Security Now! #462 - 07-01-14

Cloud Storage Solutions

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!

- Microsoft's security news hits Canadian anti-SPAM legislation
- Apple updates iOS
- Paypal's security misfires
- And speaking of which... a quick look at ProtonMail
- Greenpeace and the EFF go flying
- Facebook social-engineering mischief
- A frightening comment in Android's code.
- And more…

Security News:

Microsoft stops delivering security news by eMail
Today being July 1st, Next Tuesday will be the earliest possible 2nd Tuesday of the month.
CASL - Canada's Anti-Spam Law

- Signed into law last January, with six-month "get ready" grace period.

Brian Krebs Reports: Experts are baffled by Microsoft's decision:

- <"> Neil Schwartzman, executive director of the Coalition Against Unsolicited Commercial Email (CAUCE), said CASL contains carve-outs for warranty and product safety and security alerts that would more than adequately exempt the Microsoft missives from the regulation.
- Brian writes: Indeed, an exception in the law says it does not apply to commercial electronic messages that solely provide "warranty information, product recall information or safety or security information about a product, goods or a service that the person to whom the message is sent uses, has used or has purchased."
- Schwartzman said: "I am at a complete and total loss to understand how the people in Redmond made such an apparently panicked decision," noting that Microsoft was closely involved in the discussions in the Canadian parliament over the bill's trajectory and content.
- Schwartzman said: "This is the first company I know of that's been that dumb."
- **But then, yesterday: Update, 5:40 p.m. ET:** In an apparent reversal of its decision, Microsoft now says it will be re-starting its security notifications via email early next month. From a Microsoft's spokesperson: "On June 27, 2014, Microsoft notified customers that we were suspending Microsoft Security Notifications due to changing governmental policies concerning the issuance of automated electronic messaging. We have reviewed our processes and will resume these security notifications with our monthly Advanced Notification Service (ANS) on July 3, 2014."

Paypal freezes ProtonMail's IndieGoGo Campaign Funds (Yesterday)

- https://protonmail.ch/blog/paypal-freezes-protonmail-campaign-funds/
- This morning, we received an email and telephone call from PayPal notifying us that our account has been restricted pending further review. At this time, it is not possible for ProtonMail to receive or send funds through PayPal. No attempt was made by PayPal to contact us before freezing our account, and no notice was given.

  Like many others, we have all heard the PayPal horror stories, but didn't actually think it would happen to us on our campaign since PayPal promised, very recently, to improve their policies. Unfortunately, it seems those were hollow promises as ProtonMail is now the latest in a long string of crowdfunding campaigns to be hit with account freezes. (For examples, just look here, here, and here).

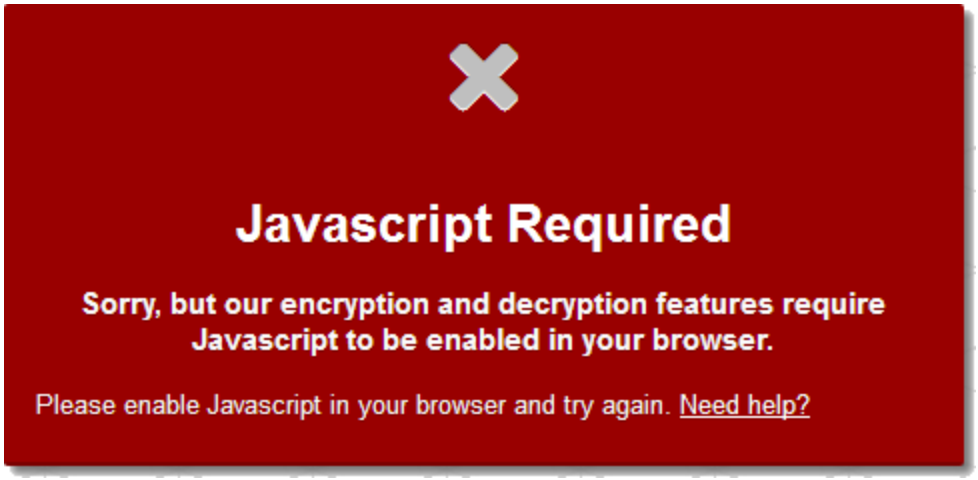
  While the $275,000 ProtonMail has raised in the past 2 weeks is a large amount, it pales in comparison to many other crowdfunding campaigns that have raised sums in excess of $1,000,000 so we can't help but wonder why ProtonMail was singled out. When we pressed the PayPal representative on the phone for further details, he questioned whether ProtonMail is legal and if we have government approval to encrypt emails. We are not sure which government PayPal is referring to, but even the 4th Amendment of the US constitution guarantees:

  > "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures…."

- Paypal has now unfrozen the account.

ProtonMail:

- Swiss secure eMail crowdfunded startup
- Web-based, cross-platform, browser-side JavaScript encryption.



Their points:

- Zero Access to User Data : Your data is never accessible to us.
  - ProtonMail's segregated authentication and decryption system means logging into a ProtonMail account requires two passwords. The first password is used to

authenticate the user and retrieve the correct account. After that, encrypted data is sent to the user. The second password is a decryption password which is never sent to us. It is used to decrypt the user's data in the browser so we never have access to the decrypted data, or the decryption password. For this reason, we are also unable to do password recovery. If you forget your decryption password, we cannot recover your data.
    - (Why not simply use a hash of the hash?... much as Lastpass does?)

- Securely communicate with other email providers : Even your communication with non-ProtonMail users is secure.
    - We support sending encrypted communication to non-ProtonMail users via symmetric encryption. When you send an encrypted message to a non-ProtonMail user, they receive a link which loads the encrypted message onto their browser which they can decrypt using a decryption passphrase that you have shared with them. You can also send unencrypted messages to Gmail, Yahoo, Outlook and others, just like regular email.

- Self Destructing Messages. :("With ProtonMail, emails are no longer permanent."
    - You can set an optional expiration time on ProtonMail's encrypted emails, so they will be automatically deleted from the recipient's inbox once they have expired. This way there are no "trails" of sent messages. Similar to SnapChat in a way, we've added a way for you to have even more ephemeral communication.

Apple updates iOS to v7.1.2

- http://support.apple.com/kb/HT6297
- Update the iOS certificate root store
- Rather LONG list of fixes
    - Many remote code execution fixes
    - eMail data protection for attachments
    - Malicious "Find My Phone" disabling
    - Two Lock screen bypasses
    - Siri Hack
    - Many fixes to WebKit

- Mac OS X and Apple TV updates were nearly identical -- common codebase.
- ***(Remember to re-disable Bluetooth!)***

Beautiful High-Res Pics of the new Utah NSA Data Center:

- http://bit.ly/nsa-in-utah-1
- http://bit.ly/nsa-in-utah-2
- Greenpeace & EFF overflew the NSA Utah Data Center in a lighter-than-air ship.

Alexa's Top 50 HTTPS Results: http://bit.ly/alexahttps
Some interesting takeaways:

- 29 out of 50 (58%) worked perfectly over https
- Google (internationally) consistently offers SSL everywhere, and in some countries like US and Canada, even defaults to SSL on its own
- It appears that every Alexa-ranked company from China offers NO SSL, which facilitates gov censorship
- Amazon, Yandex, Instagram, Ebay, Craigslist all force HTTP (as does OpenDNS non-dashboard use), likely due to mixed content.

Facebook and the Ethics of User Emotional Manipulation

- http://techcrunch.com/2014/06/29/facebook-and-the-ethics-of-user-manipulation/
- http://www.pnas.org/content/111/24/8788.full
- http://www.forbes.com/sites/kashmirhill/2014/06/29/facebook-doesnt-understand-the-fuss-about-its-emotion-manipulation-study/
- Two Cornell University and a Facebook researcher.
- 689,003 users' Facebook News Feeds were deliberately manipulated to see whether it would elate or depress them. Based upon an analysis of their subsequent behavior... it did.
- Facebook's justification: Buried in the 9,045-work Terms of Service, there's a line acknowledging that any user's data may be used for "research."
- "How we use the information we receive"
    - We use the information we receive about you in connection with the services and features we provide to you and other users like your friends, our partners, the advertisers that purchase ads on the site. For example, in addition to helping people see and find things that you do and share, we may use the information we receive about you:
        - for internal operations, including troubleshooting, data analysis, testing, research and service improvement.

Serious Android crypto key theft vulnerability affects 86% of devices

- (Later corrected to be 10.3% of devices -- only v4.3)
- http://arstechnica.com/security/2014/06/serious-android-crypto-key-theft-vulnerability-affects-86-of-devices/
- This was SO BAD that IBM privately disclosed this to the Android team NINE MONTHS AGO, on September 9th, 2013... and then waited until Android v4.3 was replaced by KitKat and mostly drained out of the market.
- Android v4.3 has a stack-based buffer overflow in the code designed to protect Android's "KeyStore" where applications store their highly sensitive cryptographic keys and other material.
- Due to other exploit thwarting countermeasures, including ASLR and DEP, successful exploitation requires a malicious app to be installed onto the device.
- Fixed in KitKat -- v4.4.
- IBM Security Researchers
    - http://securityintelligence.com/android-keystore-stack-buffer-overflow-to-keep-things-simple-buffers-are-always-larger-than-needed/#.U67SaLEyC6L

    - Title: Android KeyStore Stack Buffer Overflow: To Keep Things Simple, Buffers Are Always Larger Than Needed
    - Comment in the vulnerable source code:

      ```
      /* KeyStore is a secured storage for key-value pairs. In this implementation,
       * each file stores one key-value pair. Keys are encoded in file names, and
       * values are encrypted with checksums. The encryption key is protected by a
       * user-defined password. To keep things simple, buffers are always larger than
       * the maximum space we needed, so boundary checks on buffers are omitted. */
      ```

    - Though things are simple, buffers are not always larger than the maximum space they needed.

- Successfully exploiting this vulnerability leads to a malicious code execution under the keystore process. Such code can:
    - Leak the device's lock credentials. Since the master key is derived from the lock credentials, whenever the device is unlocked, 'Android::KeyStoreProxy::password' is called with the credentials.
    - Leak decrypted master keys, data and hardware-backed key identifiers from the memory.
    - Leak encrypted master keys, data and hardware-backed key identifiers from the disk for an offline attack.
    - Interact with the hardware-backed storage and perform crypto operations (e.g., arbitrary data signing) on behalf of the user.

Miscellany:

Charlie Gulf @CharlieGulf

- @SGgrc Re: last week's Google Docs question. New anonymous users seemed to be created every time you view the doc link w/o signing in first.

A "Hydrogen Economy?" or an Ammonia Economy

- Hydrogen breakthrough could be a game-changer for the future of car fuels
- http://phys.org/news/2014-06-hydrogen-breakthrough-game-changer-future-car.html
- http://bit.ly/NH3-Cracking
- Ammonia = NH3
- http://en.wikipedia.org/wiki/Ammonia_production

SQRL:

- Crowdin.net: 60 languages, 414 translators
- Now gluing all of the pieces together.

SpinRite:

Date: Thu, 26 Jun 2014 07:05:54 -0700
From: "Steffen Zacher Nielsen"

Hello Steve

I've just purchased Spinrite, as the only tool which was able to solve the problem I had with a damaged hard drive. Spinrite was able to repair the drive so that I was then able to restore about 3500 VERY important files to another drive.

I must say, it is very satisfying to use a strong and cheap tool like Spinrite, and afterwards having such a good experience. Thank You very much, I can wipe off the sweat from my face and take a deep reliefing breath.

I've spread the good news of my experience with Spinrite to all my friends on Facebook, so perhaps your sales will increase in the future, who knows?

Steffen.

Cloud Storage Solutions

Why are we doing this?

- Cloud storage is "a thing"
    - Collapsing mass storage costs
    - Rising bandwidth and falling costs
    - Personal photos, movies, media collections.
- Cross-device
- MANY providers are not TNO secure.

Project Goal:

- We don't all have the same needs:
    - Some use Windows, some use Mac, some use Linux, some iOS, some Android.
    - We don't all have the same AMOUNT of data to store.
    - For some, the "free plan" is enough. Others need terabytes.
    - The economics of storage makes this practical.
    - “Buy a Plan” or “Pay for what you use?”
    - "Fitness Club Membership" or "Gift Cards" -- purchased but not used.
    - Amazon S3: Pay for what you actually use.
        - June: $2.51 / $0.0300 per GB - first 1 TB / month of storage used
        - 82.849 GB-Mo
        - Additional features
            - Reduced Redundancy Storage

            - "Glacier" (write-mostly with slower retrieval)
            - AWS Import/Export -- shipping TrueCrypt encrypted drives back and forth.
            - AWS Direct Connect -- dedicated network connection.
            - Popular services collect many add-ons.
        - Plenty of S3 browser extensions and clients.

    - Some people also have local NAS storage

    - Turnkey -or- Toolkit?
        - "Carbonite" users just want "turnkey" set and forget.
        - Not TNO, but zero-config ease-of-use IS what matters.
        - Better that than nothing... which would be the likely alternative.

    - Toolkit:
        - My *personal* sweet spot: A "decoupled" multi-platform client and a solid storage provider.
        - MUST be more involved and take more responsibility, but get more flexibility in return
        - Freedom to choose the optimal client.
        - Freedom to choose the optimal provider.
        - Less lock-in: Ability to migrate across providers if necessary.

    - Hybrid Solutions:
        - Google Drive:
        - Strong web-based convenience for casual cloud sharing.
        - And automated client-side access to "The Vault".
        - But perhaps S3 for the vault and Google Drive for the browser.

Solution Components:

- Internet-based storage provision
- Client Side Tools
- Roaming Web Access

My current list:

- Air Backup
- Amazon S3
- ArqBackup
- Bitcasa
- BoxCryptor
- BackBlaze
- CloudBerry
- CrashPlan
- Duplicati.com
- Filosync
- Mega

- OneDrive (Azure?)
- Tresorit
- SpiderOak
- Sync.com
- SyncThing.net
- Tarsnap
- Younited
- Viivo
- Wuala
- Zoolz.com
- >>> what have I missed? <<<

Cloud Storage Solutions Framework:

- http://bit.ly/sn-css
- https://docs.google.com/spreadsheets/d/1j4S6veVDiuIhwT7hxfxtO5xRaBQFdEmE5-kXjT5rM2w/edit?usp=sharing

Send feedback for next week: