Security Now! #479 - 10-28-14

Q&A #199

Link Tracking Warning!
This document was first authored in Google Docs, then Downloaded as a PDF. So, Google has thoughtfully (ha!) added "tracking" redirections to all of the links here. (I have no idea why, but that's Google.) If that bothers you, simply copy the text of the link into your browser's URL field.

This week on Security Now!

- Apple Pay -- versus -- CurrentC
- Verizon (and AT&T) inserting sticky cookie
- RC4 gets a wonderful upgrade tweak!
- Terrific feedback from our great listeners.

Security News:

ApplePay versus CurrentC (MCX)

- http://www.mcx.com/

Verizon (and AT&T) caught inserting persistent, unblockable, tracking cookies

- http://www.wired.com/2014/10/verizons-perma-cookie/
- Verizon: "PrecisionID" technology.
- Simple testing site: http://lessonslearned.org/sniff
- When I disabled WiFi on my Verizon iPhone and my AT&T iPad... BOTH revealed persistent tracking tags.
    - Browser/agent: Mozilla/5.0 (iPhone; CPU iPhone OS 8_1 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12B411 Safari/600.1.4
    - Do Not Track: Enabled
    - Broadcast UID: [X-UIDH] Mzc5njg5MTIyAIv58QyiYlDSpWAfsJwliNwHRR3WSuXvksX7lwFVB+Pd
    - IP address: 70.209.198.226
- Jonathan Mayer (Stanford U)
- http://webpolicy.org/2014/10/24/how-verizons-advertising-header-works/
- What:
    - Opaque token broadcast to every website.
    - Receiving sites or advertisers -- anyone receiving a web browser query -- can submit the special Verizon, with payment, and receive paid user profile information.
    - But... Opting out does not eliminate the cookie, only rescinds information disclosure permission.
    - Anecdotal reports are that the Verizon super-cookie value changes weekly, but it's definitely static in the short term.

    - Note that since this is tied to the user account, this can be used to bridge across other cookie deletion to keep a lock on an individual... even without Verizon.

"Spritz"... a welcome update to RC4: (and thanks to Simon Zerafa for the tweet!)

https://www.schneier.com/blog/archives/2014/10/spritz_a_new_rc.html
http://people.csail.mit.edu/rivest/pubs/RS14.pdf
Bruce Writes:
Last week, Ron Rivest gave a talk at MIT about Spritz, a new stream cipher by him and Jacob Schuldt. It's basically a redesign of RC4, given current cryptographic tools and knowledge.

RC4 is an example of what I think of as a too-good-to-be-true cipher. It looks so simple. It is so simple. In classic cryptographic terms, it's a single rotor machine. It's a single self-modifying rotor, but it modifies itself very slowly. Even so, it's very hard to cryptanalyze. Even though the single rotor leaks information about its internal state with every output byte, its self-modifying structure always seems to stay ahead of analysis. But RC4 been around for over 25 years, and the best attacks are at the edge of practicality. When I talk about what sorts of secret cryptographic advances the NSA might have, a practical RC4 attack is one of the possibilities.

Spritz is Rivest and Schuldt's redesign of RC4. It retains all of the problems that RC4 had. It's built on a 256-element array of bytes, making it less than ideal for modern 32-bit and 64-bit CPUs. It's not very fast. (It's 50% slower than RC4, which was already much slower than algorithms like AES and Threefish.) It has a long key setup. But it's a very clever design.

Here are the cores of RC4 and Spritz:

```
RC4:

1: i = i + 1
2: j = j + S[i]
3: SWAP(S[i];S[j])
4: z = S[S[i] + S[j]]
5: Return z

Spritz:

1: i = i + w
2: j = k + S[j + S[i]]
2a: k = i + k + S[j]
3: SWAP(S[i];S[j])
4: z = S[j + S[i + S[z + k]]]
5: Return z
```

That's the core. There are also functions for turning the key into the initial array permutation, using this as a stream cipher, using it as a hash function, and so on. It's basically a sponge function, so it has a lot of applications.

What's really interesting here is the way Rivest and Schuldt chose their various functions. They basically tried them all (given some constraints), and chose the ones with the best security properties. This is the sort of thing that can only be done with massive computing power.

I have always really liked RC4, and am happy to see a 21st-century redesign. I don't know what kind of use it'll get with its 8-bit word size, but surely there's a niche for it somewhere.

Miscellany:

- iPad Air 2
- (I moved the AT&T SIM from my existing iPad Air.)

SpinRite:

Steve Ellison in Bradford, Pennsylvania...
Subject: "Spinrited", neologisms abound

Steve, Long time listener here. In listening to the discussions about the new term "SpinRited" I wanted to put forth our tech groups take on the term, et. al.

Working as a Technical Analyst at a regional campus of a large US university, when we get a spare moment we like to pontificate on such topics as, "What should a drive that has successfully passed SpinRite be called?", "What should a drive that has been fixed by SpinRite be called?", and "What should a drive that fails, even after the magic of SpinRite, be called?".

So, we propose that a drive that has been through a SpinRite operation, with nothing bad found, should be referred to as having been Spun.

Penultimately, a drive that is fixed by a SpinRite operation should be referred to as having been SpinRighted.

Last, but in no way the least, a drive that fails even after SpinRite, should be referred to as being SpinRotten.

Just our (mine, my brother (whom I work with)), and our work-study students' two cents on some neologisms that should be added to the jargon of the tech mainstream.