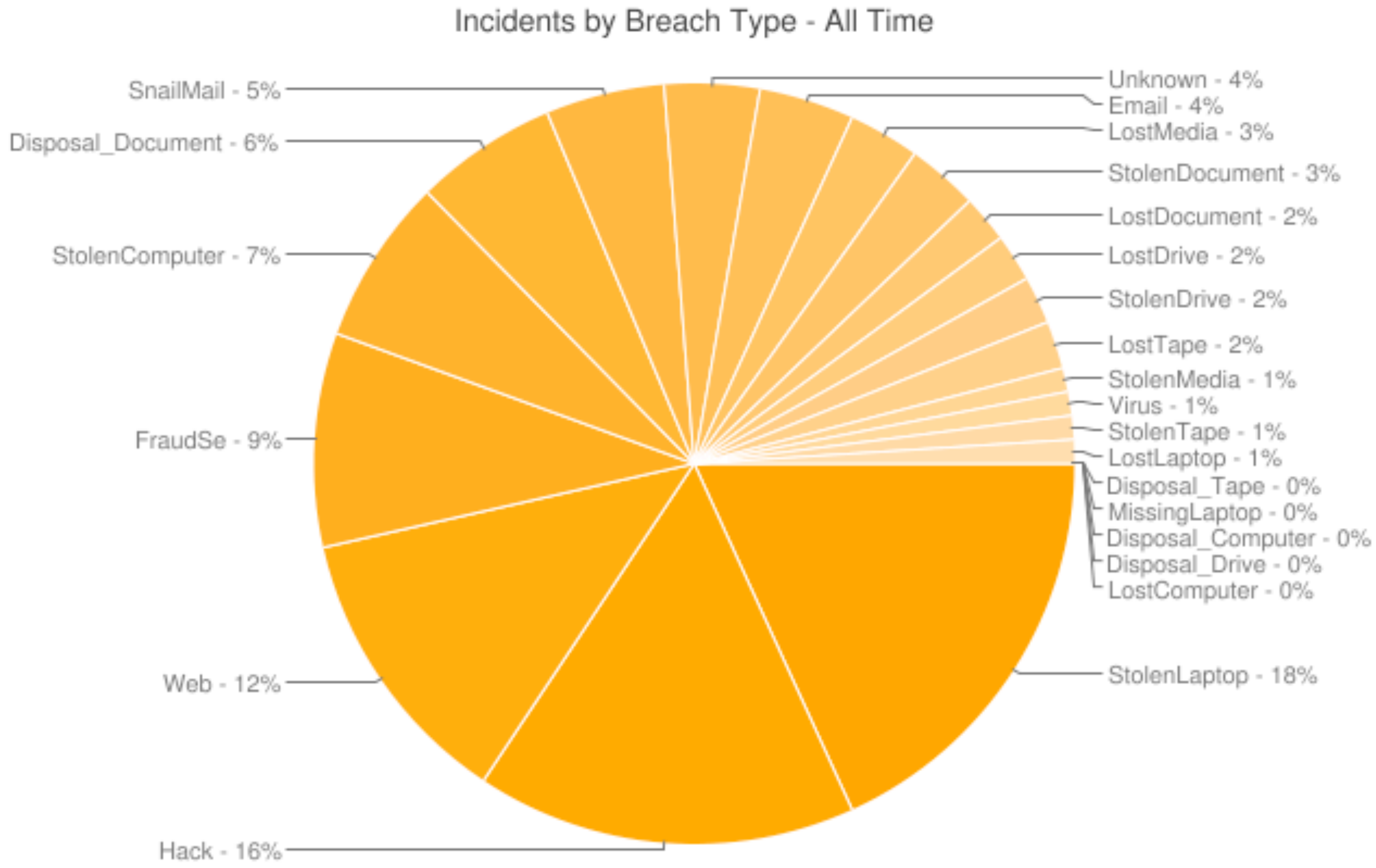
Mobile Security

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

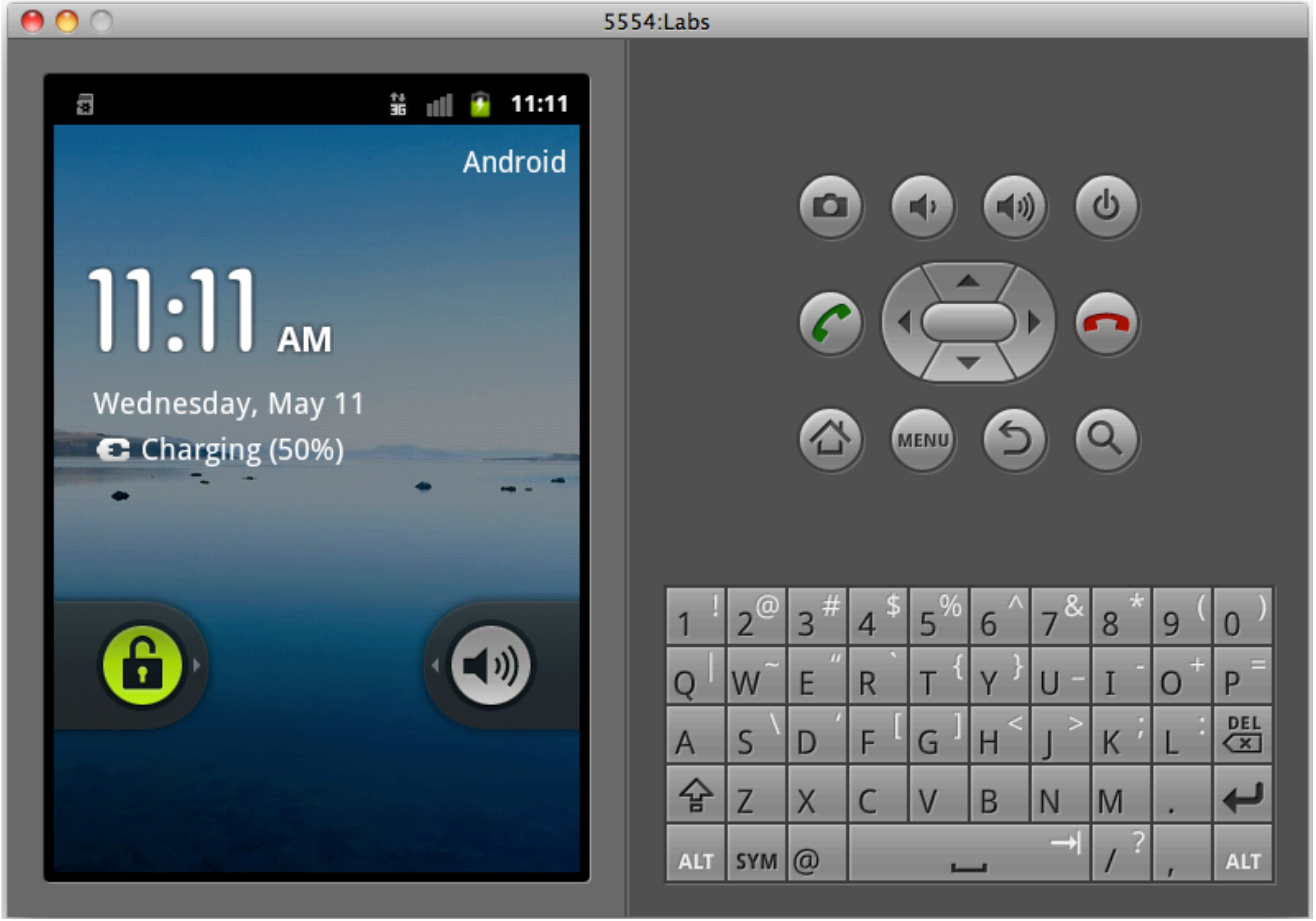
But I can remotely wipe my phone!

Faraday Cage

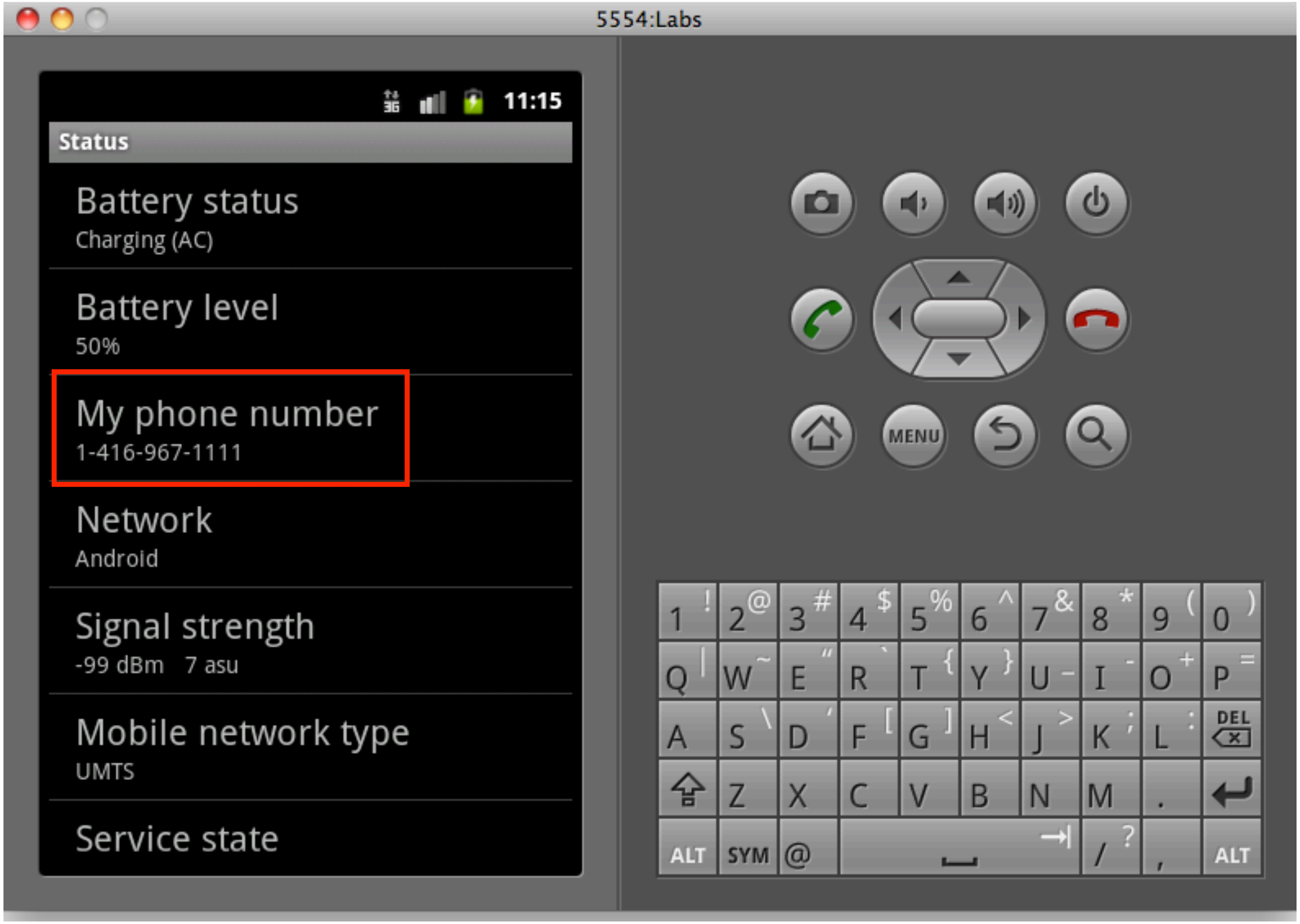
Faraday Cage

At least they won’t be able to pose as me.

Cloning


5554:Labs
11:11
Android
11:11 AM
Wednesday, May 11
Charging (50%)
MENU
1 2 3 4 5 6 7 8 9 0
Q W E R T Y U I O P
A S D F G H J K L DEL
Z X C V B N M
ALT SYM @ ALT

Cloning



Status

Battery status
Charging (AC)

Battery level
50%

My phone number
1-416-967-1111

Network
Android

Signal strength
-99 dBm 7 asu

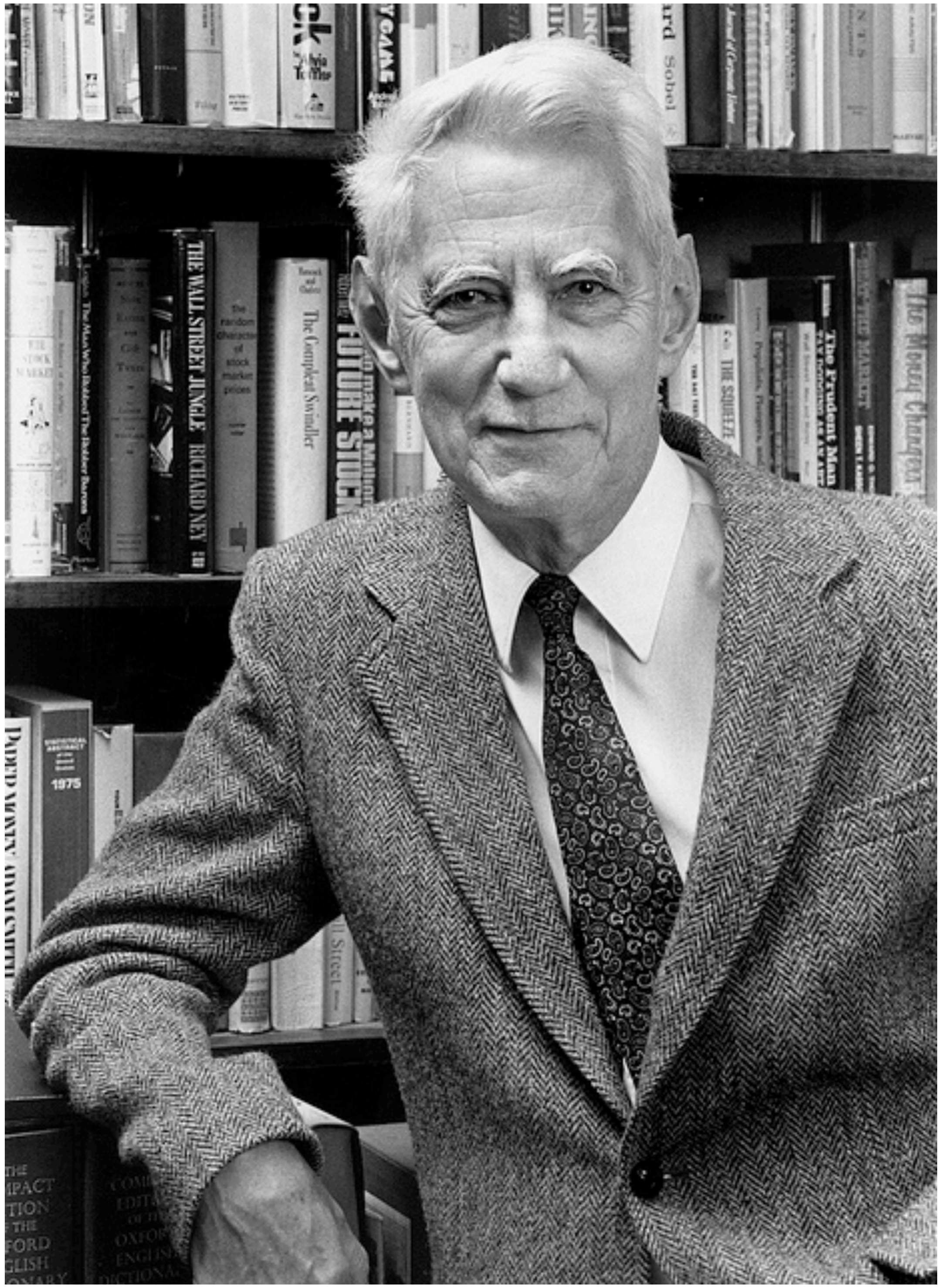
Mobile network type
UMTS

Service state

Spoofing identifiers

Weaponizing the Android Emulator

- Blog post forthcoming
- https://github.com/SecurityCompass/android_emulator_spoofing

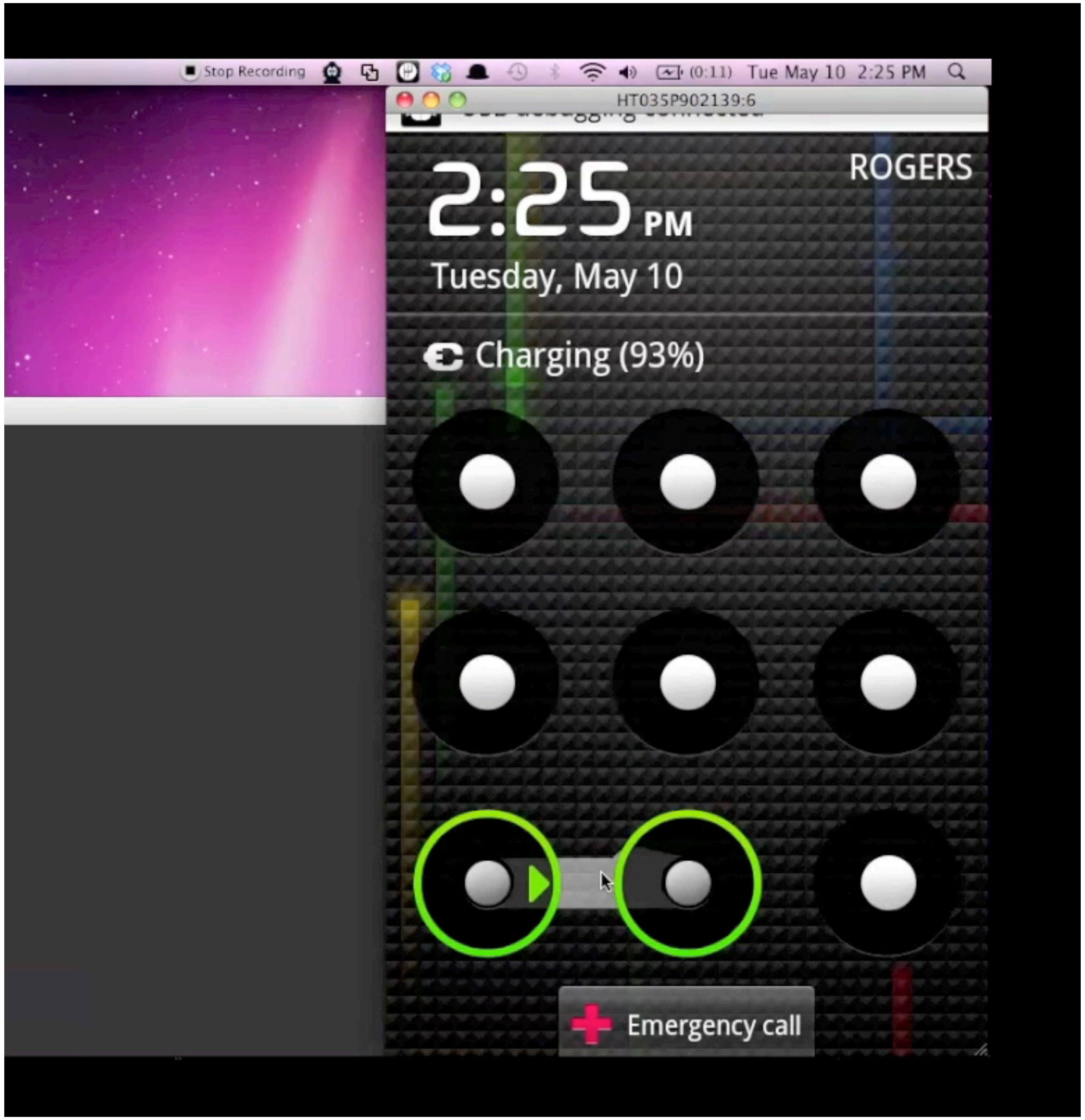


“The enemy knows the system”

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 != Game Over

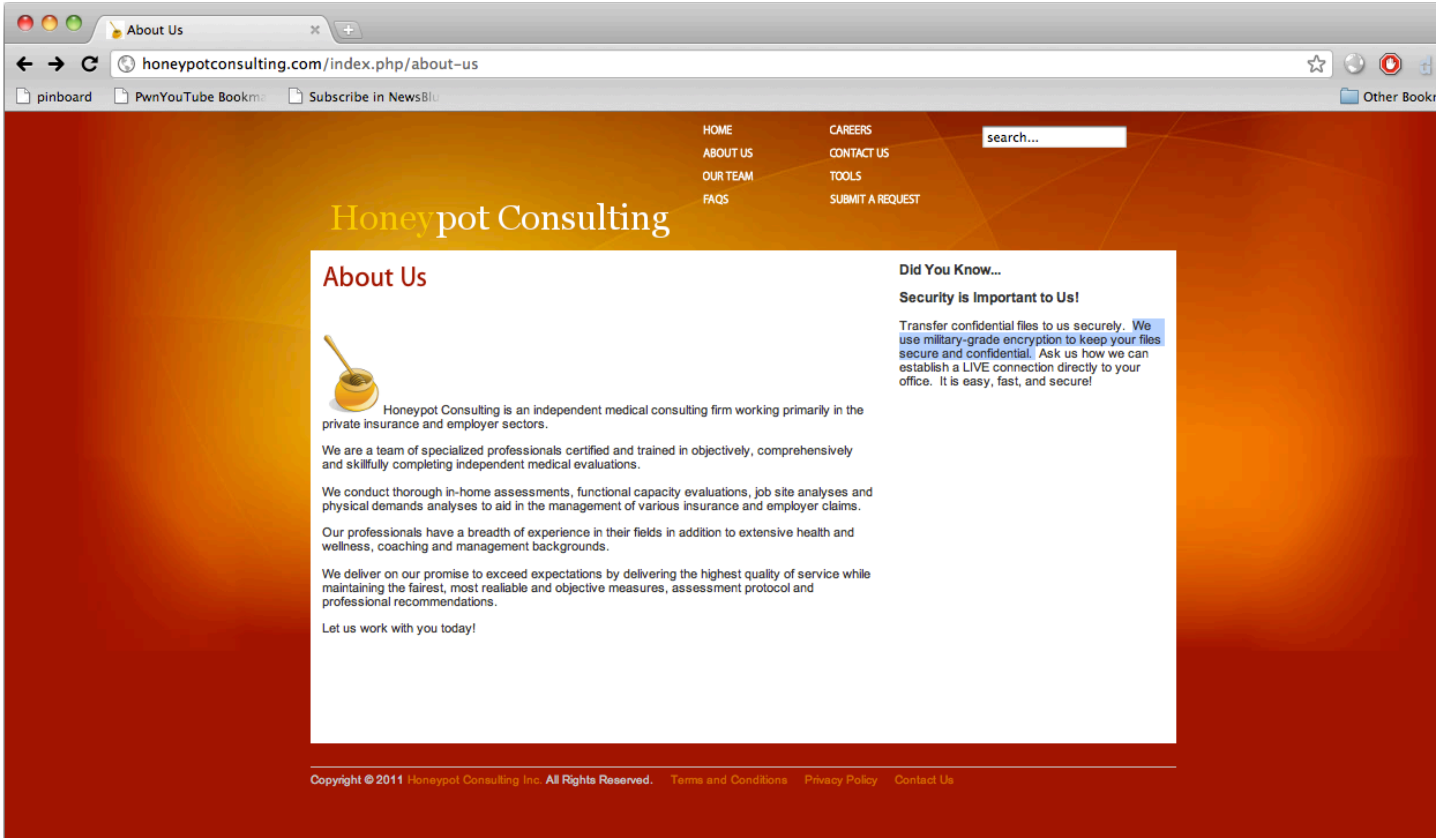
What can you do?

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 realiable and objective measures, assessment protocol and professional recommendations.

Let us work with you today!

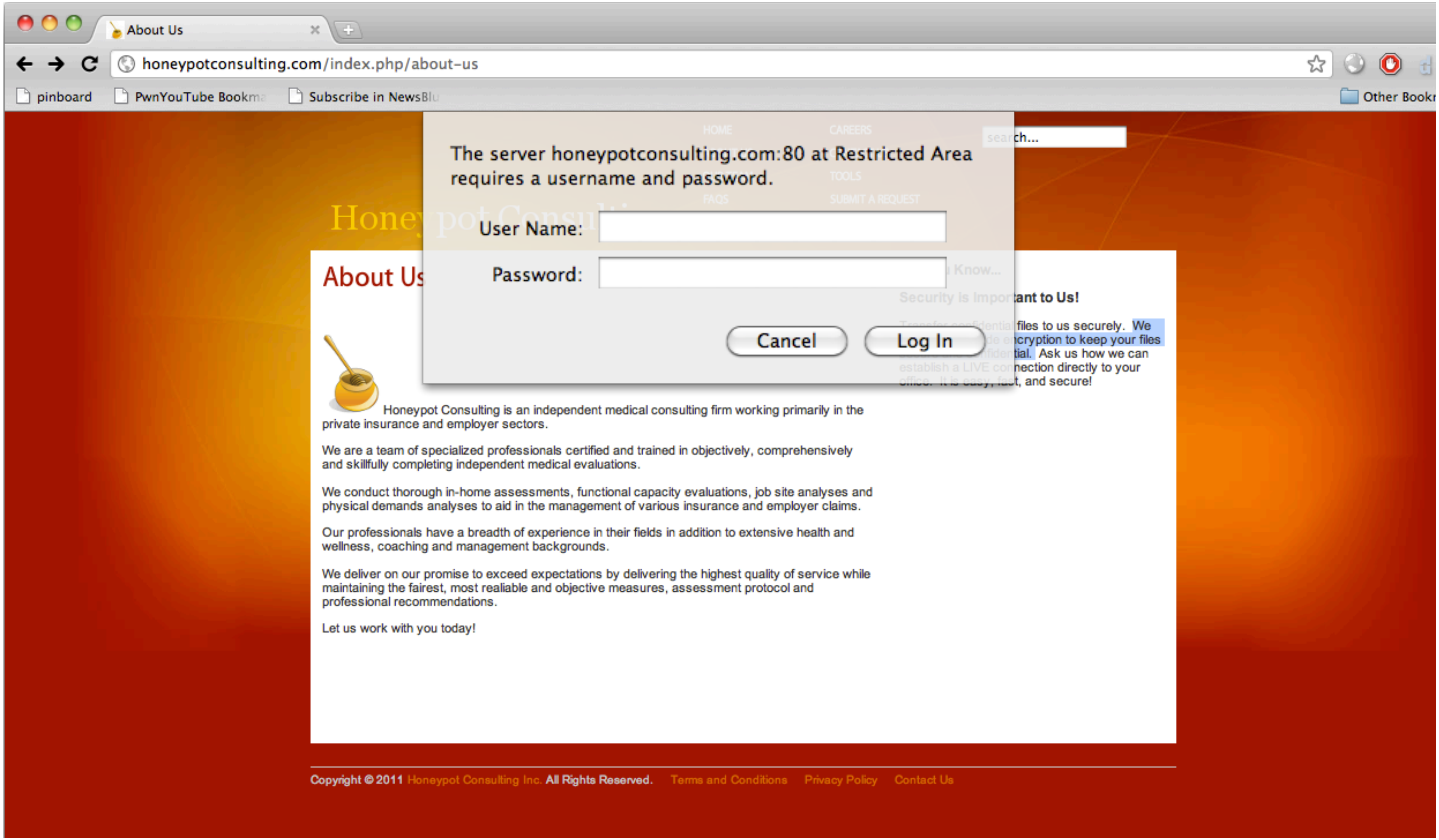
Did You Know...

Security is Important to Us!

Transfer confidential files to us securely. We use military-grade encryption to keep your files secure and confidential. Ask us how we can establish a LIVE connection directly to your office. It is easy, fast, and secure!

Copyright © 2011 Honeypot Consulting Inc. All Rights Reserved. Terms and Conditions Privacy Policy Contact Us

Military grade encryption



The server honeypotconsulting.com:80 at Restricted Area requires a username and password.

User Name:

Password:

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 realiable and objective measures, assessment protocol and professional recommendations.

Let us work with you today!

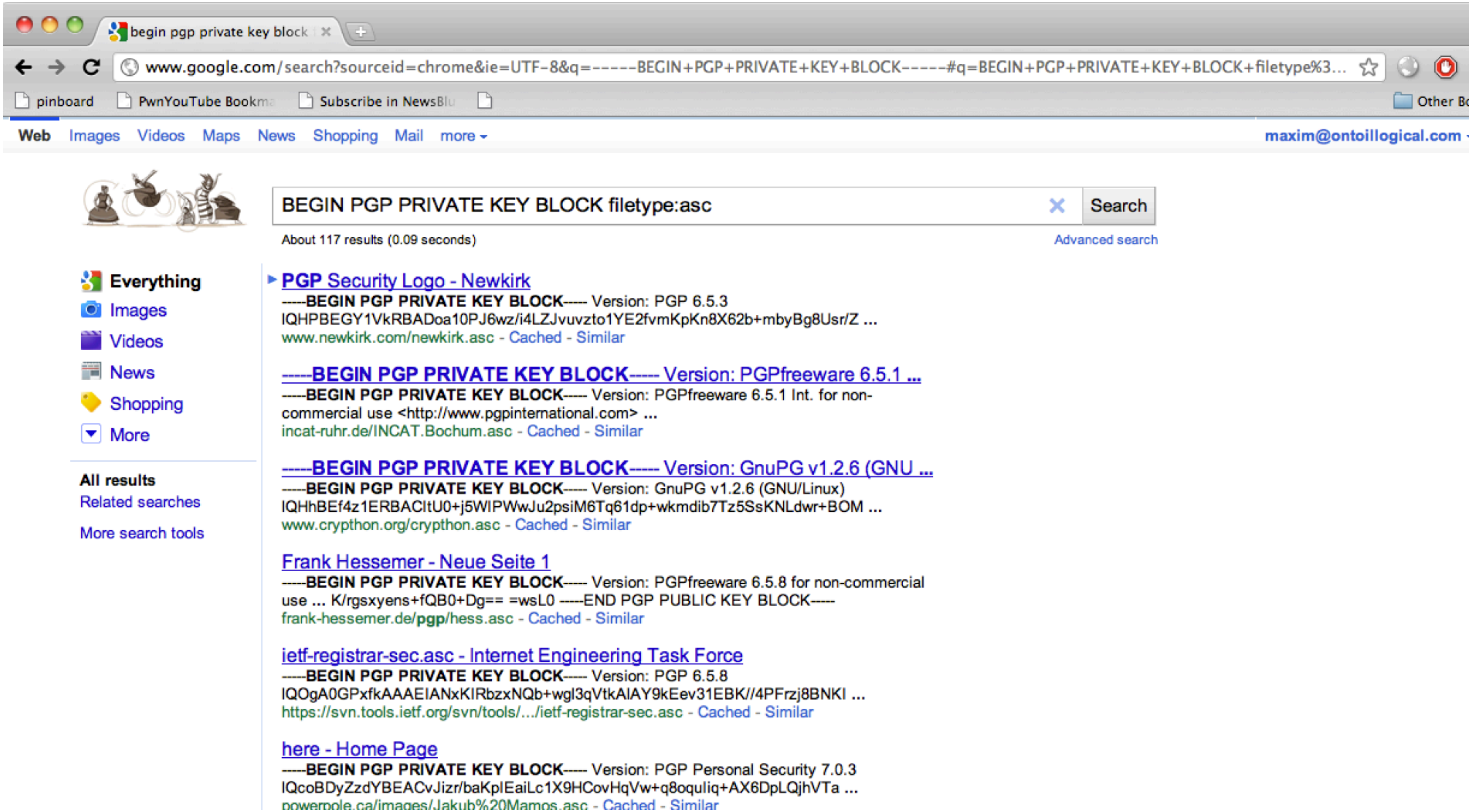
Did You Know...

Security is Important to Us!

Transfer confidential files to us securely. We [illegible]de encryption to keep your files [illegible] confidential. Ask us how we can establish a LIVE connection directly to your office. It is easy, fast, and secure!

Copyright © 2011 Honeypot Consulting Inc. All Rights Reserved. Terms and Conditions Privacy Policy Contact Us

Military grade encryption



www.google.com/search?sourceid=chrome&ie=UTF-8&q=-----BEGIN+PGP+PRIVATE+KEY+BLOCK-----#q=BEGIN+PGP+PRIVATE+KEY+BLOCK+filetype%3...

BEGIN PGP PRIVATE KEY BLOCK filetype:asc

About 117 results (0.09 seconds)

PGP Security Logo - Newkirk
-----**BEGIN PGP PRIVATE KEY BLOCK**----- Version: PGP 6.5.3
lQHPBEGY1VkRBADoa10PJ6wz/i4LZJvuvzto1YE2fvmKpKn8X62b+mbyBg8Usr/Z ...
www.newkirk.com/newkirk.asc - Cached - Similar

-----**BEGIN PGP PRIVATE KEY BLOCK**----- Version: PGPfreeware 6.5.1 ...
-----**BEGIN PGP PRIVATE KEY BLOCK**----- Version: PGPfreeware 6.5.1 Int. for non-commercial use <http://www.pgpinternational.com> ...
incat-ruhr.de/INCAT.Bochum.asc - Cached - Similar

-----**BEGIN PGP PRIVATE KEY BLOCK**----- Version: GnuPG v1.2.6 (GNU ...
-----**BEGIN PGP PRIVATE KEY BLOCK**----- Version: GnuPG v1.2.6 (GNU/Linux)
lQHhBEf4z1ERBACltU0+j5WlPWwJu2psiM6Tq61dp+wkmdib7Tz5SsKNLdwr+BOM ...
www.crypthon.org/crypthon.asc - Cached - Similar

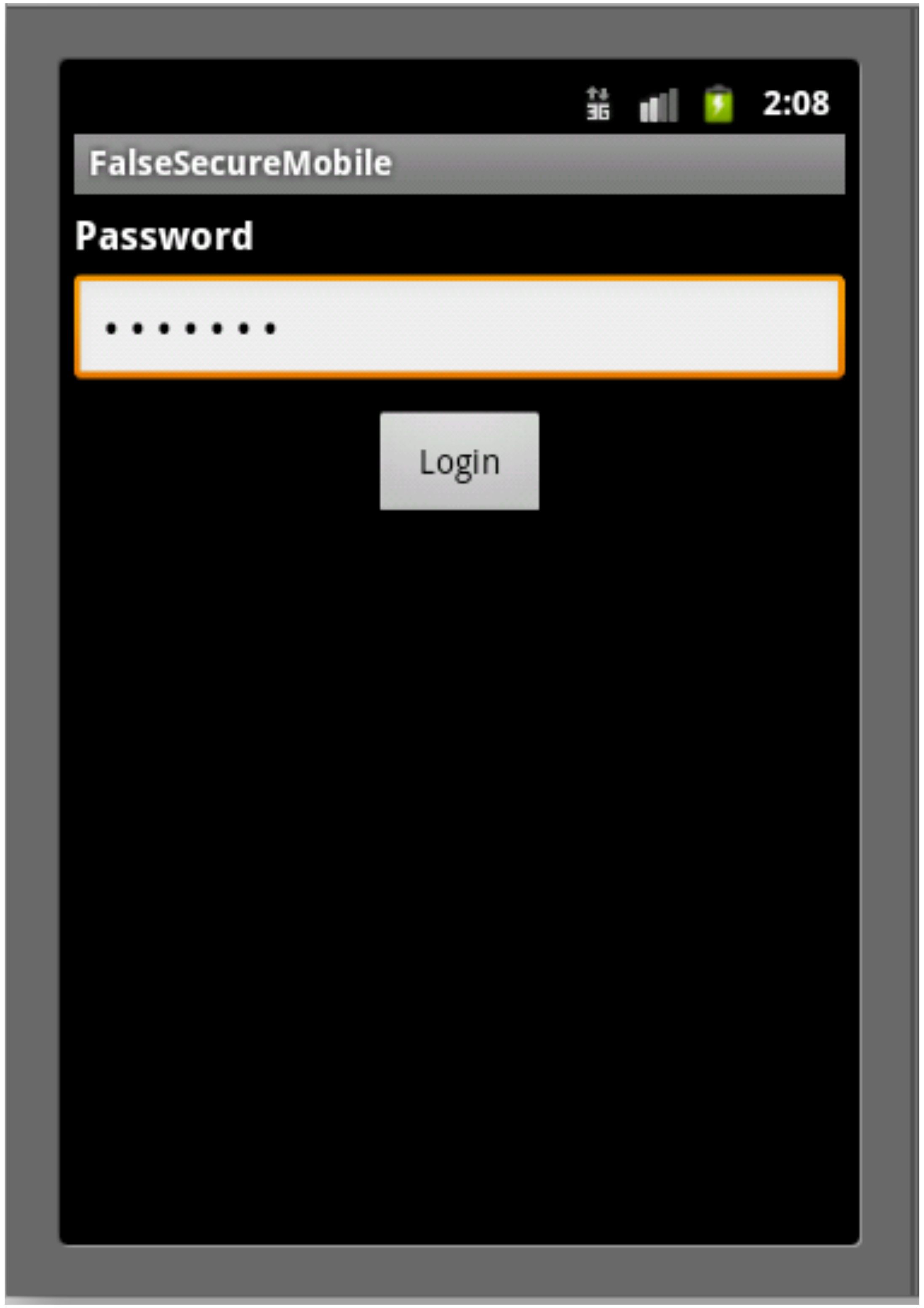
Frank Hessemer - Neue Seite 1
-----**BEGIN PGP PRIVATE KEY BLOCK**----- Version: PGPfreeware 6.5.8 for non-commercial use ... K/rgsxyens+fQB0+Dg== =wsL0 -----END PGP PUBLIC KEY BLOCK-----
frank-hessemer.de/**pgp**/hess.asc - Cached - Similar

ietf-registrar-sec.asc - Internet Engineering Task Force
-----**BEGIN PGP PRIVATE KEY BLOCK**----- Version: PGP 6.5.8
lQOgA0GPxfkAAAEIANxKIRbzxNQb+wgl3qVtkAIAY9kEev31EBK//4PFrzj8BNKI ...
https://svn.tools.ietf.org/svn/tools/.../ietf-registrar-sec.asc - Cached - Similar

here - Home Page
-----**BEGIN PGP PRIVATE KEY BLOCK**----- Version: PGP Personal Security 7.0.3
lQcoBDyZzdYBEACvJizr/baKplEaiLc1X9HCovHqVw+q8oquliq+AX6DpLQjhVTa ...
powerpole.ca/images/Jakub%20Mamos.asc - Cached - Similar

Military grade encryption

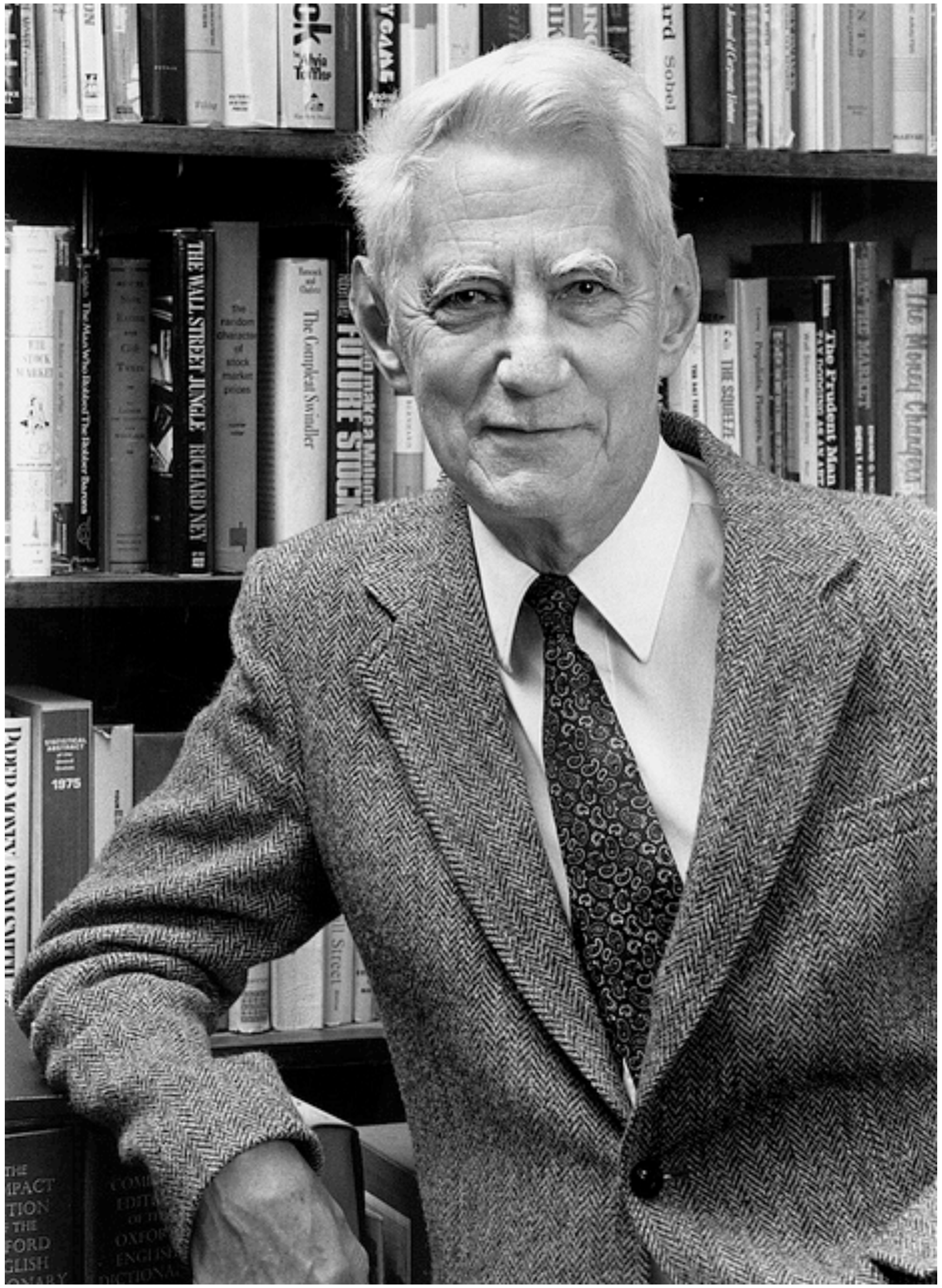
Where do you put keys?



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

https://www.owasp.org/index.php/OWASP_Mobile_Security_Project

Develop guidelines

Encrypting data at rest

Develop guidelines

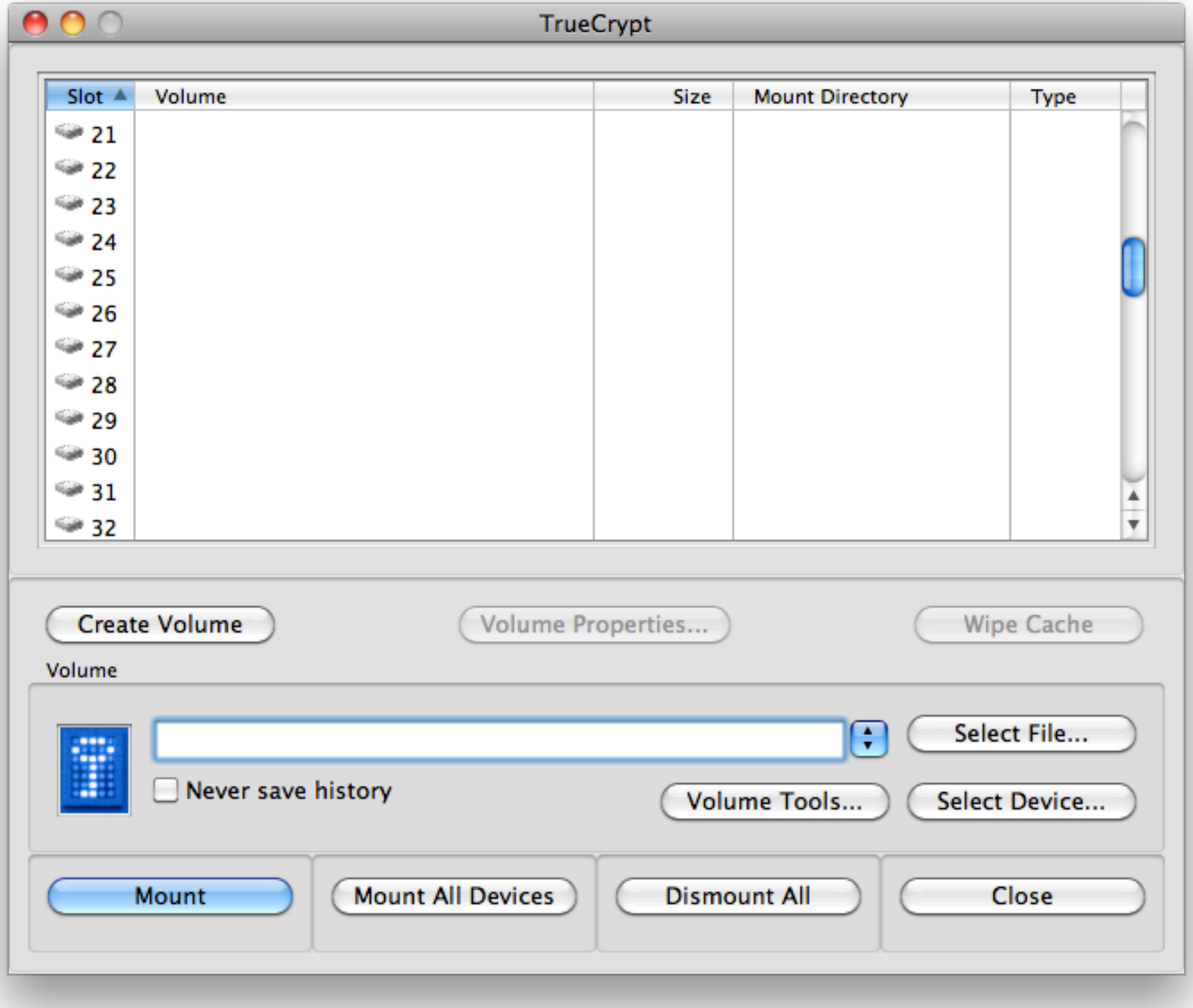
Defensive mobile coding

Develop guidelines

Mobile incident response

What can you do?

As a user



Slot	Volume	Size	Mount Directory	Type
21				
22				
23				
24				
25				
26				
27				
28				
29				
30				
31				
32				

□ Never save history

This is how we mitigate the risk of stolen laptops

Tell Android I sent you!

- http://code.google.com/p/android/issues/detail?id=10809
- 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/robnwatkins/397488557/
- http://www.flickr.com/photos/miiitch/4880022048/
- http://www.flickr.com/photos/moxiemarlinspike/4730390878/

Questions?

- max@securitycompass.com
- @mveytsman (I’m a sporadic twitter user, but trying to change)