Security Now! #441 - 02-04-14

Password Policies

Link Tracking Warning!
This document was first authored in Google Docs, then Downloaded as a PDF. So, Google has thoughtfully (ha!) added "tracking" redirections to all of the links here. (I have no idea why, but that's Google.) If that bothers you, simply copy the text of the link into your browser's URL field.

This week on Security Now!

- Today's newest Firefox fixes its previous poor score.
- Today's EMERGENCY update to FLASH from Adobe.
- The return of "HoneyWords"
- The troubling rise of Malicious Ads.
- A VERY interesting Windows Firewall Add-On.
- Why tossing a coin is not fair.
- Did the NSA ask me to build a backdoor into CryptoLink?
- ... all that and more, coming up on Security Now!

Security News:

Firefox v27 Released Today.

- TLS 1.2 has been implemented
- Continuing movement toward improved standards support and interoperability.
- https://www.howsmyssl.com/
    - Ratings:
        - Now "Probably Okay", up from "Bad"
        - (about:config... then search for 'tls')
            - Highlights show user overrides.
            - Right-click and 'reset'
        - Also... fixed this:
            - Supports: SSL_RSA_FIPS_WITH_3DES_EDE_CBC_SHA
            - "This cipher was meant to die with SSL 3.0 and is of unknown safety."

Adobe issues emergency FLASH update for 0-day flaw:

- Adobe TODAY released a security update for Flash Player to address a vulnerability that could allow an attacker to remotely take control of users' computers.
- Kaspersky found it in the wild.
- An Integer Underflow bug that allows for remote code execution in the computer.
- Affects Windows PCs AND Macs (and Linux)
- Unless you're using the latest versions of Chrome or Internet Explorer, you'll want to manually update Adobe Flash immediately. You can get the latest version now directly from the Adobe Download Center.

Honey Passwords (aka HoneyWords)

- http://gizmodo.com/sneaky-honey-encryption-stops-hackers-by-drowning-the-1511718913
- http://www.net-security.org/secworld.php?id=16283
- May 2, 2013: Ari Juels of RSA Labs & Ron Rivest at MIT:
  - "HoneyWords: Making Password-Cracking Detectable
  - http://people.csail.mit.edu/rivest/honeywords/paper.pdf
- May 6th, 2013
  - Bruce Schneier Blogged: Here is a simple but clever idea. Seed password files with dummy entries that will trigger an alarm when used. That way a site can know when a hacker is trying to decrypt the password file.

Malware in ads

- http://online.wsj.com/news/article_email/SB10001424052702303743604579350654103483462-lMyQjAxMTA0MDAwMTEwNDEyWj
- RiskIQ, Inc tracking malicious ads:
  - 2011: 70,000
  - 2012: 205,000
  - 2013: 384,000
- Google:
  - 2013: disabled ads from more than 400,000 sites containing malware
  - 2012: 123,000
- Malware Scanning?
  - Recent malicious ads are missed by 44 of 47 A/V programs.

Intelligence Law Blog:

- http://intelligencelaw.blogspot.com/2013/12/did-nsa-threaten-steve-gibson-cryptolink.html
- "Did the NSA or FBI Threaten Steve Gibson to Force Him To Abandon CryptoLink?"
- Blog notes that I was speaking of CryptoLink often and enthusiastically, and once said:
  - *"If you ever hear of me or learn of me discontinuing CryptoLink for no reason, you'll know that for whatever reason I felt no longer able to offer something whose security I could put my reputation behind. Because I'll kill it before I would compromise it."*

Windows Firewall Control

- http://www.binisoft.org/wfc.php
- Windows Firewall Control is a nifty little application which extends the functionality of the Windows Firewall and provides quick access to the most frequent options of Windows Firewall. It runs in the system tray and allows user to control the native firewall easily without having to waste time by navigating to the specific part of the firewall. This is the best tool to manage the native firewall from Windows 8.1, 8, 7, Vista and Server 2008. Windows Firewall Control offers four filtering modes which can be switched with just a mouse click:

    - High Filtering - All outbound and inbound connections are blocked. This setting blocks all attempts to connect to and from your computer.
    - Medium Filtering - Outbound connections that do not match a rule are blocked. Only the programs that you allow can initiate outbound connections.
    - Low Filtering - Outbound connections that do not match a rule are allowed. The user can block the programs he doesn't want to initiate outbound connections.
    - No Filtering - Windows Firewall is turned off. Avoid using this setting unless you have another firewall running on your computer.

- **Program features:**
    - Intuitive and easy accessible interface in the system tray, next to the system clock.
    - Full support with standard user accounts. Elevated privileges are required only at installation.
    - Create temporary rules which are automatically deleted when they expire or on program restart.
    - Disable the ability of other programs to add Windows Firewall rules.
    - Multiple and easier ways of creating new rules in Windows Firewall.
    - Integrated support of creating, modifying and deleting Window Firewall rules.
    - Lock feature which can disable the access to the settings of the program and Windows Firewall.
    - Shell integration into the right click context menu of the executable files.
    - Search for invalid rules with the possibility to delete them.
    - Search for executable files through folders and create new rules in seconds.
    - View recently blocked connections and create new rules from the logs: inbound and outbound.
    - Choose if you want the program to start at user log on.
    - Import, export and restore the firewall rules.
    - Protection against unauthorized uninstallation.
    - Possibility to restore previous settings at uninstallation.
    - And many, many more…

- $10 donation get multi-system lifetime registration:
    - Adds notification of firewall rule events
        - High - Display notifications for all outgoing connections that were blocked, including System and Svchost.exe.
        - Medium - Display notifications only for regular programs, without notifications for System and Svchost.exe.
        - Low - Automatically allow digitally signed programs. Notifications are displayed only for unsigned programs.
        - Disabled - Notifications are disabled.

- Also from these guys:
    - USB Flash Drives Control:
        - Enable/Disable USB Flash Drives
        - Deny Execution from Flash
        - Mount Read-Only (deny any writing to drives.)

ChewBacca -- POS Malware Stealing Payment Card & Personal Info

- https://blogs.rsa.com/rsa-uncovers-new-pos-malware-operation-stealing-payment-card-personal-information/
- http://www.darkreading.com/attacks-breaches/point-of-sale-system-attack-campaign-hit/240165813/
- RSA: "ChewBacca", with its keylogging and memory-scraping features, is tied to a specific Poiint Of Sale attack campaign out of the Ukraine against retailers.
- Uses a Tor-hidden server infrastructure.
- RSA wrote: "In our analysis, when we reverse-engineered the binaries, located the command & control, and determined that it was Tor-enabled. We identified the drop site" for the stolen data."
- Running command-and-control communications over the Tor network masks the real IP address of servers and encrypts traffic between the infected machines and the servers.
- Infection vector still unknown.
- Trojan is self-contained and installs a copy of itself in the Windows Start > Startup folder as a Windows print spooler service.
- Most POS systems are Windows-based systems.
- What we're seeing is a "land grab" with malware such as ChewBacca and BlackPOS vying for residency in worldwide POS systems.

Senate Hearing hours ago: Nieman Marcus @ Target & Nieman Marcus breach hearing:

- Reuters Tweeted:
  - Neiman Marcus CIO says maximum of 1.1 million accounts potentially exposed to malware in data breach, but actual number was 'less than that'
  - Data breach at Neiman Marcus potentially exposed payment card information from transactions at 77 of 85 stores between July and October of 2013, company says
- The CC technology is being blamed... but if Windows XP is your infrastructure... all bets are off!

The Physics of Coin Tossing:

- http://www.codingthewheel.com/archives/the-coin-flip-a-fundamentally-unfair-proposition/
- http://statweb.stanford.edu/~susan/papers/headswithJ.pdf
  - "Dynamical Bias in the Coin Toss" (31 pages)
  - Abstract:
    We analyze the natural process of flipping a coin which is caught in the hand. We prove that vigorously-flipped coins are biased to come up the same way they started. The amount of bias depends on a single parameter, the angle between the normal to the coin and the angular momentum vector. Measurements of this parameter based on high-speed photography are reported. For natural flips, the chance of coming up as started is about .51.

- Takeaways:
  - If the coin is tossed and caught, it has about a 51% chance of landing on the same face it was launched. (If it starts out as heads, there's a 51% chance it will end as heads).

    - If the coin is spun, rather than tossed, it can have a much-larger-than-50% chance of ending with the heavier side down. Spun coins can exhibit "huge bias" (some spun coins will fall tails-up 80% of the time).
    - If the coin is tossed and allowed to clatter to the floor, this probably adds randomness.
    - If the coin is tossed and allowed to clatter to the floor where it spins, as will sometimes happen, the above spinning bias probably comes into play.
    - A coin will land on its edge around 1 in 6000 throws, creating a flipistic singularity.
    - The same initial coin-flipping conditions produce the same coin flip result. That is, there's a certain amount of determinism to the coin flip.
    - A more robust coin toss (more revolutions) decreases the bias.

Wired article about Zero-Knowledge Proof breakthrough

- https://www.simonsfoundation.org/quanta/20140130-perfecting-the-art-of-sensible-nonsense/
- http://www.wired.com/wiredscience/2014/02/cryptography-breakthrough/
- <quote> As a graduate student at the Massachusetts Institute of Technology in 1996, Amit Sahai was fascinated by the strange notion of a "zero-knowledge" proof, a type of mathematical protocol for convincing someone that something is true without revealing any details of why it is true. As Sahai mulled over this counterintuitive concept, it led him to consider an even more daring notion: What if it were possible to mask the inner workings not just of a proof, but of a computer program, so that people could use the program without being able to figure out how it worked?
- SN#363: Ali Baba's Cave ... and Zero-Knowledge Interactive Proofs
- August 1st, 2012
- https://www.grc.com/sn/sn-363.pdf

Miscellany:

- http://bit.ly/sgtid (SG TouchID)

SQRL:

- Key Flow (page #5 of 20)
- https://www.grc.com/sqrl/key-flow.htm
- UI work now underway...

SpinRite: Testimonial from Philip Cooke:

I started my day with a blue screen of death, advising that I had an unmountable_boot_volume!!

Efforts by a Dell tech only lead him to the conclusion that we should reformat the drive and lose all my data. Nothing would recognize the drive and all of the chkdsk commands in the book could not even see it or result in anything but the same blue screen on every reboot. A Maxtor utility I ran advised me to return the drive for a replacement. But I couldn't.

After getting estimates ranging from $400.00 to $2700.00 to recover my data and trying numerous other "tricks" recommended by online chats, etc, I was fortunate to come across SpinRite. At first the glowing testimonials seemed just too good to be true and I will admit that I thought they may even have been "fake"!

So, I invested the $89.00, downloaded the file and fired it up. At first I thought that it was going nowhere, cause after 4 hrs it still said 2% complete. I figured I would leave it running and imagine my surprise when I came in this morning, saw the message that it had completed, it booted up, ran chkdsk and then started Windows!! All I can say is WOW!

Thanks you for taking the time to create this program. It's bad enough losing data, but I also saved the hours it would have taken to recreate my desktop, links, etc. Needless to say I am impressed!

Philip Cooke

Internet Password Policy 2014 Update

Our current identity and password ecosystem:

Non-multifactor:

- User-generated, low-entropy, reusable, "secrets"
- Websites store in plaintext or unsalted simple hashes
    - ... and then their data gets leaked
    - Other personal information: credit cards, PINs, names & addresses, etc. UNENCRYPTED.
    - The problem is:
        - Security is invisible.
        - It is NOT seen as a beneficial feature.
        - We only hear about it when it breaks.
        - We get apologies.
        - The fine print holds everyone harmless.
        - It is seen as an annoyance -- both to the website and to the user.
            - "This finicky website won't let me use my favorite password."
        - If there was a security certification... would anyone really care?
    - (One of the cool things about SQRL is that it's not POSSIBLE for a SQRL-based site to have poor login authentication security... because the site keeps no secrets there's literally nothing to steal.)

Password Managers:

- High-entropy passwords - protection from "common password" attacks
- Encourages per-site secrets
- All of the password management burden is placed on the user.
- If the site stores passwords in the clear, loss of database allows impersonation.
- But if the PW's are hashed at all, the user will be safe.

Multifactor

- The best current solution.
- Typically not free (unless cellphone loop)
- Not zero-friction to use (must always have token with you.)

Dashlane:

https://www.dashlane.com/download/securityroundup_2014_q1/The_Illusion_of_Personal_Data_Security_in_E-Commerce_%28Press%20Release%29.pdf

Who is Dashlane?

- Another standard password & wallet manager
- Must pay $30/yr to get:
    - Secure Account Backup
    - Cross device synchronization
    - Web access to passwords
    - Priority Support

- LastPass: Usable FREE version
    - $12/yr adds:
    - Platform-specific mobile apps
    - Yubikey support
    - No ads
    - Priority Support

- Raw Data:
    - http://bit.ly/sn441 (Large scrollable PNG)
    - http://bit.ly/sn441a (Large scripted scrollable online HTML)
    - Jon M (@Liquidretro)
    - http://bit.ly/sn441sheet (all lowercase)
    - http://bit.ly/SN441sheet

Observations:

- Minimum password length:
  - 1: Just means "non-blank" (Northern Tool, 1-800-Flowers)
  - 2: "Build"
  - 3: CafePress(!), Scholastic, Inc., Fanatics, Urban Outfitter, Nutrisystem,
  - 4: KarmaLoop, Vitacost, Fresh Direct, Shutterfly, Victoria's Secret, ShopNBC,
  - Who's going to write code to set a minimum length of 2, 3, 4, etc?

- Password visible during entry.
  - I've never really understood that one.
  - ... and EVERYONE has passwords masked.

- Strong Password Advice Offered:
  - VERY worthwhile.
  - Remember who MOST people are.

- Mixed-Case Required:
  - Clearly a good thing.

- On-Screen Password Strength Meter:
  - Still a rarity -- only 7 of the top 100 retail sites

- Blocks logins after 4 misses:
  - Apple, NewEgg, Nordstrom, Hayneedle, Oriental Trading Co., FootLocker, CostCo, Gilt Group, Staples, ShopNBC (though ShopNBC also allows a 4-char password)

- Blocks logins after 10 misses:
  - Microsoft, Target, CDW, Amway, Musician's Friend, WW Grainger, Walgreens, CVS... etc.

Summary:

- 73% accept passwords having 6 or fewer characters.
- 62% do not require a mixture of letters and numbers.
- 55% accept 10 of the most commonly used (weak) passwords “123456”, “111111” or “password”
- 51% make no attempt to block entry after 10 incorrect password entries (including Amazon, Dell, Best Buy, Macy’s and Williams-Sonoma)
- 61% do not provide any advice on how to create a strong password during signup, and 93% do not provide an on-screen password strength assessment
- Only 10% scored above the threshold for good password policies (i.e. 45 points or more in the roundup)
- 8 sites, including Toys “R” Us, J.Crew and 1-800-Flowers.com, send passwords in plain text via email
- (Yahoo! says: "New password too similar to previous password".)

- Apple received the highest rating and was the only retailer to receive a perfect score.
- Newegg, Microsoft, Chegg -- tied for 2nd
- Target rounded out the top 3 ranking.
- MLB.com, Karmaloop and Dick’s Sporting Goods received the three lowest scores.
- (MLB.com allows "baseball" as their password.)
- Amazon, Walmart, Victoria’s Secret and Toys “R” Us were also among the lowest ranked sites receiving scores of -35 or below.

Simple Password Management Advice:

- Require that passwords contain at least 8 characters, and a combination of upper/lower-case letters, numbers and symbols.
- Block account access after 4 failed login attempts.
- Provide users with on-screen advice on how to choose a strong password during signup.
- Provide users with an on-screen assessment of password strength while they're choosing a password.