Security Now! #448 - 03-25-14

iOS Security, Pt.3

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!

- An important Fix-It for a new 0-day vulnerability in Microsoft Word.
- What is the "Enhanced Mitigation Experience Toolkit" (EMET) ???
- Has WPA2 WiFi been cracked?
- Can you "text" ATM's to induce them to dispense cash?
- Gmail security advancement
- Perhaps Snowden oversteps?
- Another FireFox version on the way.

Security News:

New 0-Day in Microsoft Word

- The RTF renderer in Microsoft Word for Office 2003, 2007, 2010
- http://technet.microsoft.com/en-us/security/advisory/2953095
- <quote> Microsoft is aware of a vulnerability affecting supported versions of Microsoft Word. At this time, we are aware of limited, targeted attacks directed at Microsoft Word 2010. The vulnerability could allow remote code execution if a user opens a specially crafted RTF file using an affected version of Microsoft Word, or previews or opens a specially crafted RTF email message in Microsoft Outlook while using Microsoft Word as the email viewer. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. Customers whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights. Applying the Microsoft Fix it solution, "Disable opening RTF content in Microsoft Word," prevents the exploitation of this issue through Microsoft Word. See the Suggested Actions section of this advisory for more information.

  The vulnerability is a remote code execution vulnerability. The issue is caused when Microsoft Word parses specially crafted RTF-formatted data causing system memory to become corrupted in such a way that an attacker could execute arbitrary code. The vulnerability could be exploited through Microsoft Outlook only when using Microsoft Word as the email viewer. Note that by default, Microsoft Word is the email reader in Microsoft Outlook 2007, Microsoft Outlook 2010, and Microsoft Outlook 2013.

- Technet Blog:
  - http://blogs.technet.com/b/srd/archive/2014/03/24/security-advisory-2953095-r

ecommendation-to-stay-protected-and-for-detections.aspx

- <quote> The in the wild exploit takes advantage of an unspecified RTF parsing vulnerability combined with an ASLR bypass, which depends by a module loaded at predictable memory address.

  First, our tests showed that EMET default configuration can block the exploits seen in the wild. In this case, EMET's mitigations such as "Mandatory ASLR" and anti-ROP features effectively stop the exploit. You can find more information about EMET at http://www.microsoft.com/emet. The exploit code seems to target Word 2010 and it deeply relies on the specific ASLR bypass mentioned. We were glad to see in our tests that this exploit fails (resulting in a crash) on machines running Word 2013, due to the ASLR enforcement introduced for this product.

What is the "Enhanced Mitigation Experience Toolkit" (EMET) ???

- Adds a number of additional behavioral monitors into the Windows kernel:
  - Data Execution Prevention (DEP) Security Mitigation
  - Structured Execution Handling Overwrite Protection (SEHOP) Security Mitigation
  - NullPage Security Mitigation
  - Heapspray Allocation Security Mitigation
  - Export Address Table Filtering (EAF) Security Mitigation
  - Mandatory Address Space Layout Randomization (ASLR) Security Mitigation
  - Bottom Up ASLR Security Mitigation
  - Load Library Check – Return Oriented Programming (ROP) Security Mitigation
  - Memory Protection Check – Return Oriented Programming (ROP) Security Mitigation
  - Caller Checks – Return Oriented Programming (ROP) Security Mitigation
  - Simulate Execution Flow – Return Oriented Programming (ROP) Security Mitigation
  - Stack Pivot – Return Oriented Programming (ROP) Security Mitigation

- v4.1 currently, v5.0 coming (at technical preview)
- <quote> The Enhanced Mitigation Experience Toolkit (EMET) is a utility that helps prevent vulnerabilities in software from being successfully exploited. EMET achieves this goal by using security mitigation technologies. These technologies function as special protections and obstacles that an exploit author must defeat to exploit software vulnerabilities. These security mitigation technologies do not guarantee that vulnerabilities cannot be exploited. However, they work to make exploitation as difficult as possible to perform.

- ((Why not just built in??))
  When EMET mitigations are applied to certain software or certain kinds of software, compatibility issues may occur because the protected software behaves similarly to how an exploit would behave.

- The following is a list of specific products that have shown compatibility issues with the mitigations that are offered by EMET. You will have to disable specific incompatible mitigations if you want to protect the product by using EMET. Be aware that the list takes into consideration default settings for the product. Compatibility issues may be introduced when you install certain add-ins or additional components to the standard software.

        - 7-Zip Console/GUI/File Manager
        - Adobe Acrobat/Acrobat Reader
        - Certain AMD/ATI video drivers
        - Apple iTunes
        - DropBox
        - Google Chrome
        - Google Talk
        - Oracle Java
        - Skype
        - Windows Media Player
        - Windows Live Photo Gallery

    - Fix-It: https://support.microsoft.com/kb/2953095
    - Disables RTF rendering in Word
    - Office 2013 has enforced ASLR and thus the vulnerability but immunity.

WPA2 WiFi Security Cracked!

- Science Daily / "Your source for the latest research news"
    - http://www.sciencedaily.com/releases/2014/03/140320100824.htm
    - "WPA2 wireless security cracked"
    - There are various ways to protect a wireless network. Some are generally considered to be more secure than others. Some, such as WEP (Wired Equivalent Privacy), were broken several years ago and are not recommended as a way to keep intruders away from private networks. Now, a new study reveals that one of the previously strongest wireless security systems, Wi-Fi protected access 2 (WPA2) can also be easily broken into on wireless local area networks (WLANs).

- Science Spot / Science News with Inderscience Research Spot
    - http://sciencespot.co.uk/wpa2-wireless-security-cracked.html
    - "WPA2 wireless security cracked"
    - Achilleas Tsitroulis of Brunel University, UK, Dimitris Lampoudis of the University of Macedonia, Greece and Emmanuel Tsekleves of Lancaster University, UK, have investigated the vulnerabilities in WPA2 and present its weakness. They say that this wireless security system might now be breached with relative ease by a malicious attack on a network. They suggest that it is now a matter of urgency that security experts and programmers work together to remove the vulnerabilities in WPA2 in order to bolster its security or to develop alternative protocols to keep our wireless networks safe from hackers and malware.

      The researchers have now shown that a brute force attack on the WPA2 password is possible and that it can be exploited, although the time taken to break into a system rises with longer and longer passwords.

- International Journal Information and Computer Security, Vol. 6, No. 1, 2014
- "Exposing WPA2 security protocol vulnerabilities"
    - "Icecream" & "transsubstantiation"
    - Results: "In some of the cases the key was very simple (case 1, 2), whereas in the other ones the key was too complex (case 3–10)."

- "Discussion"
  WPA/ WPA2 are considered amongst the most secure protocols. This is due to the fact, that even having an instance of the preshared key, it requires a dictionary attack to break it, which can last from a few minutes to several weeks, depending on the complexity of the key and the pluralism in words- records of the correspondent dictionary. The more complex the password is, the safer the network security will be. More precisely, words like: icecream, computer, clouds, wireless, mynet, airhouse, etc are commonly used, increasing the probability of finding the key in a short period of time. On the other hand, if the key consists of different types of characters (a combination of lower case, upper case, special characters and numbers) the complexity would be increased. Hence, the adversary must have a dictionary consisting of all the different combinations of all the printable ASCII characters of all the possible lengths, in order to ensure that (s)he will be able to find the secret key. In order to have a complete dictionary with all the different combinations of all the standard printable ASCII characters, the length (records) of the dictionary will be:

  <<< equation here >>>

  By performing the calculations, the complete dictionary would consist of 3.991929703310227 x 10^124 records. Thus, this procedure (that creates and searches the dictionary) will last several weeks using a simple computer, due to the required time which will be extremely high.

Symantec: "Texting ATMs for Cash Shows Cybercriminals' Increasing Sophistication"

- http://www.symantec.com/connect/blogs/texting-atms-cash-shows-cybercriminals-increasing-sophistication
- There is a growing chorus of voices calling for businesses and home users to upgrade existing Windows XP installations to newer versions of Windows, if not for the features, then at least for the improved security and support. ATMs are basically computers that control access to cash, and as it turns out, almost 95 percent of them run on versions of Windows XP. With the looming end-of-life for Windows XP slated for April 8, 2014, the banking industry is facing a serious risk of cyberattacks aimed at their ATM fleet. This risk is not hypothetical — it is already happening. Cybercriminals are targeting ATMs with increasingly sophisticated techniques.

  In late 2013, we blogged about new ATM malware in Mexico, which could let attackers force ATMs to spew cash on demand using an external keyboard. That threat was named Backdoor.Ploutus. Some weeks later, we discovered a new variant which showed that the malware had evolved into a modular architecture. The new variant was also localized into the English language, suggesting that the malware author was expanding their franchise to other countries. The new variant was identified as Backdoor.Ploutus.B (referred to as Ploutus throughout this blog).

  What was interesting about this variant of Ploutus was that it allowed cybercriminals to simply send an SMS to the compromised ATM, then walk up and collect the dispensed cash. It may seem incredible but this technique is being used in a number of places across the world at this time.

Gmail going HTTPS ONLY!

- Thursday, March 20th...
- http://gmailblog.blogspot.com/2014/03/staying-at-forefront-of-email-security.html
- <quote> Starting today, Gmail will always use an encrypted HTTPS connection when you check or send email. Gmail has supported HTTPS since the day it launched, and in 2010 we made HTTPS the default. Today's change means that no one can listen in on your messages as they go back and forth between you and Gmail's servers—no matter if you're using public WiFi or logging in from your computer, phone or tablet.
- <quote> In addition, every single email message you send or receive—100% of them—is encrypted while moving internally. This ensures that your messages are safe not only when they move between you and Gmail's servers, but also as they move between Google's data centers—something we made a top priority after last summer's revelations.

"Crypto 101" / https://www.crypto101.io/

- "Crypto for everyone."
- "Crypto 101 is an introductory course on cryptography, freely available for programmers of all ages and skill levels."

N.S.A. Breached Chinese Servers Seen as Security Threat

By DAVID E. SANGER and NICOLE PERLROTHMARCH 22, 2014
http://www.nytimes.com/2014/03/23/world/asia/nsa-breached-chinese-servers-seen-as-spy-peril.html

- <quote> The agency pried its way into the servers in Huawei's sealed headquarters in Shenzhen, China's industrial heart, according to N.S.A. documents provided by the former contractor Edward J. Snowden. It obtained information about the workings of the giant routers and complex digital switches that Huawei boasts connect a third of the world's population, and monitored communications of the company's top executives.

- One of the goals of the operation, code-named "Shotgiant," was to find any links between Huawei and the People's Liberation Army, one 2010 document made clear. But the plans went further: to exploit Huawei's technology so that when the company sold equipment to other countries — including both allies and nations that avoid buying American products — the N.S.A. could roam through their computer and telephone networks to conduct surveillance and, if ordered by the president, offensive cyberoperations.

- "Many of our targets communicate over Huawei-produced products," the N.S.A. document said. "We want to make sure that we know how to exploit these products," it added, to "gain access to networks of interest" around the world.

Firefox 29 Beta...

- (IT seems like just yesterday we were updating to FFv4.)
- http://thenextweb.com/apps/2014/03/20/firefox-29-beta-arrives-new-sync-tool-customization-mode-mozillas-user-interface-overhaul-australis/
- Complete UI overhaul
- Continued forward progress in standards support.

SQRL Update:

- Crowdin.net: 49 languages, 297 translators.
- (Last language: Korean)... will make 50.
- Where I am…
    - "Why I code" : https://www.grc.com/miscfiles/BinarySearch.png

SpinRite Testimonial:

From: Dick Snicket
Location: New York
Subject: SpinRite Saves Music
Date: 16 Mar 2014 19:33:13

Hi Steve,
I'm a music major in college and have a LOT of Sibelius music files on my computer. (Sibelius is a program for music notation/scores.) My computer died a few days ago and I had a backup on an external drive that was a week old. But during that week I had made quite a number of changes to woodwind and percussion parts of two movements of a marching band show for my former high school. The changes were quite precise, and I had sat down and consulted a professor to help me adjust the parts to the students' skill level. In short, if I lost these changes, it would have been a nightmare to reimplement them.

So I bought a copy of SpinRite, which I had heard about on the podcast. It took three hours to finish, and then the computer booted successfully and I got all of my files back. I have since set up Crashplan backup so that all of these important files get backed up. Next step: Choreograph the drill (peoples' positions on the field).

Thanks for such an awesome product and podcast! I can now get back to real work, without worrying about damage to anything I do in future. SpinRite is truly magic.

iOS Security / The White paper Part 3

http://images.apple.com/iphone/business/docs/iOS_Security_Feb14.pdf

So far:

- Secure Boot Chain (everything digitally signed).
- Software update security (custom per-device updates).
- Secure Enclave
    - Security co-processor with strictly limited communications.
- Hardware-enforced protection
- Locking and Unlocking
- Wear-Leveling Bypass
- Passcodes
- File System Protection
    - Data Protection Classes
    - “Complete Protection”
    - “Protected Unless Open”
    - “Protected Until First User Authentication”
    - “No Protection”

- App Security
    - Only Apps written by known and recognized developers can obtain a code signing certificate whose signatures iOS will verify and allow to load and execute.
    - Businesses can write in-house apps that do NOT need to go through Apple.
        - iOS Developer Enterprise Program (iDEP)
        - Obtain a "provisioning profile" to permit apps to run on devices it authorizes.
        - (Essentially allows a business to authorize its own apps.)

- Process Security
    - Apps are inherently "sandboxed" without any access to other apps resources, unless deliberately arranged by each end.
    - Installed in a randomly named file system directory.
    - ASLR is enabled for all Xcode-produced code.
    - iOS uses ARM's "Execute Never" (XN) feature which restricts where code can execute.

- Accessories
    - Require an authentication chip available from Apple.

Continuing:

AirDrop
iOS devices that support AirDrop use Bluetooth Low-Energy (BTLE) and Apple-created peer-to-peer Wi-Fi technology to send files and information to nearby devices.

When a user enables AirDrop, a 2048-bit RSA identity is stored on the device. Additionally, an AirDrop identity hash is created based on the email addresses and phone numbers associated with the user's Apple ID.

When a user chooses AirDrop as the method for sharing an item, the device emits an AirDrop signal over BTLE. Other devices that are awake, in close proximity, and have AirDrop turned on detect the signal and respond with a shortened version of their owner's identity hash.

By default, AirDrop is set to share with Contacts Only. Users can also choose if they want to be able to use AirDrop to share with Everyone or turn off the feature entirely.

In Contacts Only mode, the received identity hashes are compared with hashes of people in the initiator's Contacts. If a match is found, the sending device creates a peer-to-peer Wi-Fi network and advertises an AirDrop connection using Bonjour. Using this connection, the receiving devices send their full identity hashes to the initiator. If the full hash still matches Contacts, the recipient's first name and photo (if present in Contacts) are displayed in the AirDrop sharing sheet.

When using AirDrop, the sending user selects who they want to share with. The sending device initiates an encrypted (TLS) connection with the receiving device, which exchanges their iCloud identity certificates. The identity in the certificates is verified against each user's Contacts. Then the receiving user is asked to accept the incoming transfer from the identified person or device. If multiple recipients have been selected, this process is repeated for each destination.

In the Everyone mode, the same process is used but if a match in Contacts is not found, the receiving devices are shown in the AirDrop sending sheet with a silhouette and with the device's name, as defined in Settings > General > About > Name.

The Wi-Fi radio is used to communicate directly between devices without using any Internet connection or Wi-Fi Access Point.

iMessage -- A bit of misdirection here:
<quote> Apple iMessage is a messaging service for iOS devices and Mac computers. iMessage supports text and attachments such as photos, contacts, and locations. Messages appear on all of a user's registered devices so that a conversation can be continued from any of the user's devices. iMessage makes extensive use of the Apple Push Notification Service (APNs). Apple does not log messages or attachments, and their contents are protected by end-to-end encryption so no one but the sender and receiver can access them. Apple cannot decrypt the data.

<quote> When a user turns on iMessage, the device generates two pairs of keys for use with

the service: an RSA 1280-bit key for encryption and an ECDSA 256-bit key for signing. For each key pair, the private keys are saved in the device's keychain and the public keys are sent to Apple's directory service (IDS), where they are associated with the user's phone number or email address, along with the device's APNs address.

How iMessage sends and receives messages

Users start a new iMessage conversation by entering an address or name. If they enter a phone number or email address, the device contacts the IDS to retrieve the public keys and APNs addresses for all of the devices associated with the addressee. If the user enters a name, the device first utilizes the user's Contacts to gather the phone numbers and email addresses associated with that name, then gets the public keys and APNs addresses from the IDS.

The user's outgoing message is individually encrypted using AES-128 in CTR mode for each of the recipient's devices, signed using the sender's private key, and then dispatched to the APNs for delivery. Metadata, such as the timestamp and APNs routing information, is not encrypted. Communication with APNs is encrypted using TLS.

Siri

In order to facilitate Siri's features, some of the user's information from the device is sent to the server. This includes information about the music library (song titles, artists, and playlists), the names of Reminders lists, and names and relationships that are defined in Contacts. All communication with the server is over HTTPS.

When a Siri session is initiated, the user's first and last name (from Contacts), along with a rough geographic location, is sent to the server. This is so Siri can respond with the name or answer questions that only need an approximate location, such as those about the weather. If a more precise location is necessary, perhaps to determine the location of nearby movie theaters for example, the server asks the device to provide a more exact location. This is an example of how, by default, information is sent to the server only when it's strictly necessary in order to process the user's request. In any event, session information is discarded after 10 minutes of inactivity.

The recording of the user's spoken words is sent to Apple's voice recognition server. If the task involves dictation only, the recognized text is sent back to the device. Otherwise, Siri analyzes the text and, if necessary, combines it with information from the profile associated with the device. For example, if the request is "send a message to my mom," the relationships and names that were uploaded from Contacts are utilized. The command for the identified action is then sent back to the device to be carried out.

iCloud -- Appears to be **ALMOST** completely solid.

Keychain syncing:

When a user enables iCloud Keychain for the first time, the device establishes a circle of trust (which will exist among devices owned by the individual) and creates a syncing identity for itself. A syncing identity consists of a private key and a public key. The public key of the syncing

identity is put in the circle, and the circle is signed twice: first by the private key of the syncing identity, ***then again with an asymmetric elliptical key (using P256) derived from the user's iCloud account password.*** Also stored with the circle are the parameters (random salt and iterations) used to create the key that is based on the user's iCloud password.

The signed syncing circle is placed in the user's iCloud key value storage area.

- It cannot be **read** without knowing the user's iCloud password,
- And cannot be **modified** without having the private key of the syncing identity of its member.

This is the **ONLY reference** to Apple use of the NIST P-256 elliptic curve… and both Dan Bernstein and Bruce Schneier now declare ANY use of the NSA/NIST curves unsafe.

http://safecurves.cr.yp.to/index.html
http://www.hyperelliptic.org/tanja/vortraege/20130531.pdf
Jerry Solinas at NSA

So what is "Jailbreaking" ??

- Discovering flaws in the implemention, then attempting to exploit them by defeating all of the various mitigations.