Security Now! #480 - 11-04-14

Q&A #200

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!

- Important correction to my answer last week about same-origin policy enforcement.
- "CurrentC" user privacy didn't last long...
- Deliberate Tempest Broadcasting to jump the AirGap.
- Mac OSX Privilege Elevation
- TextSecure Audit Results
- EFF's Secure Messaging Scorecard
- Fingerprint but not Password.
- Are you watching your TV... or is IT watching YOU?

Security News:

"Department of Corrections"

- Correcting the Record: Adam Langley & Imperial Violet
- Three Tweets Wednesday Morning:
    - Realized that I missed the point Adam Langley was making about POODLE: JavaScript cannot get INTERNAL access to other domains,
    - ...but JavaScript CAN cause the browser to make queries to other domains… and that's all we need, since the attacker is OUTSIDE to observe.
    - I'll correct my confusion at the top of next week's podcast. In the meantime… that point I made was wrong!

(Also Wednesday morning): "CurrentC" early user eMail addresses leaked.

- Merchant Customer Exchange (MCX)
- Dekkers Davidson, CEO of MCX, stressed that it was the company's email provider that got hacked, not the CurrentC application.
- Also confirmed: Retailers who use MCX *CANNOT* use anything else (ApplePay).
- However... there are no fines associated with exiting the consortium.
- Davidson DID SUGGEST that at some point retailers might be able to use both CurrentC and ApplePay.
- ApplePay saw more than one million credit card activations in the first three days.

"AirHopper" -- *Deliberate Tempest Broadcasting Possible*

- At MALCON (IEEE 9th International Conference on Malicious and Unwanted Software)
- http://arstechnica.com/tech-policy/2014/10/virginia-judge-police-can-demand-a-suspect-unlock-a-phone-with-a-fingerprint/
- Turning Monitors into FM radios
- Mainframes with AM radios, then Minicomputers -- Core Memory pulses.
    - Core Memory works by electromagnetic fields.
    - PDP/8 consumed a precious "slot" to contain a shield between the CORE and the processor cards.
- AirHopper:
    - Smartphone with an FM receiver.
    - 1 to 7 meters range
    - 60 bytes/second.

"RootPipe" MAC OS X Privilege Elevation

- http://www.net-security.org/secworld.php?id=17575
- www.macworld.com/article/2841965/swedish-hacker-finds-serious-vulnerability-in-os-x-yosemite.html
- A Local Privilege Elevation attack against an Admin Account, gaining root privilege.
- No details revealed until Apple patches, expected in January.
- Workaround: create and use a non-admin MAC OSX account... or don't worry about it.

TextSecure Audit Results

- http://www.net-security.org/secworld.php?id=17575
- The auditors published a results paper...
- "How Secure is TextSecure" ??
    - https://eprint.iacr.org/2014/904.pdf
- ... detailing a so-called "Unknown Key-Share Attack", and mitigations.
- <quote from the paper's abstract>
    - In this paper, we present the first complete description of TEXTSECURE's complex cryptographic protocol and are the first to provide a thorough security analysis of TEXTSECURE. Among other findings, we present an Unknown Key-Share Attack on the protocol, along with a mitigation strategy, which has been acknowledged by TEXTSECURE's developers. Furthermore, we formally prove that—if our mitigation is applied—TEXTSECURE's push messaging can indeed achieve the goals of authenticity and confidentiality.
- TextSecure developers are doubtless addressing that right now.
- (Threema, for the moment, being closed source is not getting an open audit.)

The EFF's Secure Messaging Scorecard

- https://www.eff.org/secure-messaging-scorecard
- 7 Criteria:
    - Encrypted in transit?
    - Encrypted from provider?
    - Verifiable contact identity?
    - Forward secrecy?
    - Open code for independent review?
    - Proper security architecture?
    - Has the code actually BEEN independently audited?
- Two Winners:
    - CryptoCat
    - TextSecure
- Even more comprehensive scorecard:
    - http://projects.propublica.org/graphics/privacy-tools

Fingerprint can be compelled... but not knowledge

- http://arstechnica.com/tech-policy/2014/10/virginia-judge-police-can-demand-a-suspect-unlock-a-phone-with-a-fingerprint/
- **A Virginia Circuit Court judge ruled on Thursday** that a person does not need to provide a passcode to unlock their phone for the police. The court also ruled that demanding a suspect to provide a fingerprint to unlock a phone would be constitutional.
- "Giving police a fingerprint is akin to providing a DNA or handwriting sample or an actual key, which the law permits. A passcode, though, requires the defendant to divulge knowledge, which the law protects against."
- "A communication is 'testimonial' only when it reveals the contents of your mind. We cannot invoke the privilege against self-incrimination to prevent the government from collecting biometrics like fingerprints, DNA samples, or voice exemplars because the courts have decided that this evidence doesn't reveal anything you know. It's not testimonial."

Who's watching whom?

- http://www.salon.com/2014/10/30/im_terrified_of_my_new_tv_why_im_scared_to_turn_this_thing_on_and_youd_be_too/
- Michael Price contributed this short observation to Salon. He's counsel in the Liberty and National Security Program at the Brennan Center for Justice at NYU School of Law.
- <quote>
  I just bought a new TV. The old one had a good run, but after the volume got stuck on 63, I decided it was time to replace it. I am now the owner of a new "smart" TV, which promises to deliver streaming multimedia content, games, apps, social media and Internet browsing. Oh, and TV too.

  The only problem is that I'm now afraid to use it. You would be too — if you read through the 46-page privacy policy.

  The amount of data this thing collects is staggering. It logs where, when, how and for how long you use the TV. It sets tracking cookies and beacons designed to detect "when you have viewed particular content or a particular email message." It records "the apps you use, the websites you visit, and how you interact with content." It ignores "do-not-track" requests as a considered matter of policy.

  It also has a built-in camera — with facial recognition. The purpose is to provide "gesture control" for the TV and enable you to log in to a personalized account using your face. On the upside, the images are saved on the TV instead of uploaded to a corporate server. On the downside, the Internet connection makes the whole TV vulnerable to hackers who have demonstrated the ability to take complete control of the machine.

  More troubling is the microphone. The TV boasts a "voice recognition" feature that allows viewers to control the screen with voice commands. But the service comes with a rather ominous warning: "Please be aware that if your spoken words include personal or other sensitive information, that information will be among the data captured and transmitted to a third party." Got that? Don't say personal or sensitive stuff in front of the TV.

  You may not be watching, but the telescreen is listening.

A GitHub JS implementation of the new Spritz cipher.

- https://github.com/therealjampers/spritzjs
- Very nice and clean. Deliberately designed to be a companion to the formal specification document, using the same variable names, clear and explicit design, etc.

Miscellany

"Ex Machina" Trailer -- April 2015

- https://www.youtube.com/watch?v=EoQuVnKhxaM

SpinRite:

Chris Day
Location: Princes Risborough, Buckinghamshire, UK
Subject: Your Security Now feedback/comment/question
Date: 04 Nov 2014 02:03:53
:
SpinRite recovers a Samsung SSD 840 EVO from the "Performance Restoration Software"

Hi Steve

I've been a SpinRite owner for several years now and used your excellent product from time to time on my systems & servers at home.

I recently heard about the problems with the Samsung Evo SSDs slowing down on your brilliant Security Now podcast with Leo (I'm a CISSP and learnt all I needed to know about crypto, hashing, etc. etc., to pass the CISSP exam just from listening to your podcast over the last 10 years). As my laptop has a Samsung SSD 840 EVO and Samsung have recently released the "Performance Restoration Software" to resolve the slowdown issues I decided to apply the update to my system. What harm could it do?? ;-)

I downloaded and ran the software following all the instructions (apart from the back-up as all my data is synchronised with my server and I have a base-build image of a patched Win 7 OS & core programmes as I rebuild my laptop every 6 months or so). So everything went smoothly, the drive firmware was updated, the laptop rebooted and the "Performance Restoration Software" went to work rewriting every sector on the drive and completed successfully. I left the computer, and the next day when I came to start work the laptop wouldn't boot into Windows! I ran through several cycles of rebooting and not even recovery mode would work! So I grabbed my copy of SpinRite and ran a level 2 scan on my Windows drive. 30 minutes later SpinRite completed and its completion screen proclaimed all was well with nothing amiss. I rebooted the laptop and, as expected, it fired right up into Windows perfectly ;-)

Now, I can't give you a great sob story of how my life's work was on the machine without any back-ups and how SpinRite saved my children from destitution... but I CAN attest to the efficacy of the product, and tell you and your listeners that it's the best $89 I've ever spent!

Regards
Chris Day
MBA BSc (Hons) CISSP MCSE CITP MBCS
Long time "Security Now" listener & 1st time contributor