V CONFERENZA NAZIONALE

Partenariato cybersecurity privacy

Cybersecurity: stato dell'arte, sistemi di difesa e resilienza

Roma, Palazzo Wedekind, Piazza Colonna 366, 4 aprile 2022

(In)Sicurezza delle applicazioni mobili

Alessio Merlo

Il Mondo delle Applicazioni Mobili

Applicazioni Mobili: il lato oscuro

Applicazioni ad alcune con potenziali vulnerabilità di sicurezza

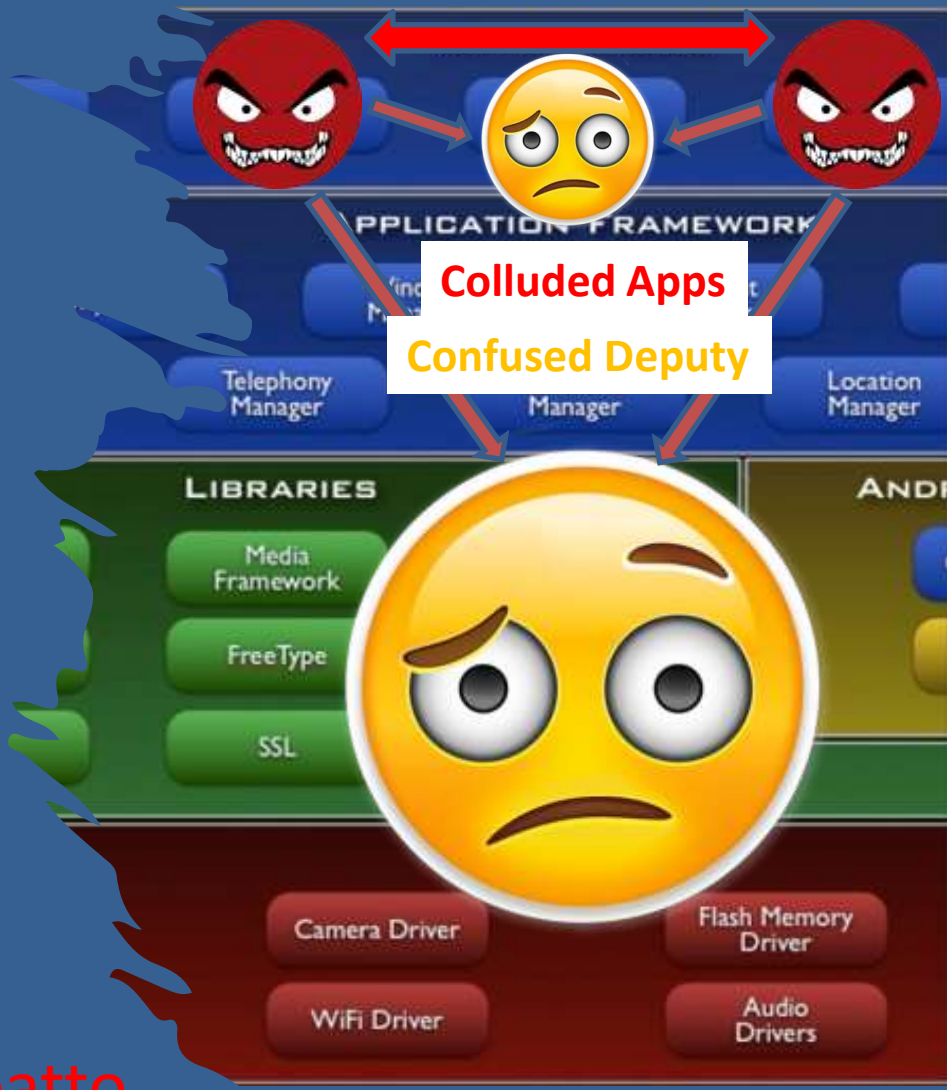
Sicurezza delle app mobili: lo scenario

Le app malevole possono sftruttare vulnerabilità sia nelle altre applicazioni sia del Sistema Operativo.

Due diversi “modelli”:

- **Confused Deputy**
- **Colluded Applications**

Rischio associato ad una vulnerabilità: Probabilità x impatto



Vulnerabilità: devo realmente preoccuparmi?

Portpass app may have exposed hundreds of thousands of users' personal data

Vaccine passport app has more than 650,000 registered users, according to its CEO

Sarah Rieger · CBC News · Posted: Sep 28, 2021 11:22 AM MT | Last Updated: September 29, 2021

Vaccine passport app Portpass may have exposed users' personal data like drivers' licences and photos. CBC was able to access the photos on the right that belong to users on the app. The IDs have been blurred to protect those users' identities and information. (Portpass/CBC)

Security bugs left unpatched in Android app with one billion downloads

The vulnerabilities impact SHAREit, an app used for sharing files between users and their devices.

Amazon's Ring Neighbors app exposed users' precise locations and home addresses

Zack Whittaker

https://www.cbc.ca/news/canada/calgary/portpass-privacy-breach-1.6191749
https://www.zdnet.com/article/security-bugs-left-unpatched-in-android-app-with-one-billion-downloads/
https://techcrunch.com/2021/01/14/ring-neighbors-exposed-locations-addresses/

Malware: devo realmente preoccuparmi?

ROBERTO F.
VIRUS ANDROID
13 MAR 2022 - 10:41
COMMENTI

Escobar è un pericoloso malware in grado di controllare i device Android

SCIENZA & TECNOLOGIA • MOBILE

Attenzione a quest'app per Android apparentemente innocua: nasconde un malware che ruba i nostri dati

Sabrina Del Fico — Pubblicato il 25 Marzo 2022

Un'applicazione dall'apparenza innocua che permette di creare simpatiche animazioni è in realtà la porta di accesso per un pericoloso malware chiamato FaceStealer

https://www.tuttoandroid.net/news/2022/03/13/escobar-malware-bancario-android-938629/
https://www.greenme.it/scienza-e-tecnologia/mobile/malware-android-ruba-dati-personali/
https://www.cpomagazine.com/cyber-security/kaspersky-discovers-about-100000-new-banking-trojans-and-warns-about-increasing-mobile-malware-sophistication/

Ma sono sempre problemi di "altri"?

App IO

2 High
10 Medium
2 Low

EasyPol - PagoPA

3 High
8 Medium
2 Low

App INPS

1 High
7 Medium
2 Low

Giustizia Civile

1 High
6 Medium

Analisi automatica eseguita tra il 30/3/2022 ed il 2/4/2022 !!!

I motivi sono molteplici:

- White label app
- Requisiti funzionali ma non di sicurezza

Alcuni problemi potrebbero essere risolti server side, ma non è sempre così

Come possiamo difenderci?

Vulnerability Assessment & Penetration Testing

Mobile App Hardening

Mobile Security Training

Come possiamo difenderci?

Vulnerability Assessment & Penetration Testing

Mobile App Hardening

Mobile Security Training

Strumenti Automatici

APPROVER

MOBSF

QUARK

Attività di Approfondimento Manuale

Come possiamo difenderci?

Vulnerability Assessment & Penetration Testing

Mobile App Hardening

Mobile Security Training

Protezione App da manomissioni e leak di informazioni

DexGuard
GUARDSQUARE

ARMANDroid

Come possiamo difenderci?

Vulnerability Assessment & Penetration Testing

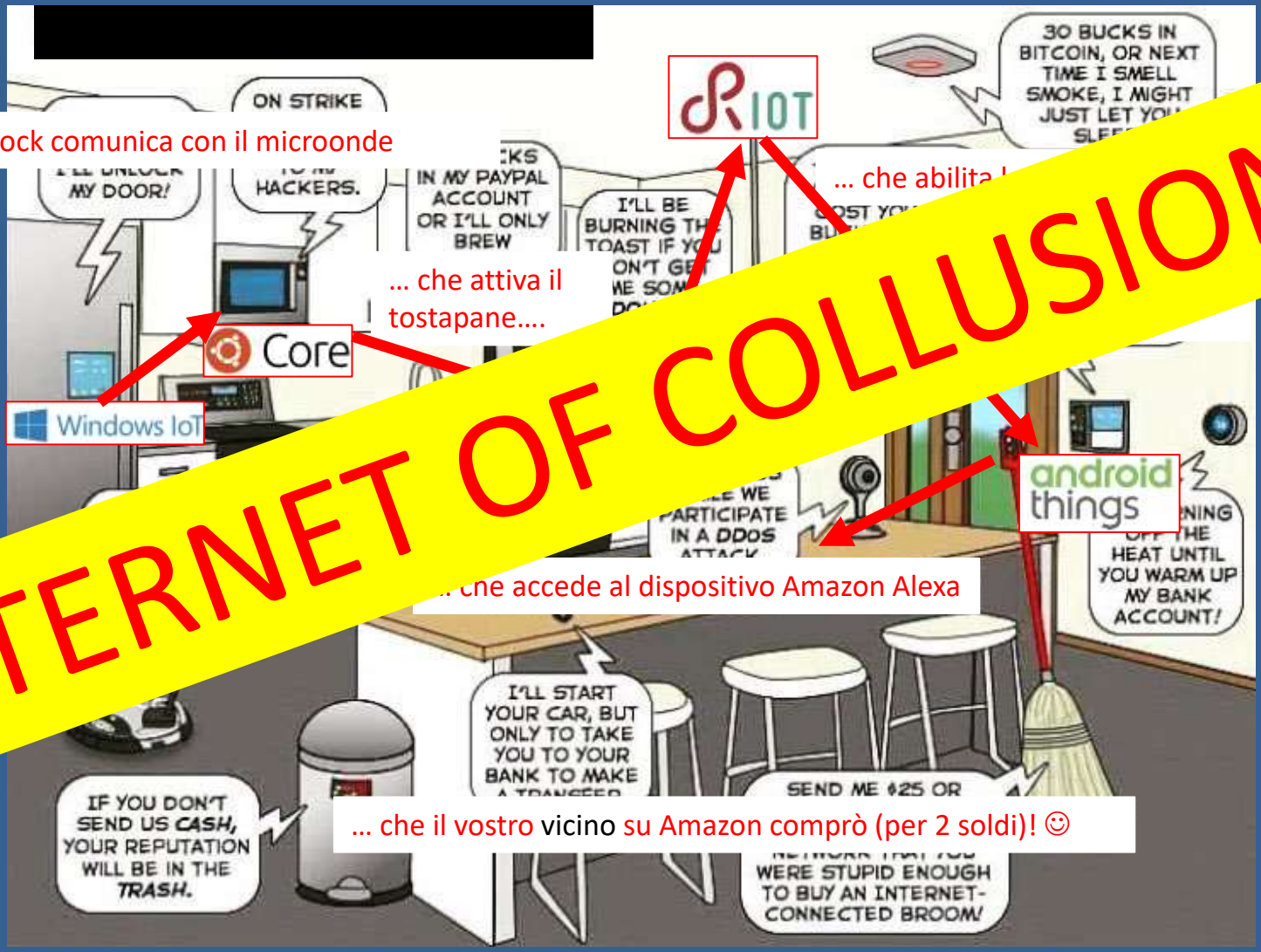
Mobile App Hardening

Mobile Security Training

Training degli sviluppatori: tecniche di sicuro di Mobile App

Training degli analisti di sicurezza mobile: VA/PT & monitoraggio

La situazione promette di peggiorare



Lo smart lock comunica con il microonde

… che abilita l

… che attiva il tostapane….

… che accede al dispositivo Amazon Alexa

… che il vostro vicino su Amazon comprò (per 2 soldi)! ☺

INTERNET OF COLLUSION

L'IoT «incontra» il Mobile

CVE-2019-11061 : Broken access control in HG100

CVE-2019-11063 : Broken access control in SmartHome app

Conclusioni

Le applicazioni sono il «ventre mollo» della sicurezza del sistema

La superficie di attacco cambierà (aumenterà?!)

Aziende e istituzioni devono fare squadra per definire approcci condivisi allo sviluppo e all'analisi di sicurezza delle applicazioni mobili

Migliorare il training di sviluppatori e analisti di sicurezza - cosi come l’awareness dell'utente - consentirebbe di mitigare le minacce

Spingere verso il trasferimento tecnologico