Security Now! #473 - 09-16-14

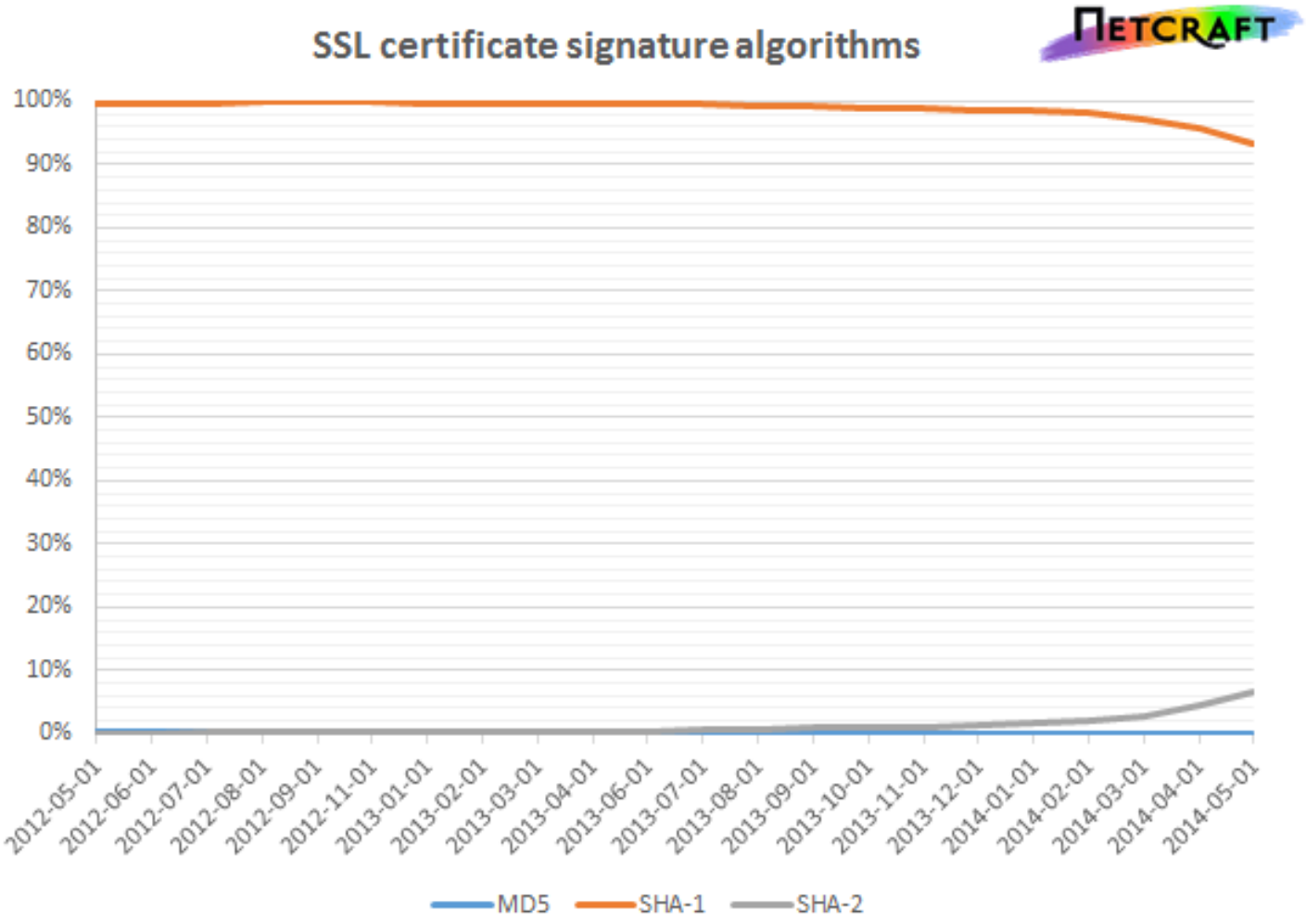
Google vs SHA-1

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!

- Comcast versus TOR?
- Apple's Tim Cook does Charlie Rose,
- A big Linked-In mistake,
- A serious newly discovered, pre-KitKat, Android problem,
- A LastPass / iOS8 announcement,
- ...and a bit of television and iPhone miscellany

The deployment of SHA-1 (red) vs SHA-256 (grey) on the Internet



Monday's Triangulation!

Dr. Lawrence Krauss
His newest book on Audible:

- A Universe from Nothing: Why There Is Something Rather Than Nothing
- <http://www.audible.com/pd/B006U0X9QG>

Quotes from among a torrent...

- The two most exicting states to be in: Confused or Wrong.

Security News:

Comcast vs TOR and Internet Privacy (SlashDot at al)

- http://www.deepdotweb.com/2014/09/13/comcast-declares-war-tor/
- Comcast customers, speaking to DeepDotWeb, claimed that Comcast repeatedly asked them which sites they were accessing using Tor.
- Reports have surfaced that Comcast agents have contacted customers using Tor and instructed them to stop using the browser or risk termination of service. A Comcast agent named Jeremy allegedly called Tor an "illegal service." The Comcast agent told its customer that such activity is against usage policies. The Comcast agent then repeatedly asked the customer to tell him what sites he was accessing on the Tor browser. The customer refused to answer. The next day the customer called Comcast and spoke to another agent named Kelly who reiterated that Comcast does not want its customers using Tor. The Comcast agent then allegedly told the customer:
- Monday - Jason Livingood:
    - http://corporate.comcast.com/comcast-voices/setting-the-record-straight-on-tor
    - Flatly denied all of this.
- My take is... it sounds like there's as much gossip within the Comcast Support teams as there is among those who are stuck using Comcast with no other choice.

Tim Cook interview on Charlie Rose:

- <quote> We're not reading your email, we're not reading your iMessages. If the government laid a subpoena on us to get your iMessages, we can't provide it. It's encrypted and we don't have the key.
- "Our customers are not our product, these gadgets are our product."
- "We go out of our way NOT to have our customer's data. We don't want it."

Linked-In:

- Benjamin Caudill & Bryan Seely, founders of Rhino Security Labs in Seattle, cleverly leveraged an unintended side effect of Linked-In: cross-referencing one's other contact lists with ALL of Linked-In's eMail addresses. Allows for semi-automated guessing by tricking Linked-In into believing that you know those people (since they're in your contact lists.

Android:

- Rafay Baloch
  http://www.rafayhackingarticles.net/2014/08/android-browser-same-origin-policy.html
- In the AOSP the default native (Android Open Source Platform) browser, before v4.4, SOP (Same Origin Policy) enforcement is completely broken and readily bypassed.
- Malform a JavaScript URL handler with a prepended null byte for complete SOP bypass.

- How could this be exploited?
  - This gives any website full access to the browser's entire DOM hierarchy (Document Object Model) which now, thanks to this bug extends cross-site. Therefore, any website visited could view the contents and login session cookies for any other pages that are simultaneously open in the browser... thus impersonating the user with their login credentials.

- KitKat (v4.4) is at 24.5%, so pre-v4.4 is about 75% of the current Android ecosystem.
  - http://www.androidcentral.com/android-version-numbers-are-kitkat-one-quarter-active-devices

- v4.2 (Jellybean) and prior are nearly 100% of the off-the-shelf, lower-end prepaid phones... and they still ship the AOSP web browser.

- For example, the vulnerability was discovered by a researcher in his Qmobile Noir A20 running Android Browser v4.2.1.
- Verified with a Galaxy S3, HTC wildfire, Sony Xperia, Motorola, and others.
- Very simple proof of concept. Now available in all versions of Metasploit.
- DO NOT USE the Android Browser before KitKat!!

LastPass and iOS8

- <quote> Following Apple's announcement of iOS 8 in June, we've been hard at work to bring the platform's new security and authentication features to the LastPass mobile experience. Now with the impending release of the platform, we're thrilled to announce the LastPass app will be available for iOS 8 with Touch ID integration and a Safari extension for automated web logins. This marks a tremendous shift in our ability to bring a seamless login experience to LastPass users on iOS.
- The LastPass Safari Extension:
  - iOS 8 now allows third-party apps to integrate directly into Safari as an extension. Once enabled in the browser, this means LastPass can fill web logins without users needing to leave the browser.
  - The extension also provides direct access to the LastPass vault, so stored logins can be accessed and new accounts can be saved with many fewer steps.
- Touch ID Integration:
  - Users will now have the option to enable Touch ID to unlock their LastPass vault to access stored accounts. While browsing in Safari and launching the LastPass extension, you can respond to the Touch ID prompt to authorize LastPass to fill a web login.

- Available SOON (but apparently not quite yet...)

Miscellany:

Gotham:

- Premiere's Monday on FOX.
- Special --> Gotham: The Legend Reborn (22 minute special) ONLINE or Saturday on FOX
- http://www.fox.com/gotham/
- (And if it's terrific -- like "Firefly" and "Almost Human")

iPhone 6 Plus

- Shipping Confirmed yesterday.

SQRL:

- Thursday, turned over the UI-complete functioning client.
- Working on WINE display anomalies and WINE printing.
- Then implement the online protocol... and we'll have easy-to-use, free, robust, secure, anonymous identity for the web.

SpinRite:

Patrick in Pittsburgh, Pennsylvania
Subject: Spinrite saves a RAID array

Steve,

I heard you discussing SpinRite and RAID arrays a few episodes back and thought I'd share a success story. I moved across the country about a year ago and during the move, a Synology disk array fell out of the back of the moving truck (while it was parked, but it was still bad). When I plugged it back in, all sorts of audible beeps, amber lights, and console messages indicated that one of the disks was past the point of repair and needed to be replaced. I took the damaged disk out of the array and put it into an old desktop then let SpinRite do its thing. When SpinRite was finished, I slipped the disk back into the array and it's been humming along for over a year now without any trouble. That's the second time SpinRite has saved me. Thank you for an amazing product and an amazing podcast.

Google vs SHA-1

Links:

- http://blog.chromium.org/2014/09/gradually-sunsetting-sha-1.html
- https://groups.google.com/a/chromium.org/forum/#!topic/security-dev/2-R4XziFc7A[51-75-false]
- https://konklone.com/post/why-google-is-hurrying-the-web-to-kill-sha-1

November 2013: Microsoft announces sunsetting of SHA-1 2017.

- No one cared. Everyone felt that was reasonable and would allow for plenty of time to deal with the consequences of the need to move to SHA-256.

Certificate Signing Refersher:

- All certificate information is hashed and that hash is cryptographically signed.
- Web clients verify the signature of certificates.
- It's ONLY the strength of the hash that prevents, for example, the domain name of a certificate from being changed. If such a change could be made, and the hash's result preserved unchanged, then the signature would still be valid... even though it was for a certificate that the CA never signed.

Remember that this DID (famously or infamously) happen with MD5...

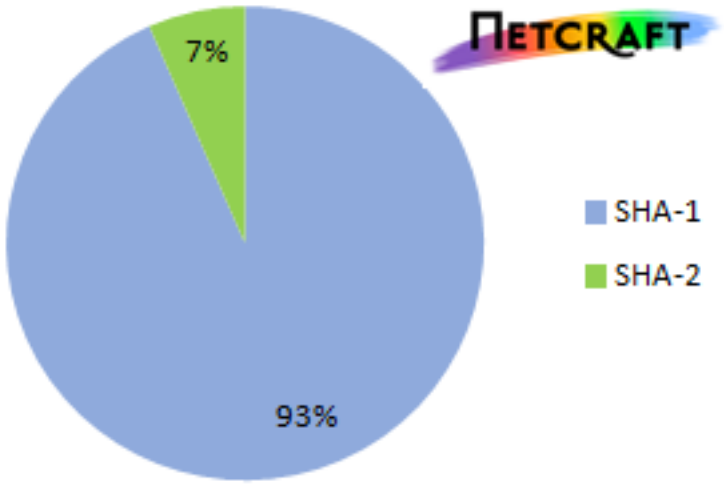
- The first chinks in MD5 were discovered in 1995, and things got progressively worse.
- Remember, as Bruce Schneier has observed: Attacks never get weaker, they only get stronger.
- 13 years later an academic MD5 collision was created in the wild.
- http://www.win.tue.nl/hashclash/rogue-ca/
- Certificate issued to: "MD5 Collisions, Inc."
- Wall of 200 PS3's.

Out of the blue, on August 19th...

- Ryan Sleevi, August 19th: "Intent to Deprecate: SHA-1 certificates"
- https://groups.google.com/a/chromium.org/forum/#!msg/security-dev/2-R4XziFc7A/NDI8cOwMGRQJ
- In three months (November) Chrome's behavior will change as follows:
- All sites using an SHA-1 cert that's valid AFTER Jan 1st, 2017 will be regarded as insecure. The user will see a "degraded" security indicator and will receive MIXED CONTENT warning REQUIRING a user interaction to proceed.
- All site using an SHA-1 cert that's valid AFTER Jan 1st, 2016 will be regarded as insecure. The user will see a "degraded" security indication but won't need to take any action.

In other words, 90 days after Ryan's unilateral pronouncement, any certs signed by SHA-1, which will still be valid after 2015, will be flagged by Chrome as INSECURE.

But 92% of all SSL certificates issued in January of THIS year were signed by SHA-1.



Reactions from CloudFlare's Nick Sullivan:
This timeline for deprecating SHA-1 is very aggressive and puts us (CloudFlare) in a bind.

Currently we provide certificates to our customers signed by GlobalSign's SHA-1 intermediate, with a 3 year expiration (i.e. all customer certificates from this year are valid for part of 2017). We still use these SHA-1 certificates because a large percentage of the web visitors of our customers are using Windows XP SP2 which does not support SHA-256. It's not realistic to expect everyone to be able to upgrade to SP3.

This change will force our customers to have to choose between having a mixed content warning on Chrome or cutting off a large portion of their visitor base.

Can we please delay this move until at least next year?

Jeremy Rowley of DigiCert:
With rekeys, duplicates, early renewal programs, etc., I think most of the certificates valid in 2016 will be replaced well before then. Considering many CAs are working to move existing SHA1 customers to SHA2 before 2016, showing a UI degradation now will probably only serve to upset website owners rather than spur faster adoption. Most of these customers are on a set transition plan that will move them to SHA2 well before the deadline, despite having a certificate currently that extends past the end of 2015. At least consider a "window" in the validity period range where the transition will likely happen before 2016 despite a post-2016 validity period (such as March 2016). Putting the degradation on certs with a validity period past March 2016 will likely have the same effect in spurring a transition to SHA2 but let people keep their current transition plan in-tact.

A heavy-handed, unilateral, abuse of power?

Here's what's rather galling: "Google's Double Standard"...

The opening line of Ryan Sleevi's now-infamous posting:

- Quote: "The use of SHA-1 within TLS certificates is no longer sufficiently secure."

Yet ALL OF GOOGLE is *CURRENTLY USING SHA-1* certs!! And since they are issuing them quarterly, they could have easily switched over to SHA-256 at iany time.

SHA-256 Compatibility:
https://support.globalsign.com/customer/portal/articles/1499561-sha-256-compatibility

The trouble is:

- If we really believe that SHA-1 is no longer secure, ALL SUPPORT for them MUST be completely removed.
- A web client doesn't "know" that a site's cert is SUPPOSED to be SHA-256.
- ... So it will happily accept a FRAUDULENT SHA-1 signed certificate.

The power of government actors?

- Who among us still believes that the NSA (or China) even needs to crack a cert? Ha!!!
- "The Hong Kong Post Office" doesn't work for us...