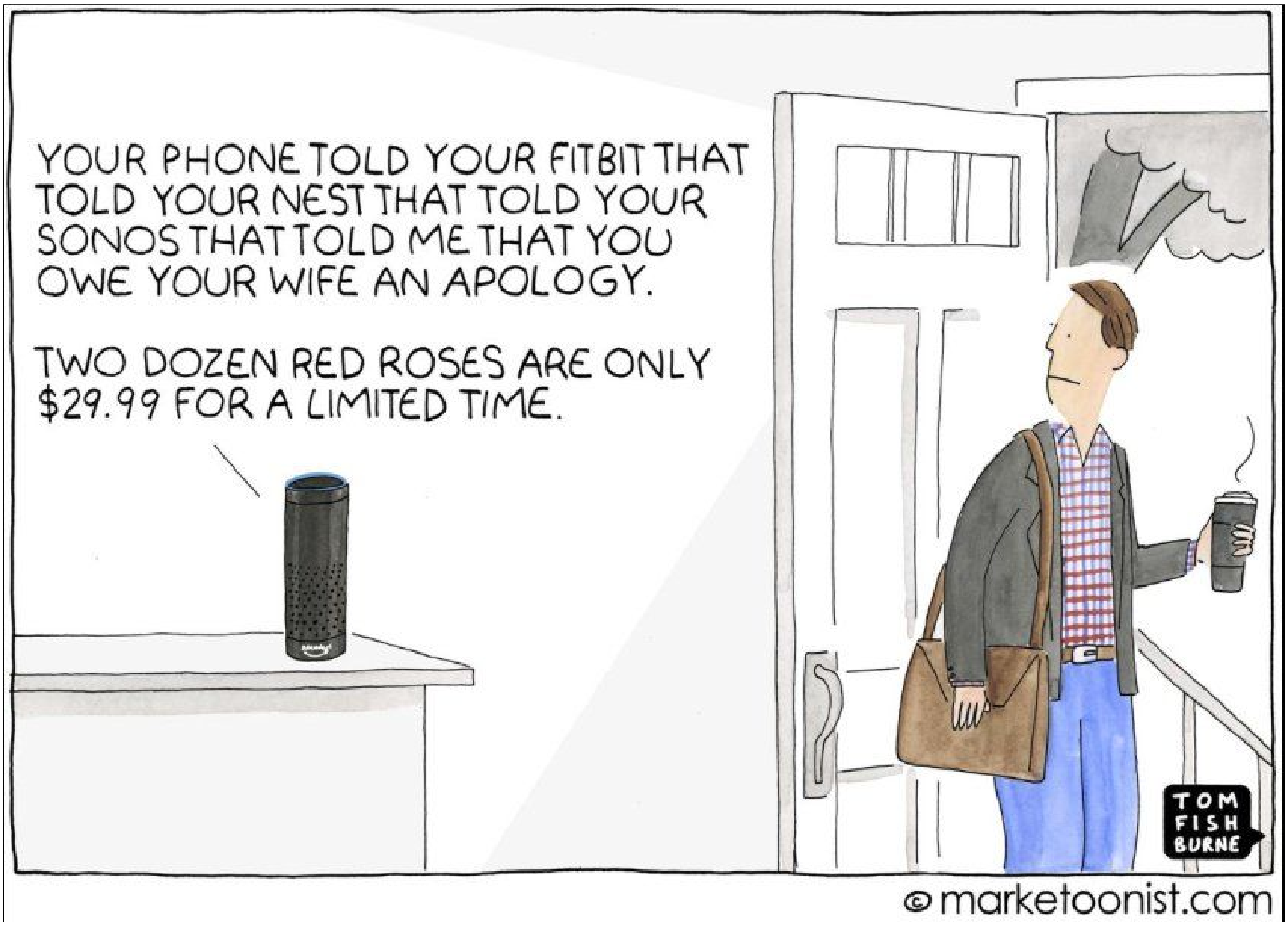
Security Now! #596 - 01-24-17

Password Complexity Calculations

This week on Security Now!

While still on probation Symantec issues additional invalid certificates, Tavis Ormandy finds a very troubling problem in Cisco's Web conferencing extension for Chrome, yesterday's more-important-than-usual update to iOS, renewed concerns about LastPass metadata leakage, the SEC looks askance at what's left of Yahoo, a troubling browser form auto-fill information leakage, Tor further hides its hidden services, China orbits a source of entangles photons?, Heartbleed three years later, a new take on compelling fingerprints, approaching the biggest Pwn2Own ever, some miscellany... and some tricks for computing password digit and bit complexity equivalence.


YOUR PHONE TOLD YOUR FITBIT THAT TOLD YOUR NEST THAT TOLD YOUR SONOS THAT TOLD ME THAT YOU OWE YOUR WIFE AN APOLOGY.
TWO DOZEN RED ROSES ARE ONLY $29.99 FOR A LIMITED TIME.
TOM FISH BURNE
© marketoonist.com

Security News

While still on probation for misissuing certificated in 2015, three Symantec-owned CAs were discovered to have improperly issued additional illegitimate HTTPS certificates.

- Andrew Ayer, a security researcher and founder of a certificate authority reseller known as SSLMate was browsing through the public "Certificate Transparency Log" maintained by Google's Certificate Transparency project... and he noticed some oddities... totaling 108 unvalidated certificates.

- Nine of the certificates were issued without the permission or knowledge of the affected domain owners.

- The remaining 99 certificates were issued without proper validation of the company information in the certificate.

- Those certificates would have enabled their holders to spoof the identities of HTTPS-protected websites.

- Even though many of the certificates issued contained the string "test" in various places, and were revoked within an hour of issuance, it is nevertheless another significant violation by Symantec or Symantec-owned CAs.

- The fact they were revoked shortly after issuance doesn't lessen the severity, because, as we all well know after the campaign I myself went on once I realized how totally broken Google's Chrome browser certificate revocation system was (it doesn't actually work at all) the most-used browser in the industry would continue to honor these certificates until and unless they were manually added to the browser's "CRLSET" list... which normally only lists revoked EV certs.

- The certificates were issued by the Symantec Trust Network, GeoTrust Inc., and Thawte Inc.

- On July 14, October 26, and November 15. The other 99 certificates were issued on many dates between October 21 and January 18.

- And as for the Certificate Transparency log... Google usually requires CAs to report only the issuance of EV (extended validation) certificates, which provide a higher level of trust due to the much more stringent verification of the holder's identity provided, well beyond just asserting control of the domain. But following Symantec's earlier 2015 mishandling, Google required Symantec to log EVERY certificate issued by the CAs it owns. Had Symantec NOT been required to report all certificates, it's highly unlikely that the violation would have ever come to light.

- Links:
    - https://www.certificate-transparency.org/

Yesterday, our old friend Tavis Ormandy was at it again...
https://bugs.chromium.org/p/project-zero/issues/detail?id=1096

- Cisco: Magic WebEx URL Allows Arbitrary Remote Command Execution

- There was a secret URL embedded into Cisco's WebEx browser extension that allowed any website to run arbitrary code:
  - "Cwcsf-nativemsg-iframe-43c85c0d-d633-af5e-c056-32dc7efc570b.html"
  - The trouble was… it wasn't bound to any web domain, allowing any site or advertisement to use the overly-powerful Cisco API.

- Cisco WebEx is Online Meetings and Video Conferencing.

- Sloppy coding in the WebEx extension for Chrome was discovered by Tavis Ormandy.

- It would have allowed no-user-interaction privileged remove code execution on any of the 20+ million machines where the WebEx extension is present in the Chrome browser. This would, for example, allow any malicious website (or advertisement you accept since it works in iframes) to silently install malware.

- The presence of a "magic URL" enabled scripting-like access to a powerful Cisco-supplied DLL which Tavis was able to leverage to execute the "calc.exe" app on the user's desktop.

- To their credit, Cisco responded VERY quickly with an update (same day over the weekend).

- Tavis was impressed by Cisco's response speed, but not so much with their fix: they now limit the use of the magic URL to the set of origins: https://*.webex.com/...

- Tavis accepts the update, but hopes that the Cisco WebEx.com site doesn't have lots of XSS problems... since now the only protection is the "same origin" lockdown... but as we know, XSS allows an attacker to inject scripting that runs as if from the vulnerable website... and would thus bypass the somewhat weak protection afforded by the URL's origin protection.

- You need v1.0.3
  - But this only presents an insufficiently frightening pop-up if you are NOT at *.webex.com.
  - So a superior solution, if you are a WebEx user, is to:
    - Uninstall WebEx
    - Create a new user profile in Chrome
    - Install WebEx only in that profile, and switch to that "Webex" profile only when you want to use Cisco's WebEx.

- For more: How to protect yourself from the WebEx extension
  - https://blog.filippo.io/webex-extension-vulnerability/

Monday's iOS update fixed some significant vulnerabilities. Update to 10.2.1 ASAP.

- Most iOS updates seem rather mundane... but Monday's fixes were not. https://support.apple.com/en-us/HT207482

- It's not huge -- about 74mb.

- Kernel (2x)
  - Impact: An application may be able to execute arbitrary code with kernel privileges
  - Description: A buffer overflow issue was addressed through improved memory handling.
  - CVE-2017-2370: Ian Beer of Google Project Zero

- libarchive
  - Impact: Unpacking a maliciously crafted archive may lead to arbitrary code execution
  - Description: A buffer overflow issue was addressed through improved memory handling.
  - CVE-2016-8687: Agostino Sarubbo of Gentoo

- WebKit
  - Impact: Processing maliciously crafted web content may exfiltrate data cross-origin
  - Description: A prototype access issue was addressed through improved exception handling.
    - CVE-2017-2350: Gareth Heyes of Portswigger Web Security

  - Impact: Processing maliciously crafted web content may lead to arbitrary code execution
  - Description: Multiple memory corruption issues were addressed through improved memory handling.
    - CVE-2017-2354: Neymar of Tencent's Xuanwu Lab (tencent.com) working with Trend Micro's Zero Day Initiative
    - CVE-2017-2362: Ivan Fratric of Google Project Zero
    - CVE-2017-2373: Ivan Fratric of Google Project Zero

  - Impact: Processing maliciously crafted web content may lead to arbitrary code execution
  - Description: A memory initialization issue was addressed through improved memory handling.
    - CVE-2017-2355: Team Pangu and lokihardt at PwnFest 2016

  - Impact: Processing maliciously crafted web content may lead to arbitrary code execution
  - Description: Multiple memory corruption issues were addressed through improved input validation.
    - CVE-2017-2356: Team Pangu and lokihardt at PwnFest 2016
    - CVE-2017-2369: Ivan Fratric of Google Project Zero
    - CVE-2017-2366: Kai Kang of Tencent's Xuanwu Lab (tencent.com)

  - Impact: Processing maliciously crafted web content may exfiltrate data cross-origin
  - Description: A validation issue existed in the handling of page loading. This issue was addressed through improved logic.
    - CVE-2017-2363: lokihardt of Google Project Zero
    - CVE-2017-2364: lokihardt of Google Project Zero

  - Impact: A malicious website can open popups
  - Description: An issue existed in the handling of blocking popups. This was addressed through improved input validation.
    - CVE-2017-2371: lokihardt of Google Project Zero

  - Impact: Processing maliciously crafted web content may exfiltrate data cross-origin
  - Description: A validation issue existed in the handling of variable handling. This issue was addressed through improved validation.
    - CVE-2017-2365: lokihardt of Google Project Zero

LastPass Does Not Encrypt Everything In Your Vault

- https://hackernoon.com/psa-lastpass-does-not-encrypt-everything-in-your-vault-8722d69b2032#.n4t7xg6wr

- It's a feature, not a bug.... and it's a well-known and previously examined feature.

- Some metadata for bookmarklets and favicons need to be accessible and exchanged with LastPass outside of the user's encrypted storage... specifically because lastPass cannot see into the user's encrypted storage.

- The URL encoded in hex is required for the Track History feature, which can be disabled.

- And the other information not encrypted on the server is:

  - The email address you use to login with LastPass
    - They need this to send emails to us.

  - The IP address of logins to LastPass
    - They use that for features such as "Country Restriction" to prevent logins from other countries.

  - The IP address of website logins
    - They use that if we have Track History enabled. This feature allows us to globally monitor a log of our your logins to see if we detect any suspicious activity. We can opt out of this feature by going to the LastPass Vault > Account Settings > Advanced Settings > Privacy > uncheck "Track History"

SEC launches Yahoo investigation over improper handling of cyberattacks

- The SEC is looking into whether Yahoo (or what's left of Yahoo after most assets were sold to Verizon) waited too long to tell their stock holding investors of the breaches.

- But we still don't have strong uniform legislation in place.

- Following the widely publicized breach at Target, the "Personal Data and Notification Act" legislation was drawn up to require companies to notify the public of data breaches within 30 days of discovery.

- It was introduced in 2015 but failed to pass through the House of Representatives subcommittee review, likely due to frantic industry lobbying... It would have carried a shockingly serious penalty of up to a $1,000 per day per person affected, and it would have superseded the 47 state laws (and the District of Columbia), which have varying standards of when notification has to be made and what types of information breach qualifies.

Browser autofill used to steal personal details in new phishing attack

- Another instance of a convenience feature being used in a way that wasn't envisioned by its creators.

- A Finnish web developer and hacker discovered that several web browsers, at least including Chrome, Safari and Opera, as well as some plugins and utilities such as LastPass, can be tricked into giving away a user's personal information through their profile-based autofill systems.

- The attack is surprisingly simple: When a user begins to fill-in information in a web-based form containing simple text boxes, such as name and email address, the autofill system, which is intended to avoid tedious repetition of standard information such as your address, etc. will input other profile-based information into any other standard identifiable text boxes – even when those boxes are not visible on the page! (Whoopsie)

- This means that when a user deliberately selected innocent, basic information into a site, the autofill system could be invisibly divulging much more sensitive information at the same time should the user confirm the autofill.

- Chrome's autofill system, which is switched on by default, stores data on email addresses, phone numbers, mailing addresses, organisations, credit card information and various other bits and pieces.

- https://anttiviljami.github.io/browser-autofill-phishing/
    - WARNING!! -- This REALLY WORKS! -- Your credit card info will be sent to "https://httpbin.org/"
    - Httpbin.org is a well known, longstanding site which provides an array of tools toecho back browser query parameters. In this case it's showing the parameters sent by an http POST query.

- Firefox doesn't have this problem, so for me it did nothing.

- But under Chrome it obtained…
  - My full street address, city, country, zip.
  - (And I barely use Chrome.)

- The attack still relies on users entering at least some information into an online form, but unsuspecting users could easily be tricked into entering more than they bargained for relatively easily.

- Users can protect themselves from this kind of phishing attack by disabling the autofill system within their browser or extension settings.

Later this year, Tor's "Dark Web Technology" will become even darker

- The change will prevent "discovery" of otherwise unknown hidden services.

- Normally Internet traffic jumps visibly from one router to the next, and it's entirely traceable.

- So the TOR project (originally an acronym for The Onion Router) started off by implementing a layered encrypted "onion" of data packets which allowed multiply-encrypted traffic to converge into a subset of the internet's routers -- the Tor network -- to emerge elsewhere and to thwart tracing specific traffic.

- But client traffic would ultimately emerge back out onto the public network... where it could be seen.

- So "Tor Hidden Services" were invented to allow the TOR network to CONTAIN the end-services that Tor users might wish to visit.

- And there have been some famous ones:
  - WikiLeaks' anonymous upload system can be visited by using "wlupld3ptjvsgwqw.onion"
  - Silk Road could be found at "silkroadvb5piz3r.onion"

- But, even without knowing a hidden service's address it has been possible for hackers, law enforcement, security firms, snoops and others to discover those services independently.

- A study shared at last year's DefCon revealed that more than 100 of the 3,000 hidden service directories were apparently being used to spy on the network.

- Developers involved with Tor have said "The only people who should know about your hidden service are the people you tell about it. While that's a pretty simple concept, it's currently not true."

- The next generation of hidden services will use a new method to protect the secrecy of those addresses. Instead of declaring their .onion address to hidden service directories, these hidden services will, instead, derive a cryptographic key from the .onion address, and THAT derived key will be placed into Tor's hidden service directories. Then, any Tor user who KNOWS the name of the hidden service they want can perform that same derivation to check the key and route themselves to the correct hidden service.

- Since the hidden service directory cannot derive the .onion address from the key, only those who know the hidden service's key can discover the hidden service's address.

- As Tor Project co-founder Nick Mathewson said: "The Tor network isn't going to give you any way to learn about an onion address you don't already know."

- The next generation of hidden services will also switch from using 1024-bit RSA encryption keys to shorter but tougher-to-crack ED25519 elliptic curve keys.

- These changes also mean that hidden service urls will change, too, from 16 characters to 50. But Nick argues that change doesn't effect the dark web addresses' usability since they're already too long to memorize.

China's 1st Hack-Proof Quantum Satellite: "Now Operational"

- http://www.dailygalaxy.com/my_weblog/2017/01/chinas-1st-hack-proof-quantum-satellite-now-operational-launches-a-new-world-.html

- Quantum entanglement

Over 199,500 Websites Are Still Vulnerable to Heartbleed OpenSSL Bug

- https://www.shodan.io/report/DCPO7BkV
- http://heartbleed.com/

- April 2014 ... nearly three years ago!!

- At the time of disclosure, some 17% (around half a million) of the Internet's secure web servers certified by trusted authorities were believed to be vulnerable to the attack, allowing theft of the servers' private keys and users' session cookies and passwords.
- The Electronic Frontier Foundation (EFF) & Bruce Schneier all considered the Heartbleed bug to be catastrophic.

- As of May 20, 2014, 1.5% of the 800,000 most popular TLS-enabled websites were still vulnerable to Heartbleed.

- Now, today, nearly three years later, a SHODAN identifies and reports at least 199,500 websites are still vulnerable.

- MOST in the USA.
  - #1 is SK Broadband (6,376 servers)
  - #2 is Amazon.com (5,163) - AmazonAWS.com
  - #3 is Verizon (4,347)

Minnesota court on the Fifth Amendment and compelling fingerprints to unlock a phone

- Courts have recently been using the argument that forcing a person to use their finger to unlock a phone is not afforded 5th amendment protection against self-incrimination because using a finger does not qualify as being testimonial.

- A recent case "State vs Diamond" was decided yesterday by the Minnesota Court of Appeals.

- In the original case the defendant, Diamond, initially refused to comply.

- The judge explained that using his finger was non-testimonial, so he could not plead the 5th, and that he would be held in contempt of court if he refused.

- So he complied.

- But then he got a fancier attorney who came up with another angle…

- On appeal, Diamond argued that the government violated his Fifth Amendment rights because the government made Diamond select which finger to use. Specifically, Diamond argued that he "was required to identify for the police which of his fingerprints would open the phone" and that "this requirement compelled a testimonial communication."

Pwn2Own Returns for 2017 to Celebrate 10 Years of Exploits

- CanSecWest Vancouver 2017

- The 17th annual CanSecWest conference will be held March 15-17th, 2017 at the Sheraton Wall Centre hotel in downtown Vancouver, BC, Canada

- Much as changed at Pwn2Own since 2007. That first year, the prizes were a laptop and $10,000. Last year more than $450,000 cash and prizes were awarded over the multiple categories.

- Ten years ago a single bug was able to exploit QuickTime. Last year, a significant chain of bugs was required to complete a compromise and fully win a category.

- THIS YEAR, the Zero Day Initiative (ZDI) which organizes and hosts the Pwn2Own competition will be offering more than $1,000,000 across five categories:

    - Virtual Machine Escape (Guest-to-Host)
    - Web Browser and Plugins
    - Local Escalation of Privilege
    - Enterprise Applications
    - Server Side

- VM Escapes:
  - VM Escapes were first added last year with VMware, and this year it's being expanded to include Microsoft Hyper-V. An attempt in this category must be launched from within the guest operating system from a non-administrative account and execute arbitrary code on the host operating system. Both the guest and the host operating system will be running the 64-bit versions of Windows 10.

  - A successful exploit in either product will net $100,000 for the contestant plus a lucky 13 Master of Pwn points.

- Web Browser and Plugins Exploits:
  - Microsoft Edge: $80,000 (10 Master of Pwn points)
  - Google Chrome: $80,000 (10 Master of Pwn points)
  - Apple Safari: $50,000 (8 Master of Pwn points)
  - Adobe Flash in Microsoft Edge: $50,000 (8 Master of Pwn points)
  - Mozilla Firefox: $30,000 (5 Master of Pwn points)

  - Moreover, contestants may earn an additional $30,000 if their entry achieves SYSTEM-level code execution on Windows-based targets, or will receive an additional $20,000 if their entry achieves root-level code execution on macOS-based targets.

  - And the Windows-based targets will be running in a VMware Workstation virtual machine. If the contestant escapes the browser or plug-in AND the containing VMware Workstation virtual machine to achieve code execution on the host operating system, the contestant will receive an additional $100,000.

Miscellany

Pete Stringer (@Pete_Stringer) - 1/19/17, 9:22 AM
@SGgrc Hi Steve, are you able to put details of your and Leo's favourite/preferred/recommended home router(s) onto GRC linkfarm page?

Amazon Echo and Echo Dot update adds "Computer" wake word to help complete the Star Trek fantasy
"My Dot has version 4812 with "Computer" wake word"
Alexa / Amazon / Echo / Computer

brad on line (@bradkovach) 1/23/17, 1:55 PM

- @SGgrc I have noticed Amazon ads for the Echo do not trigger Alexa.
  I hypothesize there is a tone that plays to kill the response
- A "notch" in the spectrum at around 5khz.
- Earlier there were complains about the Echo triggering to ads.

SpinRite

SM (sergey) in Lake Stevens, Washington wonders about "Cabling Errors"

Hey Steve,

I just finished Episode #593 and I think you're wrong on Cabling errors!!!

I am listener since episode 1 and a SpinRite user. I played with SpinRite v6 a lot, I even bought a large batch of "completely dead" drives from eBay and I was able to use SpinRite to restore most of them to full error-free operation... but...

While SpinRiting a few of the 36 drives I was getting Cabling Errors, so I would swap cable and try again, I even bought 2 different brands of SATA cables so I could use them for swapping, and despite trying everything I could, a couple of those drives were still showing "Cabling Errors", so looks like it's not always a cable's fault for cabling errors. What do you think? I think it must be something inside the drive, please explain if you can.

Can't wait till next episode.

Thank you

Password Complexity Calculations

James Brooks (@oran0007) - 1/19/17, 9:59 AM
@SGgrc If I use a pseudo-random word generator to string together 5[+] words for a pass phrase, is it still weak (re: episode 594)?

Ben Maughan (@bjmaughan) - 1/19/17, 5:17 AM
@SGgrc Love SN, listened for years. Character-based passwords just use a different dictionary from word-based pws, words can be as good...
@SGgrc (4) actually, oxford dictionary estimate about 100k nouns, so a random five-noun pw is better than 12 random chars. I think!

Fun with Logarithms!

A logarithm is a special shaped curve such that:

- log(a) + log(b) = log(x*y)
- log(3) + log(7) = log(21)

log(<some number>) / log(base) = number of items of that base.

log(alphabet) / log(2) = equivalent number of binary bits required to enumerate the alphabet.

log(alphabet) / log(10) = equivalent number of decimal digits required to enumerate the alphabet.

It does not matter which base of logarithm is used: "log" or "ln"

128 bits is a LOT!

All characters is alphabet of 95.

```
        ln(95) = 4.554
        ln(2)   = 0.6931
----------------------------
        6.57 bits of entropy per character.
```