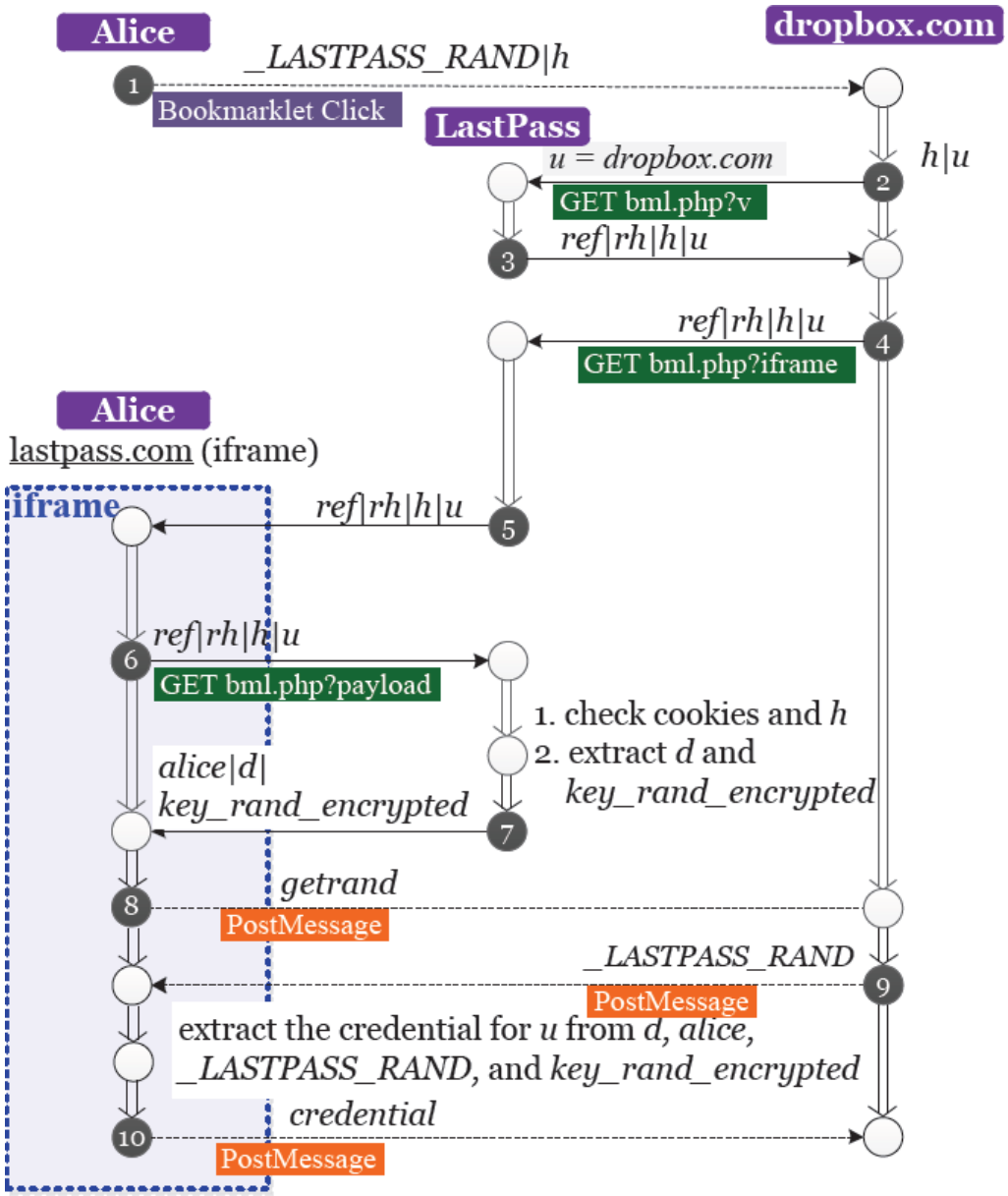
Security Now! #467 - 08-05-14

Browser Password Managers

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!

- HP's quick scan of security of ten "Internet of Things" gadgets,
- A simple PayPal 2-factor authentication bypass,
- Google spots child porn in eMail,
- How bad is "BadUSB"?
- And the takeaway on the report about Browser-based Password Managers



Security News:

"The Internet of Things Is the Hackers' New Playground"

- http://recode.net/2014/07/29/the-internet-of-things-is-the-hackers-new-playground/
- HP's "Fortify" application security unit conducted an analysis of the 10 most popular consumer "Internet things" on the market and found 250 different security vulnerabilities in the products, for an average of 25 faults each.
- Though not identifying them, HP wrote: "They were from the manufacturers of "TVs, webcams, home thermostats, remote power outlets, sprinkler controllers, hubs for controlling multiple devices, door locks, home alarms, scales and garage door openers."
- Bullet points to give us the flavor:
    - 8 of 10 devices failed to require passwords stronger than "1234" either on the device itself or on a corresponding website.
    - 7 of 10 devices tested do no encryption when communicating with the Internet or a local network.
    - 6 of the devices had weak security on their interfaces, were vulnerable to persistent cross-site scripting attacks, had weak default sign-in credentials, or transmitted sign-in credentials like passwords "in the clear."
    - 6 devices didn't encrypt software updates during the download.
    - As we know, that allows bad guys to create a valid-appearing software update to reprogram the device to do whatever they wish. If it's a webcam or the garage door to your home, that's worrisome.
    - And... 9 of the 10 devices collected at least some kind of personal information: An email address, a home address, a name or date of birth.

PayPal 2-factor Authentication Bypass

- http://blog.internot.info/2014/08/paypal-complete-2-factor.html
- http://arstechnica.com/security/2014/08/paypal-2fa-is-easily-bypassed-teenage-white-hat-hacker-says/
- Joshua Rogers, 17 year old Australian whitehat hacker found a simple way of defeating the PayPal dongle... Linked accounts in ebay don't prompt for the 2nd factor.
- Apparently… just having "=_integrated-registration" in the URL enables the bypass!

Google "sees" and reports explicitly illegal photo in eMail.

- http://www.businessinsider.com/police-say-a-google-tip-about-child-abuse-led-to-arrest-2014-8
- Google explains that it is required by law to report such discoveries.
- A Google spokesperson told Business Insider:
    - <quote> All Internet companies have to deal with child sexual abuse. It's why Google actively removes illegal imagery from our services — including search and Gmail — and immediately reports abuse to NCMEC [The National Center for Missing & Exploited Children]. This evidence is regularly used to convict criminals.

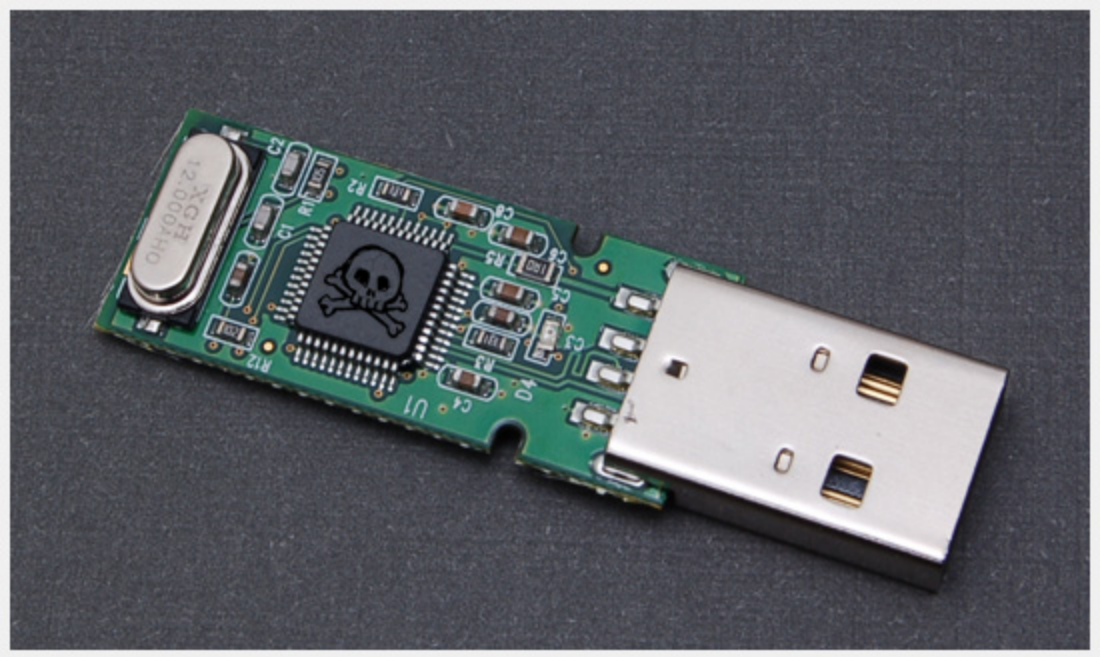
      Each child sexual abuse image is given a unique digital fingerprint which enables our systems to identify those pictures, including in Gmail.

It is important to remember that we only use this technology to identify child sexual abuse imagery, not other email content that could be associated with criminal activity (for example using email to plot a burglary).

- Jacquelline Fuller, director of "Google Giving" http://googleblog.blogspot.com/2013/06/our-continued-commitment-to-combating.html
    - In 2011, the National Center for Missing & Exploited Children's (NCMEC's) Cybertipline Child Victim Identification Program reviewed 17.3 million images and videos of suspected child sexual abuse. This is four times more than what their Exploited Children's Division (ECD) saw in 2007. And the number is still growing. Behind these images are real, vulnerable kids who are sexually victimized and victimized further through the distribution of their images.

    - Since 2008, we've used "hashing" technology to tag known child sexual abuse images, allowing us to identify duplicate images which may exist elsewhere. Each offending image in effect gets a unique ID that our computers can recognize without humans having to view them again. Recently, we've started working to incorporate encrypted "fingerprints" of child sexual abuse images into a cross-industry database. This will enable companies, law enforcement and charities to better collaborate on detecting and removing these images, and to take action against the criminals. Today we've also announced a $2 million Child Protection Technology Fund to encourage the development of ever more effective tools.

"BadUSB"



- Karsten Nohl & Jakob Lell, German Security Research Labs
- BlackHAT, Thursday, August 7th
- ***SRLabs: "Turning USB peripherals into BadUSB"*** https://srlabs.de/badusb/

- ArsTechnica: This thumbdrive hacks computers.
  "BadUSB" exploit makes devices turn "evil"
  - http://arstechnica.com/security/2014/07/this-thumbdrive-hacks-computers-badusb-exploit-makes-devices-turn-evil/

- Wired: **Why the Security of USB Is Fundamentally Broken**
  - http://www.wired.com/2014/07/usb-security/

- Gizmodo: **USB Has a Fundamental Security Flaw That You Can't Detect**
  - http://gizmodo.com/usb-has-a-fundamental-security-flaw-that-you-cant-detec-1613833339

- ExtremeTech (Extreme Hype?): **Massive, undetectable security flaw found in USB: It's time to get your PS/2 keyboard out of the cupboard**
  - http://www.extremetech.com/computing/187279-undetectable-indefensible-security-flaw-found-in-usb-its-time-to-get-your-ps2-keyboard-out-of-the-cupboard

- Their surprising discovery:
  - Many USB devices are flash-programmable in-circuit
  - No "execute only" fuse.

- USB Device Classes:
  - http://en.wikipedia.org/wiki/USB#Device_classes
  - Audio input, output
  - Modem, Ethernet, WiFi
  - Keyboard, Mouse, Joystick
  - Video Webcam, Scanner
  - Printer
  - Mass Storage
  - Hub
  - Bluetooth adapter
  - IR (IrDA)

- Reality Check...
  - USB predates security.
  - Back then, the CONVENIENCE of USB was amazing
  - Firewire and Thunderbolt are powerful bus-extending peer-to-peer systems.
  - USB is a host-polled & host-controlled Master/Slave protocol.

SQRL:

- First ***pre-completion*** code release to the newsgroup.
- AERO compositing (fixed)
- WINE font sizing
- Next to add: Import / Export / Backup ... and protocol.

SpinRite:

Steve,

All of a sudden my external hard drive was not being recognized by Windows7. The error I am getting when it's plugged in using an USB 2.0 SATA/IDE combo adapter is: "Unallocated 3.86GB unknown, not initialized" ... though the drive is 2TB. If I try to initialized the disk drive I get an error data "error (cyclic redundancy check)".

My question is, if I purchase SprinRite, is it still possible to recover data from a dying disk drive? I love your show I have been listening for over a year now and I've learned a lot.

My Reply: I can't really say for sure, but your mention of the CRC error *IS* precisely the sort of trouble SpinRite was designed to find and fix. So I'd say that the chances were good. And if not... we'll be happy to refund your full purchase price. Just tell "sales" that it didn't do what you hoped and needed. :)

Best luck!

Web Browser Based Password Managers

23rd USENIX Security Symposium -- at 2pm, Thursday, August 21st,
Four UC Berkeley researchers present:
The Emperor's New Password Manager: Security Analysis of Web-based Password Managers
https://www.usenix.org/conference/usenixsecurity14/technical-sessions

Why we web-based password managers.

Five Password Managers:

- LastPass
- RoboForm
- My1login
    - Weird MD5, separately, of odd and even password characters.
- PasswordBox
- NeedMyPassword
    - No auto-login, credential sharing, or password generation. Only credential storage on NeedMyPassword's website.... and the user's login credentials are NOT encrypted before being sent to NeedMyPassword.

Main concerns:

- Bookmarklet vulnerabilities
    - Overcomes lack of browser plug-in support.
    - Runs JS in the (possibly malicious) context of the target webpage.
- "Classic" web vulnerabilities (CSRF and XSS)
- Logic vulnerabilities
- UI vulnerabilities

Their intended contribution was to systematically identify the attack surface, security goals, and vulnerabilities in typical popular password managers.

To guide future development of password managers they provide guidance for password managers.

One early conclusion: Defense in Depth has the best chance.

Last August 2013, four of the five vendors replied promptly (NeedMyPassword never did) and all discovered and reported vulnerabilities found were fixed within days of notification.

Threat Model:

- Main threat model is the "web attacker".
- The "Web Attacker" controls one or more web servers and DNS domains and can get a victim to visit domains controlled by the attacker.

Security Goal:

- Ensure that a stored password is accessed ONLY by the authorized user and the website the password was created for.
- Master Account Security:
    - Should not be possible for an attacker to authenticate as the user to the password manager.
- Credential Database Security:
    - Bad guys should not be able to obtain unauthorized access to the protected credential database.
- Collaborator / Credential Sharing Security:
    - Keep fraudulent collaborators from gaining access to credentials.
- Unlinkability:
    - Password manager should not allow colluding web applications to track a single individual between sites.

Attack Surface:

- The KEY difference between web-based password mangers and traditional desktop managers is their need to work in web browsers.
- Four Key Concerns:
- Bookmarklet vulnerabilities
- "Classic" web vulnerabilities
- Authorization vulnerabilities
- UI vulnerabilities

Bookmarklet Vulnerabilities:

- JavaScript is a dynamic, extensible language with deep support for meta-programming. The bookmarklet code, running in the context of the attacker's JavaScript context, cannot trust any of the APIs available to typical web applications—an attacker could have replaced them with malicious code. Relying too much on these APIs has created a class of vulnerabilities unique to web-based password managers.

  To fill in a password on (for example) dropbox.com, a password manager needs to successfully authenticate a user, download the (possibly encrypted) credential, decrypt it (if necessary), authenticate the web application, and, finally, perform the login. Doing all this in an untrusted website's scripting environment (as a bookmarklet does) is tricky.

  Three of the five password managers studied provide full-fledged bookmarklet support, and all of them were vulnerable to attacks ranging from credential theft to linkability attacks. Browser extensions, which modified the webpage, faced a similar problem in the past. Currently, both Firefox and Chrome instead provide native or isolated APIs for browser extensions.

  Unfortunately, popular mobile browsers, including Safari on iOS, Chrome on Android/iPhone, and the stock Android Browser, do not support extensions. As a result, web-based password managers often rely on bookmarklets instead.

User Interface Vulnerabilities:

- A major benefit of password manager automation is their inherent immunity to phishing attacks: a similar or look-alike domain name won't fool code that needs an exact match.

- But what if the password manager ITSELF is vulnerable to Phishing attacks?

- For example, consider what happens when a user clicks on a password manager's bookmarklet while not logged in to the password manager. A simple option is asking the user to login in an iframe. Unfortunately, this is trivial for the attacker to intercept and replace the iframe with a fake dialog. Since users cannot see the URL of an iframe, there is no way for a user to identify whether a particular iframe actually belongs to the password manager and is not spoofed. We argue that this is an anti-pattern that password managers should avoid.

Bookmarklet Vulnerabilities:

- (My1login *only* offers bookmarklet support, advertising it as a feature "No Installation Required!")
- When the user attempts to use a Bookmarklet to login to Evil.com (not knowing it's evil) it was possible for evil.com to hijack the bookmarklet and change the domain name to something else... like dropbox... and cause thge retrieval of the login credentials for dropbox instead of evil.com.

Web Vulnerabilities:

- Cross-Site Request Forgery (CSRF) and Cross-Size Scripting (XSS).
    - CSRF exploits the trust a site has in a user's browser.
    - XSS exploits the trust a user has in a site.

- CSRF vulnerabilities in LastPass, RoboForm, NeedMyPassword.
  XSS vulnerabilities in NeedMyPassword.

- Attack on LastPass:
    - LastPass user must first create a OTP.
    - Attacker knows User's LastPass username and somehow arranges to run their code inside the user's browser when the user's browser is accessing the LastPass site, thus exploiting the trust the LastPass site has in the user's browser...
    - Attacker can obtain an encrypted copy of the user's LastPass credential database.
    - However, since the attacker has no way of knowing the user's OTP, they cannot decrypt the database.
    - However:
        - The stored website names are not encrypted, so the attacker can know which sites the user uses with LastPass.
        - Also, armed with the encrypted record, an attacker can brute-force the user's master LastPass password.
        - Finally, the attacker, impersonating the user through CSRF, can delete credentials from the LastPass database despite being unable to obtain them.

- CSRF in RoboForm allow an attacker to update, delete, and add arbitrary credentials to a user's credential database.

- XSS in NMP allow for complete account takeover.

Authorization Vulnerabilities:

- Credential sharing -- Examples were given where PasswordBox and My1login could be exploited given nearly impossible-to-create circumstances. In one example, My1login's credential sharing gets "authentication" and "authorization" slightly confused. This potentially allows two 2nd parties, who are sharing differing credentials of a first party, to, under some difficult to create circumstances, conspire to cross-share some of the 1st party's credentials that weren't explicitly authorized.

User Interface Vulnerabilities:

- Bookmarklets are inherently worrisome. Powerful, but worrisome.

- If the user is not authenticated to their password manager, only My1login requires them to switch to a new tab and login. The other PMW's allow the user to login-in-place, which opens them to the possibility of phishing attacks.

- For example: With a RoboForm bookmarklet, when the user who is not already logged-in to RoboForm clicks the bookmarklet to login to another site, the code contained in the RoboForm bookmarklet injects an iframe into the currennt page to create a RoboForm login form. The trouble is... the URL remains showing the 3rd-party site, and the user is being trained that this is okay. Since JS must be enabled for any of this to work, it would be possible for an evil site's JS to be designed to override the bookmarklet's own code and capture the user's RoboForm login credentials. The user, who had been trained to expect to login to RoboForm through "evilsite", would never detect any problem.

Lessons, Conclusions & Mitigations:

- Bookmarklets are currently extremely difficult to implement securely because the bookmarklet's code inherently executes in the untrusted context of the target webpage.
- There is no safe way to login to a PWM's site from within another site's JS-enabled page.
- The ONLY way to use bookmarklets safely is to ALWAYS login first in another tab.
- The convenience of same-tab login is just not worth the risk.

- Some Authorization vulnerabilities stemmed from nonces that were predictably incrementing numbers. Their predictability was the problem. Switching to cryptographically secure random numbers would eliminate that threat.