Security Now! #556 - 04-19-16

SMTP STS

- or -

“Horrible Internet Kludges Never Die”

This week on Security Now!

- 60 Minutes expose' on the inter-provider SS7 signalling system.
- The future appears black for BlackBerry (or Black and Blue Berry.)
- Quicksand for QuickTime.
- What was found in the decrypted San Bernardino phone?
- Threema vs WhatsApp vs Signal
- Then a look at SMTP STS: a new specification to add Strict Transport Security (STS) to eMail.

Security News

Sunday's 60 Minutes and Signaling System 7 (SS7)

- Signaling System 7 (SS7) is an international telecommunications standard that defines how network elements in a public switched telephone network (PSTN) exchange information over a digital signaling network. Nodes in an SS7 network are called signaling points.
- The SS7 signalling system was designed in the 1980's.
- The two mobile protocols MAP and CAMEL operate *without* authentication... leaving them wide open to abuse.
- International commercial entities sell SS7 hacking tools to governments and law enforcement.
- “Everybody who has a phone in his pocket indirectly uses SS7,” Engel said. “Every movement can be tracked and every call can be intercepted.”
- http://blog.ptsecurity.com/2014/08/cell-phone-tapping-how-it-is-done-and.html
- http://blog.ptsecurity.com/2014/04/search-and-neutralize-how-to-determine.html
- http://www.adaptivemobile.com/blog/russia-ukraine-telecom-monitoring
- http://www.slideshare.net/phdays/phd4-pres-callinterception119
- Cellular Privacy, SS7 Security Shattered at 31C3 https://wp.me/p3AjUX-sEn
- And... on top of all that...
- Persistent rumors of implementation defects in the Baseband Processor firmware.

Canadian Police Obtained BlackBerry's Global Decryption Key

Vice:

https://news.vice.com/article/exclusive-canada-police-obtained-blackberrys-global-decryption-key-how

The revelations are contained in a stack of court documents that were made public after members of a Montreal crime syndicate pleaded guilty to their role in a 2011 gangland murder. The documents shed light on the extent to which the smartphone manufacturer, as well as telecommunications giant Rogers, cooperated with investigators.

According to technical reports by the Royal Canadian Mounted Police that were filed in court, law enforcement intercepted and decrypted roughly one million PIN-to-PIN BlackBerry messages in connection with the probe. The report doesn't disclose exactly where the key — effectively a piece of code that could break the encryption on virtually any BlackBerry message sent from one device to another — came from. But, as one police officer put it, it was a key that could unlock millions of doors.

Government lawyers spent almost two years fighting in a Montreal courtroom to keep this information out of the public record.

And while neither the RCMP nor BlackBerry confirmed that the cellphone manufacturer handed over the global encryption key, and both fought against a judge's order to release more information about their working relationship, the Crown prosecutors admitted that the federal police service had access to the key.

And if the global key is still sitting on a server in the RCMP's headquarters, the potential consequences could be significant. Although it wouldn't offer police a backdoor into most of its government and business clients, who make up BlackBerry's core constituency, it would mean that police enjoyed years of access to Canadians' personal cellphones without the public being any the wiser.

In a technical report attempting to underscore the significance of this technology and filed with the Superior Court of Quebec, the RCMP stated that ithad obtained "the key that would unlock the doors of all the houses of the people who use the provider's services, and that, without their knowledge."

Motherboard:

- http://motherboard.vice.com/read/rcmp-blackberry-project-clemenza-global-encryption-key-canada
- BlackBerry (formerly RIM) encrypts all messages sent between consumer phones, known as PIN-to-PIN or BBM messages, using a single “global encryption key” that’s loaded onto

every handset during manufacturing. With this one key, any and all messages sent between consumer BlackBerry phones can be decrypted and read. In contrast, Business Enterprise Servers allow corporations to use their own encryption key, which not even BlackBerry can access.

According to more than 3,000 pages of court documents pertaining to the case that resulted from Project Clemenza, obtained by VICE Canada, the RCMP maintains a server in Ottawa that "simulates a mobile device that receives a message intended for [the rightful recipient]." In an affidavit, RCMP sergeant Patrick Boismenu states that the server "performs the decryption of the message using the appropriate decryption key." The RCMP calls this the "BlackBerry interception and processing system."

BlackBerry Says:

- http://blogs.blackberry.com/2016/04/lawful-access-corporate-citizenship-and-doing-whats-right/
- John Chen / Chairman & CEO
  - Title: "Lawful Access, Corporate Citizenship and Doing What's Right"
  - When it comes to doing the right thing in difficult situations, BlackBerry's guiding principle has been to do what is right for the citizenry, within legal and ethical boundaries. We have long been clear in our stance that tech companies as good corporate citizens should comply with reasonable lawful access requests. I have stated before that we are indeed in a dark place when companies put their reputations above the greater good.

QuickTime becomes QuickSand

- ... or "It's dead, Jim."
- PCWorld headline: "Uninstall now! Apple abandons QuickTime for Windows despite lingering critical flaws"
- Trend Micro: "Urgent Call to Action: Uninstall QuickTime for Windows Today"
- http://blog.trendmicro.com/urgent-call-action-uninstall-quicktime-windows-today/
- We're putting the word out that everyone should follow Apple's guidance and uninstall QuickTime for Windows as soon as possible.

  This is for two reasons.

  First, Apple is deprecating QuickTime for Microsoft Windows. They will no longer be issuing security updates for the product on the Windows Platform and recommend users uninstall it. Note that this does not apply to QuickTime on Mac OSX.

Second, our Zero Day Initiative has just released two advisories ZDI-16-241 and ZDI-16-242 detailing two new, critical vulnerabilities affecting QuickTime for Windows. These advisories are being released in accordance with the Zero Day Initiative's Disclosure Policy for when a vendor does not issue a security patch for a disclosed vulnerability. And because Apple is no longer providing security updates for QuickTime on Windows, these vulnerabilities are never going to be patched.

- Interesting techie details:
  Both of these are heap corruption remote code execution vulnerabilities. In one case an attacker is able to write data outside of an allocated heap buffer. The other vulnerability occurs in the "stco" atom where, by providing an invalid index, an attacker can write data outside of an allocated heap buffer. Both vulnerabilities would require a user to visit a malicious web page or open a malicious file to exploit them. And both vulnerabilities would execute code in the security context the QuickTime player, which in most cases would be that of the logged on user.

CBS News says: "Nothing significant found on San Bernardino iPhone so far"

- http://www.cbsnews.com/news/source-nothing-significant-found-on-san-bernardino-iphone/
- A law enforcement source tells CBS News that so far nothing of real significance has been found on the San Bernardino terrorist's iPhone, which was unlocked by the FBI last month without the help of Apple.

  Pat Milton, senior investigative producer, reports that it was stressed that the FBI continues to analyze the information on the cellphone seized in the investigation.

Threema vs WhatsApp vs Signal

https://threema.ch/press-files/content/the-threema-advantage_en.html

Threema:

- "In contrast to other messengers, Threema doesn't require any personal information, such as your phone number, in order to be used. Instead, a randomly generated character string serves as a unique identifier, meaning that full anonymity can be maintained."
- Clear economic model: pay a little to support the product and service.
- Payment may be made anonymously with Bitcoin (on Android, where it's possible).
- No access needed to ANY smartphone content or resources: phone contacts, camera, mic.
- VERIFICATION LEVEL always displayed with each contact.
- But... "no one" uses it.

Errata:

- Never10 v1.3.1
- Evan Katz found a parsing mistake:
    - <network drive>:\Programs and Updates\...

Miscellany

- TONIGHT!! : Set Your DVR: "The Night Manager" on AMC starring Hugh Laurie, beginning April 19th. IMDB: 8.6/10, Rotten Tomatoes: 100% -- Google for more!

- Zeo update:
    - http://zeoband.com/
    - Amazing new Android Zeo app coming soon.

SpinRite

Simon Byrne / Canberra, Australia
Subject: Spinrite recovers SSD's? YOU BET IT DOES!
Date: 18 Apr 2016 00:31:22

G'day Steve,

I bought Spinrite years ago for no other reason than to support you and the Security Now podcasts. Last Saturday I fired up my Macbook Pro with a 1 Terabyte Outer World Computing SSD installed. It got half way and then shut down...not good.

I do video production and generate very large amounts of data. I do have a good local backup regime but backing up over the web is impractical as I generate many gigabytes every day. However, I was working the day before offsite with no local backup so I was faced with losing a full day's work which equated to about 12 gigabytes.

I took the SSD drive out of my Mac and put it into one of my PC's and fired up Spinrite on level 2. 9 hours later Spinrite had finished reporting no errors recovered. I was dissapointed that no errors were shown so I was dubious as to whether it was going to work.

I tentatively put the SSD back into my MAC and turned it on and YES, it booted up perfectly! I immediately backed up all my data.

So yes, Spinrite absolutely can recover data on a SSD drive.

SMTP Strict Transport Security -- SMTP STS

https://tools.ietf.org/pdf/draft-margolis-smtp-sts-00.txt
https://tools.ietf.org/html/draft-margolis-smtp-sts-00
Google, Yahoo!, Comcast, Microsoft, 1&1 Mail & Media Development & Technology GmbH

<quote> “The goal of the new SMTP Strict Transport Security mechanism is to ensure that encrypted email traffic is not vulnerable to man-in-the-middle attacks.”

This is NOT "end-to-end" security. This is encryption for eMail transiting the Internet in plaintext.

Mail Protocols & Ports:

- Plaintext:
  - SMTP 25 (587 for client submission and requiring STARTTLS & Login)
  - POP3 110
  - IMAP 143

- TLS:
  - SMTP 465
  - POP3 995
  - IMAP 993

"Opportunistic" TLS

STARTTLS provides a relatively weak mechanism for taking an existing non-private connection and allowing both endpoints to agree to switch to TLS privacy.

SMTP STS:
DNSSEC:
Someday we'll have a truly secure Internet directory publishing system.

TOFU - Trust On First Use + Policy Caching

Policy Semantics

- New DNS resource record (RR) or as TXT records under "_smtp_sts" sub-domain.
- (Current implementations deploy using TXT records.)
- Ex: For the policy domain "example.com" retrieve policy from "_smtp_sts.example.com"

Policy Authentication

- webpki: a=webpki:<https://example.com/.wellknown/smtp-sts/current>
- For the policy to be valid, the HTTP response body served at this resource MUST exactly match the policy initially loaded via the DNS TXT method, and MUST be served from an HTTPS endpoint at the domain matching that of the recipient domain.
- DNSSEC