Android Apps
An Attacker's Perspective

QCon
SAN FRANCISCO

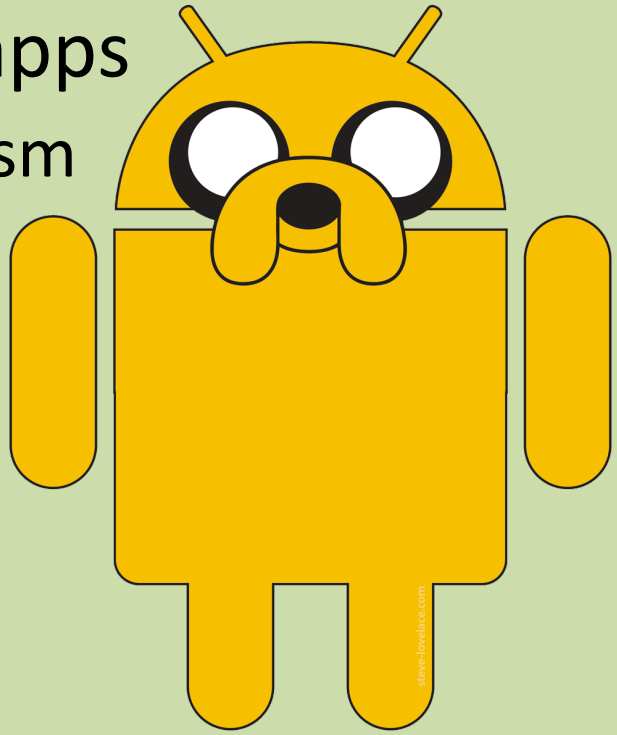
Who am I?

Tony Trummer

- Manager of Security Monitoring and Incident Response at LinkedIn
- Creator of QARK, an open-source static code analysis and exploitation tool for Android applications
- Recognized in Android Security Acknowledgements

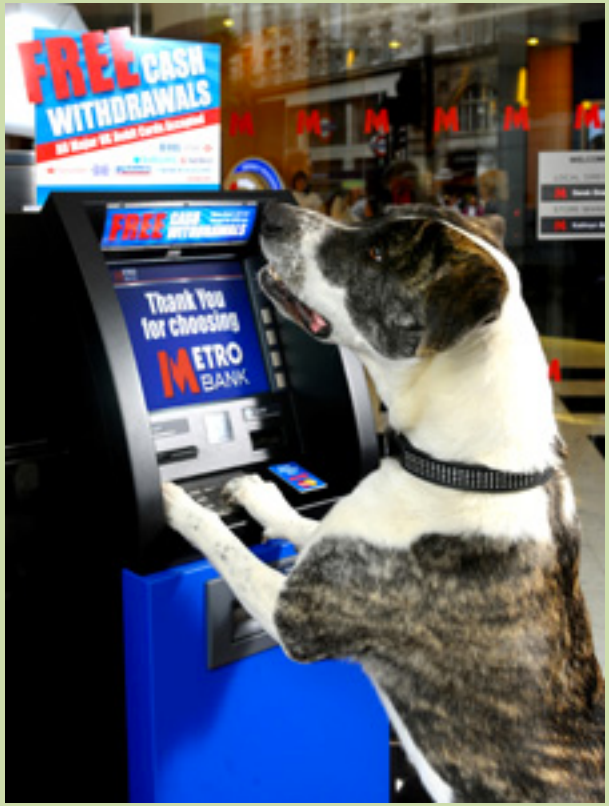
Android Apps

- Replacing the browser as the portal to the Internet
  - More users = More victims = More interesting
- Generally less secure than iOS apps
  - iOS is limited to one IPC mechanism
  - Apple gets to call the shots
  - Limited hardware variation
  - “Update or die” is okay
- Not as “juicy” as the APIs



ATMs

- What's Inside?
  - What is the "gold"
- What goes in?
  - Trust boundaries
  - Inputs
- How can I get what's inside?
  - Exfiltration
- How do I not get caught?
  - Covering your tracks



Attacker Motivations

- Kids
  - Cheating
  - Notoriety
- Criminals
  - Money
  - Sensitive data
  - Surveillance
- Nation States
  - Sensitive data
  - Surveillance

Threat Modeling

- STRIDE
  - Attacker's perspective (or exploitation type)
- DREAD
- TRIKE
- AS/NZS 4360
- OCTAVE

Attacker Desires

- Easy
- Remote
- Invisible
- Persistent
- Distributable
- Universal

Android Apps

- How to get on device?
- What's inside?
- How do I get in?
- How to get what's inside?
- How not to get caught?

Getting on the device

- Playstore
- Non-Playstore stores
- USB
- Social Engineering
- SMS,NFC,etc

What's inside?

- Passwords
- API keys
- Private data
- Money
- Privileges
- Cookies
- Personal data

How do I get in?

- Reverse the app
- IPC
- Network Requests
- File system/SDCARD
- WebViews
- OS Bugs

How to get at what's inside

- XSS
- SQL Injection
- Information Leakage
- LFI/RFI
- Command Injection
- Insecure comms
- Rooted device

How do I not get caught?

- Dynamic code
- Malicious updates
- Can you see me now?
- Know thy enemy

Won't Google Protect Us?

- Maybe
  - Bouncer
- Eventually…
  - Fragmentation
  - Prioritization
- A billions times no!
  - China

Frustrating Attackers

- Reduce Attack Surface
- Code Obfuscation
- Certificate Pinning
- Don’t store data
- Security review
- HW Backed encryption
- Layered Defenses
- Flexible design

Hey you, get QARK

https://github.com/linkedin/qark

I'm Done

https://www.linkedin.com/in/tonytrummer

@SecBro1