Security Now! #519 - 08-04-15

The Win10 Privacy Tradeoff

This week on Security Now!

- StageFright Update
- A DoS vulnerability in BIND
- PagerDuty suffered a database breach.
- OSX has a somewhat worrisome 0-day in the wild.
- NoScript versus Sandboxie
- Miscellany
- Examining what we know of the Windows 10 Privacy Tradeoff

Security News

More on StageFright

- https://www.eff.org/deeplinks/2015/07/horror-horror-stagefright-androids-heart-darkness
- Exploits HAVE appeared in kits and the vulnerability IS being exploited in he wild.
- Mitigations:
  - DEFINITELY keep device updated
  - Disable Auto-fetching of MMS for both Hangout and regular messaging apps.
  - Open Hangout:
    - Options / Settings / SMS / Advanced
      - "Auto Retrieve MMS"
  - Messages
    - More / Settings / More Settings
      - Multimedia Messages -> disable "Auto Retrieve."

Major flaw could let lone-wolf hacker bring down huge swaths of Internet

- Latest critical bug in widely used DNS server underscores its fragility.
- http://arstechnica.com/security/2015/07/major-flaw-could-let-lone-wolf-hacker-bring-down-huge-swath-of-internet/
- Transaction Key Records
- All major versions of BIND v9.
- Send a malformed packet to vulnerable servers crashes them.
- A fix was made available before the flaw was disclosed.
- Reports of the bug now being exploited in the wild.
- The trouble?... BIND (like OpenSSL) is too huge and too old.
  - It is the standard test bed for ALL possible DNS features.
  - It has grown and grown... and DNS servers do not need most of the features.

Pager Duty not only salts their passwords... they pepper them too. How do we know?

- http://www.theregister.co.uk/2015/07/31/incident_managers_pagerduty_pwned/?mt=1438638744425
- The company acknowledged the attacker "gained unauthorized access to our users' names, email addresses, public calendar feed URLs, and hashed, salted and peppered passwords".
- <quote> Based on the investigation, the attacker bypassed multiple layers of authentication and gained unauthorised access to an administrative panel provided by one of our infrastructure providers. With this access, they were able to log into a replica of one of PagerDuty's databases. The evidence indicates that the attacker gained access to users' names, email addresses, hashed passwords and public calendar feed URLs.
- Users who do not reset their password by Monday, August 3 at 12:00pm Pacific Time will be automatically logged out of the website and will receive an email prompting them to reset their password.
- <quote> We use robust hashing techniques to protect passwords. If you have logged into your account anytime this year, your password is hashed with Bcrypt with a work factor of 10, using a per-user randomly generated salt and a site-wide pepper. Older passwords were hashed with SHA-1 over multimple rounds and using the same salt and pepper approach. We have no evidence that the attacker was able to access the pepper. Both the salt and pepper are 40 characters long and are randomly generated.

0-day bug in fully patched OS X comes under active exploit to hijack Macs

- Privilege-escalation bug lets attackers infect Macs sans password.
- http://arstechnica.com/security/2015/08/0-day-bug-in-fully-patched-os-x-comes-under-active-exploit-to-hijack-macs/
- Being exploited in the wild to install malware w/o requiring any password from user.
- But... the bad code still needs to find a way to run first.
- Latest current versions 10.10.4 and beta 10.10.5 are vulnerable.
- Fixed in beta of OSX 10.11

NoScript vs Sandboxie

- The evolution of scripting and distributed content sources.

Miscellany

PodCall

- http://www.podcall.io/

SpinRite

Jeff Lunt, Evanston, Illinois
Subject: SpinRite testimonial
Date: 15 Jul 2015 18:51:49
:

Hey Steve,

Huge fan of the Security Now Podcast. Listener since episode 1 (blah, blah, blah).

I've been a fan of regularly backing up my data since my first major data loss at the age of 19, and while I've lost a drive or two in my time I can't offer one of those, "Really saved my bacon," kinds of testimonials, because since that first data loss I've always had a backup for my truly important data. That said I've also always been frustrated with disk utility tools built into OSes when something like SpinRite is the only thing that really does the complete maintenance and recovery job.

I recently bought a copy of SpinRite to fix some of the drives in my media server, and just wanted to drop you a line and say thanks for the awesome tool. While storage is cheap and it's easy to replace a dead drive (assuming you have a good backup) and go about your day, I just like the idea that I don't have to throw out a drive just because CHKDSK in Windows, or fsck in Unix/Linux, or Disk Utility on Mac can't do anything useful with it. SpinRite is a great piece work, and the stuff you're doing with Security Now, I think, qualifies you as a pretty great human being on the whole.

Keep up the great work!

The Win10 Privacy Tradeoff

In the press:

- Microsoft's Windows 10 is a privacy nightmare. Here's how to protect yourself.
  - http://www.slate.com/articles/technology/bitwise/2015/08/windows_10_privacy_problems_here_s_how_bad_they_are_and_how_to_plug_them.html
- 'Incredibly intrusive': Windows 10 spies on you by default
  - http://www.rt.com/usa/311304-new-windows-privacy-issues/
- Backlash grows over privacy in 'freemium' Windows 10
  - http://www.computing.co.uk/ctg/news/2420044/backlash-grows-over-privacy-in-freemium-windows-10

Windows 10 is not an OS for me.

- Tools or Toys?
- GRC's Windows Server 2000 -- it was a tool
  - But it didn't support the newer TLS cipher suites.
- My Windows XP machine -- it is a tool
  - Many of my utilities are 16-bits.
- I'll be moving to Windows 7
  - Support though the first term of our next President -- 2020.

A new "AdvertisingID" for each user on a device

- The ID can be used by third parties, such as app developers and advertising networks for profiling purposes.

Bitlocker's recovery keys are backed up into the OneDrive account.

WiFi Sense:

- Cross-Contact sharing must be enabled per-network.
- The only real annoyance is that when it's enabled it's with ALL contacts in a group, NOT with selected contacts.

#1 Recommendation: When installing, DO NOT CHOOSE "Express Install"

- and you can disable as Win10 is installed.

Settings / Privacy

General

- Let apps use my advertising ID for experiences across apps.
- Send Microsoft info abouthow I write to help us improve typing and writing in the future.
- Let websites provide locally relevant content by accessing my language list.
- Manage my Microsoft advertising and other personalization info
- (Link to MS webite: Microsoft personalised ad preferences)
    - https://choice.microsoft.com/en-gb/opt-out
    - "Personalized ads in this browser"
    - "Personalized ads whenever I use my Microsoft account"
        - (Including Windows, Windows phone, Xbox & other devices.)
    - Check back to see whether "Personalized ads in this browser" setting remains OFF if you have opted out... There have been early reports of it mysteriously turning itself back on.

Location

- Global -- for all users of the machine -- defaults ON
    - BUT... all individual apps default to OFF

Camera

- Defaults ON and all apps default ON.
    - App Connector, Edge, MSN Food & Drink, OneNote

Microphone

- Defaults ON and all apps default ON..
    - Edge, Voice Recorder, Xbox

Speech, Inking, Typing

- "Getting to know you"
- "Windows and Cortana can get to know your voice and writing to make better suggestions for you. We'll collect info like contacts, recent calendar events, speech and handwriting patterns, and typing history."
    - --> "Stop getting to know me" button
- Manage Cloud Info
    - Go to Bing and manage personal info for all your devices.
    - Learn more about speech, inking, and typing settings.
    - Privacy Statement.

Account Info

- Let apps access my name, picture and other account info. -- Default ON.
- Choose the apps that can access your account info…
    - <<none present or listed for me>>

Contacts

- Choose apps that can access contacts
    - App Connector
    - Mail & Calendar
    - Windows Shell Experience

Calendar

- Let apps access my calendar - Default ON
    - App Connector
    - Mail & Calendar

Messaging

- Let apps read or send messages (text or MMS) - Default ON
    - Choose apps that can read or send messages

Radios

- Some apps use radios--like Bluetooth-- in your device to send and receive data. Sometimes, apps need to turn these radios on and off to work their magic.
- Let apps control radios -- Defaults ON.
- Choose apps that can control radios
    - <<none present or listed for me>>

Other devices

- Sync with devices - Default ON
- Let your apps automatically share and sync info with wireless devices that don't explicitly pair with your PC, tablet, or phone. Example: beacons.
- Choose apps that can sync with devices.

Feedback & Diagnostics

- Feedback frequency: "Windows should ask for my feedback"
    - Automatically (Recommended)
    - Always / Once a day / Once a week / Never

Background Apps

- Let apps run in the background
- Choose which apps can receive info, send notifications, and stay up-to-date, even when you're not using them. Turning background apps off can help conserve power.
    - Alarms & clock
    - Food & drink
    - Groove Music
    - Health & Fitness
    - Mail
    - Maps
    - Microsoft Edge
    - One Note
    - People
    - Phone Companion
    - Photos
    - Store
    - Weather
    - Xbox

Cortana

- Configure what you need.
- By default Cortana has visibility into pretty much everything in order to improve performance.
- Ex: Location, location history, contacts, search history, calendar details, content and communication history from messages and apps, "and (any) other information on your device (computer).
- In Microsoft Edge, Cortana collects and uses your browsing history.
- From the Privacy Agreement:
    - To enable Cortana to provide personalized experiences and relevant suggestions, Microsoft collects and uses various types of data, such as your device location, data from your calendar, the apps you use, data from your emails and text messages, who you call, your contacts and how often you interact with them on your device.

      Cortana also learns about you by collecting data about how you use your device and other Microsoft services, such as your music, alarm settings, whether the lock screen is on, what you view and purchase, your browse and Bing search history, and more.

Whether to tie your local Windows account into your Microsoft account?

- You may wish to remove your Microsoft account from Win10 and use a local account instead.
- You lose synchronization across all Win10 PCs
- Settings / Accounts