RSAConference2015
San Francisco | April 20-24 | Moscone Center

SESSION ID: DSP-F01

Zero Knowledge Security

Martin McKeay

Senior Security Advocate
Akamai Technologies
@McKeay

You choose….

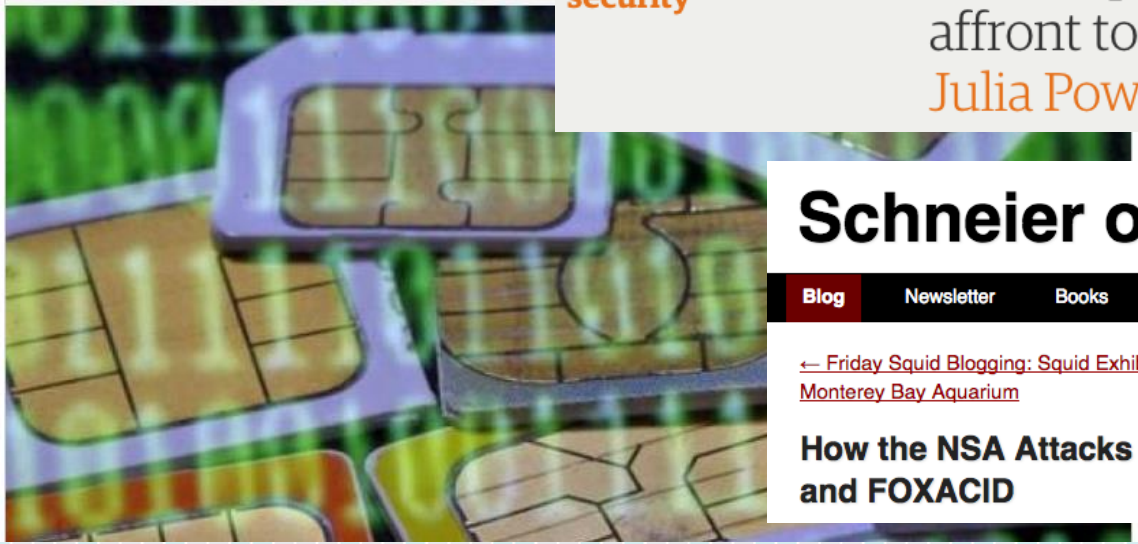

KEEP
CALM
AND
CHANGE THE
WORLD

Four Horsemen of the Privacy Apocalypse

My Government

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

Blog | Newsletter | Books | Essays | News | Schedule | Crypto | About Me

← Friday Squid Blogging: Squid Exhibit at the Monterey Bay Aquarium

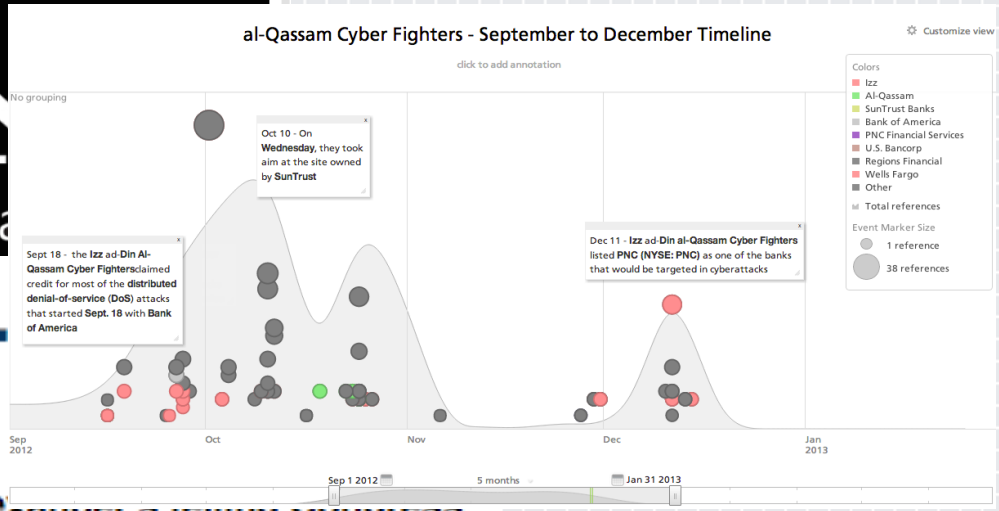
Silk Road Author Arrested Due to Bad Operational Security →

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

Their Government

Sony Hack: A Timeline

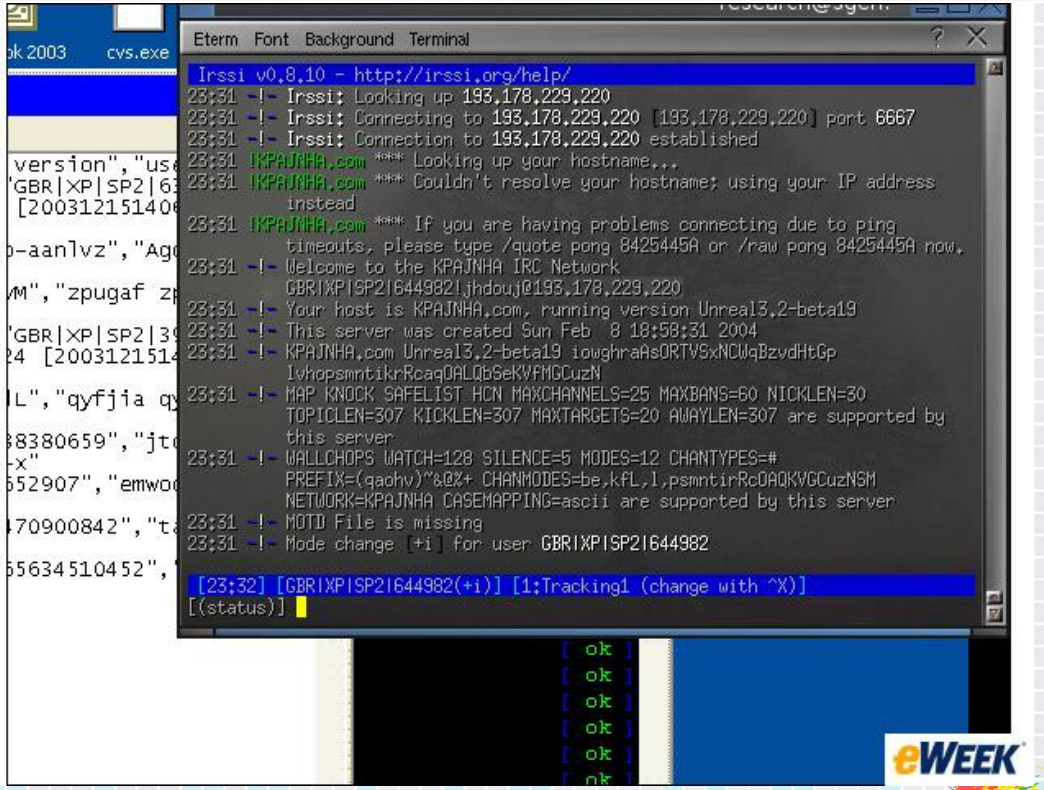
by David Robb
December 22, 2014 1:25pm



China Hacked RSA, U. Says

And RSA official responds to Gen. Keith Ale[illegible] this week that Chinese attackers were behind the SecurID breach last year

Criminals

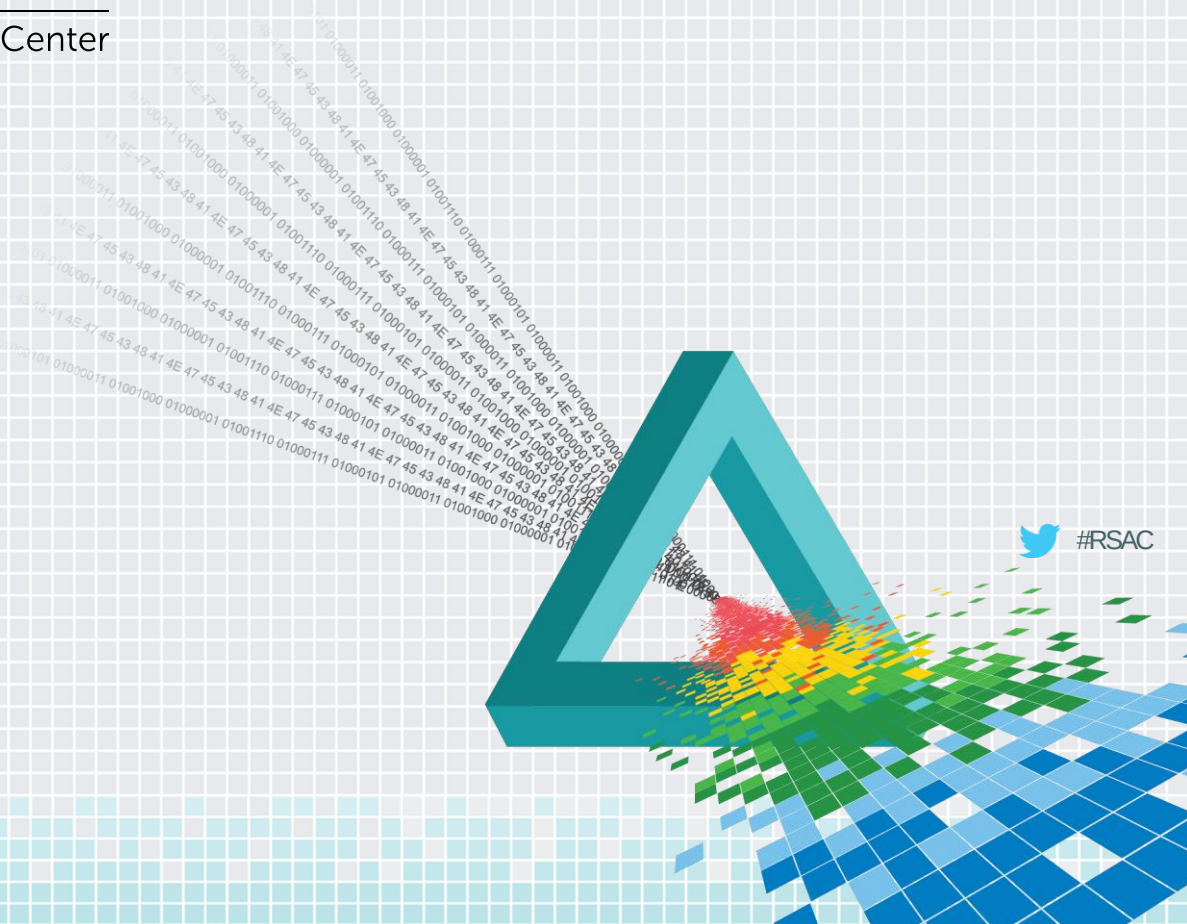

Eterm Font Background Terminal
Irssi v0.8.10 - http://irssi.org/help/
23:31 -!- Irssi: Looking up 193.178.229.220
23:31 -!- Irssi: Connecting to 193.178.229.220 [193.178.229.220] port 6667
23:31 -!- Irssi: Connection to 193.178.229.220 established
23:31 !KPAJNHA.com *** Looking up your hostname...
23:31 !KPAJNHA.com *** Couldn't resolve your hostname; using your IP address instead
23:31 !KPAJNHA.com *** If you are having problems connecting due to ping timeouts, please type /quote pong 8425445A or /raw pong 8425445A now.
23:31 -!- Welcome to the KPAJNHA IRC Network GBR|XP|SP2|644982!jhdouj@193.178.229.220
23:31 -!- Your host is KPAJNHA.com, running version Unreal3.2-beta19
23:31 -!- This server was created Sun Feb 8 18:58:31 2004
23:31 -!- KPAJNHA.com Unreal3.2-beta19 iowghraAsORTVSxNCWqBzvdHtGp lvhopsmntikrRcaqOALQbSeKVfMGCuzN
23:31 -!- MAP KNOCK SAFELIST HCN MAXCHANNELS=25 MAXBANS=60 NICKLEN=30 TOPICLEN=307 KICKLEN=307 MAXTARGETS=20 AWAYLEN=307 are supported by this server
23:31 -!- WALLCHOPS WATCH=128 SILENCE=5 MODES=12 CHANTYPES=# PREFIX=(qaohv)~&@%+ CHANMODES=be,kfL,l,psmntirRcOAQKVGCuzNSM NETWORK=KPAJNHA CASEMAPPING=ascii are supported by this server
23:31 -!- MOTD File is missing
23:31 -!- Mode change [+i] for user GBR|XP|SP2|644982
[23:32] [GBR|XP|SP2|644982(+i)] [1:Tracking1 (change with ^X)]
[(status)]
cvs.exe
[ok]
eWEEK

Corporations

If you're not paying for the product,

you are the product.

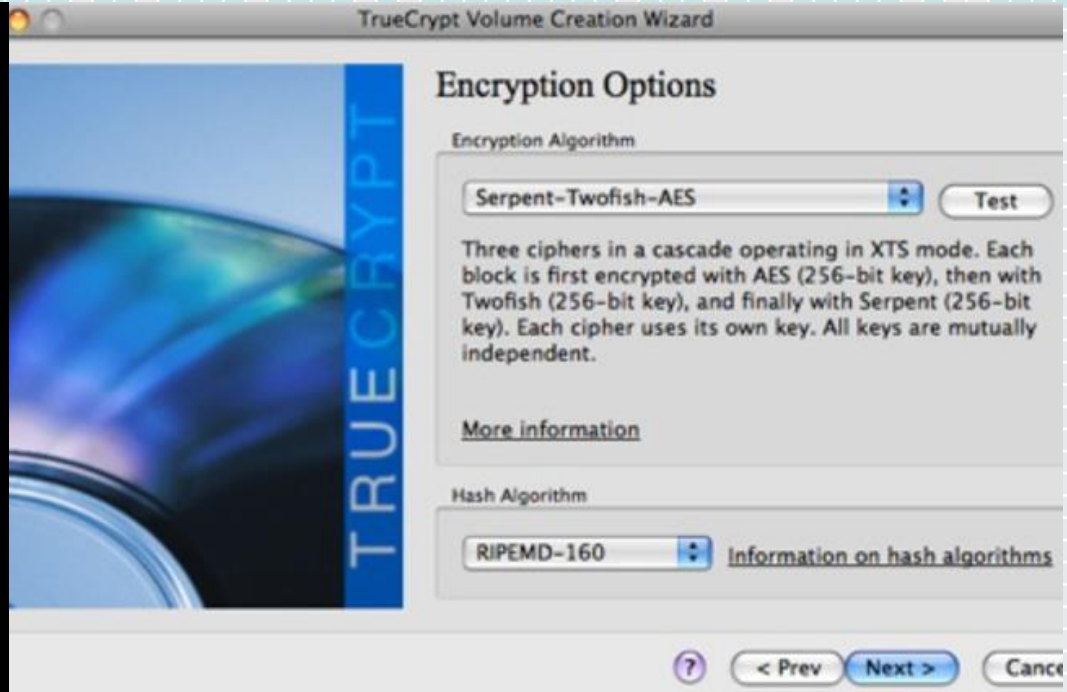
Definitions



We use military-grade encryption. This just speaks to the need to safeguard one's password with as much care as possible.

Vincent Sollitto

QUOTEHD.COM



Jargon we love to hate

Military-grade
NSA-proof

Bullet-proof
APT

Proprietary technology
PCI

Zero Knowledge Proof

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.

Zero Knowledge Encryption

A method of encryption where the organization providing the encryption can store and manage the encrypted data without access to the encryption keys.

CALEA

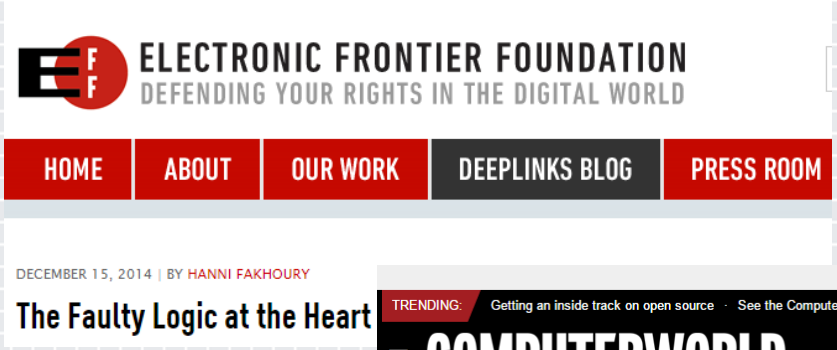
47 US Code 1002(a)(3)

"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."

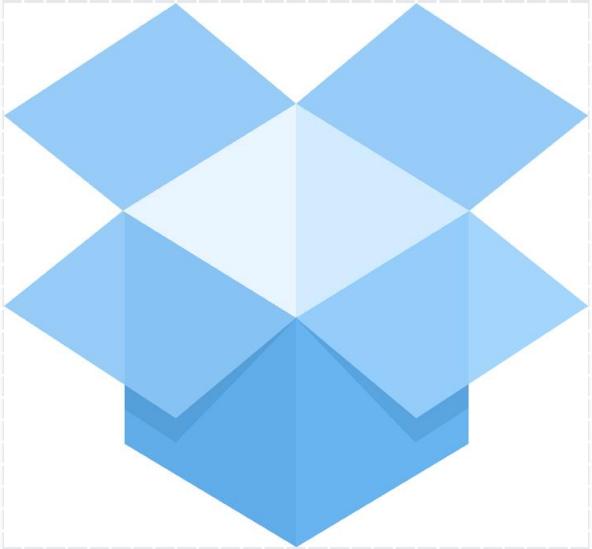
Able to decrypt by design

- Mail
  - Gmail
  - MSN
  - Hotmail
- Online file services
  - Dropbox – Deduplication
- Phones

Online Mail Services



Cloud Storage



Vs.

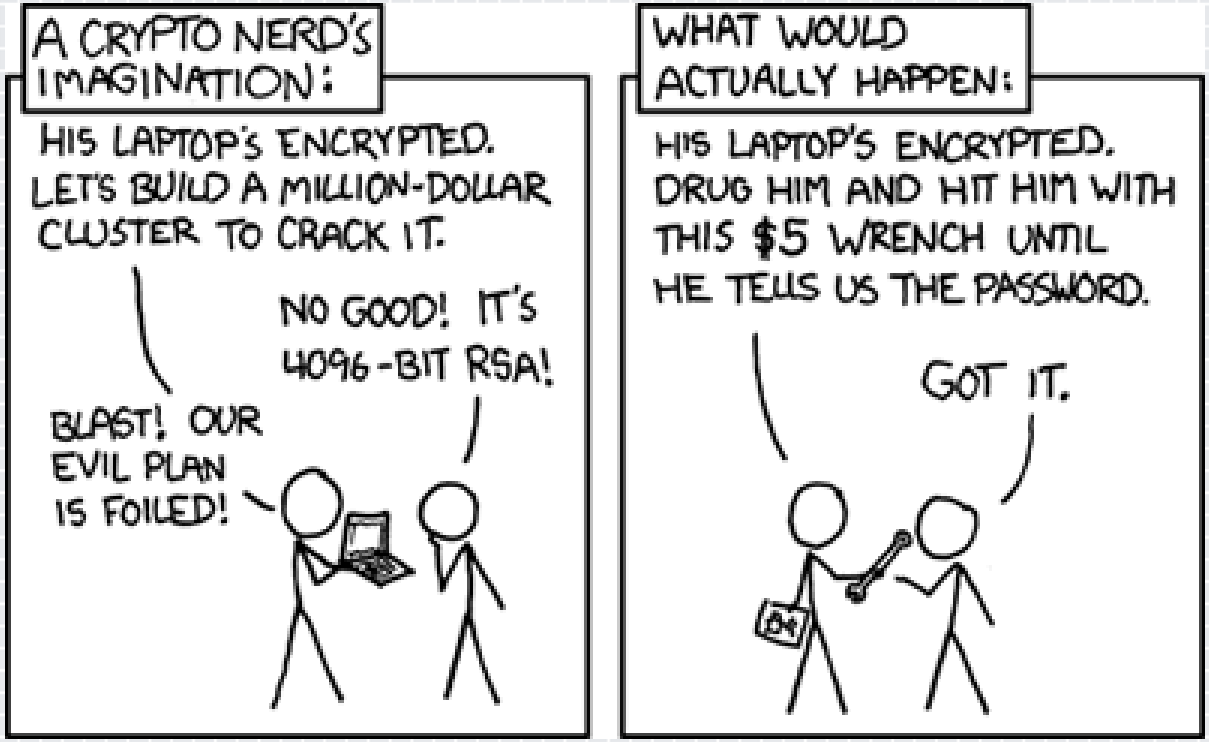
Cell phones


SONY
13:03
WALKMAN
Album
Movies
PSM


gemalto
Digital Money
Smart Cities
gemalto


StingRay II
INTERNAL CONTROLLER
CNTRL1
CNTRL2
AUX1
AUX2
AUX
DC INPUT
USB
POWER

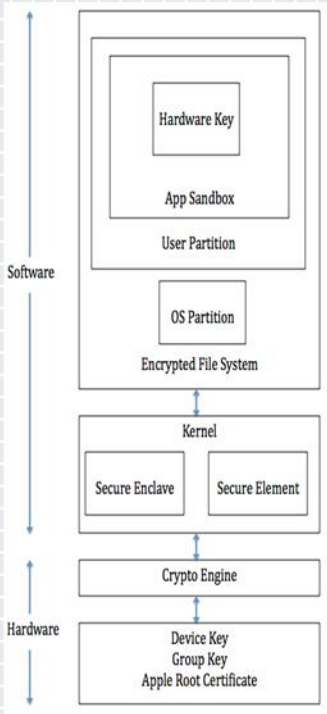
Weak or insecure cryptography



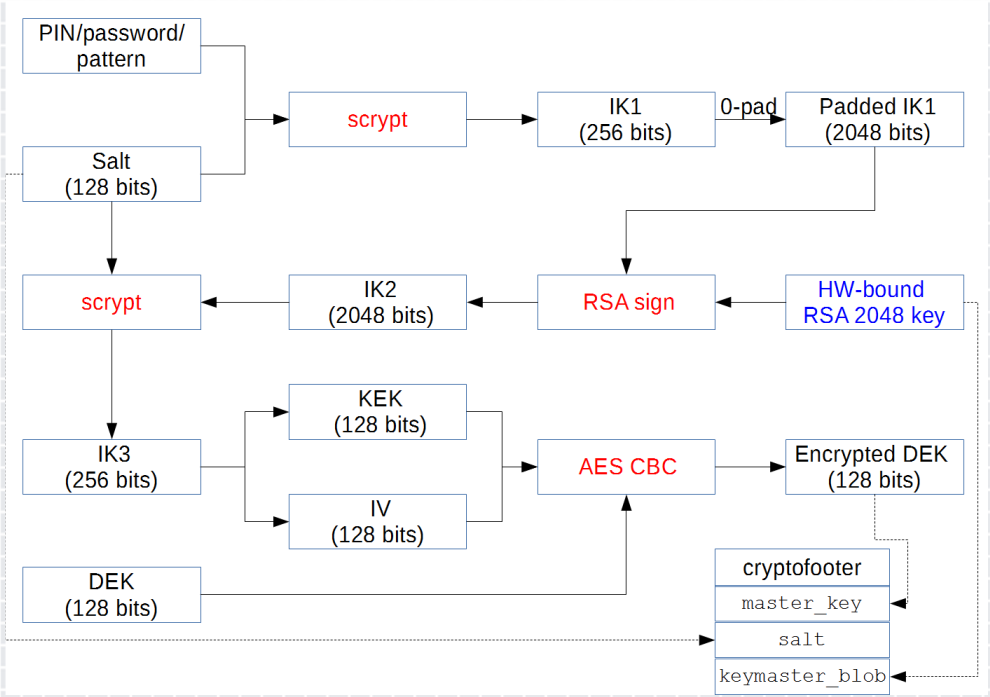
Encrypted phones

- 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)

RSAConference2015

San Francisco | April 20-24 | Moscone Center

Martin McKeay
mmckeay@akamai.com
martin@mckeay.net
@twitter