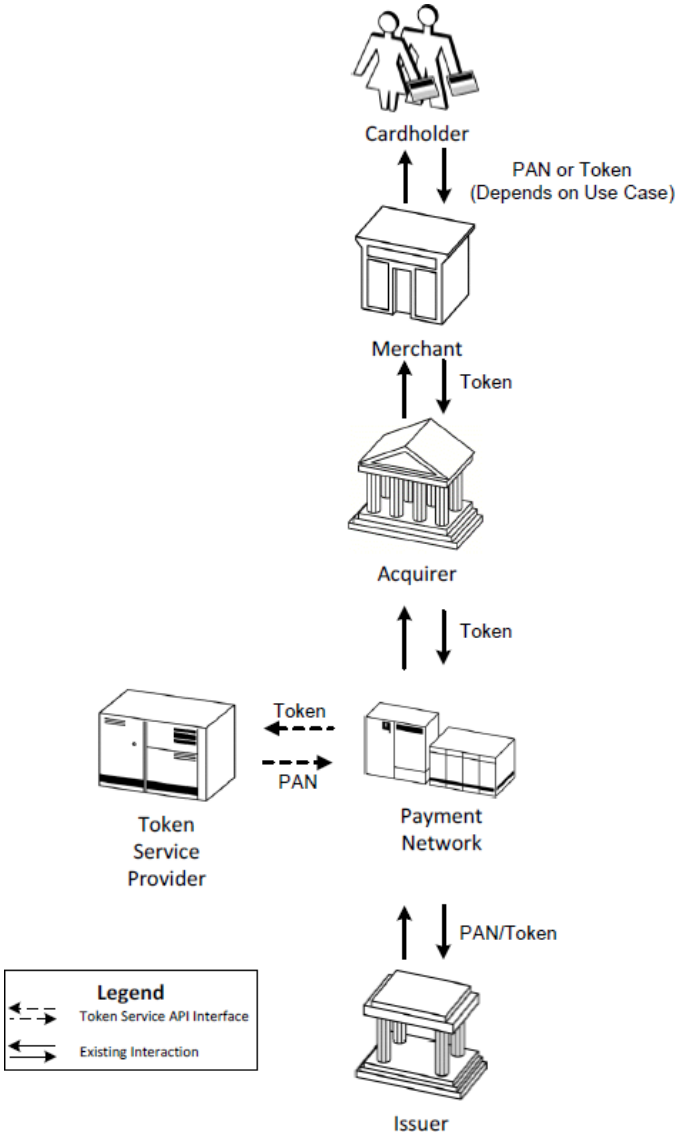
Security Now! #477 - 10-14-14

Payment Tokenization

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!

- Patch Tuesday closes a just-announced "SandWorm" targeted 0-day exploit.
- New Firefox v33
- A forthcoming SSLv3 bug to be revealed tomorrow (Wednesday).
- Another interesting battery breakthrough.
- Dropbox user account data leakage? (apparently not really...)
- Payment Tokenization: The many benefits of turning a PAN into a pointer!
    - (PAN == Primary Account Number == Credit Card #)



Security News:

Microsoft's Patch Tuesday closes an in-the-wild 0-day

- (affecting all versions of Windows AFTER XP.)

- iSightPartners "SandWorm" 0-day discovery
    - Named from its use of encoded references to Sci-Fi classic "Dune" in command and control URLs and references found in various malware samples.

- Exploited by Russians against known targets:
    - NATO
    - Ukrainian government organizations
    - Western European government organization
    - Energy Sector firms (specifically in Poland)
    - European telecommunications firms
    - An (unnamed) United States academic organization

- The SandWorm team:
    - Prefers the use of spear-phishing with malicious document attachments to target victims.
    - Many of the lures observed have been specific to the Ukrainian conflict with Russia and to broader geopolitical issues related to Russia.
    - The team has recently used multiple exploit methods to trap its targets, including the use of BlackEnergy crimeware, exploitation of as many as two known vulnerabilities simultaneously, and this newly observed Microsoft Windows zero-day.

- Vulnerability Details:
    - Vulnerability exists in the OLE package manager in Microsoft Windows and Server
        - Introduced in Vista SP2.
        - All versions of the Windows operating system from Vista SP2 to Windows 8.1
        - Windows Server versions 2008 and 2012

    - When exploited, the vulnerability allows an attacker to remotely execute arbitrary code.

    - The vulnerability exists because Windows allows the OLE packager (packager .dll) to download and execute INF files. In the case of the observed exploit, specifically when handling Microsoft PowerPoint files, the packager allows a Package OLE object to reference arbitrary external files, such as INF files, from untrusted sources.
      This will cause the referenced files to be downloaded in the case of INF files, to be executed with specific commands.
      An attacker can exploit this vulnerability to execute arbitrary code but will need a specifically crafted file and use social engineering methods (observed in this campaign) to convince a user to open it.

Firefox v33

- OpenH264 now in FF.
  - http://andreasgal.com/2014/10/14/openh264-now-in-firefox/
  - SourceCode on Github, FF browsers download verifiably directly from Cisco.
- Faster, snappier searches
- Major improvement in javascript strings
  - https://blog.mozilla.org/javascript/2014/07/21/slimmer-and-faster-javascript-strings-in-firefox/
  - Gmail memory usage cut by half.
  - Storing 8-bit chars rather than all 16-bit chars.
- OMTC (Off Main Thread Compositing)
  - Major architectural improvement.
- Session Restore -- significant reliability improvement.
  - https://dutherenverseauborddelatable.wordpress.com/2014/06/26/firefox-the-browser-that-has-your-backup/
- CSS3 (Custom Counter Styles)
  - http://dev.w3.org/csswg/css-counter-styles/#the-counter-style-rule
- DOMMatrix
  - Native 4x4 matrix representation suitable for use with 2D and 3D operations.

SSLv3 bug rumor...

- Being patched now... announced Wednesday around noon, Pacific Time.

More progress on the battery front:

- http://phys.org/news/2014-10-ultra-fast-batteries-recharged-minutes.html
- 20 year, 10,000 charge cycle time.
- Two minute charge to 70% capacity.
- Modified lithium-ion technology.
- Replaced the anode's traditional graphite with a gel made from titanium dioxide nanotubes.

Dropbox user account data leakage?

- Pastebin has been receiving "hundreds" of login credentials.
- The Pastebin poster claims that 6,937,081 account credentials have been leaked.
- Attackers are asking for money in return for the release of more credential data.
- Dropbox has reset the passwords of all posted credentials.
- Dropbox Responds:
  - Dropbox has not been hacked. These usernames and passwords were unfortunately stolen from other services and used in attempts to log in to Dropbox accounts. We'd previously detected these attacks and the vast majority of the passwords posted have been expired for some time now. All other remaining passwords have been expired as well.

SpinRite

Matthew M. Power
Subject: registered owner of spinrite question about look and feel design

I am a very satisfied owner of the SpinRite product.

Since my purchase, SpinRite has brought back THREE un-mountable drives! I firmly believe in this product. Because of SpinRite, people bring me their PCs when the other guys can't get them to boot.

I see that it is distributed in FreeDos, which is awesome! I love SpinRite's DOS Shell look! How did you do that? I would love to write a small game with that dosshell look and feel (maybe run it in freedos as well) but I have never been able to figure out how to get that look.

Are there any of your free examples I should be looking at? Or maybe you know of a site I should check out?

Remember when MS <http://edit.com>edit.com had the orange-block mouse cursor? That's the look I want. I have never read anywhere where someone knows how to do that. And yet SpinRite has it (minus the mouse).

Any help?

Thank you!

Matt

Payment Tokenization

EMVCo

- In 2002:
- E: Europay
- M: MasterCard
- V: VISA
- ... and JCB (Japan Credit Bureau) in 2004
- American Express in 2009
- China UnionPay in 2013, now sharing 1/6th interest with: VISA, MasterCard, American Express, Discover & JCB.

“Role” Terminology

“Technical Framework”

"Cryptogram" (??)

- 3-D Secure:
- Designed by VISA. Used in "Verified by VISA."

VISA:

- http://usa.visa.com/clients-partners/technology-and-innovation/visa-token-service/index.jsp

FirstData

- https://www.firstdata.com/en_us/products/financial-institutions/security-and-fraud-solutions/integrated-token-services.html
- (See 60-minute "webinar" link at bottom of page.)

Apple Pray:

- After years of background exploration, work began in earnest in January of 2014.
- VISA had 1,000 people on the project
- JPMorgan / Chase had 300+
- No banks knew of any others' involvement.

Apple API Docs:

- https://developer.apple.com/library/ios/documentation/PassKit/Reference/PaymentTokenJSON/PaymentTokenJSON.html

ApplePay

http://clover-developers.blogspot.com/2014/09/apple-pay.html
http://bankinnovation.net/2014/09/heres-how-the-security-behind-apple-pay-will-really-work
http://bgr.com/2014/09/12/apple-pay-mobile-payments/
http://bankinnovation.net/2014/09/heres-how-the-security-behind-apple-pay-will-really-work/
http://www.theverge.com/2014/9/16/6221045/paypal-apple-pay-ad-at-least-were-not-icloud