Security Now! #571 - 08-02-16

RAID, Phishing & Filtering

This week on Security Now!

- LastPass vulnerabilities, new wireless keyboard headaches, deprecating SMS as a second authentication factor, obtaining Windows 10 for free after July, a bit of errata and miscellany, then discussions of RAID storage redundancy, the pervasive problem with website spoofing, and the power and application of multi-interface packet filtering.

Robb Stark @5stringplayer
@SGgrc Now this is how you Spin Right! pic.twitter.com/NHUl6WWXVT

(This guy is a SERIOUS SpinRite user!)

Security News

LastPass Vulnerabilities
https://bugs.chromium.org/p/project-zero/issues/detail?id=884
https://blog.lastpass.com/2016/07/lastpass-security-updates.html/
LastPass Blog:

> We want to share a quick update with the LastPass community about important fixes that we have made in response to two recent security reports. Our team worked directly with the security researchers to verify the reports made and issue a fix to LastPass users.
>
> The recent report only affects Firefox users. If you are a Firefox user running LastPass 4.0 or later, an update will be pushed via your browser with the fix in version 4.1.21a. If you would like to update your client proactively, you can update with our download link here: https://lastpass.com/lastpassffx. You can check which version you are running in your LastPass browser addon, under the More Options menu in About LastPass. If you are running LastPass 3.0, you are not impacted and do not need to update.
>
> Other browsers are not impacted by this report, and users do not need to take action for other browsers.
>
> As always, we appreciate the work of the security community to challenge our product and ensure we deliver a secure service for our users. More information on these fixes will be posted here shortly.

Update:

> Security is fundamental to what we do here at LastPass. Our first priority is always responding to and fixing reports as quickly as possible.
>
> In follow-up to recent news, we want to address in more detail two security reports that have been disclosed to our team. One report was disclosed yesterday, while the other report was responsibly reported and fixed over a year ago. Notably, both exploits do require tricking a user via a phishing attack into going to a malicious website.
>
> The first report was responsibly disclosed to our team over a year ago by security researcher Mathias Karlsson, and fixed at that time. Karlsson recently posted his findings on the URL parsing bug. All browser clients were updated and Karlsson confirmed our fix at that time, requiring no action from our users.
>
> The second report was made yesterday by Google Security Team researcher Tavis Ormandy, who contacted our team to report a message-hijacking bug that affected the LastPass Firefox addon. First, an attacker would need to successfully lure a LastPass user to a malicious website. Once there, Ormandy demonstrated that the website could then execute LastPass actions in the background without the user's knowledge, such as deleting items. As noted below, this issue has been fully addressed and an update with a fix was pushed for all Firefox users using LastPass 4.0.

Thank you again to Tavis and Mathias, and others in the security community, for their responsible disclosure. We value their work that helps us build a stronger, more secure product.

Notes:
In v4 of LastPass for Firefox (not pre-v4 and not non-Firefox (I was running v3.3.1)) Tavis found a means for malicious page script to inject its own messages into the LastPass add-on for processing.

Keysniffer: More fun with wireless keyboards

- Recall that when we first covered this topic, the keyboard's 8-bit ASCII was being XORed with a static "secret"... this simply statically mapped every character to another. So a simple character frequency analysis would quickly find the XOR "syndrome" value.
- http://www.keysniffer.net/affected-devices/
- We're approaching DEFCON FUN time again! (#24 - started 24 years ago, in 1992)
    - (August 4-7, this Thursday - Sunday)

- Last Tuesday security firm Bastille revealed a new set of wireless keyboard attacks they're calling "Keysniffer". The technique, to be detailed at Defcon 24 later this week, allows any hacker with a $12 radio device to intercept the connection between any of eight wireless keyboards and a computer from 250 feet away. What's more, it gives the hacker the ability to both type keystrokes on the victim machine and silently record the target's typing.

- How? The definition of "no security through obscurity"

- Non-Bluetooth, 2.4 Ghz band, no encr

- NO ENCRYPTION was used... only obscure custom radio signals.

- And these are not no-brand keyboards!: Anker, EagleTec, General Electric, Hewlett-Packard, Insignia, Kensington, Radio Shack, Toshiba.

- Each of the vulnerable keyboards is susceptible to both keystroke sniffing and keystroke injection attacks. Keystroke sniffing enables an attacker to eavesdrop on every keystroke a victim types on their computer from several hundred feet away. The attacker can recover email addresses, usernames, passwords, credit card information, mailing addresses, and other sensitive information.

- The keyboards vulnerable to KeySniffer use USB dongles at the computer-end which continuously transmit radio packets at regular intervals, enabling an attacker to quickly survey an environment such as a room, building or public space for vulnerable devices regardless of the victim’s presence. This allows an attacker to locate vulnerable keyboards whether a user is at the keyboard and typing or not, and set up to capture information when the user starts typing.

- In addition to eavesdropping on the victim’s keystrokes, an attacker can inject their own malicious keystroke commands into the victim’s computer. This can be used to install

malware, exfiltrate data, or any other malicious act that a hacker could perform with physical access to the victim's computer.

- What to do?? The transceivers used in wireless keyboards vulnerable to KeySniffer are inherently insecure due to a lack of encryption, and do not support firmware updates. Users of vulnerable keyboards should switch to Bluetooth or wired keyboards in order to protect themselves from keystroke sniffing and injection attacks.

NIST's new guidelines -- phase out SMS 2nd-factor
http://thehackernews.com/2016/07/two-factor-authentication.html
http://fortune.com/2016/07/26/nist-sms-two-factor/
https://pages.nist.gov/800-63-3/sp800-63b.html

- "If the out of band verification is to be made using an SMS message on a public mobile telephone network, the verifier SHALL verify that the pre-registered telephone number being used is actually associated with a mobile network and not with a VoIP (or other software-based) service. It then sends the SMS message to the pre-registered telephone number. Changing the pre-registered telephone number SHALL NOT be possible without two-factor authentication at the time of the change.
- OOB [Out of band verification] using SMS is deprecated, and will no longer be allowed in future releases of this guidance."

An "Assistive Technologies" backdoor into free Windows 10 Upgrade.
https://www.microsoft.com/en-us/accessibility/windows10upgrade
"Windows 10 free upgrade for customers who use assistive technologies"

- For the general public, the free upgrade offer for Windows 10 ends on July 29. However, if you use assistive technologies, you can still get the free upgrade offer even after the general public deadline expires as Microsoft continues our efforts to improve the Windows 10 experience for people who use these technologies.
  With the Windows 10 Anniversary Update, we've taken a number of steps to improve the accessibility of Windows 10 accessibility. To learn more, read our blog that details some of these improvements.
- FAQ: When does the free upgrade offer extension end?
  - We have not announced an end date of the free upgrade offer for customers using assistive technology. We will make a public announcement prior to ending the offer.
- (So… if you've ever used and screen magnifier… :)

Never10??

- Has the push ended?
- I posed the question in GRC's "security now" newsgroup:
  Dave DeBruce: I never installed KB3035583 which installs the Get Windows 10 Installer. It has been sitting in my recommended updates for quite some time. Yesterday I noticed that after an update check, it is gone. So MS has at least pulled this update out. I know this is not what you asked but it does look as if they are pulling this stuff out.

- >1.750 million, dropping just below 10K/day

Errata

Bruce Wilson, Enterprise Architect, Oak Ridge National Laboratory. (@usethedata) confirmed my concern over Firefox not being immune to certificate tampering:
Regarding using firefox to avoid "corporate spying": If a Windows box is joined to an Active Directory domain, the corporation can run any arbitrary script on the box, including scripts to push a certificate into the Firefox certificate store. Fundamentally, if it's a corporately managed system, tools like SCCM (System Center Configuration Manager, formerly SMS (Systems Management Server)) allow the admins to do pretty much anything.

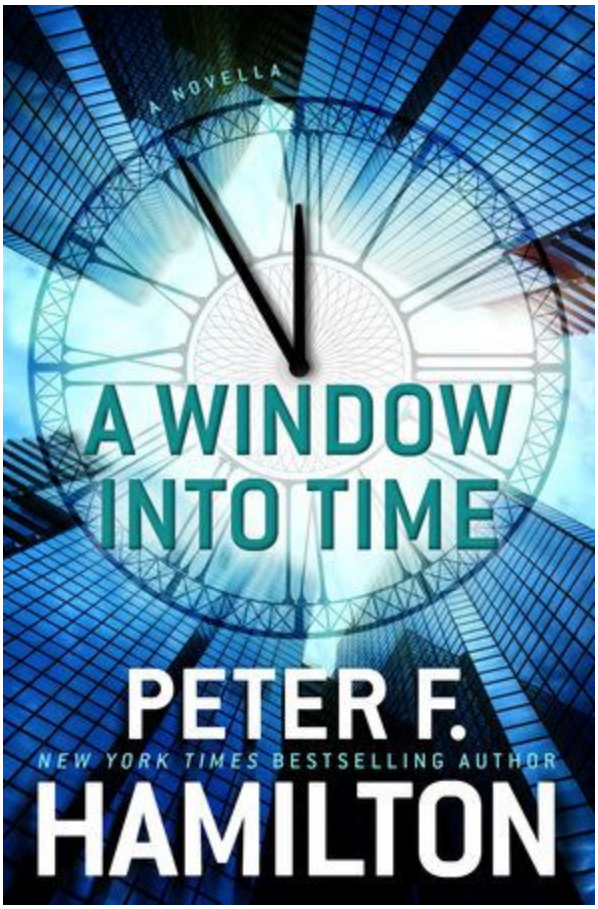
TIFF (.tif) lives!
Many people noted places where TIFF files are still in use. The two most common uses:

- Library sciences / archiving.
- Facsimile (fax) machine imaging.

I SHOULD have observed last week that file format never die. :)

Miscellany

Hamilton's new Novella "A Window into Time"



http://www.torbooks.co.uk/blog/2016/4/7/the-a-window-into-time-novella-peter-f-hamilton-cover-reveal
eBook / $4 / July 28th / 95 pages

Back Cover:
Whip-smart thirteen-year-old Julian Costello Proctor—better known as Jules—has an eidetic memory. For as long as he can remember, he has remembered everything. “My mind is always on,” he explains. But when an unexpected death throws his life into turmoil, Jules begins to experience something strange. For the first time, there are holes in his memory.

But that’s not the strangest part. What’s really weird isn’t what he’s forgotten; it’s what he remembers. Memories of another life, not his own. And not from some distant past. No, these memories belong to a man who’s alive right now.

With bravery, ingenuity, and quirky good humor, Jules devises a theory to explain this baffling phenomenon. While tracking down the identity of his mysterious doppelgänger, he finds himself enmeshed in the hopes and dreams of a stranger . . . and caught in the coils of a madman’s deadly plot.

Steverino (@DaMoisture)

- @SGgrc @AmazonKindle thanks for this fun little read, Steve! #awindowintotime was thoroughly enjoyable, and short!!

SpinRite:

Istvan Burbank / @ipburbank
Ah, I had used a Drobo for years before my own NAS, and have only good things to say about it (especially about being able to put different sized drives in. I ran SpinRite on friends broken drives, recovered the drive and copied their data to a new drive. And if the fixed drive was bigger than one of the drives in my Drobo, I would hot swap it in without much worry about the drive failing again due to the Drobo's redundancy and my Drobo's capacity would automagically increase.

RAID, Phishing & Filtering

What I learned about Drobo's BeyondRAID

- "Thin Provisioning" across multiple volumes
- The nature of redundancy
- RAID 5 - 1's compliment (XOR)
- RAID 6 - any two drives

The Phishing Problem

- If a user is NOT where they believe they are, trouble results.
- URL-based password managers provide some help here.
- QR Code systems have a challenge.
- SQRL’s “Client Provided Session” solution.

Packet Filtering

- Multi-interface packet filtering
- Traffic direction - New "connection" vs Established connection.
- Stateful packet filtering.