Mobile Security

for the forgetful
Me

• Max Veytsman
• Security Consultant at Security Compass
• max@securitycompass.com
Client-side mobile attacks
Lost and stolen computers account for a quarter of lost data
Stealing a phone

A demonstration
What’s on your phone?

- Contacts
- Call history
- Photos
- Text messages
What’s on your smartphone?

• Email
• Social networking
• GPS
• Mobile banking
• Corporate VPN
• Just about anything else you can think of
But my phone is password-protected!
Bypassing a password

A demonstration
Caveats
But I can remotely wipe my phone!
Faraday Cage
Faraday Cage
At least they won’t be able to pose as me.
Cloning
Cloning
Spoofing identifiers
Weaponizing the Android Emulator

- Blog post forthcoming
- https://github.com/SecurityCompass/android_emulator_spoofing
“The enemy knows the system”
The enemy can

- Access the filesystem
- Decompile and read your code
- Use remote debugging to:
  - Access memory at runtime
  - Step through code branches
An Aside
Earlier: we made the phone accept any password. Is that an issue?
Hi Maxim,

Thank you for your note.

An attacker with the ability to modify /data/system/gesture.key already has root access on the phone. They can do much more damage to a phone than disabling or nulling out the screen unlock. The attack scenerios described already assume a compromised device.

Regards,

Nick
The Android Security Team
Our Goal:
Root Access $\neq$ Game Over
What can you do?

As a developer
Encrypt data at rest
(Or not to store anything)
Encryption is hard
About Us

Honeypot Consulting is an independent medical consulting firm working primarily in the private insurance and employer sectors.

We are a team of specialized professionals certified and trained in objectively, comprehensively and skillfully completing independent medical evaluations.

We conduct thorough in-home assessments, functional capacity evaluations, job site analyses and physical demands analyses to aid in the management of various insurance and employer claims.

Our professionals have a breadth of experience in their fields in addition to extensive health and wellness, coaching and management backgrounds.

We deliver on our promise to exceed expectations by delivering the highest quality of service while maintaining the fairest, most reliable and objective measures, assessment protocol and professional recommendations.

Let us work with you today!

Military grade encryption
Military grade encryption
Military grade encryption
Where do you put keys?
One answer is PBE (PKCS #5)
...Or not to store anything.
Don’t trust the hardware
Be aware of Shannon's Maxim
What can we do?

As the security community
OWASP Mobile Security

Develop guidelines

Encrypting data at rest
Develop guidelines

Defensive mobile coding
Develop guidelines

Mobile incident response
What can you do?

As a user
This is how we mitigate the risk of stolen laptops
Tell Android I sent you!

- http://code.google.com/p/android/issues/detail?id=11211
Full disk encryption
WhisperCore
limited phone support
beta
Be careful!
Photos

- http://www.flickr.com/photos/ripper/273262947/
- http://www.flickr.com/photos/boyce-d/5096202428/
- http://www.flickr.com/photos/arselectronica/5056212669/
- http://www.flickr.com/photos/miiitch/4880022048/
Questions?

• max@securitycompass.com

• @mveytsman (I’m a sporadic twitter user, but trying to change)