Zero Knowledge Security

Martin McKeay

Senior Security Advocate
Akamai Technologies
@McKeay
You choose....
KEEP CALM AND CHANGE THE WORLD
Four Horsemen of the Privacy Apocalypse
US, British intelligence agencies tried hacking systems: SIM maker

February 26, 2015, 7:51 pm

Data and computer security

UK’s Drip law: cynical, misleading and an affront to democracy

Julia Powles

Schneier on Security

How the NSA Attacks Tor/Firefox Users With QUANTUM and FOXACID

← Friday Squid Blogging: Squid Exhibit at the Monterey Bay Aquarium
Silk Road Author Arrested Due to Bad Operational Security →
China Hacked RSA, U.S. Says

And RSA official responds to Gen. Keith Alexander's telling Congress this week that Chinese attackers were behind the SecurID breach last year.
Criminals
Corporations

If you’re not paying for the product, you are the product.
Definitions
Jargon we love to hate

Military-grade
NSA-proof
Bullet-proof
APT
Proprietary technology
PCI
A Zero-Knowledge Proof is a method by which one party can prove to another party that a statement is true, without conveying information apart from the fact that the statement is indeed true.
A method of encryption where the organization providing the encryption can store and manage the encrypted data without access to the encryption keys.
“A telecommunications carrier shall not be responsible for decrypting, or ensuring the government’s ability to decrypt, any communication encrypted by a subscriber or customer, unless the encryption was provided by the carrier and the carrier possesses the information necessary to decrypt the communication.”
Able to decrypt by design

- Mail
  - Gmail
  - MSN
  - Hotmail

- Online file services
  - Dropbox – Deduplication

- Phones
Feds can't seize emails stored in Ireland, Microsoft says
Cloud Storage

Vs.
Cell phones
Weak or insecure cryptography

A Crypto Nerd's Imagination:

His laptop's encrypted. Let's build a million-dollar cluster to crack it.

No good! It's 4096-bit RSA!

Blast! Our evil plan is foiled!

What Would Actually Happen:

His laptop's encrypted. Drug him and hit him with this $5 wrench until he tells us the password.

Got it.
Encrypted phones

- **IOS**
  - Key only stored on phone as of 8.0
  - 256-bit AES

- **Android**
  - `aes-cbc-essiv:SHA256` (In other words, 256-bit AES)
  - Older versions weakened by PIN strength
  - Backpedaled on encryption by default

- It doesn’t work if you don’t turn it on!
iOS Encryption
Android Encryption
Four Horsemen of the Privacy Apocalypse
Not just for your personal life

- More important for business!
- 5% of the data is worth 95% of the value
- Stopping the data from leaving is almost impossible, so make sure it’s as secure as possible while it’s out there
- Use your own keys
- Many products allow you to encrypt outside the application
- Read the fine print, don’t believe the marketing
- Ask for products that give you the power
Apply

- Review the technical documentation
- Understand where the keys are and who has access to them
- Request more control of keys from vendors
- Vote with your wallet (personally and as a corporation)
Martin McKeay
mmckeay@akamai.com
martin@mckeay.net
@twitter