GRAZ UNIVERSITY
OF TECHNOLOGY

SECURE
INFORMATION
TECHNOLOGY
AUSTRIA

Manifest Problems: Analyzing Code Transparency For Android Application Bundles

ACSAC 2024

Florian Draschbacher
Graz University of Technology, Graz, Austria
Secure Information Technology Austria, Vienna, Austria
florian.draschbacher@tugraz.at

Lukas Maar
Graz University of Technology, Graz, Austria
lukas.maar@tugraz.at

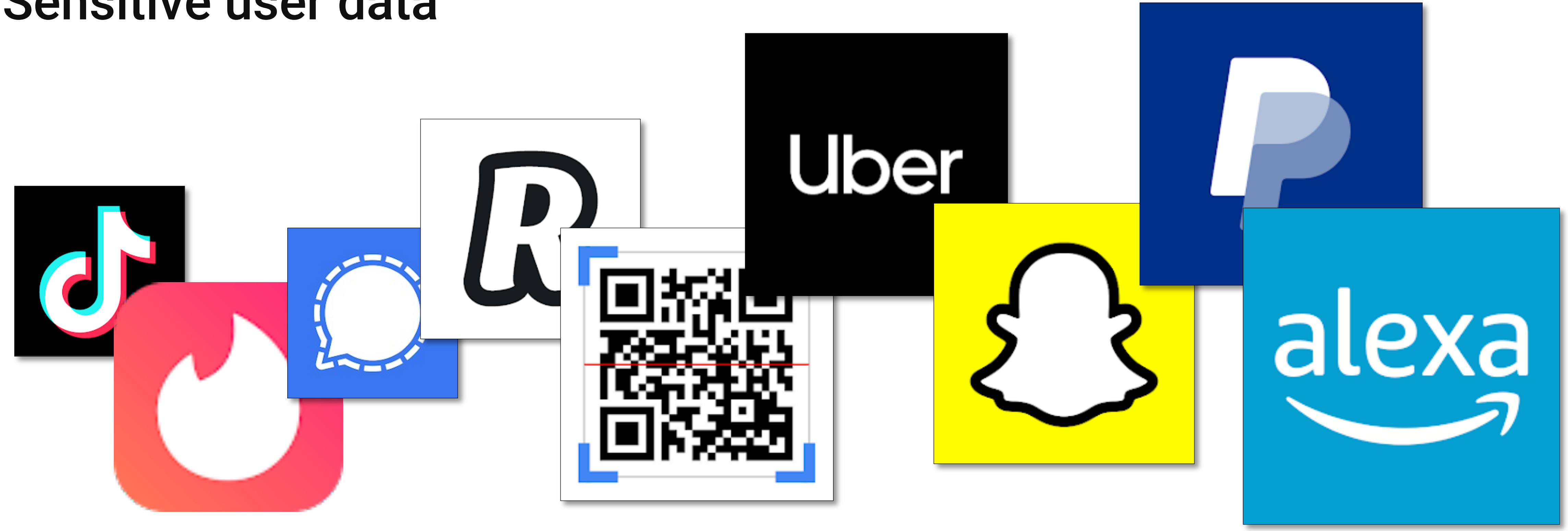
December 13th, 2024

Mobile App Security

- New mobile computing use cases

Mobile App Security

- New mobile computing use cases
  - Sensitive user data



Mobile App Security

- New mobile computing use cases
  - Sensitive user data
- Attractive for attackers

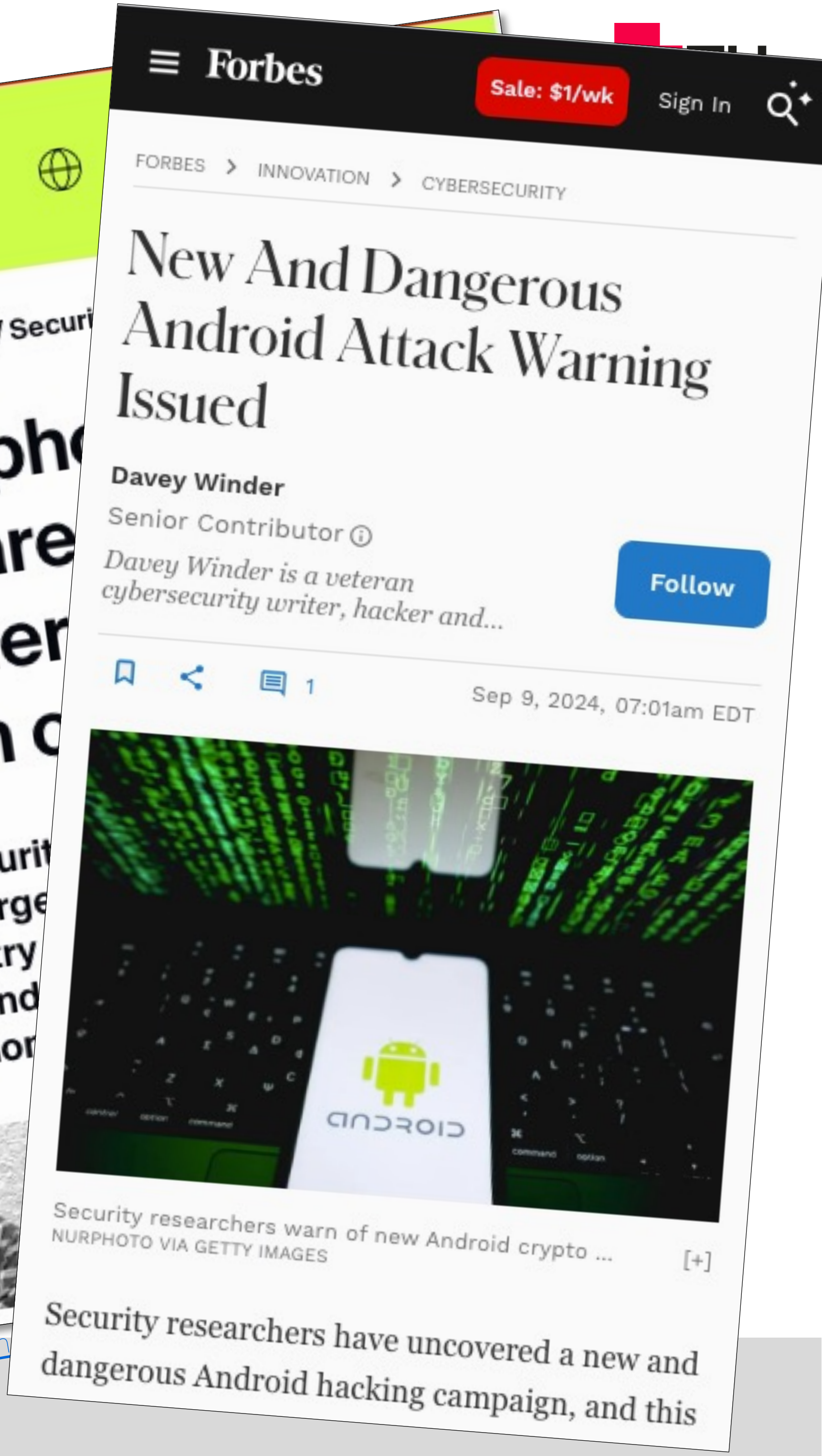
ZDNET

Home / Innovation / Securi

Smartph
malware
rise, her
watch o

Cybersecurit
500% surge
hackers try
details and
smartphon

zdnet.com



FORBES > INNOVATION > CYBERSECURITY

New And Dangerous Android Attack Warning Issued

Davey Winder
Senior Contributor

Davey Winder is a veteran cybersecurity writer, hacker and...

1

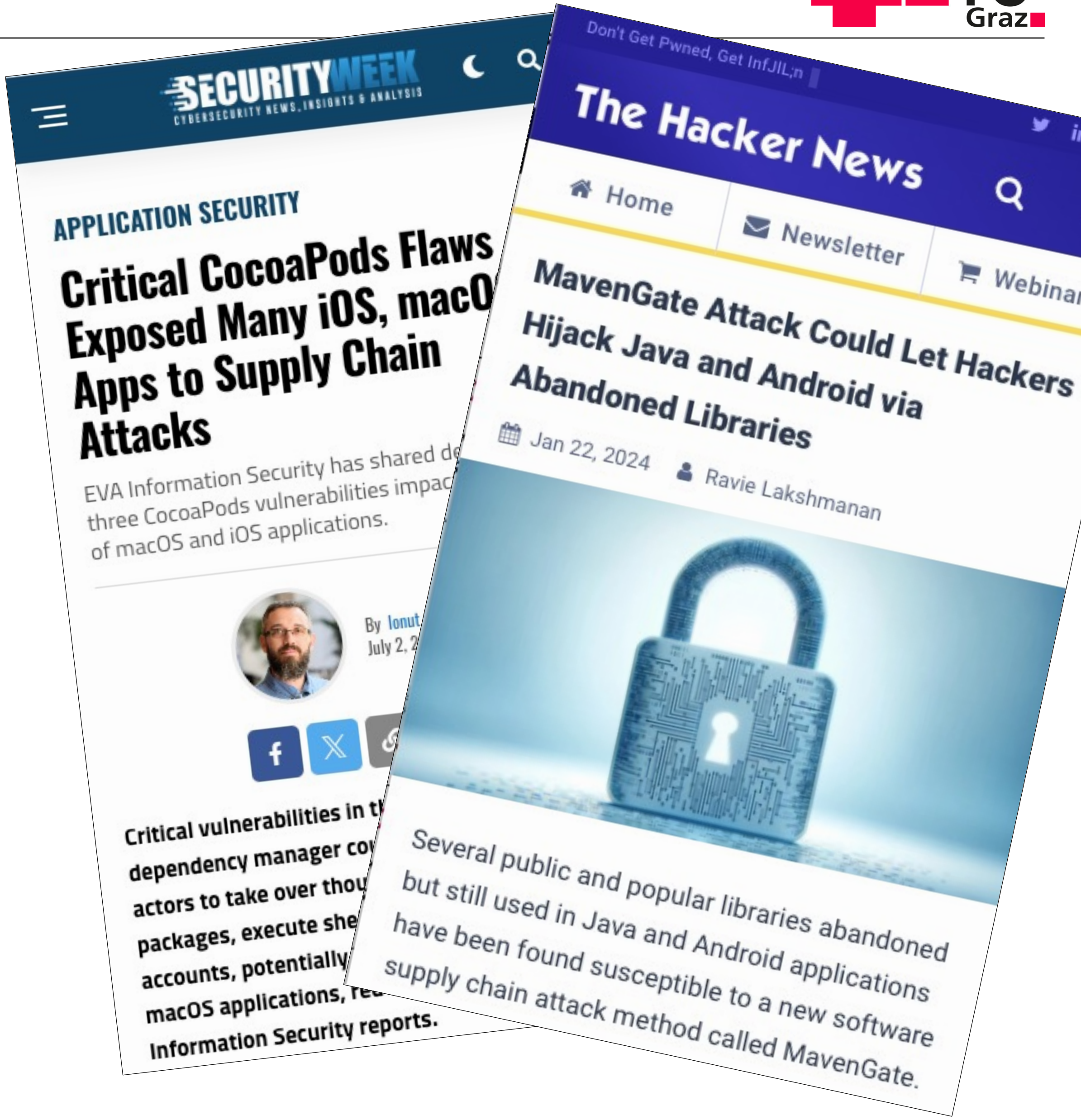
Sep 9, 2024, 07:01am EDT

Security researchers warn of new Android crypto ...
NURPHOTO VIA GETTY IMAGES

Security researchers have uncovered a new and dangerous Android hacking campaign, and this

Mobile App Security

- New mobile computing use cases
  - Sensitive user data
- Attractive for attackers
- Recent attack trend:
  - Supply Chain attacks


SECURITYWEEK
CYBERSECURITY NEWS, INSIGHTS & ANALYSIS

APPLICATION SECURITY

Critical CocoaPods Flaws Exposed Many iOS, macO Apps to Supply Chain Attacks

EVA Information Security has shared de three CocoaPods vulnerabilities impac of macOS and iOS applications.

By Ionut July 2, 2

Critical vulnerabilities in t dependency manager co actors to take over thou packages, execute she accounts, potentially macOS applications, re Information Security reports.

Don't Get Pwned, Get InfJIL;n

The Hacker News

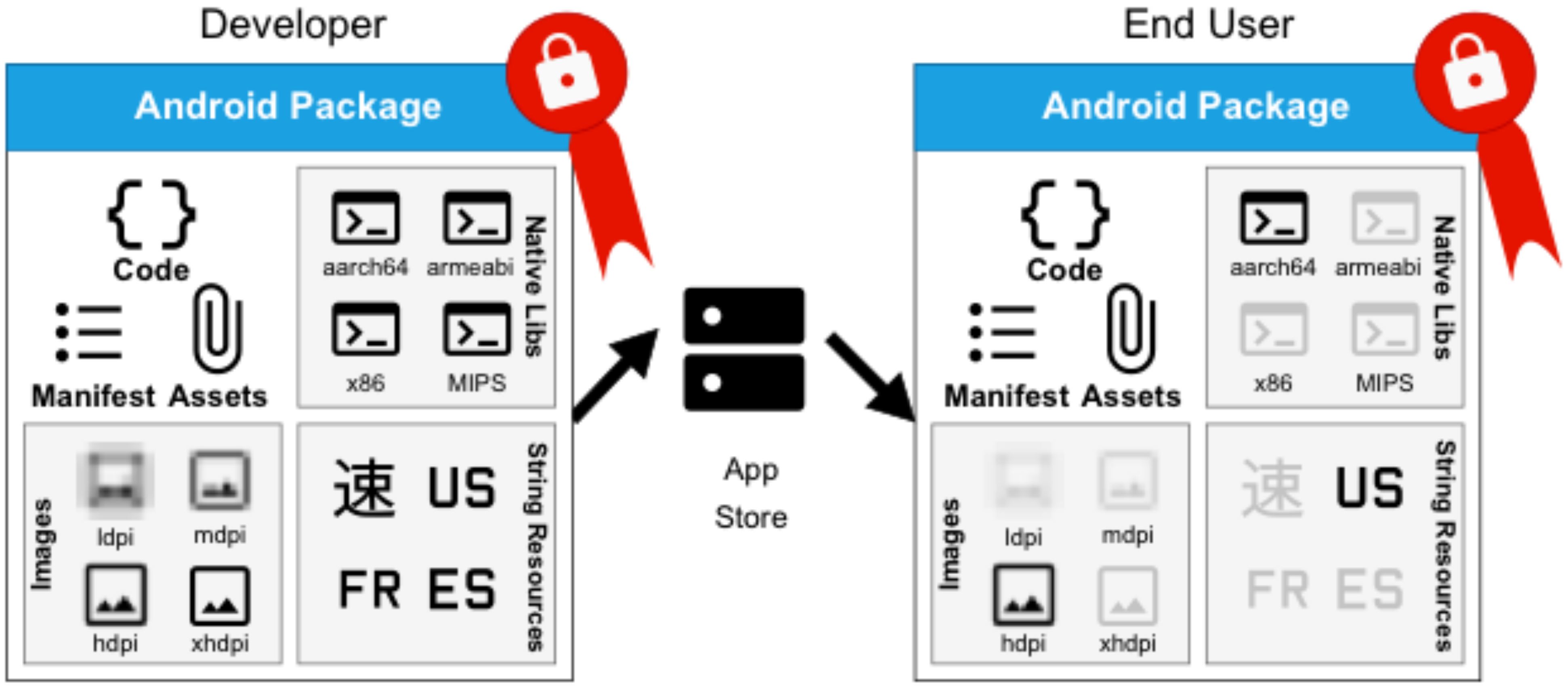
Home Newsletter Webina

MavenGate Attack Could Let Hackers Hijack Java and Android via Abandoned Libraries

Jan 22, 2024 Ravie Lakshmanan

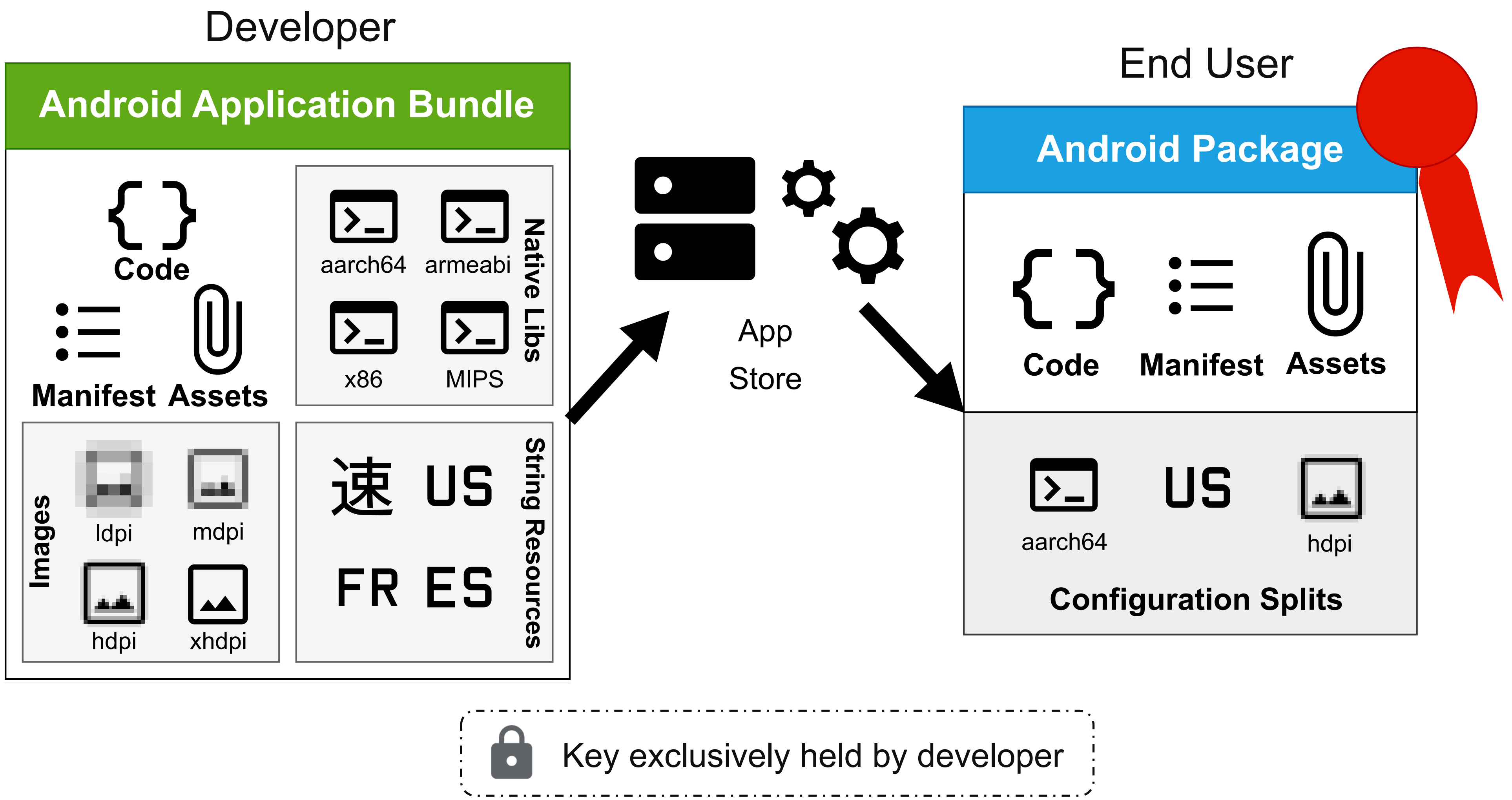
Several public and popular libraries abandoned but still used in Java and Android applications have been found susceptible to a new software supply chain attack method called MavenGate.

<2018: Direct APK Distribution

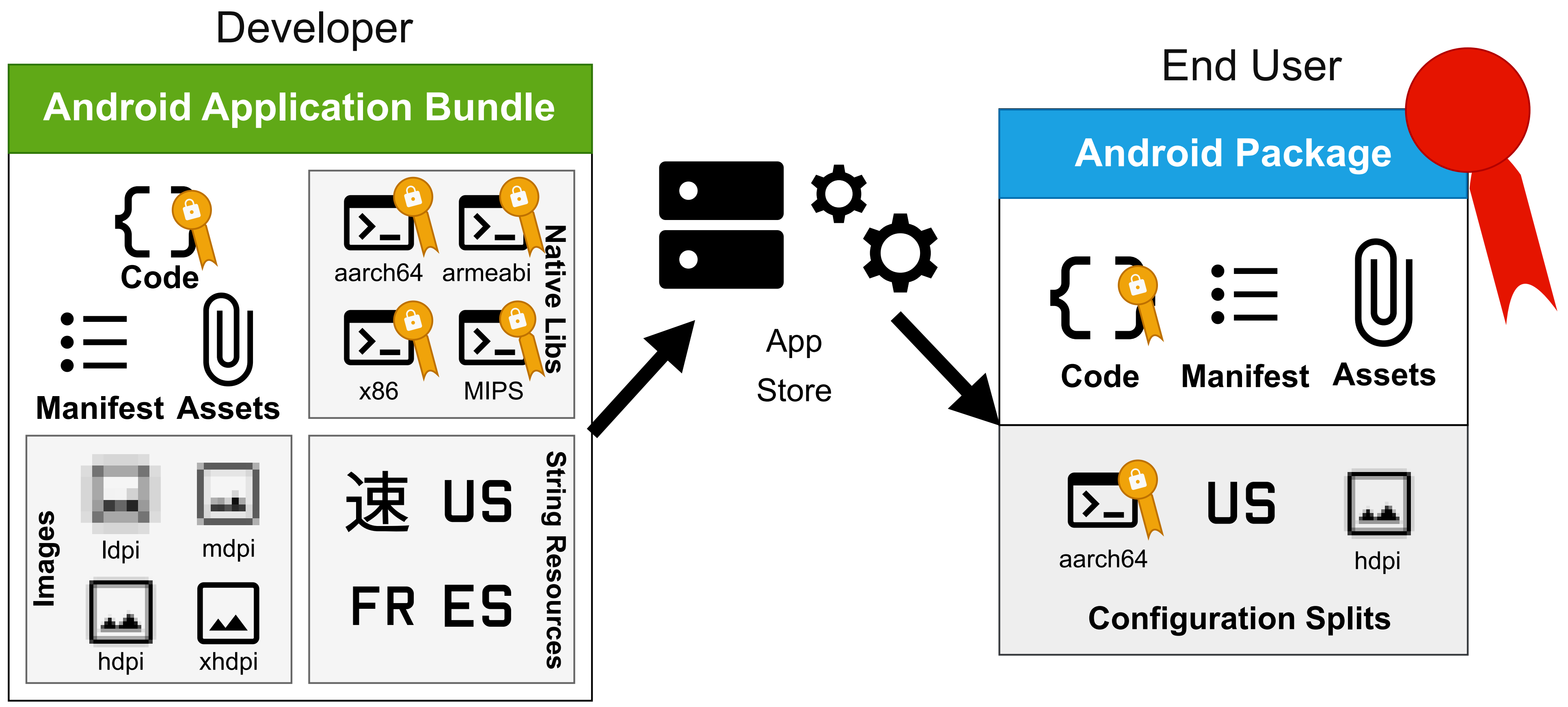


🔒 Key exclusively held by developer

2018: Android Application Bundle (AAB)



2021: Code Transparency for AAB



Key exclusively held by developer

Problem Statement & Approach

Code Transparency for AAB

- Google heavily promotes AAB format
  - APK signing keys in hands of app store operator
  - Breaks integrity guarantees based on APK signature
- Optional Code Transparency
  - Provable integrity guarantee for key parts of the app
  - Ensure code executed matches code built by developer
- No **security analysis** of this scheme so far

Approach

- **Manual analysis of CT design and implementation**
  - Multiple flaws
- **Attacks exploiting flaws**
  - Code execution while retaining valid CT
- **Large-scale survey of CT in practice**
  - Use of CT and AAB on Google Play and Huawei AppGallery
  - Susceptibility to vulnerabilities

Attacker Models

- **Privileged App Store**
  - Preinstalled with privileged permissions
- **Unprivileged App Store**
  - Third-party store e.g. installed by user
- **Other Role in Supply Chain**
  - Can manipulate APK delivered to user

Design and Implementation Flaws

Design Flaws

- **Optionality**
  - Code Transparency is not required!
- **Scope**
  - Only covers DEX and SO files
- **Communication Channel**
  - How to find out legitimate public key?

Implementation Flaws in bundletool

- **Certificate Reuse**
  - APK signing certificate != CT signing certificate
- **DEX or SO in Assets**
  - Even untampered files fail validation
- **App Archives**
  - Inject binary DEX file by design

Evaluation

Attacks

Attack	Attacker	Condition
Stripping CT	Any	None
Modifying Assets	Any	Relevant Assets
Inject Shared Library	Privileged / Unprivileged	None
Debuggable Flag	Privileged	None
Backup Opt-In	Privileged	< Android 14

Goal: **Code Execution** in Context of Target App OR **Data Extraction**

Large-Scale Analyses

- **Apps that use AAB and Code Transparency**
  - Google Play: 46% (AAB), 0.0014% (CT) of 3.3m apps
  - Huawei AppGallery: 0.04% (AAB), 0% (CT) of 240k apps

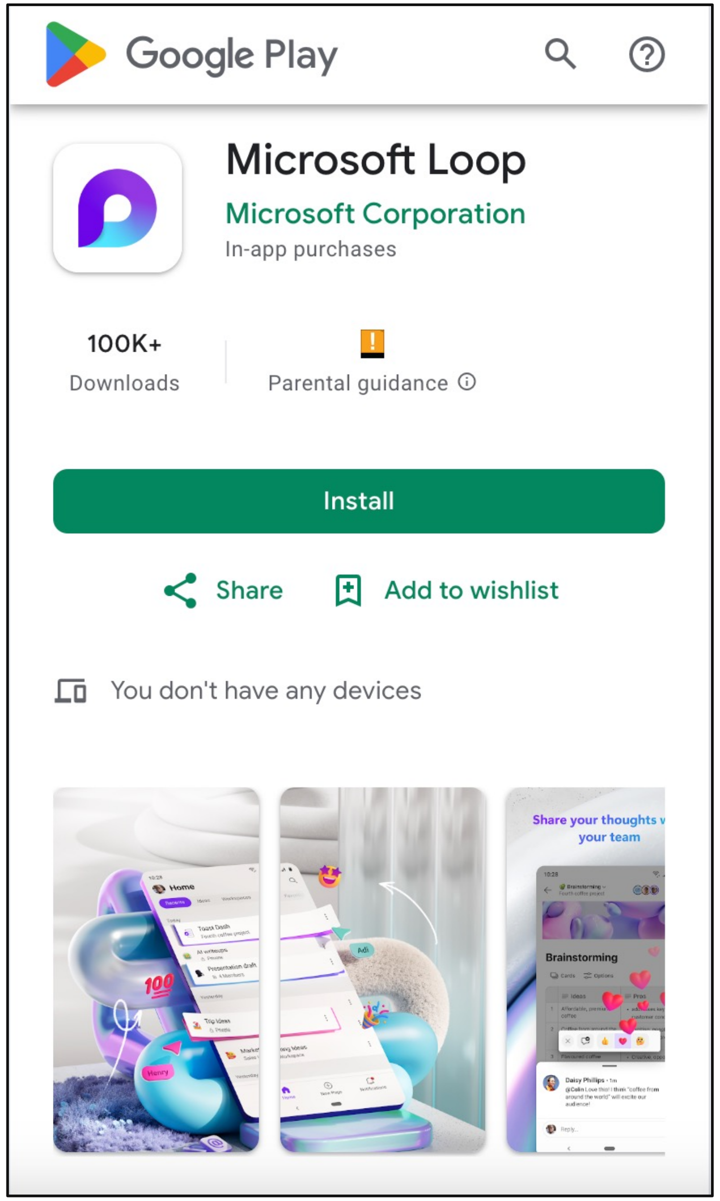
- **Executable Assets in Popular Google Play Apps**
  - 22% of 6648 apps cannot use CT (DEX/SO in assets)
  - 52% susceptible to code execution through asset manipulation
    - If they used CT

Case Study

- Microsoft Loop (uses CT)
- Inject **shared static library** into app manifest:

```
<uses-static-library
    android:name="com.attack.library"
    android:version="1"
    android:certDigest="f7…9d">
</uses-static-library>
```

- Bundletool still reports intact CT


Google Play

Microsoft Loop
Microsoft Corporation
In-app purchases

100K+
Downloads
Parental guidance

Install

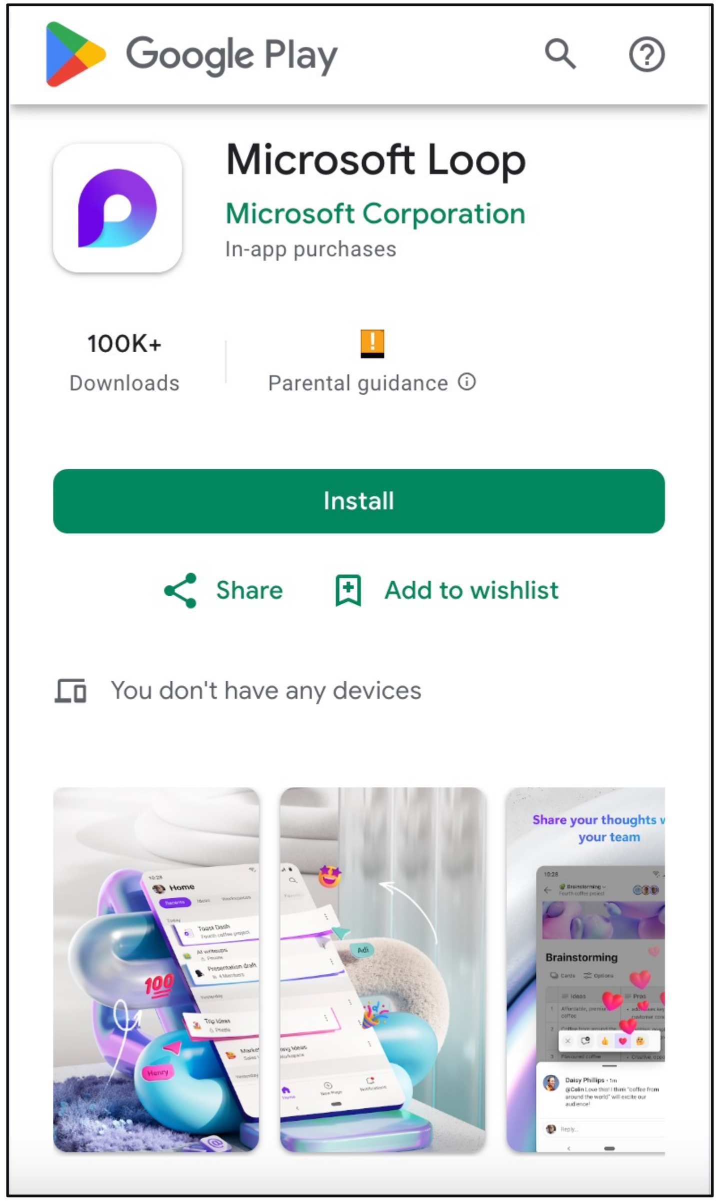
Share
Add to wishlist

You don't have any devices

Case Study

```
$ bundletool check-transparency --mode=apk , --apk-
zip=loop-patched-apks.zip
APK signature is valid. SHA-256 , fingerprint of the apk
signing key certificate (must be compared with  the
developer's public key manually): 94 … 6B
Code transparency signature is valid. SHA-256
fingerprint of the code transparency key certificate
(must be compared with the developer's public key
manually): 52 … 02
Code transparency verified: code related file contents
match the code transparency file.
```

- **Bundletool still reports intact CT**

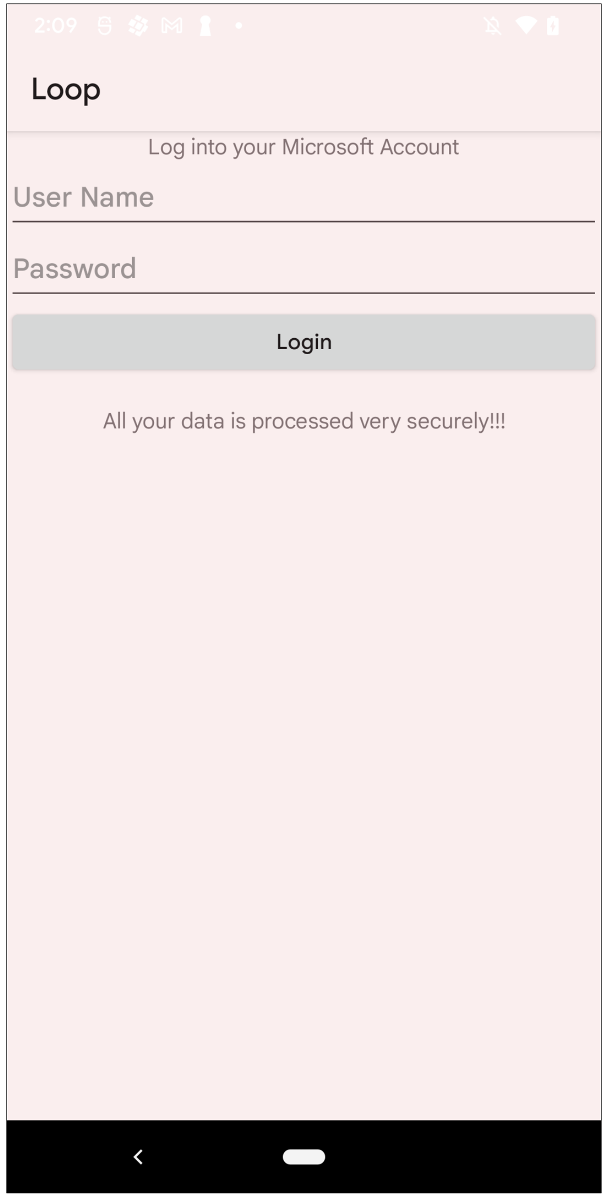


Case Study

- Microsoft Loop (uses CT)
- Inject **shared static library** into app manifest:

```
<uses-static-library
    android:name="com.attack.library"
    android:version="1"
    android:certDigest="f7…9d">
</uses-static-library>
```

- Bundletool still reports intact CT
- **Static library executes in context of MS Loop**


Loop

Log into your Microsoft Account

User Name

Password

Login

All your data is processed very securely!!!

Conclusion

Manifest Problems

- First security analysis of Code Transparency for Android App Bundles
- Severe consequences of AAB
  - Yet CT is hardly used
  - Even apps that use CT are vulnerable
- Discussions with Google
  - Transparency Log, …

Questions?