Security Now! #620 - 07-18-17

Calm Before the Storm

This week on Security Now!

This week, while waiting for news from the upcoming BlackHat & DefCon conventions, we discuss another terrific security eBook bundle offer, a Net Neutrality follow-up, a MySpace account recovery surprise, another new feature coming to Win10, the wrong-headedness of paste-blocking web forms, Australia versus the laws of math, does an implanted pacemaker meet the self-incrimination exemption?, an updated worse-case crypto-future model, it's surprising what you can find at a flea market, another example of the consumer as the product, a SQRL technology update, and some closing-the-loop feedback from our terrific listeners.

"We have patched that vulnerability you reported..."

Security News

Another security-oriented Charitable Donation Humble Bundle offering:
https://www.humblebundle.com/books/cybersecurity-wiley

$1 or more:

- Social Engineering: The Art of Human Hacking
- The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws, 2nd Edition
- Practical Reverse Engineering: x86, x64, ARM, Windows Kernel, Reversing Tools, and Obfuscation
- Threat Modeling: Designing for Security

For $8 or more and ALSO receive:

- Security Engineering: A Guide to Building Dependable Distributed Systems, 2nd Edition
- The Shellcoder's Handbook: Discovering and Exploiting Security Holes, 2nd Edition
- Cryptography Engineering: Design Principles and Practical Applications
- The Art of Deception: Controlling the Human Element of Security
- The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory

For $15 or more, ALSO receive:

- Malware Analyst's Cookbook and DVD: Tools and Techniques for Fighting Malicious Code
- Unauthorised Access: Physical Penetration Testing For IT Security Teams
- Secrets and Lies: Digital Security in a Networked World, 15th Anniversary Edition
- CEH v9: Certified Ethical Hacker Version 9 Study Guide
- Applied Cryptography: Protocols, Algorithms and Source Code in C, 20th Anniversary Edition

Looks like the offer runs through the end of July.
I think every listener who discovered this shot me a tweet to make sure I was aware. So on behalf of all of us, a big thanks to everyone who made sure I knew!

Wednesday, July 12th, was "The Internet-Wide Day of Action to Save Net Neutrality"
(not really a very catchy title).

Then, yesterday, major tech companies clashed with internet service providers over whether this landmark 2015 net neutrality order barring the blocking or slowing of web content should be scrapped by the U.S. Federal Communications Commission.

The Internet Association, which represents major technology firms including Alphabet, Facebook, Amazon, Microsoft, Netflix, Twitter, Snap and many others urged the FCC to abandon plans to rescind the rules barring internet service providers from hindering consumer access to web content or offering paid "fast lanes", writing that dismantling the rules "will create significant uncertainty in the market and upset the balance that has led to the current virtuous circle of innovation in the broadband ecosystem."

Meanwhile, major internet service providers including AT&T, Comcast and Charter Communications and Verizon urged the FCC to reverse the rules enacted during former President Barack Obama's administration... while vowing not to hinder internet access.

Verizon said the Obama order had "injected uncertainty into the marketplace, restricted innovation, and chilled investment." It called the prospect of future rate regulation "a toxic approach if the goal is to encourage investment or the entrance of new competitors into the market."

Comcast said the order "represented an unfortunate, unnecessary, and profoundly unwise wrong-turn for the broadband economy and consumers more broadly."

AT&T said the FCC in 2015 "grossly exaggerated the need for public-utility-style regulation while ignoring its costs."

The month before last, the FCC voted 2-1 to advance the FCC Chairman Ajit Pai's plan to withdraw the former Obama administration's order reclassifying internet service providers as if they were utilities. The problem is, access the Internet has evolved from a luxury to a near-necessity. And in every meaningful way its provision is no different from electricity. When I purchase electricity from, in my case, Southern California Edison, I pay the same price for, and the electricity flows just as well to my air conditioner as to my coffee pot, and this is true even IF SoCal Edison owns their own air conditioning company. They are not permitted to charge me a higher rate if I use a competitor's air conditioner. But you can imagine that in such a situation they would love to if they could, to subsidize their own private interests at the expense of the competition... and ultimately at the expense of the public.

The FCC Chairman argues that the Obama order unnecessarily harms jobs and investment. So he has not committed to retaining ANY rules, saying that he favors an "open internet." But this appears to mean an "unregulated Internet." And as a proud capitalist myself I would be happy to have that if we also had choice among providers. But the first thing the various Internet providers have done was to deliberately remove competition. Recall how, on this podcast in years past we have noted the series of mergers of already massive providers into fewer and fewer. And as I've often noted I have exactly one choice of broadband provider: Cox Communications. And Cox offers their own pay per view and movie streaming services. So they certainly see the likes of NetFlix and other content providers as competition.

Meanwhile, the Internet Association said there was “no reliable evidence” that investment by providers had fallen.

Twelve state attorneys general including from Illinois and California urged the FCC not to overturn the Obama rules, saying that would "expose consumers to the risk that their internet access will be interfered with and disrupted."

More than 8.4 million public comments have been filed on the proposal (it would be nice to know whether that was bot-filtered or not)

And tomorrow, Wednesday, July 19th, Pai will face questions on the issue during a U.S. Senate

hearing.
I'll make a non-partisan observation that, mostly, I'm troubled that we're seeing such an expanded use of executive orders in place of Congressional legislation. It's true that congress moves slowly and with great deliberation (when it moves at all.) But that's the way it was designed to function. The inertia means that things change gradually only after being examined and debated at length and that they can be tuned and tweaked as needed over time. But, when issues become politically partisan, with the party holding the office of the executive switching back and forth as the country experiments with different leadership styles, we wind up creating a climate of tremendous uncertainty... which is arguably the worst of all worlds. In this case president Obama's administration put this in place by executive order and president Trump's is considering removing it. I hope that congress finds the will to consider this important issue at length, and take it once and for all, out from under ANY president's pen... except to sign that new legislation into law.

MySpace: Where nearly half a billion past users' personal "zombie data" lives on...
In May of 2016 we discussed the fact that MySpace lost control of 427 million passwords which were offered to buyers for $2,800.

Yesterday, a frustrated security researcher at Positive Technologies by the name of Leigh-Anne Galloway, finally disclosed a troubling vulnerability after having first responsibly disclosed the issue to MySpace nearly three months ago... in reaction to which MySpace was irresponsibly silent.

Leigh-Anne described MySpace as "an enormous graveyard of personal data" and noted that companies have a duty of care to users, both present AND past. Leigh-Anne told Motherboard, who reported on this, that when she discovered the flaw she was "horrified" and "shocked" by "the complete lack of due diligence" on MySpace's part.

So what's the problem?

Unlike nearly every other password recovery system, which is at least anchored to a user-controlled eMail address, MySpace offers an account recovery process for people who have ALSO lost access to their email account.

At first glance this doesn't look too bad, since MySpace presents a comprehensive and somewhat intimidating form asking for a great many of an individual's details:

http://myspace.desk.com/customer/widget/emails/new?t=150416

The form states that ALL of the following information MUST be provided, including the email address associated with profile, date of birth, zip code listed on account, name listed, the city and state of the account owner.

But, it appears that some heuristic logic operating behind the scenes processes the form's data so as to minimize support costs. So it likely has an "if any three or more are valid in the whole form" acceptance threshold.

Consequently, what Leigh-Anne discovered and reported, and MySpace ignored, was that anyone having ONLY a MySpace user's full name, username, and date of birth is able to establish themselves as the new owner of any existing MySpace account.

In their reporting, Motherboard verified this, writing: "Once we finished the recovery process we had full access to two accounts: we could write new posts, read old messages, and basically do whatever the account owner's could do. (Thanks again to the two brave volunteers who let us break into their old MySpace accounts.)

"Do Not Have Access To Old Email Address"
https://help.myspace.com/hc/en-us/sections/200421370-Log-in

That form page above can be used to delete your profile, and they also provide a specific page for doing so: "Delete your Profile"
https://help.myspace.com/hc/en-us/articles/202241380-Delete-your-Profile

We have recommended in the past that our listeners proactively remove any residual MySpace accounts. So this is a reminder that doing so is still a good idea.

Speaking of account recovery...
Windows 10 Fall Creators Update will be adding an "I forgot my password" option to Windows 10's login/lock screen.

Apparently this is a much-requested feature which has appeared in the latest preview of Windows 10 Fall Creators Update.

People configured to use Windows Hello mode or a PIN will also be able to access the new password reset option by going to the other sign-in options.

Once the password reset process has been started Windows 10 Cortana will guide the user through the reset process. Cortana will first ask the user to verify themselves with a secondary eMail, test message or Authenticator app. Once verified the user will be allowed to reset their password.

Speaking of passwords...
A listener's tweet reminded me that one thing we haven't discussed is the counterproductive practice which some brain dead websites have started adopting of blocking form fill automation. Naturally, this fights against password managers, and even those who use an old school offline password database or text file, then manually copy and paste to transfer a complex password into the online web form.

Since this makes absolutely no sense, and I cannot see any rational right-thinking justification for the practice, I did some digging around to see whether there was some hidden benefit that hadn't occurred to me.

Troy Hunt is a well known security researcher who writes a widely read blog. His short bio states that he creates courses for Pluralsight, is a Microsoft Regional Director and MVP who travels the world speaking at events and training technology professionals.

Troy examined this question a little over three years ago under the heading of "The Cobra Effect" with a fun anecdote about the mistake the British made way back when they were in a conquering mood. They encountered a problem on the subcontinent of India: cobras. Turns out there were a lot of them wandering around India and taking bites out of the British. Ingenious as the Brits were, they decided to offer a bounty on cobras in the hopes that the indigenous inhabitants would round'em up in return for cash. But this turned cobras into a form of currency that could be bred... so cobra breeding became a thing, and after the British saw the error of their ways and terminated the bounty, the excess cobras were released back into the wild, which of course resulted in the cobra problem now being worse than it originally was.

https://www.troyhunt.com/the-cobra-effect-that-is-disabling/

But... I digress. Troy's analogy was meant to make the point that sometimes trying to fix something to make it better, actually has the reverse effect.

And now I understand why this didn't occur to me. The blocking of login automation is apparently a completely wrong-headed attempt to prevent automated brute force login attempts -- presumably being made by something that's using a web page's automation for brute force login guessing.

But anyone who understands how the web actually works knows that the web browser page is merely a front-end which puts a pretty face onto an eventual HTTP form query. So no sane brute force attacker is going to automate the form, they're going bypass that completely and directly submit the form's data to the remote web server for it's approval or rejection.

Another way to say this is that it's not possible to robustly prevent brute forcing in the web browser client because the browser is trivially bypassed by making direct server queries. Thus, the only people inconvenienced by this ill advised tactic are a site's valid users who simply want to login.

What's stronger? Australian law or the laws of nature?

The first several times people sent me a link to this article in The Guardian I checked out the headline and subhead and thought "okay, we've already covered Australian legislative nonsense." But then around midnight last night, upon encountering another link, I finally read into the article and the quotes were so far beyond cringe-worthy that I needed to share it.

The headlines were of little surprise. They read: "New law would force Facebook and Google to give police access to encrypted messages." Subhead: "Under government plan, internet companies would be obliged to give law enforcement agencies warranted access."

Malcolm Turnbull said on Friday the law would be modelled on Britain’s Investigatory Powers Act, passed in November, which gave intelligence agencies some of the most extensive surveillance powers in the western world.

Under the law, internet companies would have the same obligations as telephone companies to help law enforcement agencies. Police would need warrants to access the communications. Turnbull said the legislation was necessary to keep pace with advances in technology that could facilitate crime.

"We need to ensure that the internet is not used as a dark place for bad people to hide their criminal activities from the law," he said.

(Here it comes...)

Asked by reporters how legislation would prevent users simply moving to encryption software not controlled by tech companies, Turnbull said Australian law overrode the laws of mathematics. "The laws of Australia prevail in Australia, I can assure you of that. The laws of mathematics are very commendable, but the only laws that apply in Australia is the law of Australia."

(O... kay.)

Turnbull denied the government's plans involved the use of a "back door" into programs to allow access to encrypted messages on platforms such as WhatsApp and Telegram.

"A back door is typically a flaw in a software program that perhaps the developer of the software program is not aware of, and that somebody who knows about it can exploit," Turnbull said. "If there are flaws in software programs, obviously, that's why you get updates on your phone and your computer all the time. So we're not talking about that. We're talking about lawful access."

(Okay. Translation: Apparently if it's a lawful backdoor then, by definition, it's not a backdoor... it's a handy new feature.)

Then, pressed on whether the government's plans meant it would ask companies such as Facebook and Apple to keep a copy of encryption keys used by customers, Turnbull said:

"I'm not a cryptographer (yeah... surprise!), but what we are seeking to do is to secure their assistance (that is... the assistance of actual cryptographers. Although I would argue that it's less "seeking their assistance" than "compelling their assistance.") "They have to face up to their responsibility. They can't just, wash their hands of it and say it's got nothing to do with them."

The attorney general, George Brandis, said the legislation would "impose an obligation upon device manufacturers and service providers to provide appropriate assistance to intelligence and law enforcement on a warranted basis". It could be used to tackle terrorism, or serious organized crime such as paedophile networks. (That's right, march out the criminal sexual molesters... their rights to privacy are much more difficult to defend.)

Brandis said: "It is vitally important that the development of technology does not leave the law behind." Brandis said the bill, which would be introduced to parliament by November, would allow courts to order tech companies to quickly unlock communications

Australian Federal Police deputy commissioner Mike Phelan said “the vast majority” of investigations now involved some sort of encryption.

“Whether that’s encryption of phones, whether it’s encryption of computers that we seize or whether ... it’s traffic that goes between conversations over the internet, then that’s the sort of thing that we need to get behind. At the end of the day, what has happened here is legislation has not yet kept pace with technology.”

(Indeed... still, somehow Australian Law overrides mathematical law.)

First it was a smart water meter, then a listening audio home device...
Now it's a suspect's own heart rate as recorded by his own implanted pacemaker.
Engadget's headline reads: "Judge allows pacemaker data to be used in arson trial"
Sub: The suspect tried and failed to get the judge to disregard his own heartbeat as evidence.

We covered this story at the time...

Recall that authorities in Ohio arrested a man named Ross Compton on the charge of arson and insurance fraud based on his pacemaker data. Compton told the police that when he saw his house burning on September 19th last year, he packed his suitcases, threw them out his bedroom window and carried them to his car. However, since has a serious heart condition and other medical issues that would have made it extremely difficult for him to do all of that, investigators were able to secure a search warrant for his pacemaker data.

According to court documents, a cardiologist who reviewed his heart rate, pacer demand and cardiac rhythms before, during and after the fire said:

"...it is highly improbable Mr. Compton would have been able to collect, pack and remove the number of items from the house, exit his bedroom window and carry numerous large and heavy items to the front of his residence during the short period of time he has indicated due to his medical conditions."

That data became a key piece of evidence that allowed law enforcement to indict the accused, though they also detected gasoline on his shoes and clothing.

I should note that the EFF is not too happy about this. Stephanie Lacambra, an Electronic Frontier Foundation staff attorney told SC Magazine at the time that cases like this "could be the canary in the coal mine concerning the larger privacy implications of using a person's medical data." She explained: "Americans shouldn't have to make a choice between health and privacy. We as a society value our rights to maintain privacy over personal and medical information, and compelling citizens to turn over protected health data to law enforcement erodes those rights."

Ross's attorney tried to convince the court to disregard that evidence, arguing that it was obtained in an illegal search. But the judge who heard the case didn't see it that way. He has decided to allow the suspect's pacemaker results to be used as evidence against him in an upcoming trial.

However, something the judge said is troubling...

Engadget reported that Judge Charles Pater said he does not think the data's use has bigger privacy implications, but his exactly quote makes even that rather murky: "There is a lot of other information about things that may characterize the inside of my body that I would much prefer to keep private rather than how my heart is beating. It is just not that big of a deal."

TechDirt's Karl Bode posted yesterday under the (Mis)Uses of Technology

I want to share this piece of reporting, then further stretch our thinking about the possible future of Internet encryption...

The global war against privacy tools, VPNs and encryption continues utterly-unhinged from common sense, and the assault on consumer privacy remains a notably global affair. Reddit users recently noticed that India's fifth largest ISP, YOU Broadband, is among several of the country's ISPs that have been trying to prevent customers from using meaningful encryption. According to the company's updated terms of service, as a customer of the ISP you're supposed to avoid using encryption to allow for easier monitoring of your online behavior:

"The Customer shall not take any steps including adopting any encryption system that prevents or in any way hinders the Company from maintaining a log of the Customer or maintaining or having access to copies of all packages/data originating from the Customer."

Of course enforcement of such a requirement is largely impossible. [This is what I will address in a minute, because it is actually and significantly incorrect.]

But You Broadband isn't just being randomly obtuse, and while the ISP's TOS is making headlines, this effort isn't really new. Most Indian ISPs are simply adhering to a misguided (and still not adequately updated) set of 2007 guidelines imposed by India's Department of Telecommunications (word doc) demanding that ISPs try and prevent their subscribers from using any encryption with greater than a 40 bit key length if they want to do business in India:

"The Licensee shall ensure that Bulk Encryption is not deployed by ISPs connecting to Landing Station. Further, Individuals/Groups/Organizations are permitted to use encryption upto 40 bit key length in the symmetric key algorithms or its equivalent in other algorithms without having to obtain permission from the Licensor. However, if encryption equipments higher than this limit are to be deployed, individuals/groups/organizations shall do so with the prior written permission of the Licensor and deposit the decryption key, split into two parts, with the Licensor."

Which is and of itself is rather hysterical, given that since 1996 or so, most folks have considered a 40 bit key length to be the security equivalent of wet tissue paper. In fact, Ian Goldberg won $1,000 from RSA for breaking 40 bit encryption in just a few hours way back in 1997, saying this at the time:

"This is the final proof of what we've known for years: 40-bit encryption technology is obsolete."

And yeah, that was twenty years ago. But this sort of policy is pretty standard fair in India, which is no stranger to censorship, internet filtering, and blind, often-mindless expansion of surveillance. India's government has also been at the forefront of attempting to impose backdoors in encryption, and there's a recent effort in some corners to attempt to ban Whatsapp as well.

I've yet to see any ISP successfully enforce this ridiculous governmental restriction. But it's still part of an over-arching mindset that sees standard, intelligent privacy and security practices as an enemy that must be thwarted. Usually either to expand government surveillance, prop up idiot ham-fisted internet filters (as we're seeing in Russia, China and India), or to erode consumer rights in the face of what are endless attempts to monetize your online behavior.

The problem is: ISPs COULD technically enforce this, as a consequence of the use of encryption standards and historical support of shorter keys. In the past, we've discussed TLS downgrade attacks. The trouble is that while an encrypted channel is being established, the pre-encryption setup is necessarily performed in the clear. The client openly shares the list of encryption protocols it supports, and from among those the server picks the best one that it also supports. One of the past -- and now abandoned -- encryption standards is the use of "export grade" 40-bit symmetric keys. The point is... the code is out there and it would be interesting to see what would happen if India were to actually enforce this upon their ISPs, because it is technically -- if not practically -- feasible. And it would be interesting and entertaining to see. This would, of course, require the use of web browser which once again offered to use weaker 40-bit symmetric key protocols, and -- more significantly -- it would also require any server connected to, to also support 40-bit symmetric encryption protocols.

Since requiring the world's servers to return to obsolete and weak encryption only to allow permitted low-security connections from visitors in India seems is unlikely. But there's an intermediate step, again, if Indian government was really determined about this: Indian ISPs could establish cross-strength encryption proxies. The Indian ISPs could require their customers to use browsers supporting 40-bit protocols and to also accept that ISPs PKI CA root certificate. The "cross-strength" proxy would enforce 40-bit encryption to the customer while offering globally-compatible full-strength encryption to the world's web servers.

Of course, this leads us back around to the most probable (dreaded) future, which really worries me because it's so possible, where all of an ISP's customers are required to accept their ISP's CA root cert. Or, even more likely, legislation requires that today's established certificate authorities provide pre-trusted intermediate certificates to ISPs which have the ability to sign server certificates.

This is what Google did which allows them to mint their own certs. Google obtained a certificate authority certificate from the GeoTrust Global CA. That certificate is the "Google Internet Authority G2" and is used to sign Google's end-point server certificates.

And PLEASE don't get me wrong. I'm not saying that I think this is a good idea. I shudder at a possible future where every, or any, mom and pop ISP is able to legally obtain a signing certificate used to intercept, decrypt, log, and reencrypt their customer's web traffic. I'm just saying... it's possible. Our previously articulated model of this nightmare scenario seemed safer

and less likely to occur because every customer device would have needed to have a custom ISP CA root certificate installed. But if ISPs, themselves, are allowed to obtain CA certificates from our existing root CAs -- much as Google has -- then the scenario where our connectivity providers are able to perform so-called "deep packet inspection" of our traffic becomes an immediate reality.

And not only that, there's another architectural possibility:

For an ISP to intercept ALL of the customer traffic would be hugely burdensome. So it might be that either (a) ISPs are able to respond to law enforcement requests for monitoring of specific customers, or (b) that they are NOT able to, themselves, intercept and decrypt their customers' traffic, but that they can selectively forward specific customer traffic to a central law enforcement proxy which contains an already-trusted intermediate CA certificate and is, therefore, able to decrypt and inspect all of the traffic running through it.

To me, this second design seems like the most technically feasible solution. It minimizes distributed trust by keeping it centralized. In the US it follows and maintains the existing constitutional model of lawful search-warranted intercept, and it only requires ISPs, who are already routing traffic, to be able to selectively route specific customers' traffic to a central law enforcement hub.

Browsers such as Chrome which deliberately pin the fingerprints of Google's known endpoint certificates would be modified to check the chain and accept certificates signed by the US government law enforcement intermediate CA certificate.

It was an Enigma...
http://www.bbc.com/news/world-europe-40583718

BBC News:
So... a cryptography professor is wandering through a flea market spots a "typewriter" for sale for 100 Euros. Immediately recognizing it for what it actually is, a original model I German Enigma machine, he expresses mild interest and hands the seller 100 EU, smiles, and walks off with a Enigma machine. That machine later sold at auction for 45,000 euros, so a handy profit. But he may not have obtained the best value possible. Perhaps his machine was in less than pristine condition, or the pool of available bidders was too small or mistargeted, since last month the famous Christie's auction house in New York sold an Enigma machine for $547,500.

Speaking of typewriters: The standard keyboard on the HTC 10 has begun showing ads
https://www.reddit.com/r/mildlyinfuriating/comments/6nhyur/the_standard_keyboard_on_the_htc_10_has_begun/

Miscellany

SQRL's Install/Update/Uninstall technology
Integrated. UAC-friendly. Requires a brief privilege elevation.
The SQRL executable is signed with a DigiCert Authenticode certificate. But that in itself doesn't provide sufficient security, since today's high quality trusted software is signed with Authenticode. So any random attacker could similarly sign their own malware. To prevent this, after downloading an update as a temporary file, SQRL's self-updater not only validates that new download's Authenticode signature, but also verifies that the certificate was issued to "Gibson Research Corporation" and that the issuer was "DigiCert."

Pinning the certificate to the "Issued By" and "Issued To" identities is not QUITE as strong as pinning it to the certificate's fingerprint. But, as we know, certificates expire every few years. So pinning updates to a specific certificate would require updates to contain the fingerprints of not yet valid future certificates so that the update process could straddle the signing certificate's lifetime. And that seems like overkill. By simply verifying that the SQRL certificate was issued to Gibson Research Corporation by DigiCert, we're able to transparently straddle individual certificate expirations, while preventing any use of aberrant certificates.

Errata:

Whoops... SpinRite is 30 years old, not 40!

SpinRite

Michael
Location: Glasgow ('Glass-go'), Scotland
Subject: What's heavier, 1 ton of zeros or 1 ton of ones?

Hey Steve,

Long time spinrite user here - it's an amazing product, that I, like many of your listeners, treasure.

I was thinking about Oxford's question from episode 617, on whether it's better to 'spinrite' before formatting a drive or after. The intuition he had about it probably making no difference is interesting. You agreed with him, of course.

My question is this. Does spinrite take the same amount of *time* in both cases? Say that there's a 1TB drive chock-full of years of data and detritus, but in good working order with no serious problems.

Will spinrite finish working in the same amount of time as a blank, completely empty 1TB drive fresh out of the factory? I've never tried it but I guess it must? My gigantic folder structures and sizeable data files have never felt so light!

Closing The Loop

This is Nighthawk! (@shadyhotdog)
DNSThingy is amazing! Flashed my ASUS router with their firmware and now I can do all sorts of cool stuff! Thanks @SGgrc

Byron Lee (@byron27)
@SGgrc Steve, my security conscious friends won't touch my mobile Facebook Live video streams. What is a good simple alternative?

Matt Warner (@_mwarner)
@SGgrc Looks like @Twitter disabled 2FA using push notifications, and now uses SMS only. Is it better to not use 2FA at all?

Jerry Yu (@hweetty)
@SGgrc On #SN619 you mentioned Broadcom exploit that got patched for Android. Looks like patched in iOS 10.3.1: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6975
Quote: "Wi-Fi in Apple iOS before 10.3.1 does not prevent CVE-2017-6956 stack buffer overflow exploitation via a crafted access point."

Michael Rickman (@lstlaugh)
@SGgrc uh, did you see this?
https://www.indiegogo.com/projects/fuze-card-your-whole-wallet-in-one-card-money-technology#/
Fuze Card: Your Whole Wallet in One Card
Secure, Slim, Convenient. Electronic Card with EMV Chip. Holds Up to 30 Credit, Debit, or Gift Cards

qrex (@qrex)
@SGgrc Confused re: sn619 HTML5.
So privacy and security are good, unless it's media, and it's between a company and their subscribers? Explanation?

The MPAA fought mightily to completely prevent the commercialization of consumer home recording. When that inevitably failed, content providers attempted to thwart the consumer's LEGAL RIGHT to make copies of their legally obtained media. Early analog VHS tapes were "protected" with a system known as Macrovision which deliberately messed up the Automatic Gain Control (AGC) of recorders, preventing the duplication of such protected content. This also lowered the delivered quality of the result, but the publishers didn't care. It also didn't work. Before long, Macrovision stripping boxes appeared which removed that protection. So it increased the cost of everything, reduced the quality of the result... and didn't prevent anyone who actually wanted to make a copy from doing so. Pirates continued to pirate.

In the US, our copyright laws provide exception for "fair use", but media DRM does not honor that right. The most famous example are DVD's whose encryption was broken long ago, allowing owners of those DVD's to legally -- even if against the overly restrictive expressed wishes of the media's publisher -- rip and decrypt DVDs for more convenient (and more reliable) storage and use..

And more recently we have HDMI's HDCP (High-bandwidth Digital Content Protection) which forces another significant compromise. Once upon a time it was possible to instantly switch media sources and destinations -- in the blink of an eye. But that smooth operation has been messed up by HDMI's HDCP. Now, when switching, it's necessary to wait for at least several seconds for the endpoints to renegotiate their secure connection... and when that fails as it occasionally does, it's necessary to switch away and back again, and hope. And HDCP limits cable lengths which can be used because it's the most finicky protocol in the system. And HDCP, also, has been completely bypassed. The market is full of $39 Chinese HDMI HDCP decrypting / capture cards which contain all of the standardized and the well-known HDCP keys and render the entire system ineffective. If pirates wish to pirate, they can and do. But in the meantime everyone else, all legal and legitimate users, suffer a significantly lower quality experience... because the MPAA once again won their legislative lobbying victory.

So.... will the web be any different? Of course not. It will be every bit as possible for pirates to decrypt and capture web-delivered media as it has been for them all along the way. You can place your bets on that right now. The people who realistically understand this know that we're going to get a fragile and unnecessarily complex system which will be less comfortable and convenient for legitimate and legal use, while doing little to actually thwart those who are intent upon pirating the web-delivered content.

The bottom line is... what the MPAA and RIAA want is simply impossible for technology to deliver. Yet the money WE have paid THEM allows them to continually screw up -- with no apparent success -- their media's delivery channel.

So, yeah... this is a bit different from protecting our logon password and session cookies.

Simon Zerafa (@SimonZerafa)
@SGgrc Prediction of the Week: Windows 7 will not sunset on schedule.
To many businesses still using it ??

~30~