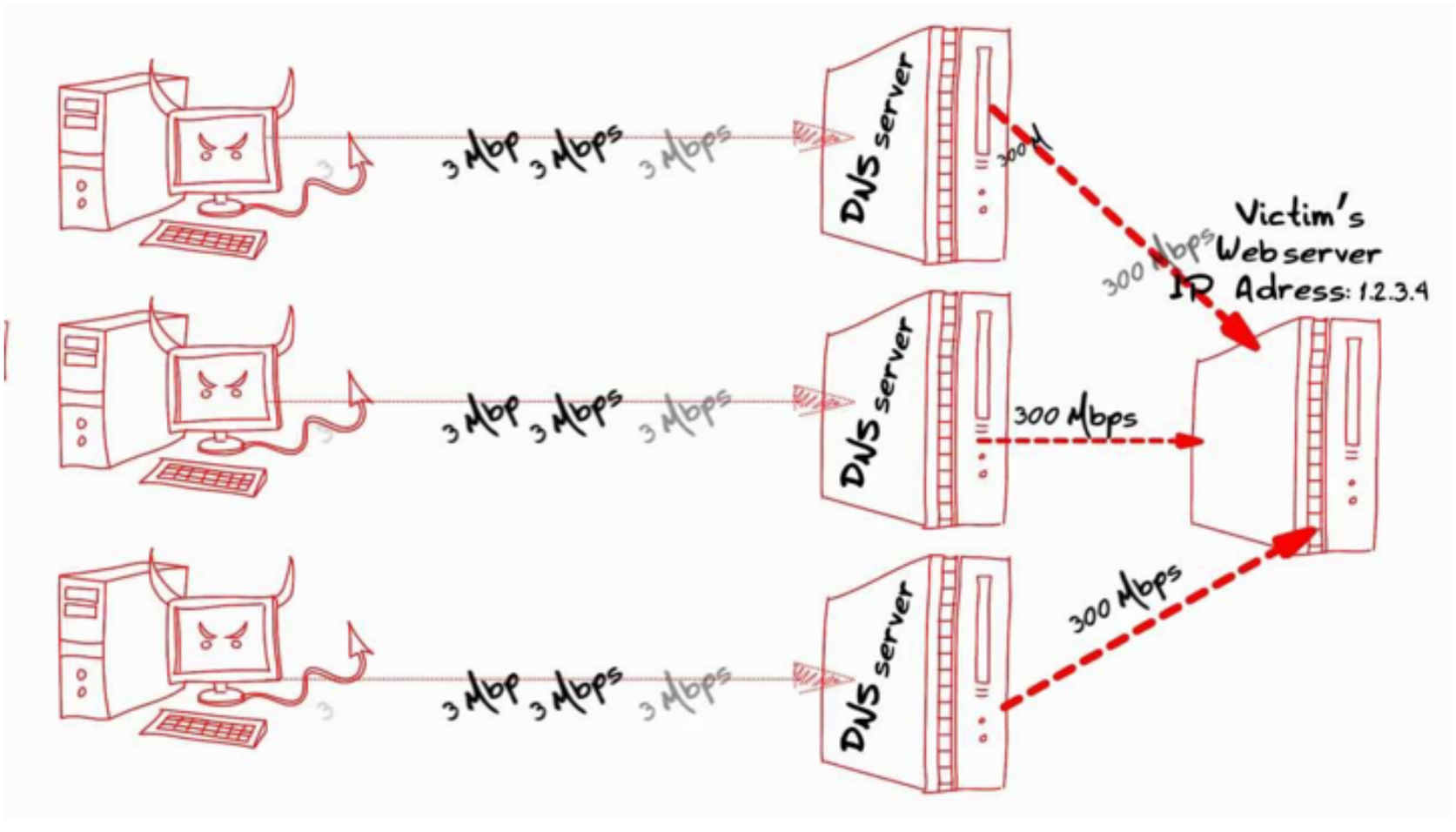
The software intercepts all web requests and introduces ads which generate revenue for Lenovo

The HTTPS interception created a major vulnerability which compromised all SSL/TLS on affected machines



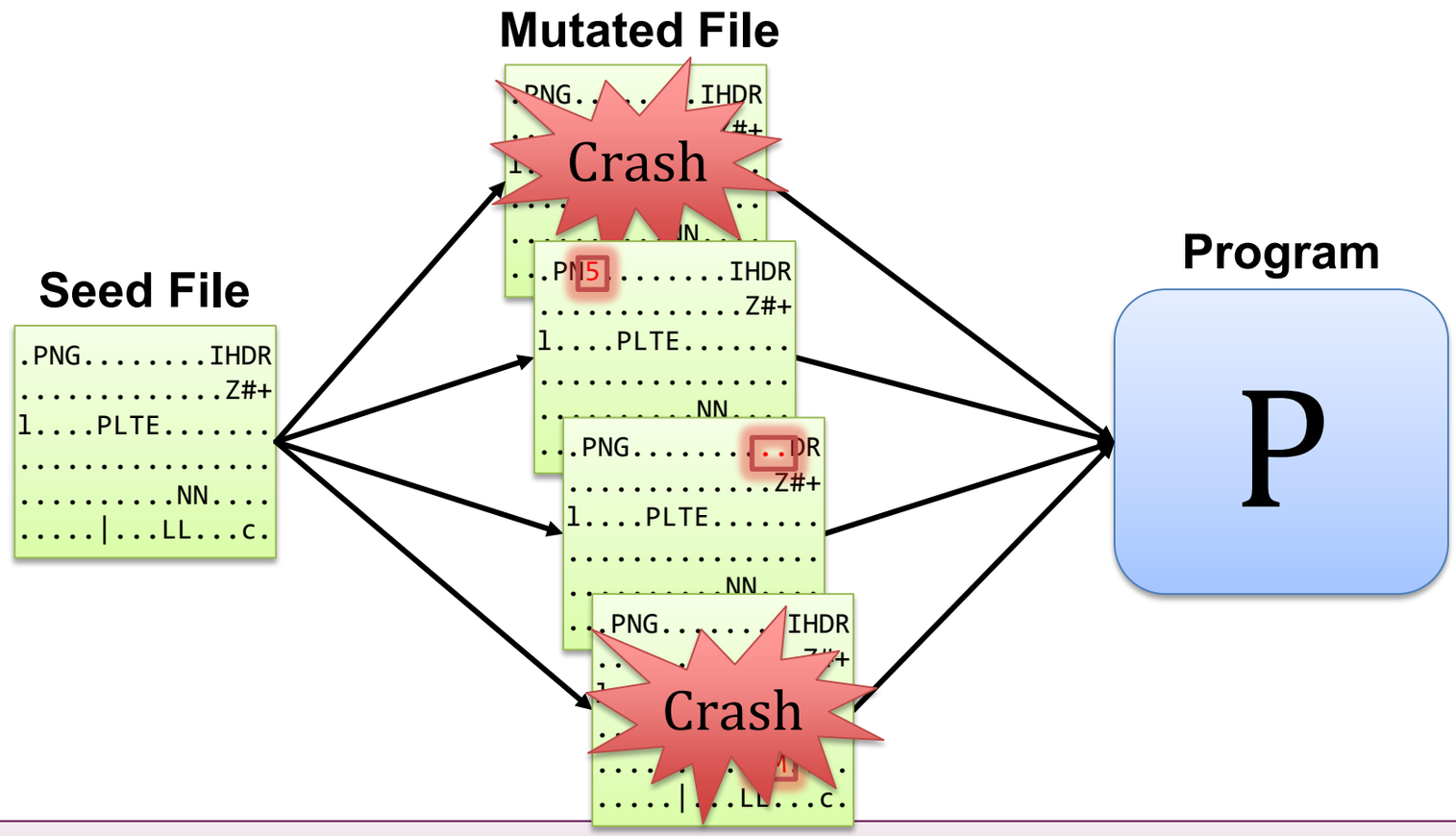
Project Ideas

- DNS Amplification Attack



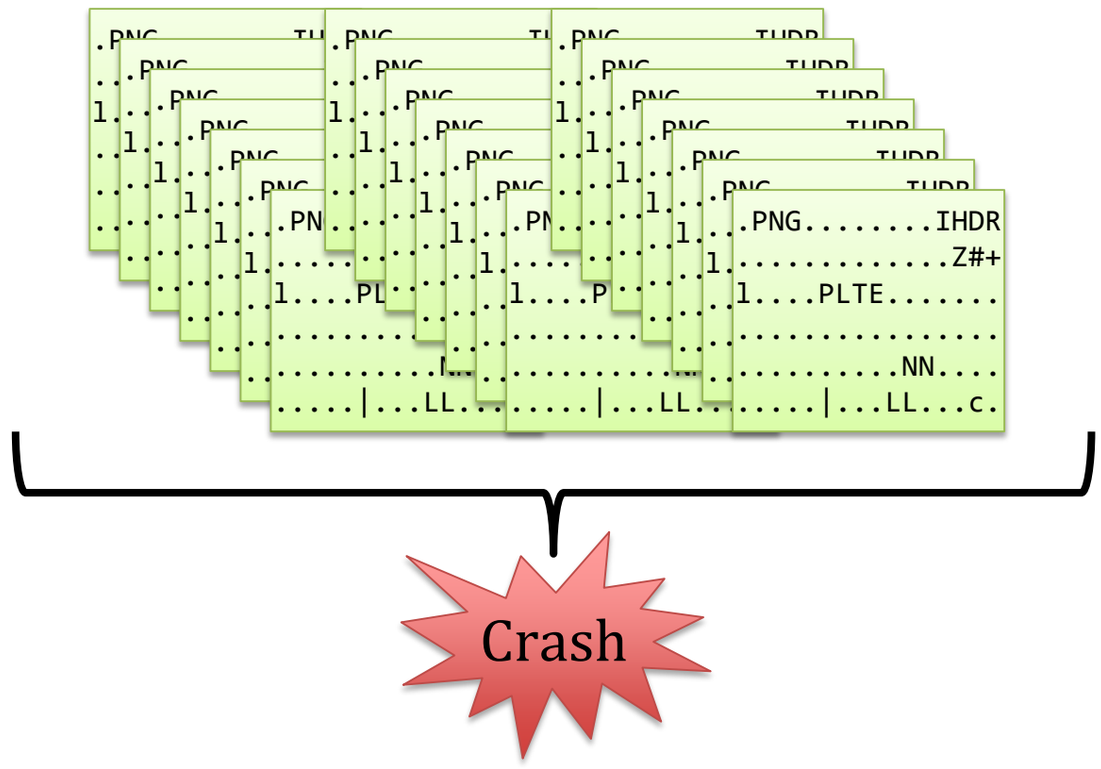
Vulnerability Discovery

Background: Mutational Fuzzing of Software



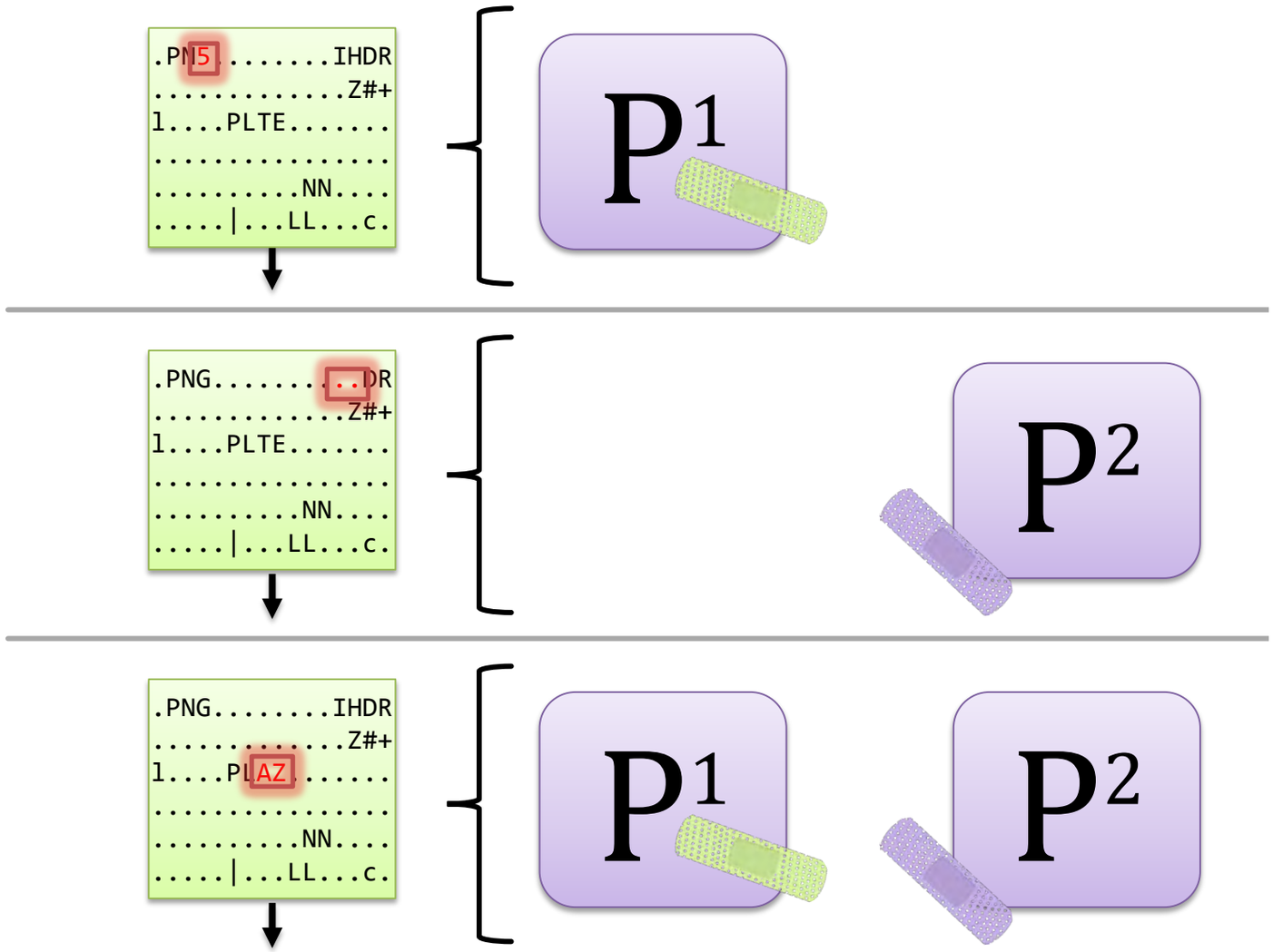
Testing of programs by randomly mutating program inputs (seeds)

Challenge: How Many Software Vulnerabilities are There?



The Idea: Patches Define Vulnerabilities

Any crash that is fixed by the patch is also affected by vulnerability V


.PNG.....IHDR
.....Z#+
l....PLTE.....
.....NN....
.....|...LL...c.
P1
.PNG.....IHDR
.....Z#+
l....PLTE.....
.....NN....
.....|...LL...c.
P2
.PNG.....IHDR
.....Z#+
l....PLAZ.....
.....NN....
.....|...LL...c.
P1
P2

Patching ImageMagick

Fuzzed old ImageMagick with the CERT BFF fuzzer

- 1 week
- 130,000 crashes found