



Project Ideas

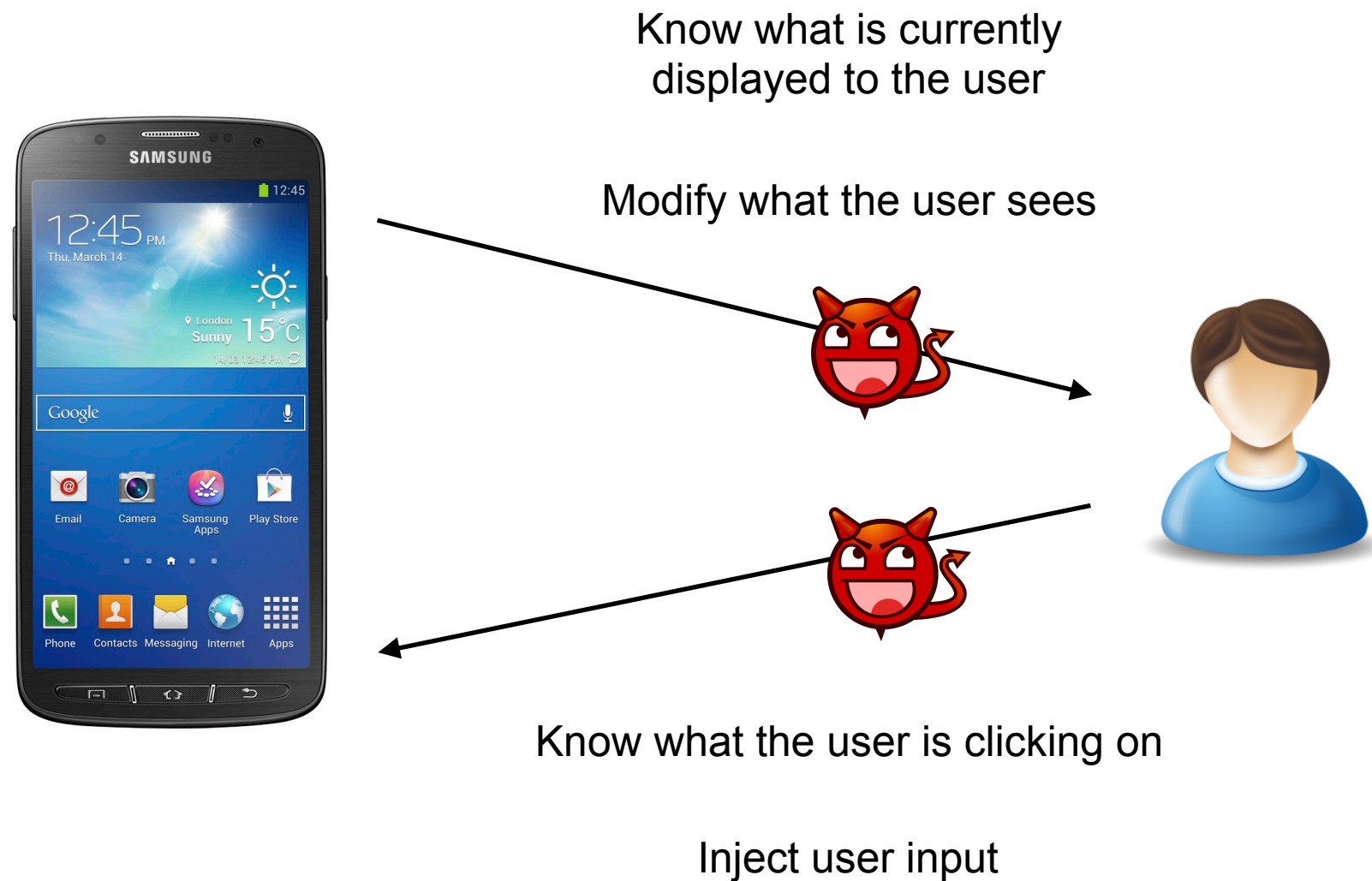


Project Ideas

- 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

EDITION: [US](#) ▼



[VIDEOS](#) [5G](#) [WINDOWS 10](#) [CLOUD](#) [AI](#) [INNOVATION](#) [SECURITY](#) [MORE](#) ▼ [NEWSLETTERS](#) [ALL WRITERS](#)

MUST READ: [Microsoft to release an alpha of WinUI 3.0 next week](#)

Nasty PHP7 remote code execution bug exploited in the wild

New PHP7 bug CVE-2019-11043 can allow even non-technical attackers to take over servers.



By [Catalin Cimpanu](#) for [Zero Day](#) | October 26, 2019 -- 07:00 GMT (00:00 PDT) | Topic: [Security](#)

NGINX servers with [PHP-FPM](#) enabled are vulnerable.

Project Ideas

- APACHE STRUTS 2
CVE-2017-5638

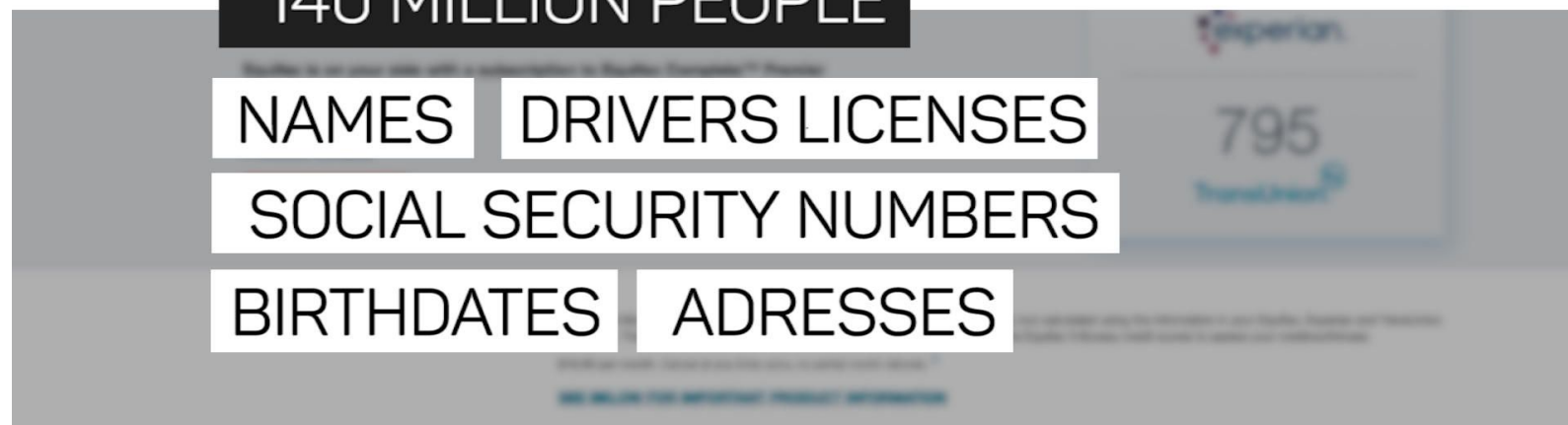
EQUIFAX®

140 MILLION PEOPLE

NAMES DRIVERS LICENSES

SOCIAL SECURITY NUMBERS

BIRTHDATES ADDRESSES



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

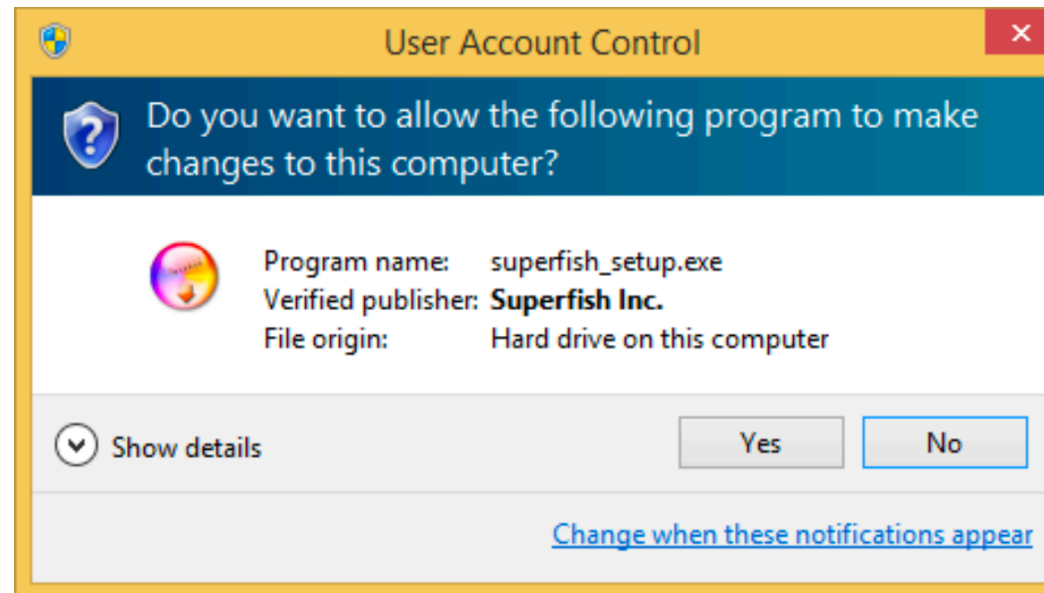
Affects almost every Bluetooth enabled devices

Project Ideas

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

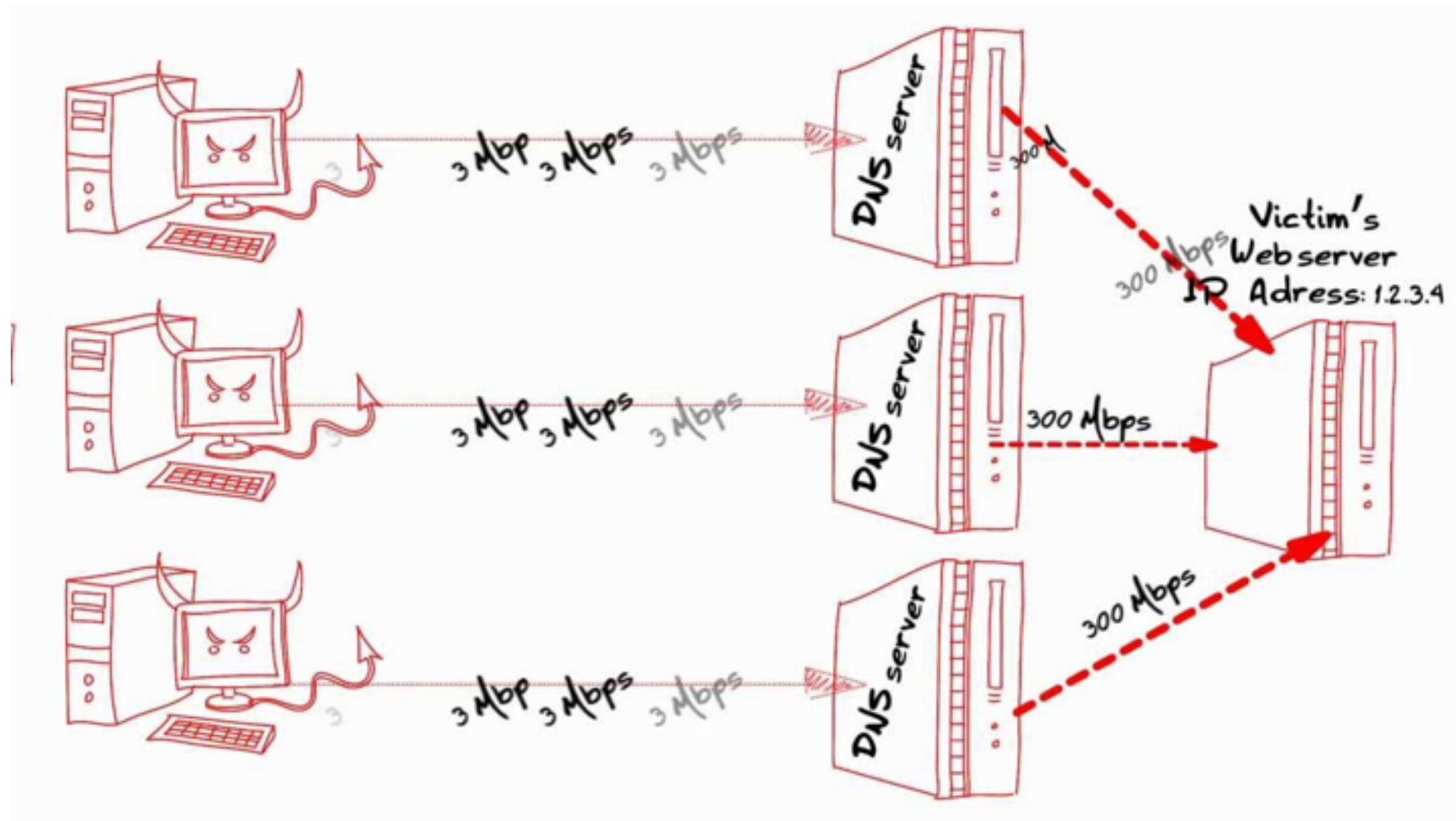
The software intercepts all web requests and introduces ads which generate revenue for Lenovo

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



Project Ideas

- DNS Amplification Attack

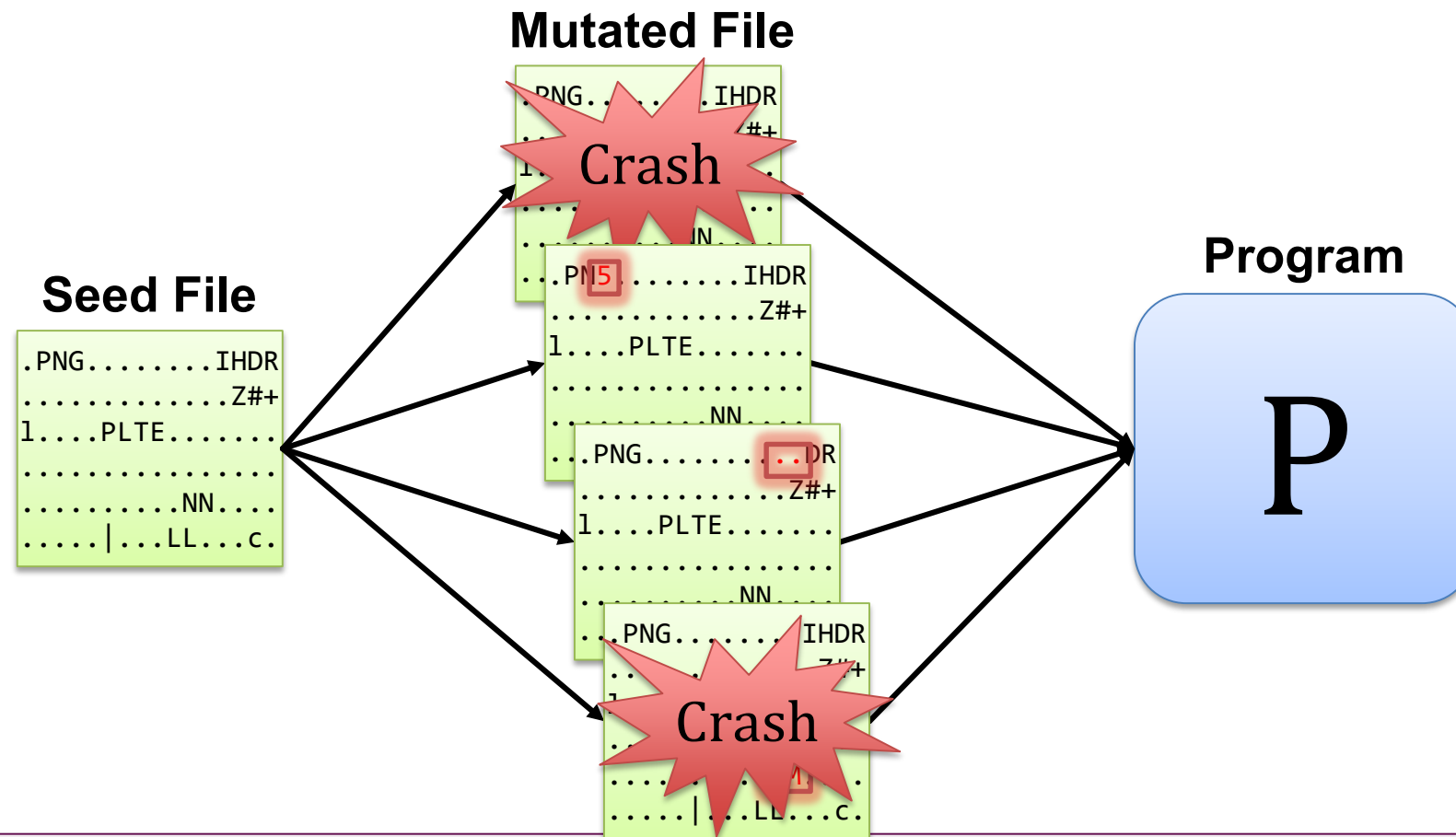




Vulnerability Discovery

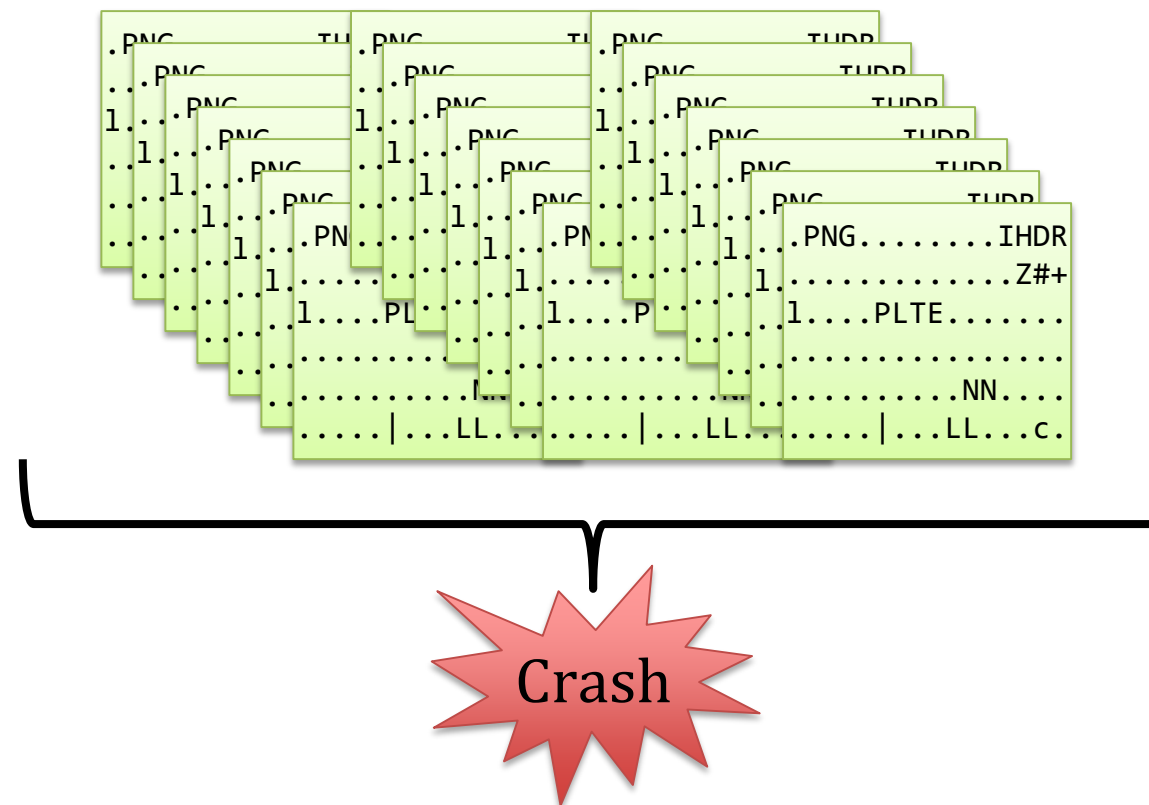


Background: Mutational Fuzzing of Software

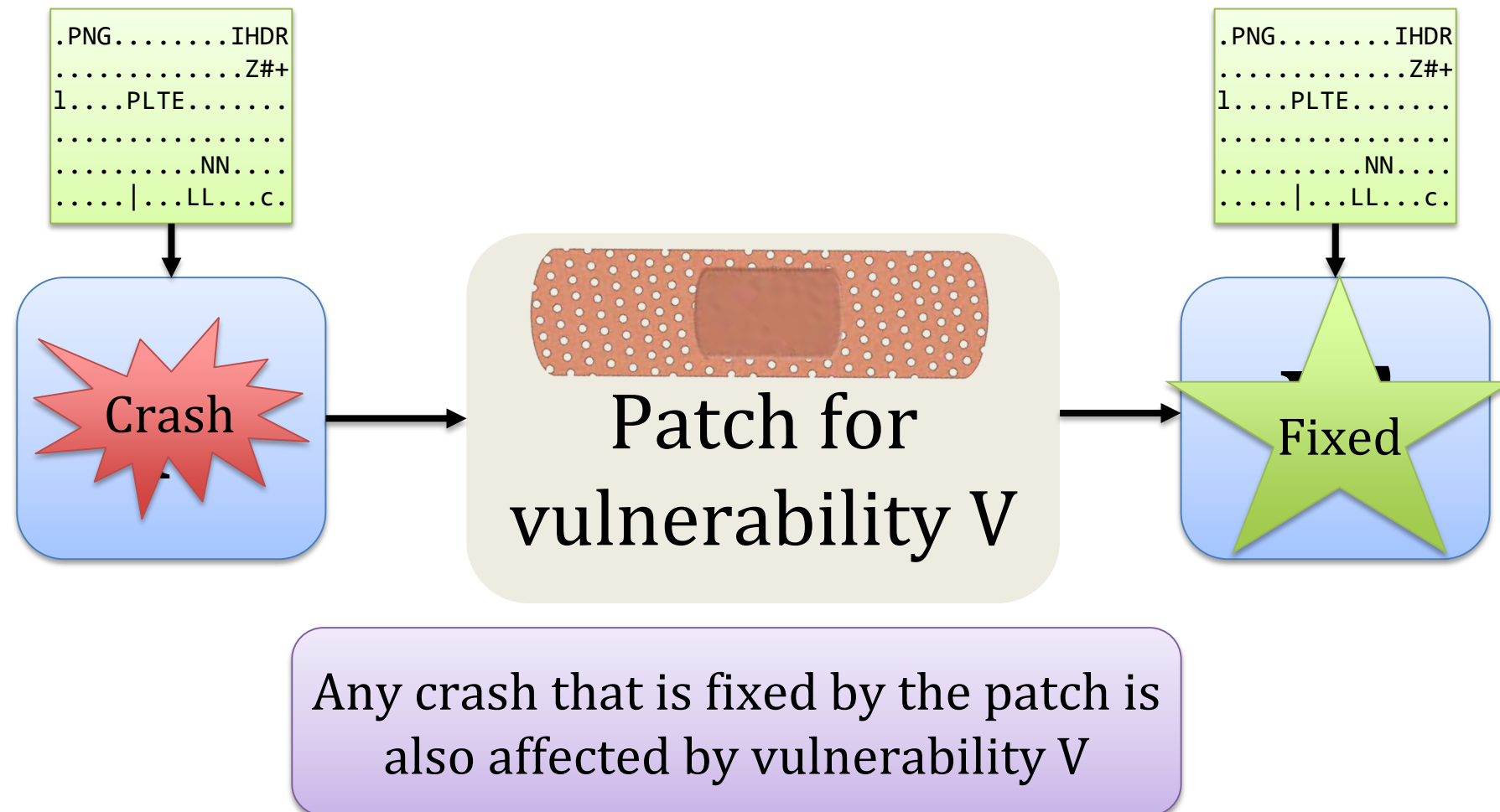


Testing of programs by randomly mutating program inputs (seeds)

Challenge: How Many Software Vulnerabilities are There?



The Idea: Patches Define Vulnerabilities



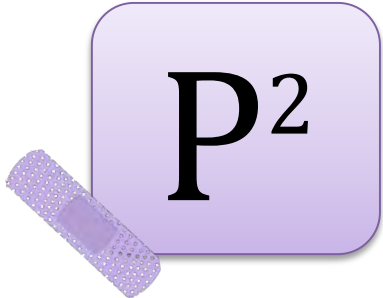
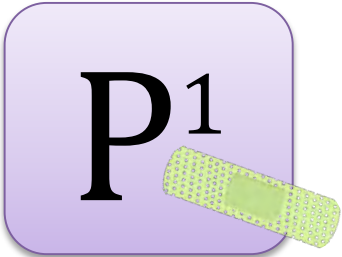
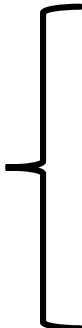
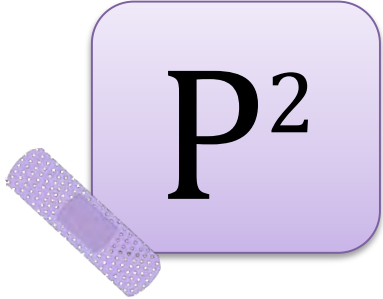
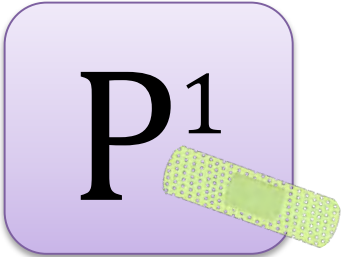
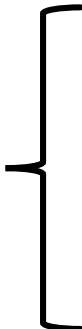
.PN5.....IHDR
.....Z#+
1....PLTE.....
.....NN.....
.....|...LL...C.



.PNG.....DR
.....Z#+
1....PLTE.....
.....NN.....
.....|...LL...C.



.PNG.....IHDR
.....Z#+
1....PLAZ.....
.....NN.....
.....|...LL...C.



Patching ImageMagick

Fuzzed old ImageMagick with the CERT BFF fuzzer

- 1 week
- 130,000 crashes found

