Security Now! #517 - 07-21-15

Q&A #216

During Leo's Trip:

- Steve loses his T1's after many years
- The official SQRL Logo (see below)
- The Crypto Gurus author a damning indictment of "Exceptional Access"

This week on Security Now!

- Auto hacking matures from "connect" to "Internet"
- Microsoft's emergency out-of-cycle update.
- Progress in attacking RC4.
- Miscellaneous tidbits
- And... 10 Q&A

SQRL's Official Logo & Icon

https://www.grc.com/sqrl/logo.htm

Security News

With Chrysler... "Uconnect"... and so do hackers!

- Charlie Miller and Chris Valasek
  - In 2013 they needed physical access.
  - In 2015... it's across the Internet.

- DefCon / BlackHat security conference, August.

- Last Thursday Jeep/Chrysler offered a "Uconnect" patch
  - http://www.driveuconnect.com/software-update/
  - Must be manually implemented via a USB stick or by a dealership mechanic.

- Wired: "Hackers Remotely Kill a Jeep on the Highway—With Me in It"
  - http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/
- The Verge: "New vulnerability lets attackers hijack Chrysler vehicles over the web"
  - http://www.theverge.com/2015/7/21/9009213/chrysler-uconnect-vulnerability-car-hijack

- ~471,000 Uconnect-vulnerable vehicles on the road.

- Hacks:
  - Fully kill the engine
  - Cut the transmission -- disengaging the engine.
  - Completely disable or abruptly engage the brakes.
  - Working on steering control—for now they can only hijack the wheel when the Jeep is in reverse.
  - Surveillance: They can track a targeted Jeep's GPS coordinates, measure its speed, and even drop pins on a map to trace its route.

- TheVerge quote> "Chrysler's UConnect system uses Sprint's cellular network for connectivity, so researchers were able to remotely locate cars. There's no apparent firewall, so once attackers have located the auto's IP, they can deploy previously developed exploits to rewrite Uconnect's firmware and control the car as if they had physical access. The result is that once an attacker has a car's IP address, it can be targeted from anywhere in the world.

- Over the Internet:
  - Locate Uconnect-enabled Chrysler autos.
  - Re-write some of the entertainment system's firmware to obtain access to the CAN bus.
  - Now =on= the CAN bus... do anything they wish.

Microsoft's Emergency Out-Of-Cycle Patch

- ANOTHER Hacking Team 0-Day Exploit!
- https://twitter.com/Laughing_Mantis/status/623188721676881920/photo/1
- http://j00ru.vexillium.org/?p=2520
- http://www.zdnet.com/article/microsoft-releases-emergency-patch-for-critical-windows-flaw/
- http://www.engadget.com/2015/07/20/windows-opentype-security-fix/
- OpenType font rendering flaw.
- =ALL= supported versions of Windows - Vista through Windows 10 pre...

RC4 No More

- Paper to be presnted at the USENIX Security 2015, Aug 12-15th
- http://www.rc4nomore.com/
- Perspective:
  - The first attack >2000 hours.
    - Required 13·2^30 requests @ 1700 requests per second.
    - Performed against simulations.
  - Improved attack ~75 hours
    - Requires ~9·2^27 requests @ 4450 requests per second.
    - Attack was performed against real devices.
- Leverages two RC4 keystream statistical biases:
  - Two consecutive bytes are biased towards certain values.
  - A pair of consecutive bytes is likely to repeat itself.

Miscellany:

Interesting Mr.Robot Theory/Question:

- Is the Christian Slater character Elliot's split personality?

GRC's FLASH-free Video...

- https://www.grc.com/sr/themovie.htm
- https://www.grc.com/sr/whatitdoes.htm
- https://www.grc.com/image/GRC%27s_Flash-Free_Video_Player.png

Chris Rhodus (@ChasingRockets)

- @SGgrc I wish that I had not forgotten to pack my @harrys razor. I've lost a quart of blood so far.

Baigent's #InfoSec ? @baigents

- @SGgrc just received my PDP8 kit from Oscar. Well worth the wait. Now need to find a quiet space to #geek out.

KickStarter (via Taylor Hornby)

- https://www.kickstarter.com/projects/fbz/knityak-custom-mathematical-knit-scarves
- KnitYak
- Less than 48 hours remaining

SpinRite:

Dan Long in Elgin, Illinois experienced what he called "The Miracle of SpinRite"

"The Miracle of Spinrite."
My wife's laptop stopped booting. I had purchased a copy of SpinRite for my computer a year or so ago, so I started running SpinRite on her laptop. This drive had serious problems, so SpinRite took some time, during which my wife was getting impatient. I asked her to have a faith in the process and let it finish.

I titled this the "Miracle of SpinRite", understanding that the function of SpinRite is not a miracle, it is a product of a deep understanding of the technology and writing code to elegantly address that technology. The Miracle occurred once SpinRite was finished. My wife was telling me that this would never work, and that I should just throw it out. I saw that SpinRite it was working on the last region, the less critical slack space. So I stopped SpinRite and rebooted. While my wife was in mid-sentence, telling me how this was doomed to fail, the windows logo appeared on her screen and that is when the Miracle occurred: My wife stopped in mid-sentence and was . . . speechless. This was the first time in more than 20 years I have ever seen her speechless. That is the Miracle of SpinRite. Not only that, after this we were able to recover all of the data and move it to a new laptop. Steve, I want to thank you for your work in bringing that moment to me. I will treasure it always.