Securing Mobile Devices & Protecting the Privacy of Users

Martina Lindorfer
Technische Universität Wien
martina@iseclab.org
https://martina.lindorfer.in
@lindorferin
About Me

• Assistant Professor at TU Wien (Security & Privacy Division) since October 2018
• Postdoc at the University of California, Santa Barbara 2016-2018
• PhD from TU Wien 2011-2016
• Researcher at SBA Research 2013-2015
Research Interests

Malware Analysis

Privacy Leak Detection

System Security

Machine Learning
Research Goals

- Systematic study of mobile apps and operating systems for
  - malicious & harmful behavior
  - privacy leaks
  - vulnerabilities

- Build scalable analysis techniques

- Provide large-scale datasets to the community

- Advance the state-of-the-art of dynamic analysis approaches
Research Impact

- Users
- Developers
- Media
- Law Enforcement
- Regulators
- OS Vendors
- App Stores
- ISPs
Threats to Users’ Privacy

- Targeted advertising
- Price discrimination
- Sensitive information
- Trust developer to secure information?

→ Increasing interest from regulators

“If you are not paying for it, you are the product.”
RECON: Revealing Privacy Leaks (MobiSys 2016)

- Identify PII leaks on a wide range of devices through network flow analysis
- Collect data from real users
  - Analysis automation ("login walls")
  - Feedback from users about detection accuracy
- Give users control over leaked information

https://recon.meddle.mobi
User Feedback Loop
Privacy Dimensions

Information Type
- Tracking IDs
- User information
- Location
- Installed apps
- Passwords
- ...

Transport Security
- Plaintext
- or
- Encrypted

Destination
- First Party
- or
- Third Party
Privacy Leak Trends (NDSS 2018)

- Users are becoming more privacy aware, but are developers?
- Study 7,665 (512) app releases over 8 years
- Quantify privacy risk for a specific app version
- Consider personal privacy “preferences”
Privacy Dashboard
Security Impact

- Plaintext password leaks in > 25 apps
- Passwords sent to third parties
- Affects millions of users
- Responsible disclosure (3 months)
Developer Responses

“Thank you for responsibly disclosing this”

“We can’t fix this because our vendor went out of business”

“Sending passwords in plaintext is intentional”

“We do not claim to be a secure messaging app”
PANOPTISPY: Unexpected Media Leaks (PETS 2018)

- Identify & measure media (audio, images, video) exfiltration at scale
- Unexpected privacy leaks in media data
  - Finding 1: No evidence of audio/video surveillance
  - Finding 2: Server-side photo editing
  - Finding 3: Screen recording
    - Recording of users’ interactions exposing private information
These Academics Spent the Last Year Testing Whether Your Phone Is Secretly Listening to You

No, your smartphone is not listening to you, researchers say, but it may be watching you.

Smartphone apps don't listen to your conversations, but they do something equally creepy.

The researchers found that while smartphone applications did not send audio clippings to third-party domains, they did send screenshots or screen recordings to them.

Uh-oh. Boffins say most Android apps can slurp your screen – and you wouldn't even know it.

Fancy that.

Your phone is probably spying on you

By Andy Meek, BGR

Yes, your phone is spying on you... but not how you think it is.

Yahoo Finance Video • July 5, 2018
“Google constantly monitors apps and analytics providers to ensure they are policy-compliant. When notified of our findings, they reviewed GoPuff and Appsee and took the appropriate actions.”
Thank you!

✉️ martina@iseclab.org
🌐 https://martina.lindorfer.in
🐦 @lindorferin