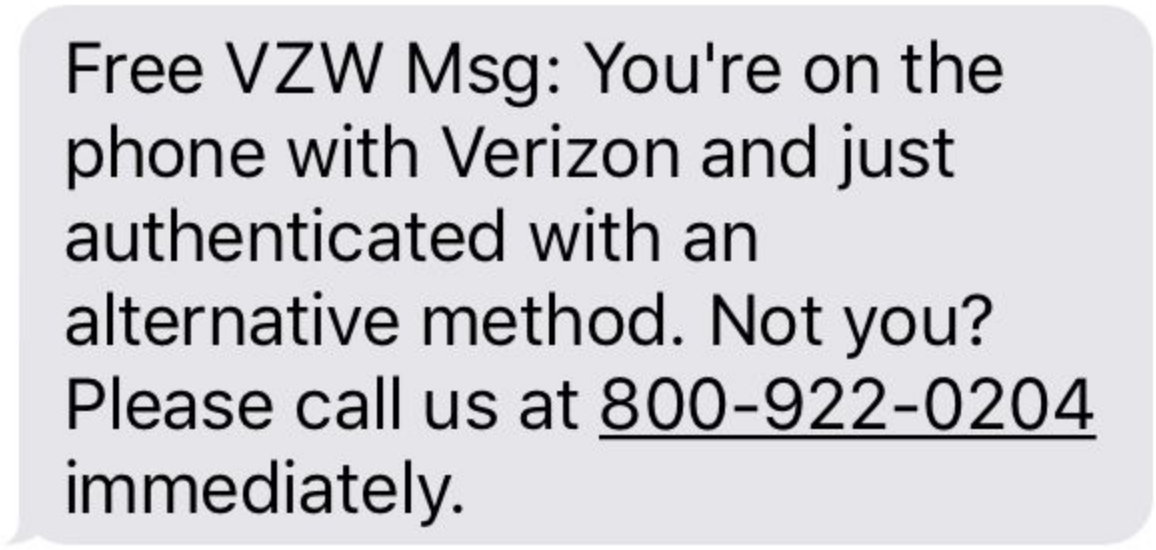
Security Now! #615 - 06-06-17

Legacy's Long Tail

This week on Security Now!

This week we discuss an embarrassing high-profile breach of an online identity company, an over-hyped problem found in Linux's sudo command, the frightening software used by the UK's Trident nuclear missile submarine launch platforms, how emerging nations prevent high school test cheating, another lesson about the danger of SMS authentication codes, another worrisome SHODAN search result, high-penetration dangerous adware from a Chinese marketer, another "that's not a bug" bug in Chrome allowing websites to surreptitiously record audio and video without the user's knowledge, the foreseeable evolution of hybrid crypto-malware, the limp return of Google Contributor, Google continues to work on end-to-end eMail encryption, a follow-up on straight-to-voicemail policy, "homomorphic encryption" (what the heck is that?), and "closing the loop" follow up from recent discussions.

Our Picture of the Week



Security News

OneLogin Breach:

- OneLogin is a single-sign-on provider using OAuth.
- So rather than "sign in with Google" it's "Sign in with OneLogin."
- OneLogin implemented their cloud-based infrastructure using Amazon AWS cloud services.
- Around 9pm PST in the evening last Wednesday, they detected that odd usage patterns had been occurring within their database instances for the previous seven hours.
- They shutdown the unauthorized access and began to look at what had been happening.
- The bottom line is: It doesn't get any worse.
    - Many have criticized their public response for being opaque and deliberately lacking in detail because they provided much more information non-publicly via eMail to their subscribers.
    - They stated that their AWS keys had been lost, allowing decrypted access to their private databases.
    - <quote> "The threat actor was able to access database tables that contain information about users, apps, and various types of keys. While we encrypt certain sensitive data at rest, at this time we cannot rule out the possibility that the threat actor also obtained the ability to decrypt data. We are thus erring on the side of caution and recommending actions our customers should take, which we have already communicated to our customers."
    - In private eMail to their customers, users were told to generate new API keys and OAuth tokens; create new security certificates as well as credentials; recycle any secrets stored in OneLogin's Secure Notes feature; have every end-user update their passwords, and more.
    - In other words, start everything over from scratch... for every OneLogin corporate customer and every one of those users.
- SQRL: As we know, I have been invested a great deal of time in nailing down every last detail required to turn a simple and theoretically strong concept into a useful reality with SQRL. So when I encounter stories like this I naturally test the SQRL system against the same vulnerabilities.

  At its core, what makes SQRL unique is that it operates in an entirely different way. The slogan I've coined to describe this is: "SQRL gives websites no secrets to keep." If a service has no secrets to keep it has no secrets to lose.

Traditional logon, and even modern logon such as OAuth, relies upon first entrusting a server with a secret, or a safer derivative of a secret (a hash). Then, in subsequent visits you show the server that you still remember the original secret.

But SQRL uses a simple cryptographic proof of knowledge... without EVER sharing that knowledge. This means that what the site holds for the user can ONLY EVER be used to verify the user's assertion of who they are -- it cannot be used to generate such an assertion. Therefore, there is zero value in the theft of that information from the site.

- Recent SQRL work: Changing its policy about anti-spoofing enforcement with CPS.

- Links:
  - http://www.bbc.com/news/technology-40118699
  - https://motherboard.vice.com/en_us/article/identity-manager-onelogin-has-suffered-a-nasty-looking-data-breach
  - http://www.zdnet.com/article/onelogin-hit-by-data-breached-exposing-sensitive-customer-data/
  - http://thehackernews.com/2017/06/onelogin-password-manager.html
  - https://arstechnica.com/security/2017/06/onelogin-data-breach-compromised-decrypted/
  - https://arstechnica.co.uk/security/2017/06/onelogin-data-breach-compromised-decrypted/

High-Severity Linux Sudo Flaw Allows Users to Gain Root Privileges

- Last Tuesday / http://www.openwall.com/lists/oss-security/2017/05/30/16
- http://thehackernews.com/2017/05/linux-sudo-root-hack.html
  A rather difficult-to-leverage local privilege escalation flaw discovered in the sudo command processor.
  CVE-2017-1000367.
  Discovered by researchers at Qualys Security in Sudo's "get_process_ttyname()" function for Linux.
- Could allow a user with Sudo privileges to run commands as root or elevate privileges to root.
- Note: not 0-day, not known to be in use, local privilege escalation only.
- sudo == superuser do // allows transient elevation to root for command execution.
- The details of this exploit would make your eyes cross.
- Marked "High Severity" and affecting Sudo v1.8.6p7 through 1.8.20
- Already patched in Sudo v1.8.20p1.
- Fixes are rolling out quickly:
  - Red Hat pushed out patches for Red Hat Enterprise Linux 6, 7 and Server.
  - Debian has also released fixes for its Wheezy, Jessie and Sid releases.
  - SUSE Linux has rolled out fixes for a number of its products.

UK's Trident nuclear submarines 'vulnerable to catastrophic hack'

- http://www.basicint.org/publications/stanislav-abaimov-paul-ingram-executive-director/2017/hacking-uk-trident-growing-threat
- http://www.basicint.org/sites/default/files/HACKING_UK_TRIDENT.pdf
- https://www.theguardian.com/uk-news/2017/jun/01/uks-trident-nuclear-submarines-vulnerable-to-catastrophic-hack-cyber-attack

So I'm reading along in The Guardian a report titled "UK's Trident nuclear submarines 'vulnerable to catastrophic hack'"... where a security thinktank doesn't believe that the fact that submarines are inherently "air gapped" should support the level of complacency that the bureaucrats appear to have.

The 38-page report titled "Hacking UK Trident: A Growing Threat" states that the UK's Trident submarine fleet is vulnerable to a "catastrophic" cyber-attack that could render Britain's nuclear weapons useless. It warns that a successful cyber-attack could "neutralize operations, lead to loss of life, defeat or perhaps even the catastrophic exchange of nuclear warheads (directly or indirectly)".

Okay, so that doesn't sound good. The report says: "Trident's sensitive cyber systems are not connected to the internet or any other civilian network. Nevertheless, the vessel, missiles, warheads and all the various support systems rely on networked computers, devices and software, and each of these have to be designed and programmed. All of them incorporate unique data and must be regularly upgraded, reconfigured and patched."

The UK has four nuclear missile-carrying submarines, which are in the process of being replaced. Their replacements are scheduled to go into service in the early 2030s.

But then, as I'm reading, I encounter this "Gobsmacking" paragraph (as I believe the English might put it)... "The report comes after the cyber-attack last month that disrupted the NHS, which uses the same Windows software as the Trident submarines.

WHAT?????????????!!!!!!! Yes.... The UK's Trident submarines are running Windows XP!

Page 23: The Submarine Command System (SMCS) was first created for the Vanguard-class submarines as their tactical information and torpedo weapon control systems. It has a long and complex pedigree. Its updated versions are based upon a version of Windows XP and known colloquially as 'Windows for Warships'. These have now been installed on all active Royal Navy submarine classes. Both Windows-based and Linux-based operating systems hold the legacy of vulnerabilities from the original systems, even though they operate on obscure and classified equipment and run bespoke programmes.

In 2002, it was proposed to convert SMCS to run on standard x86 hardware redesigned specifically for naval command systems. The plan was to convert the SMCS infrastructure and applications to run on the Microsoft Windows operating system and known as SMCS-NG ("Next Generation"), or "Windows for Warships". This is based upon a variant of Windows 2000 and Windows XP. SMCS-NG was retrofitted into all Royal Navy submarines by December 2008. The software is supplied as a universal release configured for the sensor and weapon fit of each submarine.

The report continues... "Windows has an entangled monolithic structure, as opposed to a modular architecture. It is therefore impossible to change the proprietary operating system by means of reconfigurations and third-party modules. This structure of the consumer- friendly (it's hardly "consumer-friendly" if a nuke lands in your neighborhood!) operating system exposes potentially vulnerable services and features that might not be required for the adequate functioning of the submarine.

Also last Tuesday… The nation of Ethiopia "turned off" their access to the Internet to prevent student cheating.
The Guardian reported last Wednesday: Ethiopia shut down the internet yesterday ahead of a scheduled national examination that is underway in the country today. Social media users noted that the internet service was interrupted from around 7 pm on Tuesday -- reportedly to prevent exam leaks. About 1.2 million students are taking their 10th grade national exams, with another 288,000 preparing for the 12th grade university entrance exams that will take place next week.

From a report:

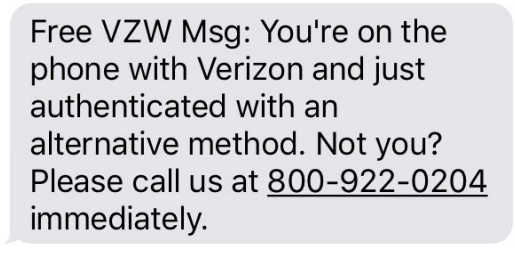
Outbound traffic from Ethiopia was shutdown around 4pm UK time on Tuesday, according to Google's transparency report, which registered Ethiopian visits to the company's sites plummeting over the evening. By Wednesday afternoon, access still had not been restored.

A year ago, activists leaked the papers for the country's 12th grade national exams, calling for the postponement of the papers due to a school shutdown in the regional state of Oromia. Now, the government appears to have taken the move to shut down internet access as a preventative measure.

It's worth noting that an emerging economy such as Ethiopia has a far lesser dependence upon the Internet than any post-emergent economy. The US has become so dependent upon the Internet that our entire economy would collapse overnight if networking disappeared.

https://www.theguardian.com/technology/2017/may/31/ethiopia-turns-off-internet-students-sit-exams

Cody Brown gets hacked
https://medium.com/@CodyBrown/how-to-lose-8k-worth-of-bitcoin-in-15-minutes-with-verizon-and-coinbase-com-ba75fb8d0bac
He received a TXT message from Verizon stating that he was on the phone with them right then... except that he wasn't. The message said: If this is not you on the phone, please call us immediately!



Cody took immediate action, trying to phone Verizon at the number provided, only to receive the "You have reached us outside of our normal business hours..."
Cody then watched, powerless, as his Google Mail account was taken over and his password was changed, then $8000 of cryptocurrency was drained from his account at Coinbase.

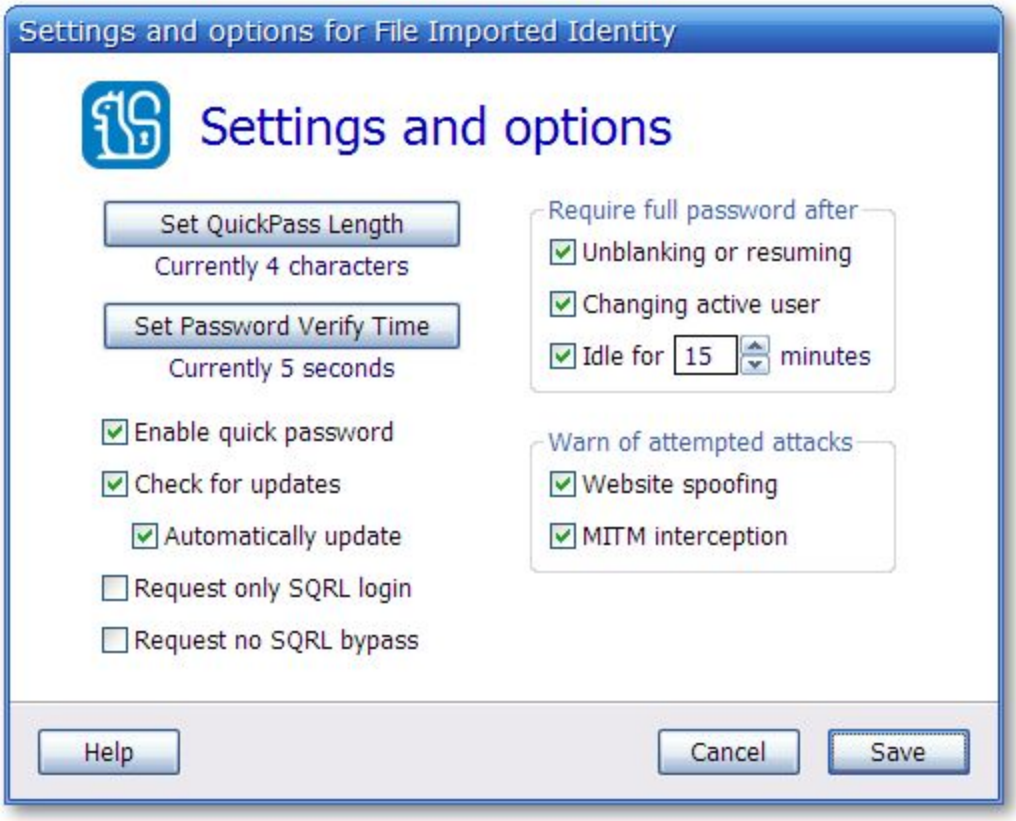
What happened? The attacker managed to convince Verizon that he had "changed phones" despite being unable to provide ANY of the previously arranged secret information designed to prevent EXACTLY this from occurring and using only publicly-available billing information.

Q: What's your password?
A: I forgot it.

Q: What's your PIN?
A: Uhhh… It's been so long since I used it, I forgot it too.

Q: Do you have your Verizon billing information?
A: Oh... yes, THAT I have!

Once again... I test SQRL against this:



Hadoop Servers Expose Over 5 Petabytes of Data

- https://www.bleepingcomputer.com/news/security/hadoop-servers-expose-over-5-petabytes-of-data/
- https://blog.shodan.io/the-hdfs-juggernaut/

- Hadoop (named after the toy elephant belonging to the son of one of the project's early originators) is an open-source Apache-based evolution of an original Google project.

- HDFS is the Hadoop Distributed File System.

- Shodan's founder, John Matherly, was curious to see whether, and how many if any, HDFS protocol server's, probably mostly running Hadoop, were exposed to the Internet. And how much data was aggregated behind those servers.

- He found 4,487 instances of HDFS available via public IP addresses -- without authentication -- which were exposing a total of 5,120 TB of data. (5.1 Petabytes!)

- I dug into this a little bit and learned that setting up HDFS security is a bit of a nightmare. It requires far far more configuration, involving Kerberos authentication servers, than just getting something going... so it typically doesn't happen.

Fireball Malware Infects 250 Million Computers Worldwide

- https://threatpost.com/fireball-malware-infects-250-million-computers-worldwide/126027/
- FIREBALL – The Chinese Malware of 250 Million Computers Infected
- http://blog.checkpoint.com/2017/06/01/fireball-chinese-malware-250-million-infection/
- "Rafotech", a Chinese digital marketer, is behind the spread of a malware family called "Fireball" that has turned ~250 million web browsers (their own P.R. claims 300 million) into ad-revenue generating "zombies." Rafotech- or Fireball-laced apps have infected 20 percent of corporate networks around the world.

- Check Point explained in their report published last Thursday that the malware hijacks browsers and generates revenue for the Beijing-based digital marketing agency. Check Point termed this "possibly the largest infection operation in history," adding that the Fireball infections could be turned into a distributor of any other malware family.

- Leo often notes that I (Steve) coined the term "Spyware." This occurred in March of 2000 (a little over 17 years ago) after I downloaded and installed "WinZip" and noticed something foreign running in my machine. It was the "Aureate" adware which many similar "Freeware" apps were bundling. coined the term "spyware" because, aside from providing embedded advertising to freeware, it monitored and logged all programs the user ran and phoned this data home to the Aureate mothership. They claimed this was for monitization of all Aureate-enabled apps, but it was done entirely without user knowledge or approval.

- So... 17 years later, in a VERY different world, we're back here again.

Chrome Flaw Allows Sites to Secretly Record Audio/Video Without Indication

- http://thehackernews.com/2017/05/browser-camera-microphone.html

- Modern web browsers use the WebRTC features of HTML5 to stream audio and video from webpages, allowing teleconferencing, etc. without the need for 3rd-party add-ons.

- Permission IS required *once* on a per-site basis... but that permission is sticky and remains until explicitly revoked.

- Google's Chrome browser shows a red "recording" indication on the tab of any page which is currently streaming the user's microphone and/or camera.

- BUT, the main window tabs are the ONLY place this indication is shown, while pop-up (and pop-under) windows created by previously-enabled sites are also able to enable media streaming.

- This was observed and reported to Google eight weeks ago on April 10th, 2017... and Google replied that it was not a bug because it's not "a valid security issue" and so would not be changed.

- https://medium.com/@barzik/the-new-html5-video-audio-api-has-privacy-issues-on-desktop-chrome-5832c99c7659

- Proof-Of-Concept demo page:
    - https://internet-israel.com/internet_files/webrtc/index.html

Jaff Malware Probe Uncovers Link to Cybercrime Marketplace

- https://threatpost.com/jaff-malware-probe-uncovers-link-to-cybercrime-marketplace/126060/

- From our: "This Was Inevitable" department -- A newly discovered cryptomalware is no longer content to simply encrypt the user's drive and then demand a ransom payment in return for the decryption key.

- The latest "JAFF" malware is being actively spread through an active and aggressive large-scale eMail campaign using PDFs containing embedded MS Word documents which function as the initial ransomware downloader.

- Security researchers have made associations between the Jaff activity and subsequent theft of financial data, leading them to conclude that before encrypting the user's file data, the malware rifles through their drive scraping, copying and forwarding all useful financial information to back-end servers where the data is sold on the dark web... separately from the encryption of the user's data, which then occurs only after everything useful has been obtained.

- Because... of course.

The return of Google Contributor *(kinda)*

- ZDNet: Sick of ads? Now you can pay Google not to see them, plus sites can charge ad-blocker users.
  Google rolls out its wider plan to beat back the threat of ad blockers to revenues.

- http://www.zdnet.com/article/sick-of-ads-now-you-can-pay-google-not-to-see-them-plus-sites-can-charge-ad-blocker-users/
- https://contributor.google.com/v/marketing

- Buy an ad removal pass for the web. The Contributor pass works with your Google account to remove ads from participating sites.

- But but but...
  - Enrollment is now "per site" with ONLY 4 sites at this time??
    Grub Street: (New York Magazine's Food and Restaurant Blog)
    - Each page without ads that you view on Grub Street costs $0.03. You will be informed in advance if Grub Street changes the price.
    - $1 will give you access to 33 pages without ads on Grub Street.
    - You can cancel at any time and you will receive a full refund of your remaining account balance.
  - WWG: (a division of ComicBook) / ComicBook / Popular Mechanics: $0.01

- The original Google Contributor worked on all Google-provide ads wherever you went.

Google: E2EMail research project has left the nest

- https://security.googleblog.com/2017/02/e2email-research-project-has-left-nest_24.html
- https://security.googleblog.com/2014/06/making-end-to-end-encryption-easier-to.html
- https://github.com/e2email-org/e2email

- <quote> E2EMail is a simple Chrome application - a Gmail client that exchanges OpenPGP mail.

  Google writes: E2EMail is not a Google product, it's now a fully community-driven open source project, to which passionate security engineers from across the industry have already contributed.

  E2EMail offers one approach to integrating OpenPGP into Gmail via a Chrome Extension, with improved usability, and while carefully keeping all cleartext of the message body exclusively on the client. E2EMail is built on a proven, open source Javascript crypto library developed at Google.

No, Your Phone Didn't Ring. So Why Voice Mail From a Telemarketer?

https://www.nytimes.com/2017/06/03/business/phone-ringless-voicemail-fcc-telemarketer.html
A company called "All About the Message" is asking the F.C.C. to rule that its "direct to voice mail messages" are not phone calls, and therefore can be delivered by automatic telephone

dialing systems using an artificial or prerecorded voice. In its petition, the company argued that the law "does not impose liability for voice mail messages" when they are delivered directly to a voice mail service provider and subscribers are not charged for a call.

They wrote: "The act of depositing a voice mail on a voice mail service without dialing a consumers' cellular telephone line does not result in the kind of disruptions to a consumer's life — dead air calls, calls interrupting consumers at inconvenient times or delivery charges to consumers."

The underlying technology was developed by a company named "Stratics Networks" whose somewhat ironically named CEO "Josh Justice" said that their technology, which can send out 100 ringless voice mail messages per minute, had existed for 10 years and had not caused a widespread nuisance. It was intended for businesses like hospitals, dentist's and doctor's offices, banks, and shipping companies to reach customers, for example, and for "responsible marketing."

The Republican National Committee (RNC), which is in favor of ringless voice mail, goes as far as to argue that prohibiting direct-to-voice-mail messages may be a violation of free speech. Telephone outreach campaigns, it said, are a core part of political activism. In the RNC's letter to the FCC, they wrote: "Political organizations like the R.N.C. use all manner of communications to discuss political and governmental issues and to solicit donations — including direct-to-voice-mail messages."

Consumer Complaints:
https://consumercomplaints.fcc.gov/hc/en-us/requests/new?ticket_form_id=39744
Public Comments Solicited:
https://www.fcc.gov/ecfs/search/filings?q=(proceedings.name:((02-278*))%20OR%20proceedings.description:((02-278*)))&sort=date_disseminated,DESC

Miscellany

- Monument Valley II
- Yesterday, Monument Valley II, the sequel to the 2014 iPad game of the year.
- $5 for iOS (Android release coming soon) by Ustwo Games
- More than 30 Million downloads of the first version.
- The success of the first release put huge pressure on the original 8-person team to give the world more. But until yesterday they had only managed to create the small "Forgotten Shores" extension to the original.
- After that, the 8-person company felt burned out on the concept and wanted to do something else. But today, three years later, the company is 20 people and ALL of the new hires came to the company because they loved Monument Valley. They brought a ton of new ideas and reinvigorated the entire concept.
- Our listeners know that I most enjoy relaxing, thoughtful, cerebral and non-temporal (reflexes optional) puzzle games . Monument Valley I was wonderful and I look forward to taking my time to move through Monument Valley II.

SpinRite

Al Spaulding (Al Spaulding) / 6/3/17, 11:23 AM
Steve, Another SpinRite story. I started getting Outlook errors, like can't load profile, and eventually, Outlook would not load at all. Company IT looked at it and created a new "profile". That worked for about 24 hours, then it all started again.

Al Spaulding (Al Spaulding) / 6/3/17, 11:23 AM
Finally, ran SpinRite and no problems for 5 days now. Thanks for a great product.

Homomorphic Encryption

- A neat data sharing technique

- https://stuartward.wordpress.com/2017/06/02/a-neat-data-sharing-technique/

- From Wikipedia: Homomorphic encryption is a form of encryption that allows computations to be carried out on ciphertext, thus generating an encrypted result which, when decrypted, matches the result of operations performed on the plaintext. https://en.wikipedia.org/wiki/Homomorphic_encryption

- Stuart Ward (@stuartward) / 6/2/17, 1:24 PM
  @SGgrc I work for visa and that is where Google is getting the data. We believe they are also getting similar from MasterCard but not privy to that

- The key is that RSA encryption is a commutative process like multiplication:
  - A x B x C … / B … == A x C

Closing The Loop

Robert (@Really_Evil_Rob) / 6/2/17, 11:18 PM
@SGgrc I've been thinking about your system of printed QR codes for your authenticator tokens. What about saving them to a USB flash drive?

~30~