Security Now! #530 - 10-20-15

Doing It Wrong

This week on Security Now!

- An emergency Adobe FLASH vulnerability
- Sneaking naughty iOS apps past Apple's scrutiny
- Thoughts about iPhone memory-gate, recent movies, pfSense
- A look at four examples (from just this week) of doing it wrong.
  - 1Password
  - Target stores public address system
  - Chip & Pin design
  - Sandboxie

MY COMPUTER DOESN'T WORK! THE HARD DRIVE CRASHED! WHAT DO I DO?!
DID YOU BACK UP?
WHY? IS IT GONNA BLOW?!
STEINFELD ©96

Security News:

New Adobe Flash Zero-Day Used in Pawn Storm Campaign Targeting Foreign Affairs Ministries

- http://blog.trendmicro.com/trendlabs-security-intelligence/new-adobe-flash-zero-day-used-in-pawn-storm-campaign/
- https://threatpost.com/emergency-adobe-flash-update-coming-next-week/115050/
- https://bgr.com/2015/10/15/adobe-flash-player-security-vulnerability-warning/
- Last Tuesday was not only Patch Tuesday, but also Flash Tuesday... but shortly afterward a new 0-day was found in the wild.
- Researchers at Trend Micro have discovered the current Flash zero day exploits used in spear phishing emails with relevant political or military theme subject lines. The emails contain links to websites hosting the zero day exploit.
- Adobe confirms major Flash vulnerability, and the only way to protect yourself is to uninstall Flash
- Adobe admirably rushed out a fix VERY quickly
- v19.0.0.226

iOS Apps Caught Using Private APIs

- https://sourcedna.com/blog/20151018/ios-apps-using-private-apis.html
- http://www.iclarified.com/52062/ad-sdk-caught-collecting-private-user-information-apple-pulls-hundreds-of-apps
- Apple removes apps from store that could spy on data traffic
  - http://www.computerworld.com/article/2991254/mac-os-x/apple-removes-apps-from-store-that-could-spy-on-data-traffic.html
- Objective C APIs are invoked by string names.
- The strings can be assembled on the fly to avoid static analysis.
- The Youmi SDK first played with obtaining the "Frontmost App name"
- Then... they became more aggressive:
  - Enumerate the list of installed apps or get the frontmost app name
  - Get the platform serial number
  - Enumerate devices and get serial numbers of peripherals
  - Get the user's AppleID (email)
- SourceDNA writes: Apple has been locking down private APIs, including blocking apps from reading the platform serial number in iOS 8. Youmi worked around this by enumerating peripheral devices, such as the battery system, and sending those serial numbers as a hardware identifier.
- Users of the SDK were likely innocent.
- The Youmi SDK sends the data back to Youmi servers.
- But, but, but…
  - Relying on a "string search" to find the names of functions applications are not allowed to call... is the worst, most ridiculous and error-prone approach imaginable.

Miscellany:

Via Simon Zerafa:

- https://twitter.com/FioraAeterna/status/656152979913863168
- When someone notices that there's a 0.2% difference in memory performance between different brands of memory used in iPhones, we will at least have the consolation that it'll be called "NAND-gate"! (Thanks Simon.)

Movies:

- Brent England (@brentos) 10/19/15, 5:36 AM
  - @SGgrc have you posted your comments/review of the Martian movie? Interested in your thoughts.
- The Martian...
- Steve Jobs...

pfSense:

- Greg Mackay (@gregmackay) 10/18/15, 5:13 PM
  - @SGgrc You're using pfSense now? Roll your own or off the shelve box? More details in future episode of Security Now?

- Mike in Tracy, CA (Subject: Sprinrite recovers Tivo Drive)
  - Date: 15 Oct 2015 06:06:37

    Steve,

    Thank you
    SpinRite repairs non bootable Tivo Premiere HDD.
    After SpinRite level 2 repaired the drive to a bootable condition.
    I then promptly copied the contents to a larger drive.

    Several weeks ago you talked about PfSense can you tell us more about how you have it configured?

    Thank you, Mike

SpinRite:

Al in Wisconsin
Date: 19 Oct 2015 09:22:47
:
Hi Steve and Leo

Last month I had 5 laptops come into the shop with "It's slow" complaints and it turned out that all 5 had hard drive issues quickly detected by SpinRite. Afterward my clients reported immediate and sometimes unbelievable speed increases. Thank you for making me look great to my clients.

Doing It Wrong: 1Password
http://myers.io/2015/10/22/1password-leaks-your-data/
http://www.telegraph.co.uk/technology/internet-security/11939920/Password-manager-1Password-criticised-for-leaking-users-bookmarks.html

Dale Myers, Microsoft software engineer currently working on Office for iOS and OS X.
Title: "1Password Leaks Your Data"
1st line: "Seriously."

<Paraphrasing Dale for Brevity> "1PasswordAnywhere" is a feature of 1Password which allows you to access your data without needing their client software. If you browse to your .agilekeychain “file” on disk, you find that it is actually a directory. Inside this directory is a file named “1Password.html”. If you access this file over HTTP, you will be greeted with a grey page which has a lock image and a password field. Enter your password and your keychain will unlock and you have a read only view of your data.

So what’s the problem? Well, it turns out that none of the accompanying metadata is encrypted!

I discovered this (writes Dale) after having a sync issue with Dropbox (I use Dropbox to host my keychain). The file that had issues was 1Password.agilekeychain/data/default/contents.js. Being a curious kind of guy I opened the file to see what was in there. The answer is the name and address of every item that I have in 1Password. Every single one. In plain text.

For those of you thinking “So what?”, perhaps you have nothing of interest in there, but there are other considerations. Perhaps I signed up for somespecificpornsite.com and this isn’t something I want to broadcast. However, I’ve done just that. Anyone who knows the link to the main log in page for my keychain can obtain this file. They can go through and find out exactly what shady sites I have accounts on, what software I have licenses for, the bank card and accounts I hold, the titles of any secure notes I have, any anything else I’ve decided to store in there.

The second and possibly larger concern, is that the login URL is stored with the page's title -- all in plaintext. In other words, if I sign in at https://example.com/login then that URL is stored with the keychain entry. This is often not an issue, but it can be! I recently signed up with a large ISP in the UK and had to reset my password due to a bug on their system. I was sent an email with a reset link in the email. I click the link, enter a new password, and press submit. At this point two things happen. The first is that my password is reset. The second is that 1Password prompts to save my credentials. Since I used an auto-generated password and I like to keep my passwords secure, I click save. Now my new password is stored in my keychain. But what if my ISP's website didn't properly expire that eMail link after its use? Website developers aren’t perfect. We make bad decisions and sometimes dangerous ones. Maybe these guys made a mistake that is all too common… So I go back to my email and click the password reset link again. Sure enough, I get prompted with a screen where I can reset my password again. They didn’t check to see if I had already used the link. And now that reusable password reset link to my account is stored in my publicly accessible 1Password metadata. Anyone can go and paste this link into their browser and they have full access to my account.

(Dale writes:) Presumably I don't need to explain any more about how that is a huge issue?

But it gets worse. I decided to have a look to see just how bad things were. Thanks to people having links for easy access to their keychain on their websites, Google has indexed some of these. A simple search brings up results. By looking at one of these it was a simple matter to identify the owner of the keychain and where he lived. I know what his job is. I even know the names of his wife and children. If I was malicious, it would be easy to convince someone that I had compromised their account and had access to all of their credentials. Not to mention the fact that they have revealed their location online which may put their personal safety at risk.

So what did I do? Well, immediately I tried to reach out to AgileBits to make them aware of this serious data breach. When I received a response from one of their engineers I was given a few links to the details about their keychain and the assurance that not only were they aware of this breach, but it was by design.

> *When we built the keychain, were aware that it would be possible to see that a user has logins across different sites because it is unencrypted; while this might have some privacy implications if an attacker gained access to it, your passwords are never exposed or shared as they are encrypted by your Master Password and they do not appear in the keychain in any way.*

(Dale writes) Searching through the forums I found claims by employees that it was designed this way for performance reasons. The logic was that if all of the metadata was encrypted along with the passwords, then when the user unlocked their keychain, if they wanted to search for an entry, all entries would have to be decrypted to find what they were looking for. And that is correct. What I didn't understand, and asked AgileBits, was why not just encrypt the metadata file using the master password in some fashion, then they only have a single file to decrypt? Again, their reason was performance.

> *When we first developed AgileKeychain a few years ago, 1Password had significantly less processing power with which to function, and decrypting the keychain on the fly to do something as simple as a login search incurred huge performance penalties for our users. Because this provided a poor experience for our users, we decided against requiring extra decryption steps for this process.*

<sigh>
Moreover... I (Steve) did some more digging and discovered that back in 2012, three years ago, they were not sure whether their newer fully-encrypting solution would be completely cross-platform compatible, so they never made it the default. So there's something available, with a reduced feature set... but no one uses it.

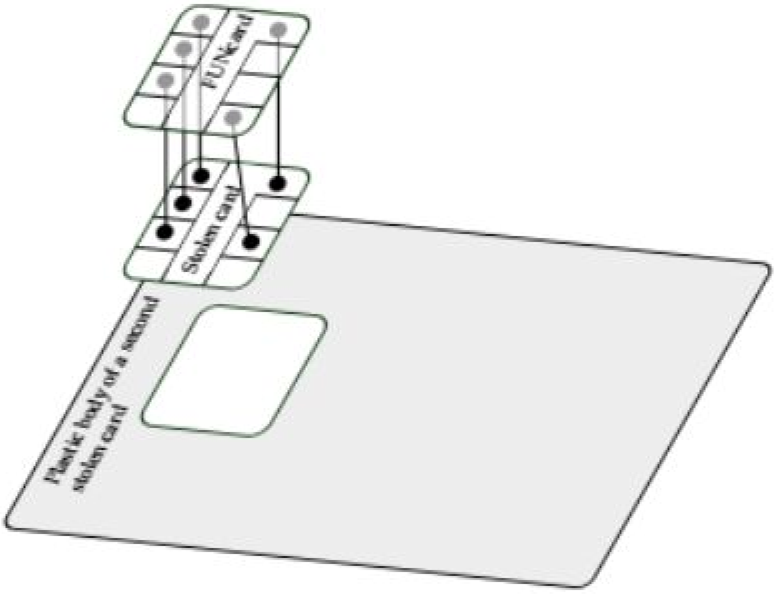
- Fundamental lack of understanding about their commitment and obligation to their users.
- Anyone can make a mistake, but these people have horrific judgement.

Doing It Wrong: Target stores attacked by pornographic prankster
http://www.bbc.com/news/technology-34556644
Dave Lee, the BBC's North American technology reporter, writes last Friday:

> *Gina Young was shopping at US superstore Target on Thursday morning - when she and the other shoppers suddenly heard a surprising announcement over the loudspeaker: Explicit audio from a pornographic film was blasted out for all to hear. And it kept playing. And playing. For 15 minutes.*
>
> *Ms. Young, who was shopping with her twin three-year-old boys, uploaded the clip to Facebook. (Obvious warning: it has rude audio.)*
>
> *"People were up in arms," she wrote. "Some people threw their things down and walked out. Others were yelling at employees."*
>
> *As pranks go, it's fairly low-grade. But Target has a problem. Staff at the store in Campbell, a small city just south of San Jose, were all but powerless to stop it due to how the PA system is designed.*
>
> *And it's not an isolated incident. According to local media, it's at least the fourth time this prank has happened since April. In one instance, a store had to be evacuated.*
>
> *So what's going on? Are mischievous staff causing trouble? Have Target's systems been hacked?*

Oh no... The Public Address system is tied into an extension on the phone. This conveniently allows anyone in the store to pickup a phone, dial the paging system, and announce anything. But... that telephone extension is universally accessible... including from the outside!
Exactly like connecting your internal network to the Internet without any firewall.

Doing It Wrong: Chip & PIN scam -- Ingenious and distressing
http://www.wired.com/2015/10/x-ray-scans-expose-an-ingenious-chip-and-pin-card-hack/
A THIN overlay authenticates any transaction.
The PIN isn't used to dynamically decrypt information on the card... but to simply verify the PIN.



Doing It Wrong: Sandboxie:
http://forums.sandboxie.com/phpBB3/viewtopic.php?f=11&t=21911&start=120
Post by Craig@Invincea » Sat Oct 17, 2015 11:10 pm

> *I would strongly recommend you update your browsers and plugins, and any other software. Please also turn off "install automatic updates" in Windows unless you have read the Microsoft notices on what these updates might affect & are comfortable with that.*
>
> *The update was a kernel patch in the OS, those causing access errors with SBIE.*
>
> *You can turn off "protected mode" in your FLASH plug-in in Firefox (we recommended that in the past) to also get around the issue.*
>
> *The new beta is v5.05.2. You also don't need flash plug in to run on all websites. Modern sites that use HTML 5 with render just fine in FF without it. Youtube and others are examples.*