Security Now! #454 - 05-06-14

Certificate Revocation Pt.2

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 patches XP after all,
- A well known vulnerability in OpenID & OAuth is breathlessly rediscovered,
- A hacker discovers that older iPhones aren't encrypting eMail attachments,
- The US Gov begins pilot-testing its somewhat worrisome Universal CyberID,
- Certificate Revocation Pt2: How Practice follows Theory.

Security News:

WinXP gets a freebie!

- Microsoft rushes an out-of-cycle update for Internet Explorer and, in their haste, apparently forgot to exclude updates for IE versions 6 through 8 on Windows XP!

- http://blogs.technet.com/b/msrc/archive/2014/05/01/out-of-band-release-to-address-microsoft-security-advisory-2963983.aspx
- <quote> We have made the decision to issue a security update for Windows XP users. Windows XP is no longer supported by Microsoft, and we continue to encourage customers to migrate to a modern operating system, such as Windows 7 or 8.1. Additionally, customers are encouraged to upgrade to the latest version of Internet Explorer, IE 11.

OAuth & OpenID - "Covert Redirect"

- Giving something a cool "sound bite" name matters more than details.
- The press froths once again over the "quote" discovery "unquote" of an already well known and well documented vulnerable characteristic affecting authentication protocols that bounce their user's among web servers, in other words... OpenID and OAuth 2.0.
- http://tetraph.com/covert_redirect/
- http://thehackernews.com/2014/05/nasty-covert-redirect-vulnerability.html
- http://www.cnet.com/news/serious-security-flaw-in-oauth-and-openid-discovered
- This issue is the topic of Section 4.2.4, page 22, if the IETF's OAuth specification.
    - http://tools.ietf.org/html/rfc6819#page-22
- The source of the trouble:
    - The user's web browser is being bounced around among websites, and…
    - The Relying Party provides the URL to which the Authenticating Party should return the then-authenticated user... but it could be anything.
- Two fixes:
    - Register your site's redirect URLs with every OAuth authentication provider
    - Never allow your own site's redirects to take visitors offsite.

iOS is not encrypting eMail attachments

- Andreas Kurtz, writing on April 23rd: "What Apple Missed to Fix in iOS 7.1.1" (his point being they knew at iOS v7.1)

  "A few weeks ago, I noticed that email attachments within the iOS 7 MobileMail.app are not protected by Apple's data protection mechanisms. Clearly, this is contrary to Apple's claims that data protection "provides an additional layer of protection for (..) email messages attachments".

  I verified this issue by restoring an iPhone 4 (GSM) device to the most recent iOS versions (7.1 and 7.1.1) and setting up an IMAP email account1, which provided me with some test emails and attachments. Afterwards, I shut down the device and accessed the file system using well-known techniques (DFU mode, custom ramdisk, SSH over usbmux). Finally, I mounted the iOS data partition and navigated to the actual email folder. Within this folder, I found all attachments accessible without any encryption/restriction..."

- This appears to be true. And it's something Apple apparently missed.
- Rene Ritchie asked Apple about it and was told: "We're aware of the issue and are working on a fix which we will deliver in a future software update."

- Rene Ritchie:
  - http://www.imore.com/apple-aware-ios-7-mail-attachment-bug-working-fix
- All iPhones AFTER the iPhone4 (4s, 5, 5s, etc.) having at least the Apple A5 chip are not vulnerable.
- Apple may have just been relying upon their later and more powerful hardware crypto, so the down-version was left a bit behind.
- An attack would require that they either successfully impersonate the user by logging in or Jailbreak the device and defeat its layers of hardware encryption.
- Rene: For those running an iPhone 4 (Apple A4 chipset or earlier), an attacker would still need prolonged access to your device to perform this attack, which also means preventing Find my iPhone from wiping it. They'd also need to get around the passcode or password. (If you don't have a Passcode set they could just launch Mail.app and see all your attachments, and everything else on your device, anyway.)

NSTIC (National Strategy for Trusted Identities in Cyberspace) Pilot program

- In the "What Could Possibly Be Wrong With This Idea":... The U.S. Government's own "National Internet ID" Experiment Begins...
- Techdirt Wrote:
  - Headline: US Government Begins Rollout Of Its 'Driver's License For The Internet' Subhead: From the seizing-the-(wrong)-moment dept
  - "An idea the government has been kicking around since 2011 is finally making its debut. Calling this move ill-timed would be the most gracious way of putting it."
- Initially in pilot use for government agencies in Michigan and Pennsylvania.
- http://www.nytimes.com/2011/09/18/business/online-id-verification-plan-carries-risks.html
- http://motherboard.vice.com/read/the-white-house-wants-to-issue-you-an-online-id

Miscellany

- A graph of Security Now lengths with and without Q&A
  - http://cyphase.com/securitynowstats

- "Almost Human" Entirely Cancelled. :(

- Halt And Catch Fire
  - *Halt and Catch Fire* is an upcoming 2014 period drama that is set to air on AMC.[1] Its 10-episode first season is slated to premiere on Sunday, June 1, 2014.[2] The name is a reference to the fictitious machine code instruction Halt and Catch Fire (HCF) which causes a computer's central processing unit to cease all meaningful function. The show is set in the early 1980s, and depicts a fictionalized insider's view of the personal computer revolution.

- EFTS in Business vs Personal Banking.

SQRL

- Finished with "The Revocation Enlightenment" -- Joyfully back to SQRL

SpinRite:

- From: Kyle Lyons
  Subject: SpinRite Brings MacBook Pro Back Up to Speed

  Add me to the now typical MacBook success story. The system was taking 10-15 minutes to boot, and just as long to launch programs. The drive was reimaged to no avail. We hooked up the MacBook's drive to a Windows machine using an IDE/SATA to USB 2.0 adapter, mounted the drive to a VMWare Player DOS virtual machine, and ran SpinRite on it. Four hours later, the drive, and the MacBook, are running like new.

  Thanks Steve!

Certificate Revocation, Pt.2

Topics::

- A brief summary of last week's certificate revocation discussion.
- Why it's so difficult: The certificate trust
- Who's doing what for us today
- Does Certificate Revocation really matter?

A brief summary of last week's certificate revocation discussion.

Certificate trust system is a mess:

- http://www.oasis-pki.org/pdfs/Understanding_Path_construction-DS2.pdf
- Backwards compatibility with older standards
- Overloading the meaning of certificate fields
- (Existing field types were later reused to also contain other data)
- Not designed with all possible uses so clever hacks kept being created

- We need to:
  - Build a (non-deterministic) path from the end certificate back to a trusted root.
  - But certificate linkages are forward-pointing and we're building a path backwards.
  - Linkages can be by:
    - Subject Name / Issuer Name
    - Subject Key Identifier / Authority Key Identifier
  - The public key algorithm and parameters are checked.
  - The current date/time is checked against the validity period of the certificate.
  - The revocation status is checked using CRL or OCSP or private lists.
  - The issuer name is checked to ensure that it equals the subject name of the previous certificate in the path.

- Name constraints are checked, to make sure the subject name is within the permitted subtrees list of all previous CA certificates and not within the excluded subtrees list of any previous CA certificate.
- The asserted Certificate Policy OIDs are checked against the permissible OIDs as of the previous certificate, including any policy mapping equivalencies asserted by the previous certificate.
- Policy constraints and basic constraints are checked, to ensure that any explicit policy requirements are not violated and that the certificate is a CA certificate.
- The path length is checked to ensure that it does not exceed any maximum path length asserted in this or a previous certificate.
- The key usage extension is checked to ensure that is allowed to sign certificates.
  - Server Authentication
  - Client Authentication
  - Secure eMail
  - Code Signing
  - Time Stamping
- Any other critical extensions are recognized and processed.
- If we reach the last certificate in the chain, with no name constraint or policy violations or any other error condition, then the certificate path validation algorithm terminates successfully.

Revocation Checking is tricky -- So WHOSE responsibility is it and who's doing it?

- In the OS vs the Browser
  - Long term --> OS makes more sense since then all OS client apps get protection.
  - Currently: Only use Firefox on Android.

- Today? The mobile platforms are all lacking.
  - Perhaps OCSP is not as bad as they think?
  - People having trouble with Google's OCSP.
  - OCSP Must-Staple WILL solve the problem.
    - What about DoSing the CAs?

- Mobile Platforms
  - Android doesn't perform ANY revocation checking at all.
    - Android's Java API lacks all features
    - Even Google's CRLSet didn't block revoked.grc.com.
  - iOS is somewhat better.
    - EV checked for Safari and LastPass Tab browser's but not Chrome.

- Desktop Platforms
  - Windows and Mac provide native services.
    - Mac appears to be buggy.
    - Windows DOES have a deeply buried "hard fail" option.
  - Linux doesn’t provide any native services but relies upon the OpenSSL library carried by individual clients.

- DANE / TLSA & CAA DNS Records
    - DNS-based Authentication of Named Entities.
    - If we have DNSSEC we have a lot.
        - Signed DNS records cannot be spoofed.
    - Today: *ANY* CA can issue a certificate for *ANY* domain.
    - DNS CAA - Certificate Authority Authorization
        - Who's allowed to sign a domain's certificate?
    - DNS TLSA
        - Used to associate a TLS server certificate or public key with the domain name where the record is found, thus forming a 'TLSA certificate association'".

Does revocation checking really matter?

- It DEFINITELY MATTERS to those whose certificates have been revoked.
    - No way would I want a GRC.COM certificate loose in the world.
    - So it's VERY DISTURBING that revocation is barely being checked.

- To exploit:
    - User's connection must somehow go to a malicious clone site.
    - DNS/IP poisoning, traffic intercept, etc.