Security Now! #525 - 09-15-15

Disconnect

This week on Security Now!

- My Mea Culpa regarding glass being a fluid (it's not!)
- Has LastPass been hacked?
- Matthew Green looks again at iMessage's assurances
- What's a "Canary Token"?
- Let's Encrypt issues first certificate
- Miscellaneous tidbits, including my thoughts about Apple's September announcements.
- A discussion with Patrick Johnson, co-founder and CTO of "Disconnect"

Errata:

Glass is not a fluid!

- "Crown glass process"
  - A lump of molten glass was rolled, blown, expanded, flattened,
  - Then spun into a disc and cut into panes.
  - The centrifugal force of spinning created a sheet that grew in thickness toward the outer edge.
  - So, when the glass was cut into panes, they were not perfectly flat.
  - And, when mounted, the heavier edge was naturally placed at the bottom.
- And... if I had stopped to consider it:
  - A "fluid" would make a HORRIBLE disc platter!!!
- Links:
  - http://math.ucr.edu/home/baez/physics/General/Glass/glass.html
  - The 'glass is a liquid' myth has finally been destroyed
  - http://io9.com/the-glass-is-a-liquid-myth-has-finally-been-destroyed-496190894
  - http://dwb.unl.edu/Teacher/NSF/C01/C01Links/www.ualberta.ca/~bderksen/florin.html
  - http://www.abc.net.au/science/k2/homework/s95602.htm

Security News:

LastPass Hacked?

- Forthcoming Blackhat Europe in The Netherlands, November 12-13
- Briefings: Even the LastPass Will be Stolen Deal with It!
- Presentation by Alberto Garcia & Martin Vigo
- https://www.blackhat.com/eu-15/briefings.html#even-the-lastpass-will-be-stolen-deal-with-it
- http://www.martinvigo.com/a-look-into-lastpass/
- Simply do not use the "Remember Password" feature.

Matthew Green on iMessage's Security and Encryption:

- <quote> How does iMessage work?

  Fundamentally the mantra of iMessage is "keep it simple, stupid". It's not really designed to be an encryption system as much as it is a text message system that happens to include encryption. As such, it's designed to take away most of the painful bits you expect from modern encryption software, and in the process it makes the crypto essentially invisible to the user. Unfortunately, this simplicity comes at some cost to security.

  Let's start with the good: Apple's marketing material makes it clear that iMessage encryption is "end-to-end" and that decryption keys never leave the device. This claim is bolstered by their public security documentation as well as outside efforts to reverse-engineer the system. In iMessage, messages are encrypted with a combination of 1280-bit RSA public key encryption and 128-bit AES, and signed with ECDSA under a 256-bit NIST curve. It's honestly kind of ridiculous, but whatever. Let's call it good enough.

  iMessage encryption in a nutshell boils down to this: I get your public key, you get my public key, I can send you messages encrypted to you, and you can be sure that they're authentic and really came from me. Everyone's happy.

  But here's the wrinkle: where do those public keys come from?

- In any modern cryptographic system we know that the KEYS *provide* the security. So it’s just this simple: If you delegate responsibility for the Keys, you delegate responsibility for the security.

- More:
  - Multiple devices means many more keys, too.
  - Apple sends a notice upon adding a device, but must they?
  - Assuming the system currently has no provision for secretly adding keys, adding that would be troublesome.
  - Apple's proprietary encryption protocols are a tangled mess, but they COULD be reverse engineered and detection of key tampering COULD be detected by a sufficiently sophisticated and motivated organization.

  - Of the inherent tension between Apple and Law Enforcement:
    - "In the long term, law enforcement continues to ask for an approach that allows them to access the plaintext of encrypted messages. And Silicon Valley continues to find new ways to protect the confidentiality of their user's data, against a range of threats beginning in Washington and proceeding well beyond.

      How this will pan out is anyone's guess. All we can say is that it will be messy."

Canary Tokens

- http://canarytokens.org/generate
  - "Don't learn of your breach from CNN.
  - A fully functioning Honeypot in under 5 minutes.
- http://blog.thinkst.com/p/canarytokensorg-quick-free-detection.html
- If it's impossible to keep people out at least we may be able to quickly detect when a breach has occurred.
- Plant your own web bug and detect when someone opens an unread eMail.
- "Map bugs" -- back in the 30's, made-up towns to prove map forgery in courts.

Let's Encrypt Schedule Update:

- https://letsencrypt.org/2015/08/07/updated-lets-encrypt-launch-schedule.html
- Everything is on track and running according to plan
- Staged roll out to be sure they get it right:
  - First certificates were issued last week (Sept 7th)
  - Full general availability: week of November 16th, 2015.
- Blog posting yesterday: "Our First Certificate Is Now Live"
  - https://letsencrypt.org/2015/09/14/our-first-cert.html
  - http://helloworld.letsencrypt.org/
    - Installed the ISRG Root Certificate (PEM) format
    - Installed both Intermediate Authority certs
- Reminder:
  - Automated issuance of DV - Domain Validation certs.
  - Not OV or EV... but DV.

Miscellany:

- Jon Schiefer's 90-minute "Algorithm" movie has 1,632,899 -> 1,641,437 (>8500)
  - https://www.youtube.com/watch?v=6qpudAhYhpc

- Apple's September Update:
  - iPhone: It sure does look pink!
    - I don't think I'm jumping on the new phone every year bandwagon.
  - iPad: It sure does look BIG!
    - I would love to have a stylus, but it's just too big for the portability I use.

- Soylent v2.0…
  - (Just be sure you treat it only as a snack!)

SpinRite:

- Jim Howard (@ShazzikinZ) 09/09/2015 @ 1:13pm
- Spinrite just saved the day again- I paid my dues today, and it saved data off of a volume that a whole team of Admins had given up on. Thanks for making me look like a rockstar!

Disconnect:

- Today's show guest: Patrick Jackson, co-founder & CTO of Disconnect
- https://disconnect.me/