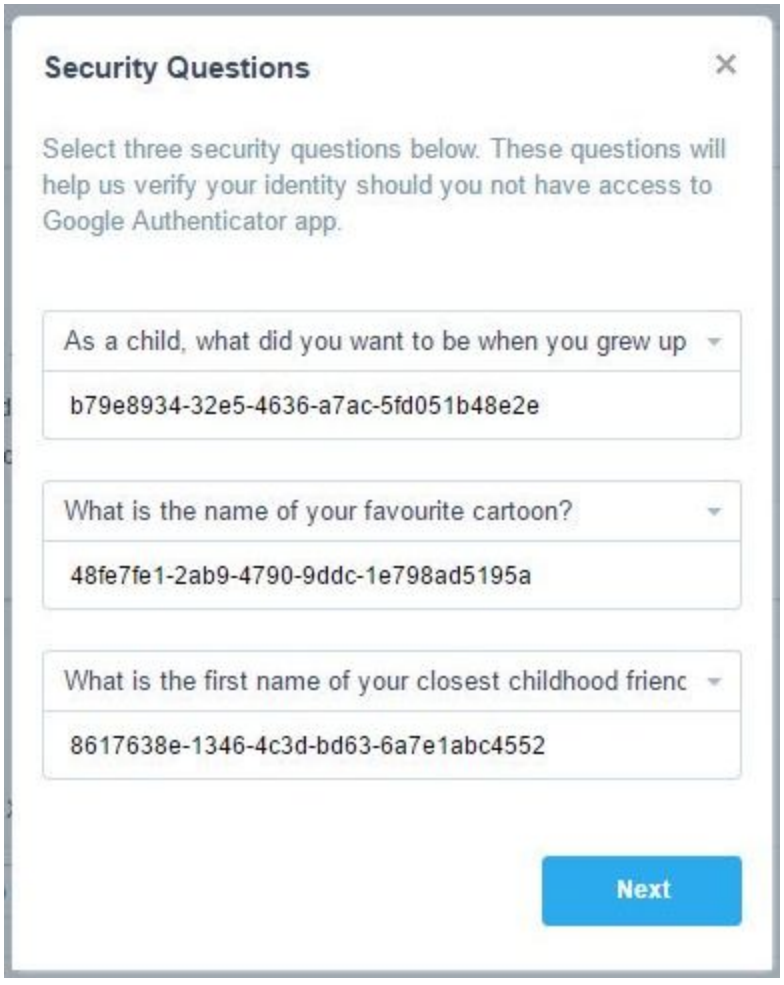
# Security Now! #624 - 08-15-17

# Twelve and Counting

## This week on Security Now!

This week we have a Marcus Hutchins update, the backstory on the NIST's rewrite of their 15 year old password guidance, can DNA be used to hack a computer?, can stop sign graffiti be used to misdirect autonomous vehicles?, the final nail in the WoSign/StartCom coffin, why we need global Internet policy treaties, this week in "researchers need protection", a VPN provider who is doing everything right, Elcomsoft's password manager cracker, a bit of errata and miscellany... and some closing the loop feedback from this podcast's terrific listeners.

## Our Picture of the Week



## Security News

**Marcus Hutchins Update:**
https://www.emptywheel.net/2017/08/14/government-changes-its-tune-about-malwaretech/

*"Marcus Hutchins, AKA MalwareTech, just plead not guilty at his arraignment in Milwaukee, WI."*

Afterward, one of his attorneys, Marcia Hofmann, called him a "hero" and said he would be fully vindicated. And a change in the tone of the government suggested that might well be the case.

Whereas at Hutchins' Las Vegas hearing the government used his appearance at a tourist-focused gun range in their attempt to deny him bail, here the government was amenable to lifting many of the restrictions on his release conditions. Hutchins will be able to live in Los Angeles, where his other attorney, Brian Klein, is located. He will be able to continue working and can travel throughout the US... though he cannot leave the country to return home. This defense tried to get him released to the UK but that was denied.

Aside from the US restriction, the only other restriction aside from GPS monitoring — is that he cannot touch the WannaCry sinkhole. (Which seems oddly random... like, what?, he's going to turn it off and release WannaCry to reproduce again?)

The government's attorney, Michael Chmelar, described Hutchins' alleged crimes as "historic," (as in historical rather than "historically sized"). Trial is currently scheduled for October, but if the government obtains a "complex designation" for the case, that will likely slide.

Chmelar said that they had or would immediately turn over Hutchins' FBI interview, as well as two other recorded phone calls. The rest of discovery will be delayed until the defense signs a protection order.

Interestingly, the Attorneys had quite some difficulty helping Magistrate William Duffin to understand what a "sinkhole" is.  The case was assigned to JP Stadtmueller, a 75-year old Reagan appointee, formerly the Chief Judge of the Eastern district of Wisconsin.

**The backstory of the 14 year old, now deprecated, NIST password guidelines.**

Whoops!  Sorry about those bad password recommendation everyone's been living with for nearly 15 years!

We talked about this at the time, back in June when the new NIST guidelines were released, but it has exploded in the popular press due to its relevance to everyone's daily life.

Back in 2003, as a midlevel manager at the National Institute of Standards and Technology (NIST), Bill Burr was the author of "NIST Special Publication 800-63. Appendix A." The 8-page primer advised people to protect their accounts by inventing awkward new words rife with obscure characters, capital letters and numbers—and to change them regularly.

Bill Burr, who is 72 years old and retired said that "Much of what I did I now regret."

The Wall Street Journal writes: The document became a sort of Hammurabi Code of passwords, the go-to guide for federal agencies, universities and large companies looking for a set of password-setting rules to follow.

The problem... is the advice ended up being largely incorrect, Mr. Burr says. Change your password every 90 days? He laments what we have often noted: most people being periodically forced to make an unwanted and unneeded change will make only minor changes that are easy to guess. (Changing Pa55word!1 to Pa55word!2 doesn't keep the hackers at bay.)

In June, Special Publication 800-63 got a thorough rewrite, jettisoning the worst of these password commandments. Paul Grassi, an NIST adviser who led the two-year-long do-over, said the group thought at the outset the document would require only a light edit. But Mr. Grassi said "We ended up starting from scratch."

The new guidelines, which are already filtering through to the wider world, drop the password-expiration advice and the requirement for special characters. Mr. Grassi said "Those rules did little for security and actually had a negative impact on usability."

Mr. Burr, who once programmed Army mainframe computers during the Vietnam War, had wanted to base his advice on real-world password data. But back in 2003, there just wasn't much to find, and he said he was under pressure to publish guidance quickly.

He asked the computer administrators at NIST if they would let him have a look at the actual passwords on their network. They refused to share them, he said, citing privacy concerns. "They were appalled I even asked," Mr. Burr said.

With no empirical data on computer-password security to be found, Mr. Burr leaned heavily on a white paper written in the mid-1980s.

Cormac Herley, a principal researcher at Microsoft Corp. said that collectively, humans spend the equivalent of more than 1,300 years each day typing passwords. Microsoft once followe the Burr code for passwords, but no more. The NIST rules were supposed to give us randomness. Instead they spawned a generation of widely used and goofy looking passwords such as Pa$$w0rd or Monkey1!  Cormac said: "It's not really random if you and 10,000 other people are all using it."

**Hacking a computer... with DNA? ... or not really**

Last Thursday,during the Usenix Security conference, a group of University of Washington researchers presented a 15-page paper titled: Computer Security, Privacy, and DNA Sequencing: Compromising Computers with Synthesized DNA, Privacy Leaks, and More

It generated a HUGE (really HUGE) amount of attention in the press and was quite hot among all those people who stop reading at the end of the headline... But our listeners though that's not what's in store for them here.

Sample headlines:

- You can hijack a gene sequencer by hiding malware in a DNA sample
- Biohackers Encoded Malware in a Strand of DNA
- Scientists Hack a Computer Using DNA
  "In what appears to be the first successful hack of a software program using DNA, researchers say malware they incorporated into a genetic molecule allowed them to take control of a computer used to analyze it."

  The biological malware was created by scientists at the University of Washington in Seattle, who call it the first "DNA-based exploit of a computer system."

  To carry out the hack, researchers led by Tadayoshi Kohno ("see "Innovators Under 35, 2007") and Luis Ceze encoded malicious software in a short stretch of DNA they purchased online. They then used it to gain "full control" over a computer that tried to process the genetic data after it was read by a DNA sequencing machine.

*Research Paper Abstract:*

The rapid improvement in DNA sequencing has sparked a big data revolution in genomic sciences, which has in turn led to a proliferation of bioinformatics tools. To date, these tools have encountered little adversarial pressure. This paper evaluates the robustness of such tools if (or when) adversarial attacks manifest. We demonstrate, for the first time, the synthesis of DNA which—when sequenced and processed—gives an attacker arbitrary remote code execution. To study the feasibility of creating and synthesizing a DNA-based exploit, we performed our attack on a modified downstream sequencing utility with a deliberately introduced vulnerability. After sequencing, we observed information leakage in our data due to sample bleeding. While this phenomena is known to the sequencing community, we provide the first discussion of how this leakage channel could be used adversarially to inject data or reveal sensitive information. We then evaluate the general security hygiene of common DNA processing programs, and unfortunately, find concrete evidence of poor security practices used throughout the field. Informed by our experiments and results, we develop a broad framework and guidelines to safeguard security and privacy in DNA synthesis, sequencing, and processing.

So, what's going on here?

There is a utility on sourceforge called "fqzcomp" also known as the "FASTQ" compression utility. It was designed to compress DNA sequences. So these guys downloaded the source and deliberately broke the code by creating a static buffer which was deliberately too small for their 177 base pair DNA so that when that program attempted to compress the DNA they provided, that buffer would overflow.

And their modified fqzcomp version used a simple 2-bit DNA encoding scheme. The four nucleotides were encoded as two bits—A as 00, C as 01, G as 10, and T as 11 -- thus packing pairs of bits into bytes starting with the most significant bits.

So, yeah... that 2-bit scheme coupled with their deliberately hacked reduced-size buffer, did, indeed, allow them to place their own bits into non-buffer space. However, even given all of this

cheating manipulation, their exploit only functioned 37.4% of the time since only error-free sequencing would produce a running exploit, and only 76.2% of the DNA sequencing was error free. Then there was the problem that DNS strands have two ends, and the sequencing might begin from either end. This cut the 76.2% success in half again, to 37.4%.

So... what we really have is a somewhat interesting, contrived synthetic demonstration of how an inherently low-reliability attack could be created using DNA as the code-carrying agent... but almost certainly only if the DNA sequence-processing pipeline had serious flaws that would cause it to crash quickly when processing non-contrived DNA. Thus it's difficult to see how such flaws could exist in the real world for long without being found and fixed.

This whole merging of medicine, DNA and computers -- it's a bit surreal. And one wonders how much the terminology from the various disciplines might be cross-pollinate. For example... incontinence might be someday be considered a buffer overflow!

**Hacking a computer: Deliberately spoofing self-driving cars**

Once again, click-bait headlines mislead and worry people:

- "A Self-driving car can be easily hacked by just putting stickers on road signs"
  Subhead: "A team of experts showed that a simple sticker attached on a sign board can confuse any self-driving car and potentially lead an accident."
- "Researchers hack a self-driving car by putting stickers on street signs"

In fairness, the audience for these articles is not our typical Security Now! listener, but they do cause concern and put unwarranted doubt into the ether.

A team of researchers from four US universities: University of Washington, University of Michigan at Ann Arbor, Stony Brook University and University of California, Berkeley.

Research paper titled: *"Robust Physical-World Attacks on Machine Learning Models"*

Notice, it doesn't say "attacks on cars", or even one car, or even a shopping cart... is says "attacks on machine learning models." And, yes, this has some relevance to the real world because we believe that autonomous self-driving automobiles also use machine-learning models. But at this point this is very different from commandeering that Jeep's management network and forcing its driver off the road into a ditch.

Okay, so what DO we have here?

ABSTRACT: Deep neural network-based classifiers are known to be vulnerable to adversarial examples that can fool them into misclassifying their input through the addition of small-magnitude perturbations. However, recent studies have demonstrated that such adversarial examples are not very effective in the physical world--they either completely fail to cause misclassification or only work in restricted cases where a relatively complex image is perturbed and printed on paper. In this paper we propose a new attack algorithm--Robust Physical Perturbations (RP2)-- that generates perturbations by taking images under different conditions into account. Our algorithm can create spatially-constrained perturbations that mimic vandalism or art to reduce the likelihood of detection by a casual observer. We show that

adversarial examples generated by RP2 achieve high success rates under various conditions for real road sign recognition by using an evaluation methodology that captures physical world conditions. We physically realized and evaluated two attacks, one that causes a Stop sign to be misclassified as a Speed Limit sign in 100% of the testing conditions, and one that causes a Right Turn sign to be misclassified as either a Stop or Added Lane sign in 100% of the testing conditions.

https://iotsecurity.eecs.umich.edu/#roadsigns
(The best thing of all is the URL of the FAQ. The very fact that there is a site called "iotsecurity" at EECS uMich.edu is quite heartening!)

FAQ: (slightly edited for additional clarity)

- Did you attack a real self-driving car?
  - No.

- Okay, what did you attack?
  - We attacked a deep neural network-based classifier for U.S. road signs. A classifier is a neural network (in the context of our work) that interprets road signs. A car would typically use a camera to take pictures of road signs, and then feed them into a road sign classifier.

    To the best of our knowledge, there is currently no publicly available classifier for U.S. road signs. Therefore, we first built our own neural net consisting of three convolutional layers followed by a fully connected layer. We then trained our network on the LISA dataset, a U.S. sign dataset comprised of different road signs like Stop, Speed Limit, Yield, Right Turn, Left Turn, etc. Our final trained road sign classifier accuracy was 91% on the test dataset. (to which it had been trained.)

- What are your findings?
  - We show that it is possible to construct physical modifications to road signs, in ways that cause the trained classifier (discussed above) to misinterpret the meaning of the signs. For example, we were able to trick the classifier into interpreting a Stop sign as a Speed Limit 45 sign, and a Turn Right sign as either a Stop or Added Lane sign. Our physical modifications for a real Stop sign are a set of black and white stickers. See the resources section below for examples.

- What resources does an attacker need?
  - An attacker needs a color printer for sticker attacks, and a poster printer for poster-printing attacks. The attacker would also need a camera to take an image of the sign he wishes to attack.

- Based on this work, are current self-driving cars at risk?
  - No. We did not attack a real self-driving car. However, our work does serve to highlight potential issues that future self-driving car algorithms might have to address.

- Should I stop using the autonomous features (parking, freeway driving) of my car? Or is there any immediate concern?
    - We again stress that our attack was crafted for the trained neural network discussed above. As it stands today, this attack would most likely NOT work as-is on existing self-driving cars.

So this IS useful and necessary research as its best, and hats off to this team. But this research is NOT properly aimed at the popular press nor today's drivers. It IS properly aimed at automakers, and the providers of future autonomous AI self-driving network subsystems. And the only real advantage of it having received so much hysterical press coverage, is that there's no chance the people who NEED to see it will not have.

The bottom line is: It is very easy to take the robust functioning of our own NATURAL intelligence, for granted. We look at those synthetically modified stop signs and see a stop sign with some weird black and white rectangles and think... okaaaaaaaay... and we stop anyway. Whereas an ARTIFICIAL intelligence, which doesn't think at all in the human sense, and is barely road-worthy to start with, is trivially confused.

This is exactly analogous to the observation we make all the time with much simpler computer bugs: Programmers, who are almost always under severe deadline pressure, stop working when the program starts working. Whereas what they SHOULD do is not stop working until no one is able to make the program stop working. But not the word we live in.

Let's hope for more, once our cars start driving themselves.

**The final nail in the WoSign / StartCom coffin:**
Microsoft has joined Mozilla, Google and Apple in the abandonment of trust in WoSign and its StartCom subsidiary. It's finally "Game Over" for those clowns... and this and the Symantec debacle should serve as a useful and cautionary tale for all other presently widely trusted certificate authorities: What you actually do matters... because that's entirely why you're in business.

https://blogs.technet.microsoft.com/mmpc/2017/08/08/microsoft-to-remove-wosign-and-startcom-certificates-in-windows-10/

Microsoft writes: Microsoft has concluded that the Chinese Certificate Authorities (CAs) WoSign and StartCom have failed to maintain the standards required by our Trusted Root Program. Observed unacceptable security practices include back-dating SHA-1 certificates, mis-issuances of certificates, accidental certificate revocation, duplicate certificate serial numbers, and multiple CAB Forum Baseline Requirements (BR) violations.

Thus, Microsoft will begin the natural deprecation of WoSign and StartCom certificates by setting a “NotBefore” date of 26 September 2017. This means all existing certificates will continue to function until they self-expire. Windows 10 will not trust any new certificates from these CAs after September 2017.

Microsoft values the global Certificate Authority community and only makes these decisions after careful consideration as to what is best for the security of our users.

---

What was not addressed in that posting was the status of the earlier, still-supported and still-in-the-majority-despite-Microsoft's-every-effort, Windows 7 and 8.1 operating systems? Note that this sort of conditional certificate acceptance, unless the facility was presciently already built in, requires custom modification of the system's certificate interpreter. Thus, users of earlier Windows operating systems cannot simply remove those root certs from their trusted root stores since StartCom's certificates were once quite popular (and are still being sold today, with 2- or 3-years-in-the-future expirations) and it is not the certificate owner's fault that the company from which they were obtained screwed up. Thus any StartCom certificate issued within the next six weeks WILL still be honored by Windows for the subsequent two or three years.

So, to be responsible, to its users, Microsoft really must similarly protect users of its earlier and still supported operating systems. Failing that, we would be forced to defensively abandon all use of IE in favor of Chrome or Firefox, whose browser vendors are remaining proactive on earlier editions of Windows.

I went over to StartCom this morning and it's business as usual. You wouldn't know, looking around, that the buglers are warming up to play taps. But, in fact, the boom is rapidly being lowered because, unless they were to start back-dating their newer certificates' start date (which would doubtless immediately extinguish what little remaining shred of forbearance the industry has for them), they WILL BE UNABLE to ever again sell any certificates which would be honored by Windows 10 starting six weeks from today.  RIP.

**Why we need global Internet treaties:**
This next interesting article brought to mind the problems introduced when we have a single globe-spanning network that inherently crosses national boundaries and interlinks disparate governing law.

BleepingComputer reports: [Last Monday] British lawmakers filed a statement of intent regarding proposals for improvements to the Data Protection Act, with a focus on criminalizing anonymous data re-identification, imposing larger fines for cyber incidents, and more user protections for British online netizens.

The modifications are part of UK's effort to comply with the EU's General Data Protection Regulation (GDPR) that's set to come into effect in May 2018, time until which EU governments must amend national laws to include its provisions.

The new bill would add many of the GDPR's provisions for GDPR compliance. For example:

- Make it simpler to withdraw consent for the use of personal data
- Make it easier and free for individuals to require an organization to disclose the personal data it holds on them
- Allow people to ask for their personal data held by companies to be erased
- Require 'explicit' consent to be necessary for processing sensitive personal data
- Enable parents and guardians to give consent for their child's data to be used
- Expand the definition of 'personal data' to include IP addresses, internet cookies and DNA
- Make it easier for customers to move data between service providers

Unfortunately, as is too often the case when aggressive new legislation meets aggressive new technology, problems in practice arise: For one thing, it's easy to drop the gavel on a law that's not possible or practical to implement. A perfect example of this would be the requirement that ISP's retain a log of everywhere each of their subscribers individually goes and everything they do out there on the Internet. Easy to write that law, but next to impossible for any ISP to actually pull it off, even if they really wanted to... which they most assuredly don't. They just want to charge for the transit of subscriber traffic across their proprietary networks.

Similarly, in this instance, it's a noble ideal to imagine criminalizing the reversal of deliberate identity anonymization. But how, exactly, do we reduce that to practice? It is, after all, the entire business model of several of the world's largest Internet entities. It underlies the somewhat awkward Hobbesian bargain we have made with these entities in exchange for accepting their "free" offerings. They track and explicitly deanonymize even in the face of many of their users explicit request that this not be done. So good luck with telling Google and Facebook (and now Microsoft-as-a-service) that this is conduct unbecoming.

So paraphrasing from BleepingComputer's report:

On top of the GDPR provisions, the Data Protection Bill (DPB) includes an extra proposa: The creation of a new criminal offence for when someone, intentionally or recklessly, re-identifies individuals from anonymised or pseudonymised data. (In practical terms: who belongs to this cookie??... because all browser cookies are inherently pseudonymous!)

The DPB reads: "Offenders who knowingly handle or process such data will also be guilty of an offence. The maximum penalty would be an unlimited fine."

Dr. Lukasz Olejnik, an independent cybersecurity and privacy researcher who is an affiliatee of Princeton's Center for Information Technology Policy, applauds the UK's efforts, writing in his blog last Monday: "The UK's GDPR implementation may have visionary traits; in that it goes beyond merely implementing the GDPR as just a legislation. The UK will introduce new criminal offences, among them reidentification."

But then he adds (oh, by the way): "There are several issues with [the] banning of reidentification. First, it won't work. Second, it will decrease security and privacy."

The biggest problem in Olejnik's view is that there's is no effective way to enforce it in practice. But, wait... since this IS Google's and Facebook's entire business model, enforcement seems

pretty simple: After the legislation is enacted (IF it should ever actually see the light of day) the UK can simply give Zuck a call and say: "Uhhhhh... you know that legislation that became law yesterday? How are you guys still in business?"

Secondly, though, adds Olejnik, the new legislation would stifle security and privacy research which often, and must often, deliberately re-identify anonymized data in day-to-day research.

The DPB statement of intent DID also mention protections for journalists and whistleblowers, but it did not provide any details.

Which brings us all the way back around to the need for transnational treaties.

We have a global network with valuable and desired content being provided free of explicit charge -- in exchange for a sacrifice of absolute privacy and anonymity -- by massive global Internet-centric enterprises operating across national boundaries. If regulation is to be imposed, that regulation cannot practically be disparate in every region of the globe.

We're still in the early days, but we are finally beginning to struggle with the big questions of encryption, privacy, and anonymity for all user's of this incredible global network. This is clearly an important and necessary conversation for us to have. But the very globalness of the Internet which creates so much of its value requires unified global regulation.

**This Week in "Researchers Need Protection"**

TechDirt wrote up a very nice piece titled: "Company Storing Families' Personal Data Blocks Users/Researchers Informing It Of A Security Flaw

It must be repeated over and over: people who discover security flaws and report them are not the enemy. And yet, company after company after company treat security researchers and concerned users like criminals, threatening them with lawsuits and arrests rather than thanking them for bringing the issue to their attention.

Kids Pass -- a UK company providing discounts for families attending restaurants, theaters, and amusement parks -- had a problem. Any user could access any other user's personal information just by altering numbers linked to user IDs in the URL. (In other words, another glaring example of atrocious web application design... which, itself, should be outlawed.)

A concerned user told security researcher Troy Hunt about the flaw:

Just this weekend I had a Twitter follower reach out via DM looking for advice on how to proceed with a risk he'd discovered when signing up to Kids Pass in the UK, a service designed to give families discounts in various locations across the country. What he'd found was the simplest of issues and one which is very well known - insecure direct object references. In fact, that link shows it's number 4 in the top 10 web application security risks and it's so high because it's easy to detect and easy to exploit. How easy? Well, can you count? Good, you can hack! Because that's all it amounted to, simply changing a short number in the URL.

Troy told the user to stop doing anything -- including accessing other users' information -- and immediately inform the company. The user did as instructed, contacting the company via Twitter direct message. Shortly thereafter, the user informed Troy Hunt that Kids Pass had blocked him on Twitter.

Troy then made an attempt to speak to someone at Kids Pass… only to find out he had been blocked as well, most likely for having the gall to retweet the concerned user's message about the security flaw.

The responsible, ethical approach -- notifying a company of a security flaw as soon as possible -- was being treated like some sort of trollish attack on Kids Pass' Twitter account. From all appearances, the company simply wanted everyone to shut up about the flaw, rather than address the concerns raised by a user.

It was only after Troy asked his followers to contact the company on his behalf that Kids Pass finally unblocked him and told everyone the "IT department was looking at it."

***(Yay, Troy!)***

However, that belated reaction doesn't make up for the initial reaction. And Kids Pass has shown it has little interest in addressing security flaws until the problem becomes too public to ignore. Troy points to a blog post by another security researcher who informed Kids Pass last December about its insecure system -- including the fact it sent forgotten passwords in plaintext via email to users. He heard nothing back, finally publishing his discoveries in July.

If you want people to be good web citizens and report breaches and flaws, you can't treat them like irritants or criminals when they do. Securing users' personal info is extremely important, but some companies seem to feel they should be able to handle it however they want and mute/sue/arrest those who point out how badly-flawed their systems are.

**On the heels of last week's horrific Hotspot Shield VPN story...**
We have the flip side of a VPN provider who is doing everything exactly right!
Their posting itself demonstrates all of the right stuff, and our listeners will recognize and appreciate the honesty and integrity it displays. So I'm going to share the entire thing -- it's not overly long -- because this is important, not only for current and prospective users of Tunnelbear, but because there are also lessons here for any and all other high-integrity VPN providers.

https://www.tunnelbear.com/blog/tunnelbear_public_security_audit/
Cure53 Audit results: https://cure53.de/summary-report_tunnelbear.pdf

Headline: “TunnelBear Completes Industry-First Consumer VPN Public Security Audit”

Consumers and experts alike have good reason to question the security claims of the VPN industry. Over the last few years, many less reputable VPN companies have abused users' trust by selling their bandwidth, their browsing data, offering poor security or even embedding malware.

Being within the industry, it's been hard to watch. We knew TunnelBear was doing the right things. We were diligent about security. We deeply respected our users' privacy. While we can't restore trust in the industry, we realized we could go further in demonstrating to our customers why they can, and should, have trust in TunnelBear.

Today, we'd like to announce TunnelBear has completed the Consumer VPN industry's first 3rd party, public security audit. Our auditor, Cure53, has published their findings on their website and we're content with the results.

https://cure53.de/summary-report_tunnelbear.pdf

A bit of history:

In late 2016, we hired Cure53, a respected security company, to do a complete audit of our servers, apps and infrastructure. Using a "white-box" approach, they were given full access to our systems and code. Our original plan was to use their findings internally to confirm we were delivering on our promise to secure your browsing and proactively identify vulnerabilities. However, the recent crisis of trust in the VPN industry showed us we needed to break the silence and share Cure53's findings publicly. Today we're sharing a complete public audit which contains both the results from last year and the results from the current audit.

As the auditor, Cure53's opinions and findings are their own, with the results being published on their website. TunnelBear was given the opportunity to provide feedback on the report, before it was published, where we felt findings were inaccurate or irreproducible. As is the case of most security audits, Cure53 was paid for their work. We wouldn't expect any cybersecurity company to spend a few hundred hours auditing our code for free.

What were the results?

If you've already looked at the results, you've seen that the 2016 audit found vulnerabilities in the Chrome extension that we weren't proud of. It would have been nice to be stronger out of the gate, but this also reinforced our understanding of the value of having regular, independent testing. We want to proactively find vulnerabilities before they can be exploited. We hadn't intended to publish the 2016 results. However, we're hoping the security community has appreciation for our candid transparency in the 2016 report and for demonstrating our investment in security over time.

All findings discovered in the 2016 audit were promptly addressed by TunnelBear's engineering team and verified to be fixed by Cure53.

In the June 2017 audit, we were more content with the results. All vulnerabilities represented low-risk findings. As Cure53 put it, "The results of the second audit clearly underline that TunnelBear deserves recognition for implementing a better level of security for both the servers and infrastructure as well as the clients and browser extensions for various platforms".

All findings discovered in the 2017 audit have also been addressed by TunnelBear's engineering team with only informational findings remaining.

You can read the full report on Cure53's website.

Our ongoing commitment to security

Our plan is to earn trust and move the VPN industry in a new direction around transparency. While many VPN companies will continue to live in obscurity, with claims of protecting your security, it's our hope that by completing the industry's first 3rd party, public security audit, experts and consumers alike can be sure that TunnelBear delivers on its security promises.

If we've learned anything from this audit, it's that good security needs constant reevaluation. Annual public audits will become routine to help us quickly identify vulnerabilities and demonstrate transparency in an industry where trust is sorely lacking. In the coming months we'll share more announcements, industry insights and how-tos to give you the information you need to make the right choices about your security.

Grizzly Regards,
The TunnelBear Team

**One Password to Rule Them All:**
Elcomsoft's blog posting's full title is: "One Password to Rule Them All: Breaking into 1Password, KeePass, LastPass and Dashlane"

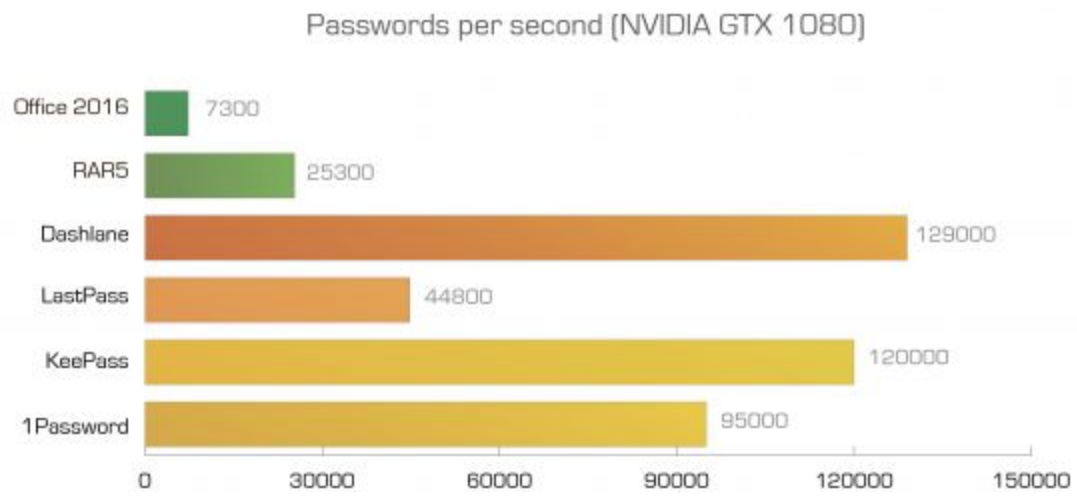
https://blog.elcomsoft.com/2017/08/one-password-to-rule-them-all-breaking-into-1password-keepass-lastpass-and-dashlane/

We've just updated Elcomsoft Distributed Password Recovery with the ability to break master passwords protecting encrypted vaults of the four popular password keepers: 1Password, KeePass, LastPass and Dashlane. In this article, we'll talk about security of today's password managers, and provide insight on what exactly we did and how to break in to encrypted vaults.

This amounts to offline GPU-accelerated, brute force password recovery.

They write:
Different password managers employ different approaches to security. As an example, LastPass generates the encryption key by hashing the username and master password with 5,000 rounds of PBKDF2-SHA256, while 1Password employs even more rounds of hashing. This is designed to slow down brute-force attacks, and it almost works. Granted, these are still nearly an order of magnitude less secure than, say, Microsoft Office 2016 documents, but even this level of security is much better than nothing.

Therefore, this is the benchmark. We've added RAR5 and Office 2016 to the chart for comparison sake. Higher numbers represent higher recovery speeds.




For some context, because this sort of local attack brute force is always a concern, the technology I designed for SQRL's PBKDF is deliberately highly acceleration resistant (using the memory-hard Scrypt function), and dynamically self-adjusting (using what we call the dynamically iterative EnScrypt function) to yield a maximum brute force rate of 0.00333 guesses per second per core. Approx one guess every 5 seconds.

## Errata

Many of our listeners confirmed that send.firefox.com is working under Safari… including the listener who originally reported it failure. So something may have been fixed.

## Miscellany

**Amazon S3**

- July billing: $2.04.
- Amazon S3: I am currently storing 88 Gigabytes at Amazon, for which I'm paying $2.02 per month. at 2.3 cents per GB per month (for the first 50TB of storage used).
- No charge for data transfer.
- 1 cent for 560 PUT requests.
- 1 cent for 852 GET requests.

**Richard Philips**

- Richard Phillips (@RhoAgenda)
  Hi Steve. Thanks for the Rho Agenda mention on last weeks show. I had a lot of fun with the final novel in that series, The Meridian Ascent.

**Colossus: The Forbin Project (1970)**

- Date of Release: April 8, 1970
- https://archive.org/details/Colossus_The_Forbin_Project_1970
- https://archive.org/download/Colossus_The_Forbin_Project_1970/Colossus%20%E2%80%93%20The%20Forbin%20Project%20(1970).mp4
- Just watch the first five minutes online in your browser… it's FUN!

## SpinRite

DanR / August 2nd..

> There are a couple of unrelated things that have mysteriously stopped working
> over the last 2-3 days. I know my aging HD is slowing down. So, I'm going to
> shut down and SpinRite the HD.

Briefly: Ran SR L2 and then L4. No sector or other issues flagged. System boots and runs noticeably faster and smoother now. Apps launch noticeably faster now. Per past experience, this effect will last 1-2 weeks then things will slow down again. I am looking for a replacement HD.

## Closing The Loop

**Grant Taylor (@DrScriptt)**
While re-listening to SN 133 (twit.tv/shows/security…)
I wondered how over provisioning worked with TrueCrypt.

**jason (@netxme)**
@SGgrc Hi Steve, just wondering if you are still on ketogenic diet? I'm kind of interested in it, but want to know your takes 5 yr after 2012

**Charles Hoskinson (@IOHK_Charles)**
@SGgrc Steve are you still on the keto diet.

**Karim Kronfli (@BullshotUK)**
@SGgrc Hi Steve any chance you could cast your eye over Google Chrome's new Smart Lock feature for password management on @SecurityNow ?

**Elkin (@coolterps)**
@SGgrc a big note on the LastPass thing, they moved mobile features to free tier months ago. The free version has everything I'd want.

**AJ Doyle @AllenDoyle**
@SGgrc just had to say thanks again. On book 5 of 15. Hands down best series I've read in my life. All the best!

**barry swatman (@barryswat)**
@SGgrc is my Nexus 5 now garbage?  #Broadpwn  Can I do anything ?

**Dan (@treyd)**
@SGgrc Good Morning, have you ever done a show on "vlans" and wether they are effective public WiFi security?

**Steven A Meyers (@stevemey)**
@SGgrc Steve, my eye doc emailed me high quality photos of my iris in the clear. Is that a security risk? Can she use send Firefox instead?

**Sofa King (@smod_me)**
@SGgrc Sir, on a scale of 1 to 10, how secure is an eight character password protected Excel spreadsheet on google drive? For my passwords?

**Brent Reusing (@breusin)**
@SGgrc why not make your very last episode number zero? Your very own so-called “zero day”!

**RG Miller (@wickedcoffee)**
@SGgrc I love the Real-Time activities display in SpinRite. Can you think of a way I could cast this to a screen so others could watch?

**C. M. Au Yong (@auyongcheemeng)**
@SGgrc XD "HTTP Error Code 418 I'm a Teapot is about to be removed from Node. We've gotta do something" redd.it/6sxea0

**agquarx (@agquarx)**
Downloading HotspotShieldVPN app, because I *want* companies to spy on me, it excites me and makes me feel important! @SGgrc

**evron Baldwin @devronbaldwin**
@SGgrc genius?

> rt: I Am Devloper @iamdevloper
> pro tip: set your password to "incorrect" and every error message becomes a password hint

~30~