The Challenges of Memory and Storage Security

Paolo Amato[1] and Niccolò Izzo[1,2]

[1] Mobile Business Unit, Micron, Vimercate

[2] Politecnico di Milano

About Micron

And Worldwide Memory Market

Summary

About Micron

And Worldwide Memory Market

Micron Technology

We are a world leader in innovative memory solutions that transform how the world uses information.

We offer the industry’s broadest portfolio and an uncompromising focus on customer solutions.

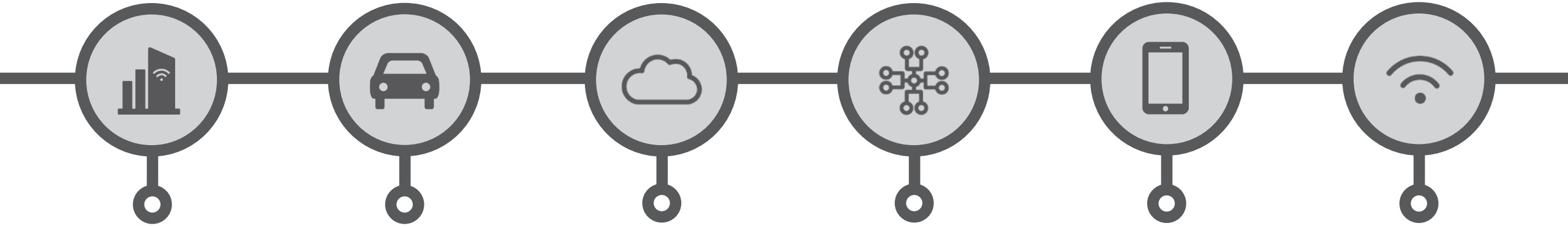
Data is the new currency

In an increasingly complex and connected world, the ability of an organization to collect, manage and analyze data effectively separates the winners from the runners-up.

Source: http://www.cioinsight.com/it-strategy/big-data/why-data-is-the-new-business-currency.html

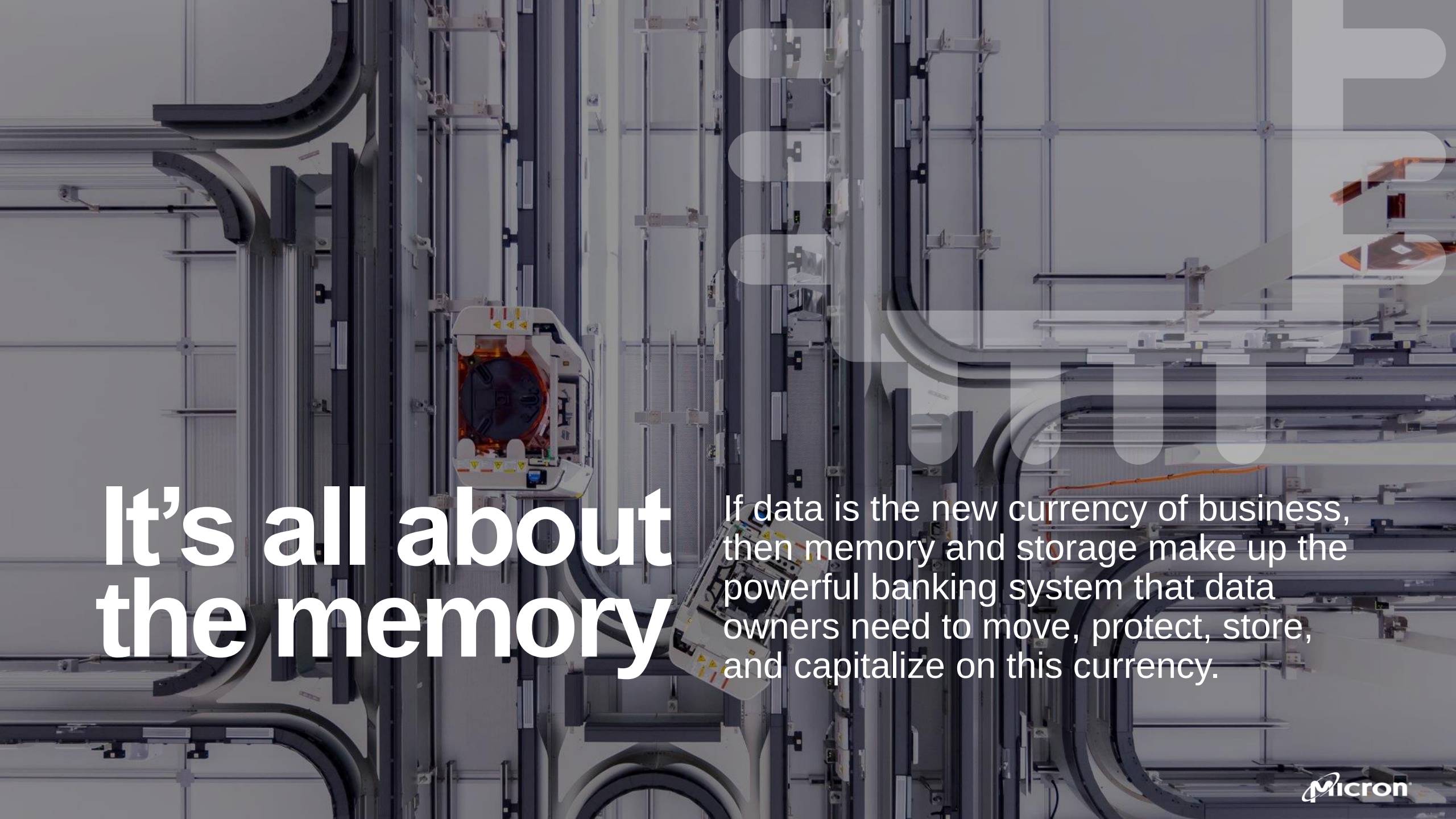
Micron

Trends Driving Increased Data Traffic



Enterprise	Automotive	Cloud/ Big Data	Networking	Mobile/ Client	IoT
Online Transaction Processing systems with low-latency in-memory compute	Global sales of autonomous vehicles to reach ~600,000 units by 2025	Data center storage installed capacity to grow ~5X to 1.8 ZB between 2015 and 2020	Global IP traffic grows at a CAGR of 24% from 2016 to 2020	Global mobile data traffic to rise ~7X between 2016 and 2021	27.1 billion networked devices by 2021

Source, September 2017: Cisco, Gartner, IDC, Automobile manufacturers
IoT – Internet of Things



It’s all about the memory

If data is the new currency of business, then memory and storage make up the powerful banking system that data owners need to move, protect, store, and capitalize on this currency.

Micron

Worldwide Memory $162B Market

(+25% Y/Y)

Semiconductor Market in 2017

$470B

(+12% Y/Y)

DRAM

- Mobile $36B
- Non-Mobile $63B

$99B

(+38% Y/Y)

Non-Volatile

- Storage $22B
- Non-Storage $41B

$63B

(+8% Y/Y)

Non-Memory Markets $308B

- Logic $218B +5% Y/Y
- Discrete $21B +5% Y/Y
- Analog $23B +4% Y/Y
- Other $45B +12% Y/Y

April 2018, Source: Gartner Q1-18

[1]Memory includes DRAM, NAND and NOR, Emerging and other

Micron

Memory and Storage are key elements for system performance and reliability, and to enable novel applications

Do they also play a role in System Security?

DRAM

NAND

A simple hardware failure mechanism can create a widespread system security vulnerability

WIRED

Forget Software—Now Hackers Are Exploiting Physics

BUSINESS | CULTURE | DESIGN | GEAR | SCIENCE

SHARE

SHARE 18276

TWEET

ANDY GREENBERG SECURITY 08.31.16 7:00 AM

FORGET SOFTWARE—NOW HACKERS ARE EXPLOITING PHYSICS

Micron

Project Zero

News and updates from the Project Zero team at Google

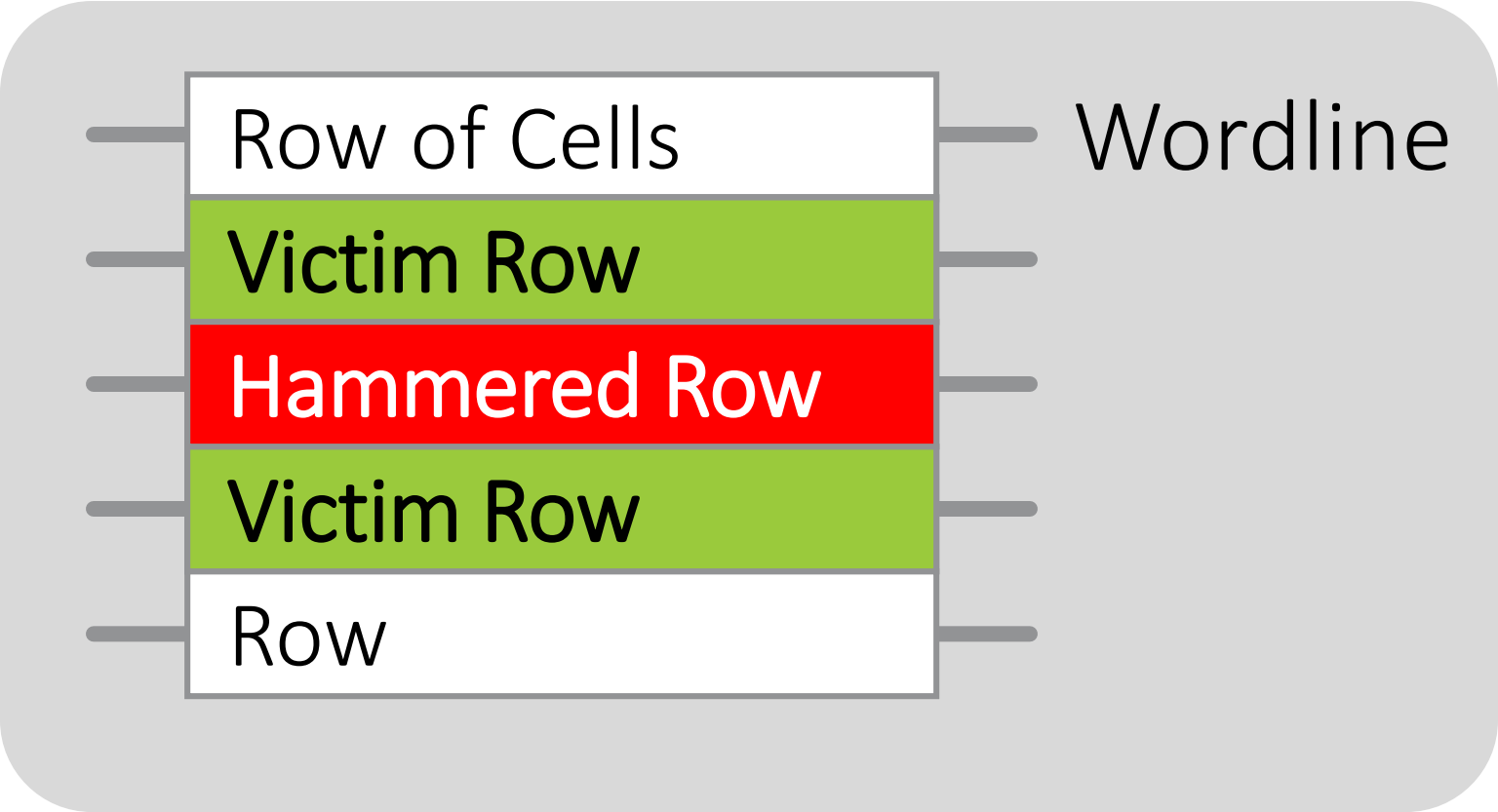
Monday, March 9, 2015

Exploiting the DRAM rowhammer bug to gain kernel privileges

Posted by Mark Seaborn, sandbox builder and breaker, with contributions by Thomas Dullien, reverse engineer

[This guest post continues Project Zero's practice of promoting excellence in security research on the Project Zero blog]

What is Rowhammer?



Repeatedly reading a row quickly enough induces **disturbance errors** in **adjacent rows** in **DRAM chips**

Slide source: Prof Onur Mutlu (ETH Zürich)

While it was originally considered mostly a reliability issue,

Rowhammer becomes a serious **Security Threat**
when an attacker coerces the OS into storing
security-sensitive data in a **vulnerable memory page**

Drammer is the first Android root exploit that relies on no software vulnerability

Drammer: Deterministic Rowhammer Attacks on Mobile Platforms, CCS'16

Image source: https://threatpost.com/rowhammer-vulnerability-comes-to-android/121480/

Drammer can gain control of a smartphone deterministically

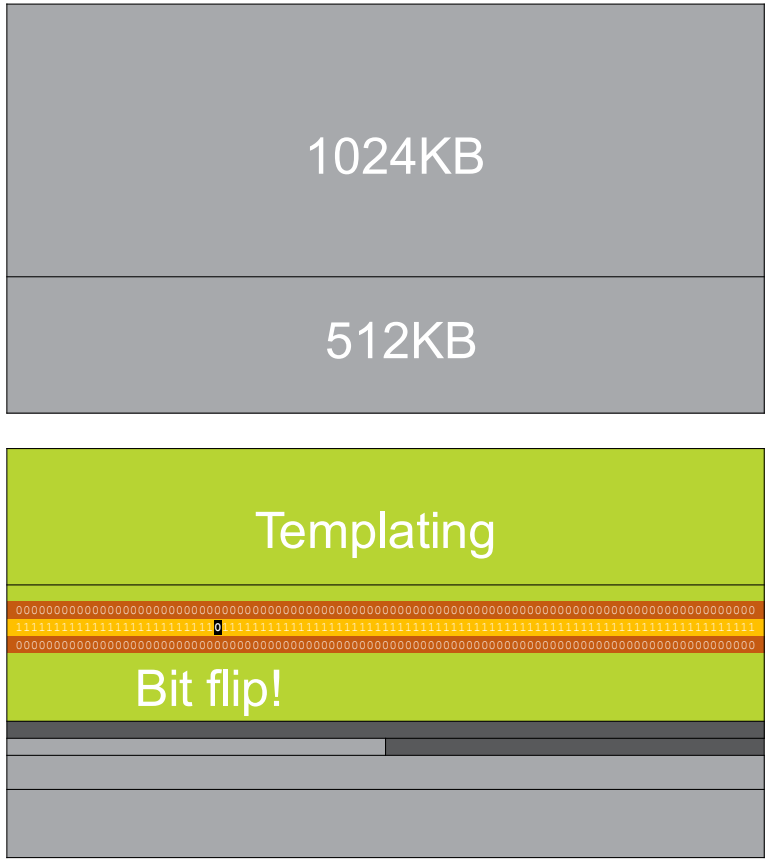
https://www.vusec.net/projects/drammer/

Drammer can gain control of a smartphone deterministically

Memory Templating

Scan Memory to find bit flips

By using direct memory access (DMA) it is possible to induce bit flips from user space



https://www.vusec.net/projects/drammer/

Drammer can gain control of a smartphone deterministically

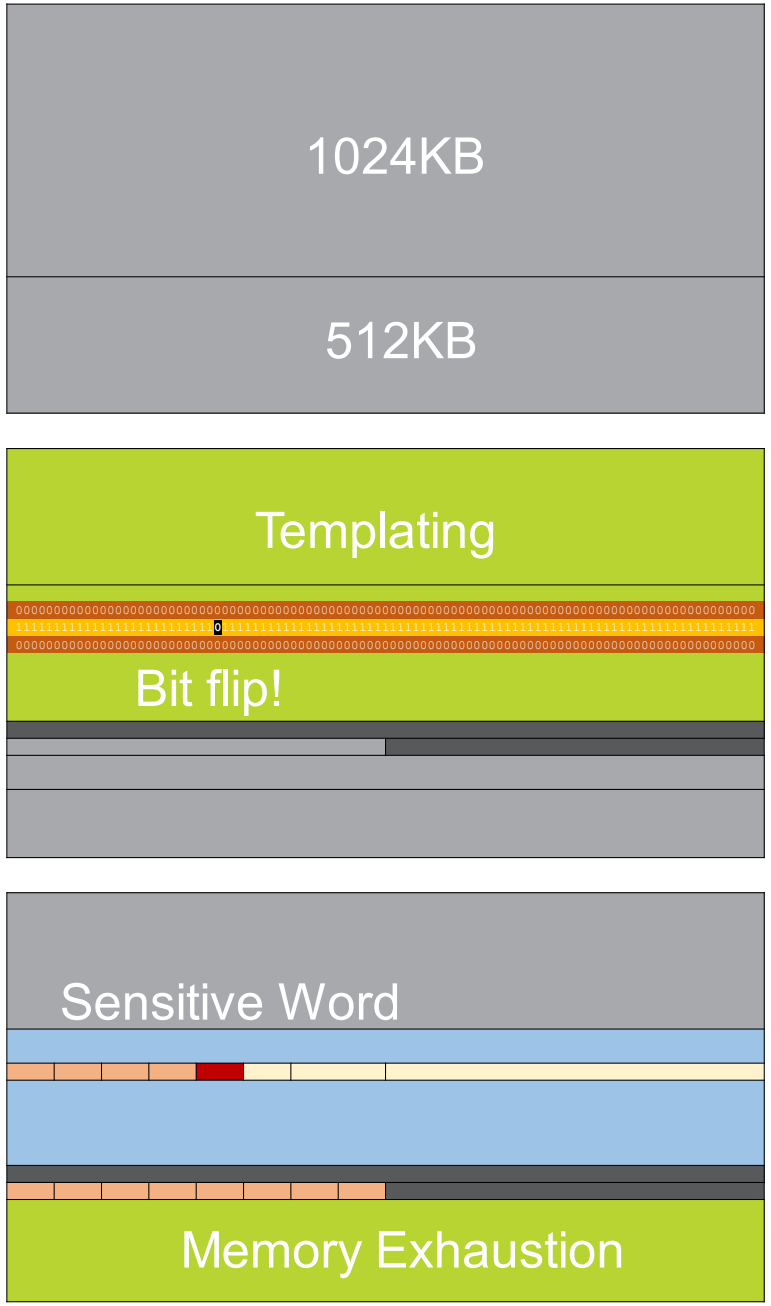
Memory Templating

Scan Memory to find bit flips

By using direct memory access (DMA) it is possible to induce bit flips from user space

Land sensitive data

Store crucial data structure on a vulnerable page



https://www.vusec.net/projects/drammer/

Drammer can gain control of a smartphone deterministically

Memory Templating

Scan Memory to find bit flips

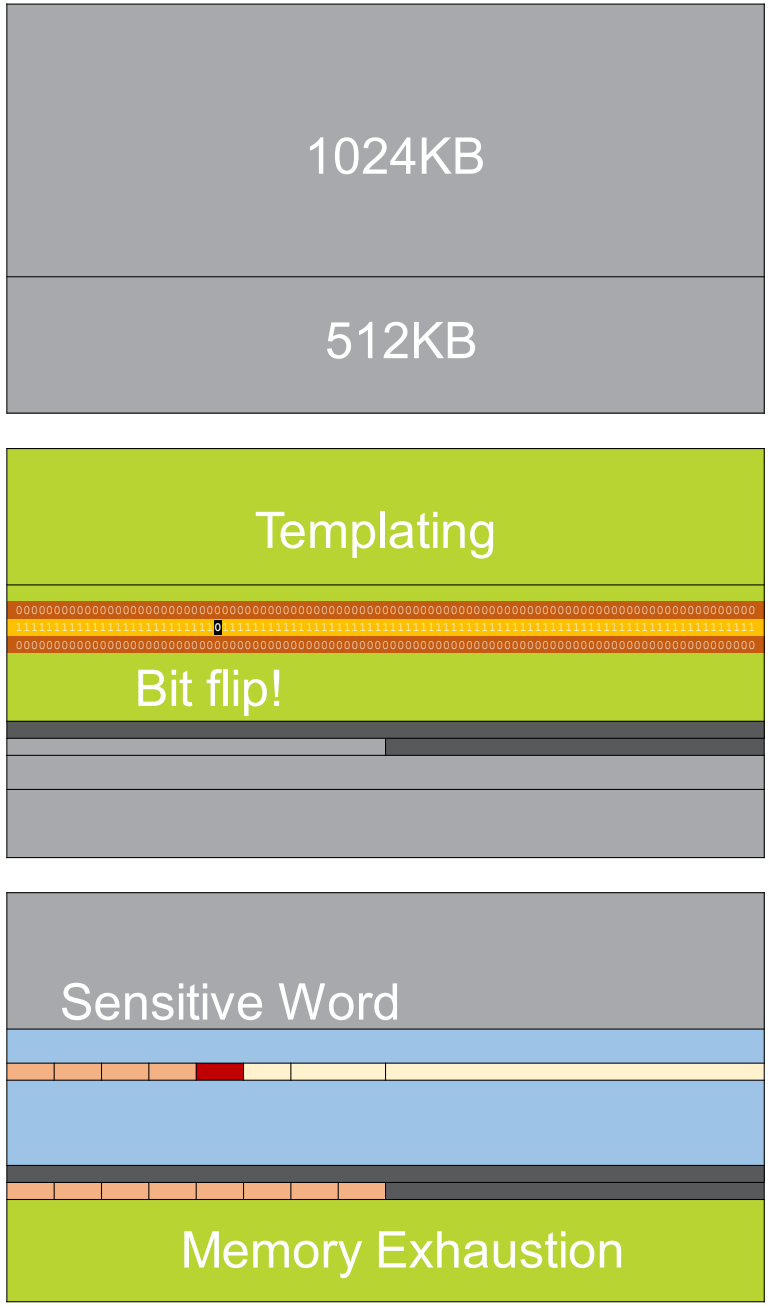
By using direct memory access (DMA) it is possible to induce bit flips from user space

Land sensitive data

Store crucial data structure on a vulnerable page

Reproduce the bit flip

Modify the data structure and get root access



https://www.vusec.net/projects/drammer/

Using Rowhammer to get kernel privileges

“It's like breaking into an apartment by **repeatedly slamming a neighbor's door** until the vibrations open the door you were after”

Citation from:
https://motherboard.vice.com/en_us/article/9akpwz/rowhammerjs-is-the-most-ingenious-hack-ive-ever-seen

Follow us

The Hacker News

Subscribe to Newsletter

GLitch: New 'Rowhammer' Attack Can Remotely Hijack Android Phones

May 03, 2018 Swati Khandelwal

For the very first time, security researchers have discovered an effective way to exploit a four-year-old hacking technique called Rowhammer to hijack an Android phone remotely.

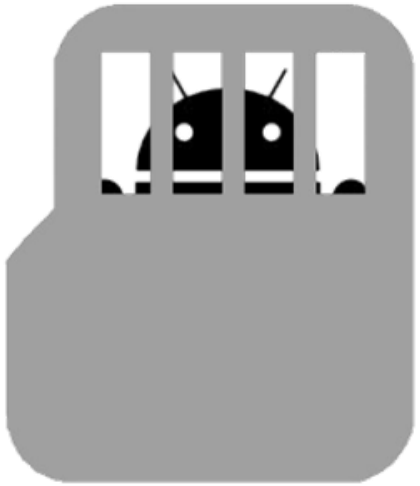
GLitch is the first remote Rowhammer technique that exploits GPU instead of the CPU.

Since the ARM processors inside Android smartphones include a type of cache that makes it difficult to access targeted rows of memory**, researchers make use of GPU, whose cache can be more easily controlled**

DRAM

NAND

Man-In-The-Disk



Slava Makkaveev

Check Point
SOFTWARE TECHNOLOGIES LTD.

DEF CON 2018

August 2018

Storage-based Man-In-The-Disk attack can break fortified Android app's sandbox protection

Careless use of External Storage by applications may open the door to an attack resulting in
silent installation of apps,
denial of service for legitimate apps,…

https://blog.checkpoint.com/2018/08/12/man-in-the-disk-a-new-attack-surface-for-android-apps/

Within the Android OS there are two types of storage

Internal Storage

- Built-in non-volatile memory
- Always available
- Private

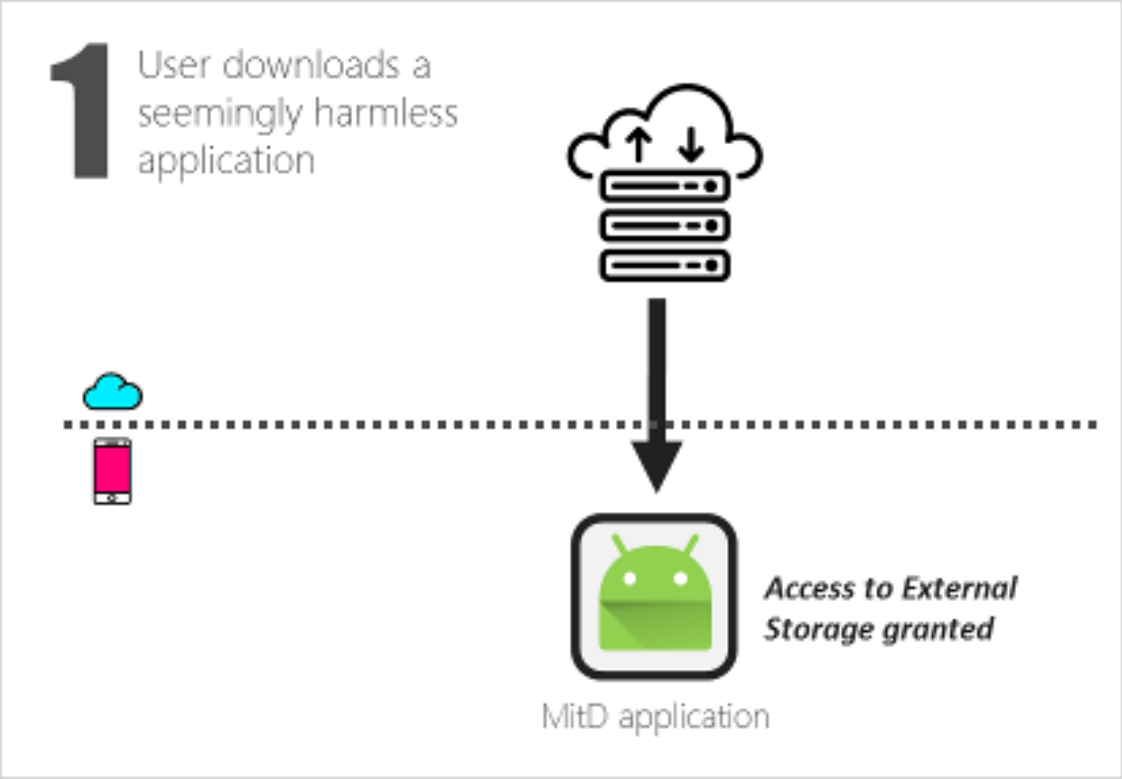
External Storage

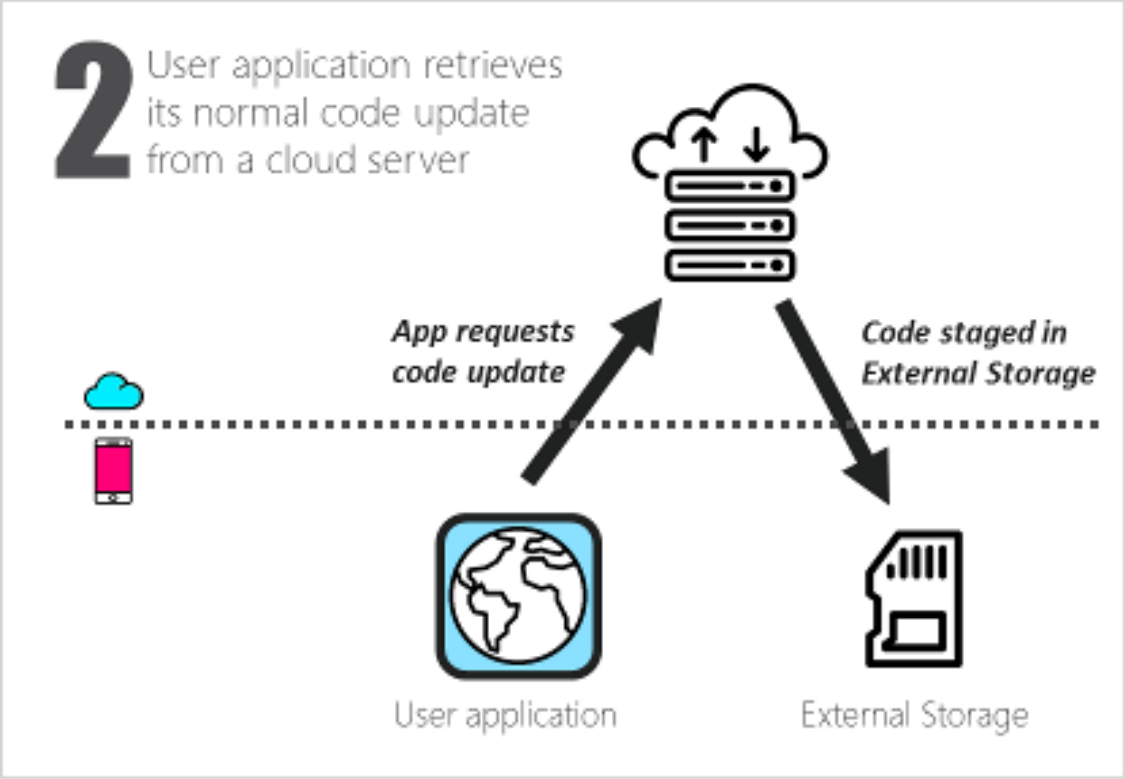
- Often over an SD card or a logical partition within the device's storage
- Public

Why use External Storage?

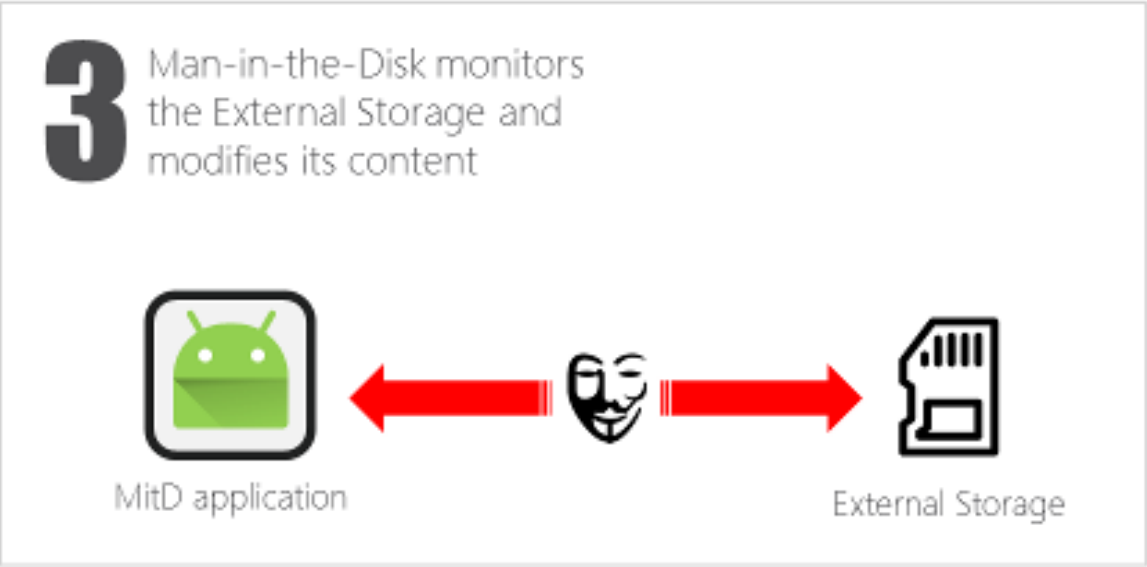
- Share media files between apps
- Transfer files between smartphone and PC
- Compatibility with limited inner storage devices
- Hide the current size of the application

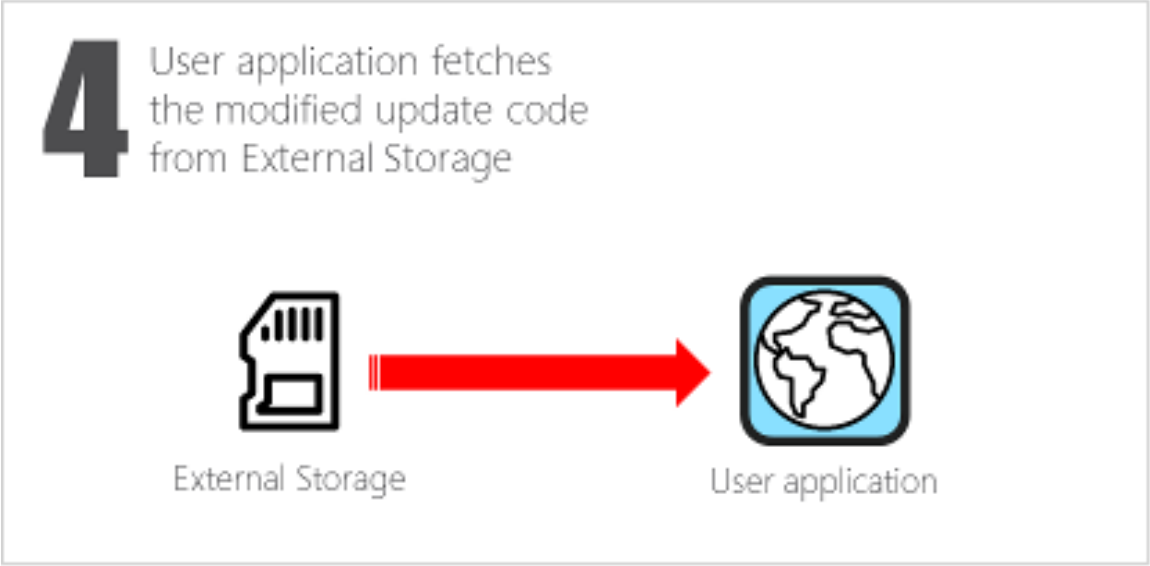
Many apps are updated or receive data from the app provider's server, and store it in the External Storage

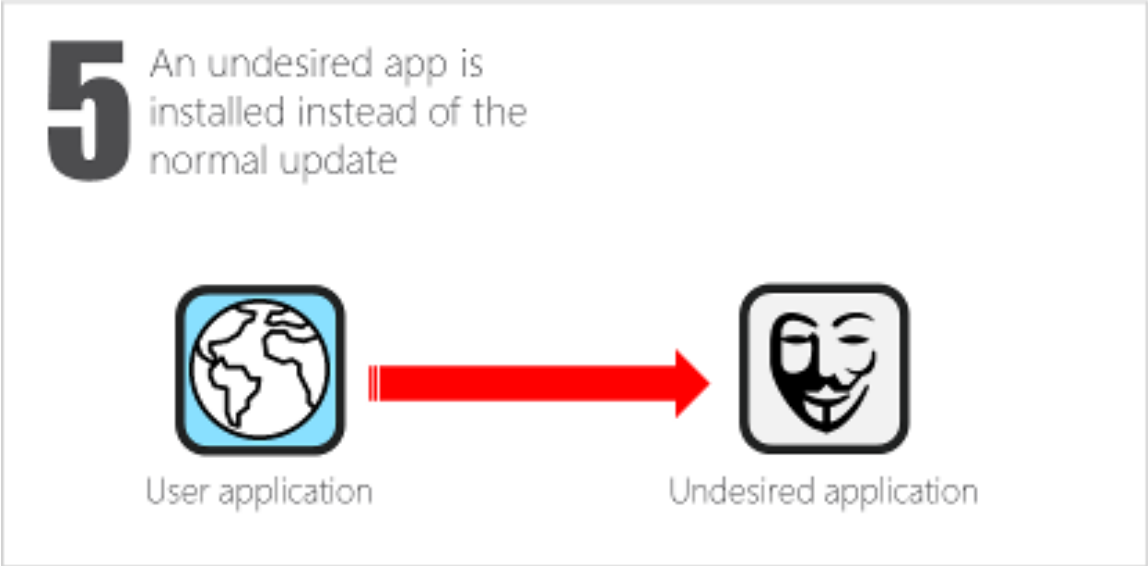




https://blog.checkpoint.com/2018/08/12/man-in-the-disk-a-new-attack-surface-for-android-apps/



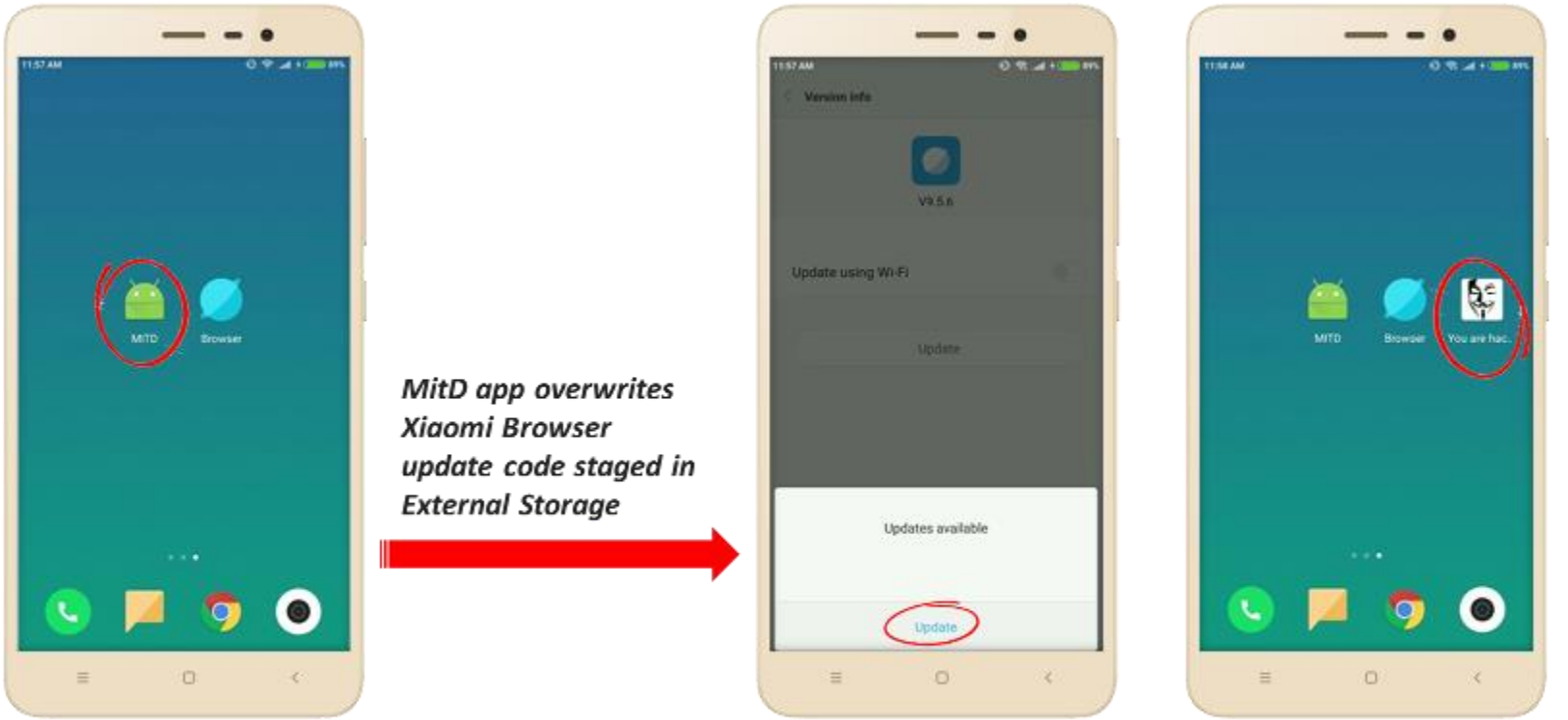




https://blog.checkpoint.com/2018/08/12/man-in-the-disk-a-new-attack-surface-for-android-apps/

Applications Where the Man-in-the-Disk Lives

Google Translate, Yandex Translate, Google Voice Typing, Google Text-to-Speech, Xiaomi Browser,…



User installs the seemingly harmless MitD application

User selects to update the Xiaomi browser

Attacker's malicious application is installed instead

https://blog.checkpoint.com/2018/08/12/man-in-the-disk-a-new-attack-surface-for-android-apps/

“Fortnite Android App Falls Victim to Man-in-the-Disk Flaw”

August 2018

https://threatpost.com/fortnite-android-app-falls-victim-to-man-in-the-disk-flaw/136931/

Summary

Summary

- Memory and Storage can be the target of dangerous security attacks
- To define effective mitigation strategies it is important to bring together researchers with know-how on:
  - Cryptography
  - Security
  - Operating Systems
  - System Architecture
  - Component design
  - Technology

Micron

Micron®