Security Now! #435 - 12-18-13

Q&A #180 Show Notes

Today on Security Now!

- All things NSA -- A big week for the Puzzle Palace
- The US Constitution, 60 Minutes, Obama, Silicon Valley and who is Edward Snowden?
- Acoustic Crypto Key Leakage
- What does the FIDO Alliance mean for SQRL?
- A few Sci-Fi tid bits
- 10 interesting Questions & Answers from our listeners.

Security News:

"The NSA is coming to town!"

- https://www.youtube.com/watch?v=8pcWlyUu8U4

The NSA on Sunday's 60 Minutes:

- Tweeted by the EFF: "We planned to write a takedown of @60Minutes' NSA puff piece yesterday, but then the DC District Court did it for us eff.org/r.fudf"
- Interesting that for an issue of THIS MASSIVE import... none of the senior 60 minutes staff handled the story. Instead it was some random guy we've never seen before. Huh.
- Most annoying for me was the flat out lies being told and unchallenged.
- It really was a "CBS rollover puff piece."

A Federal judge rules the mass collection of telephone metadata unconstitutional

- http://www.cnn.com/2013/12/16/justice/nsa-surveillance-court-ruling/

Obama met with Fifteen Tech Execs yesterday (Tues)

- Tim Cook of Apple and Eric Schmidt of Google, as well as executives from Twitter, Microsoft, Facebook, Salesforce, Netflix , Etsy, Dropbox, Yahoo!, Zynga, Sherpa Global, Comcast, LinkedIn and AT&T.
- Made it VERY CLEAR that the NSA spying revelations were damaging their bussinesses:
- http://www.washingtonpost.com/business/technology/2013/12/17/6569b226-6734-11e3-a0b9-249bbb34602c_story.html
- Washington Post: <quote> Their message was to say: "What the hell are you doing? Are you really hacking into the infrastructure of American companies overseas? The same American companies that cooperate with your lawful orders and spend a lot of money to comply with them to facilitate your intelligence collection?" said one industry official familiar with the companies' views.
- One thing to note, however... most of these companies live by tracking and profiling their users. It's literally their published business model.
    - Eric Schmidt: "We know where you are. We know where you've been. We can more or less know what you're thinking about. Your digital identity will live forever… because there's no delete button."
    - The difference is, I think, disclosure and power…. **Aureate**

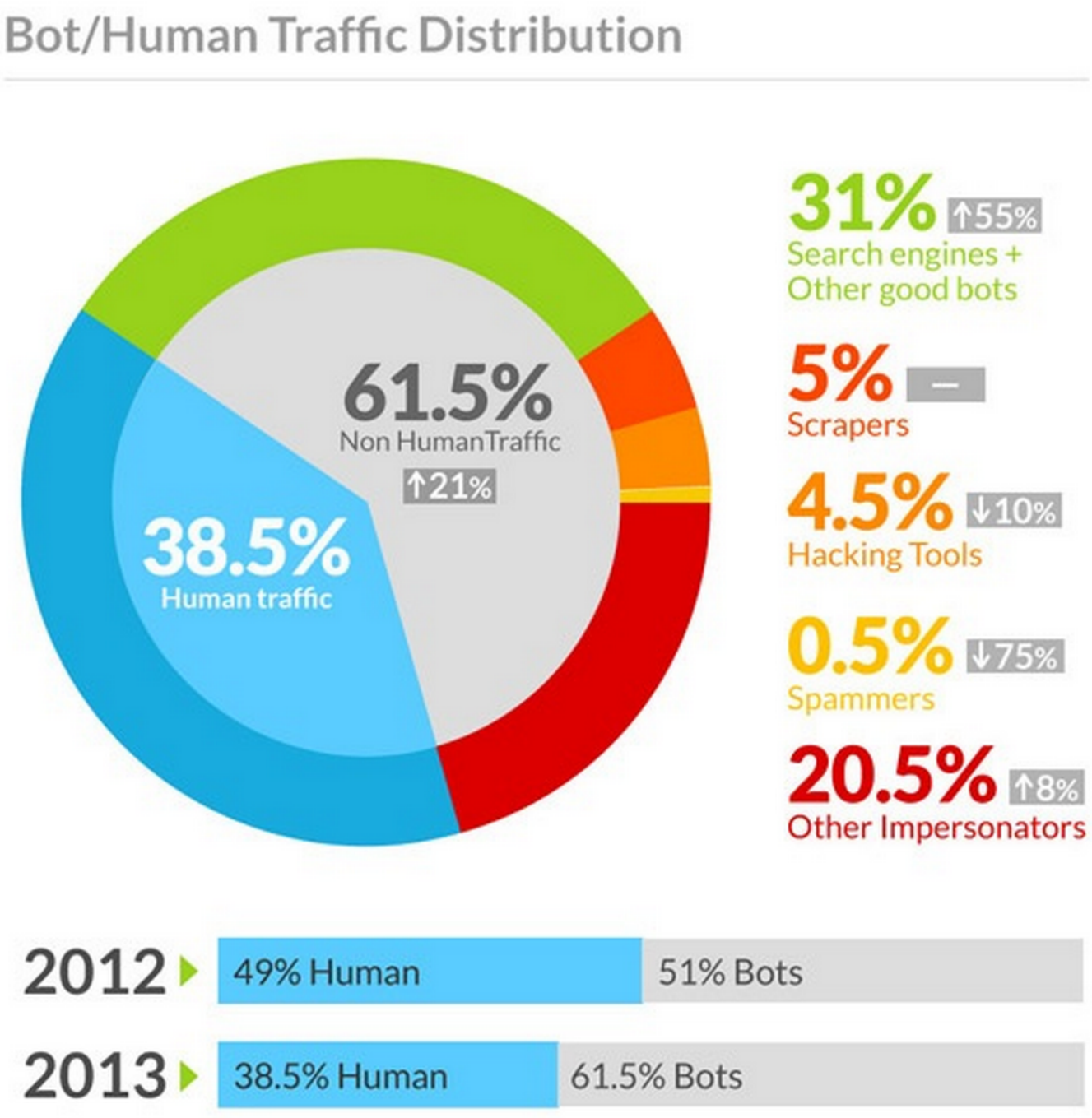
White House working group recommends taking the data out of NSAs hands.

Who is (was) Edward Snowden really?

- A high school dropout who cheated on tests to get an NSA job and betray his oath and his country? ... (so the NSA wants us to believe) ... or:
- http://www.forbes.com/sites/andygreenberg/2013/12/16/an-nsa-coworker-remembers-the-real-edward-snowden-a-genius-among-geniuses/
- Headline: "An NSA Coworker Remembers The Real Edward Snowden: 'A Genius Among Geniuses'"

The Bots are Winning!

- http://knowmore.washingtonpost.com/2013/12/12/bots-outnumber-humans-on-the-internet/



Google Mail begins proxying images:

- Gmail turned on images.
- Transcoding is the key!
- Benefits:
    - Senders cannot use image loading to get information like your IP address or location.
    - Senders cannot set or read cookies in your browser.
    - Gmail checks your images for known viruses or malware.
- (But… senders may be able to know whether an individual has opened a message with unique image links.)

Acoustic side-channel attack on 4096-bit GnuPG keys:

- http://www.cs.tau.ac.il/~tromer/acoustic/#
- "RSA Key Extraction via Low-Bandwidth Acoustic Cryptanalysis"
- Similar to listening to someone type can reveal what they type.
- <quote> Synopsis: Many computers emit a high-pitched noise during operation, due to vibration in some of their electronic components. These acoustic emanations are more than a nuisance: they can convey information about the software running on the computer, and in particular leak sensitive information about security-related computations. In a preliminary presentation, we have shown that different RSA keys induce different sound patterns, but it was not clear how to extract individual key bits. The main problem was that the acoustic side channel has a very low bandwidth (under 20 kHz using common microphones, and a few hundred kHz using ultrasound microphones), many orders of magnitude below the GHz-scale clock rates of the attacked computers.

  Here, we describe a new acoustic cryptanalysis key extraction attack, applicable to GnuPG's current implementation of RSA. The attack can extract full 4096-bit RSA decryption keys from laptop computers (of various models), within an hour, using the sound generated by the computer during the decryption of some chosen ciphertexts. We experimentally demonstrate that such attacks can be carried out, using either a plain mobile phone placed next to the computer, or a more sensitive microphone placed 4 meters away.

  Beyond acoustics, we demonstrate that a similar low-bandwidth attack can be performed by measuring the electric potential of a computer chassis. A suitably-equipped attacker need merely touch the target computer with his bare hand, or get the required leakage information from the ground wires at the remote end of VGA, USB or Ethernet cables.
- In the "olden days" we put an AM radio on minicomputers to play Christmas music. The core memory generated radio frequencies.
- Full version of the paper: http://www.tau.ac.il/~tromer/papers/acoustic-20131218.pdf

SQRL vs FIDO

- Microsoft joins the FIDO alliance
- http://nakedsecurity.sophos.com/2013/12/16/microsoft-joins-tech-giants-and-fido-in-the-fight-for-simpler-safer-authentication/
- http://fidoalliance.org/members.html
- UAF (Universal Auth Framework) or U2F (Universal Second Factor)
- https://sites.google.com/site/oauthgoog/gnubby

- Concerns:
    - Hardware token based, so never free.
    - Per-site storage in the device, or a kludge to hand off to server.
    - No handling of key lifetime management
    - Appears to be MASSIVELY over designed.
    - Still a second factor.
    - Entrenched Biases:
        - Google wants multi-factor in browser
        - Yubico wants hardware token.
        - Everyone has their territory to protect.
    - $25,000/year "dues" to have any access to what's going on.

- SQRL *feels* more like the Internet -- clean, simple, lightweight, open and free.
    - No per-site storage to copy between devices.
    - 100% free.
    - Extremely lightweight

- I think there's room for SQRL even if FIDO happens.
    - SQRL is SO LOW FRICTION that it can be easily used.

Elaine's experience in California:

- <quote> I'm too sleepy to go into detail right now, but you might want to relax a wee bit about the healthcare thing. I got it, it's painless, they ask for less information than any utility company, and the website's just to allow you to compare plans available in your area. You pick one, they send your name and address to the insurance company who sends you an invoice for the first month's premium, and that's it. You're done with the website, and you don't have to give a credit card number or any medical information. I'm tickled pink because I haven't had insurance for nearly 20 years and I'm about to need eye surgery. Your major disastrous catastrophe is my godsend. :)

- I asked Elaine if she would mind my sharing her real-world experience with our podcast audience…

- <quote> I don't mind at all. I just tried to tell my farrier I got health insurance (he got dropped last year and has two people with heart conditions in his family), and he just went nuts on me a la Fox News. So any little bit of truth and balance is a good thing.

  It's not spectacular news, like the woman who got a family policy for $3.16 or the person who got billed 13 cents, but it feels very solid and real to me. I'm getting a $580/mo policy for $170/mo, with reasonable deductibles.

  Actually, now I'm thinking it would be GREAT if you mentioned it. I'm sure lots of geeks like me have small incomes and/or have suffered catastrophe. Remember the listener from New Orleans who wrote after Katrina? You've got listeners in New England who suffered through Sandy. There must have been listeners in Colorado who lost big-time in last summer's flood. Not every working mother is the CEO of Yahoo!, and the recession still exists for lots of us. Healthcare is a definite bright spot.

Along those same lines, you can buy refurbished computers at cedarpc.com for $200-300, desktops or laptops. You could do a little "in case you've been struck by disaster" segment.

A True Hardware Random Number Generator

- http://www.jtxp.org/tech/xr232usb_en.htm
- http://www.robertnz.net/hwrng.htm
- http://www.robertnz.net/pdf/xor2.pdf
- http://www.robertnz.net/true_rng.html
- http://www.comscire.com/

Miscellany:

GRC's Windows Server 2008/R2 SSL/TLS Cipher Suite Order:
http://www.GRC.com/miscfiles/SChannel_Cipher_Suites.txt

Sci-Fi:

- Honor Harrington:
- Baen Books offers all of the books for download. There's even a CD .ISO image containing everything. But their site is somewhat bizarre, the the reading order is unclear clear, so:
    - https://www.GRC.com/miscfiles/Honor_Harrington_Kindle_mobi.zip
    - https://www.GRC.com/miscfiles/Honor_Harrington_iTunes_ePub.zip
    - http://bit.ly/HHkindle
    - http://bit.ly/HHitunes

- CBS's "Intelligence" series premieres January 7th
    - https://www.youtube.com/watch?v=wMayn0vdCpM

SpinRite: Dale Francisco in Fresno, California