Security Now! #533 - 11-17-15

Encryption: Law Enforcement's Whipping Boy

This week on Security Now!

- CMU takes a million dollar bride from the FBI
- Firmware vulnerability detection at scale
- Police body cams coming pre-infected
- WhatsApp messaging encryption bypass
- My feelings (and increased muscle mass) after a week with the iPad Pro
- Lots of fun and interesting miscellany
- The post Paris Encryption controversy

Researchers Prove Tin Foil Hats *Boost* Receptivity To Government Signals

"On the Effectiveness of Aluminum Foil Helmets: An Empirical Study" (How-To Geek)
Researchers at MIT, using a network analyzer, tested the impact of tin foil helmets on receptivity of radio-frequency signals. They highlight the method and results in the study abstract:
Among a fringe community of paranoids, aluminum helmets serve as the protective measure of choice against invasive radio signals. We investigate the efficacy of three aluminum helmet designs on a sample group of four individuals. Using a $250,000 network analyser, we find that although on average all helmets attenuate invasive radio frequencies in either direction (either emanating from an outside source, or emanating from the cranium of the subject), certain frequencies are, in fact, greatly amplified. These amplified frequencies coincide with radio bands reserved for government use according to the Federal Communication Commission (FCC). *Statistical evidence suggests the use of helmets may in fact enhance the government's invasive abilities. We speculate that the government may in fact have started the helmet craze for this reason.*

Security News:

Carnegie Mellon researchers were paid one million dollars to attack Tor users? (Last Wednesday)

- Court Docs Show a University Helped FBI Bust Silk Road 2, Child Porn Suspects
- http://motherboard.vice.com/read/court-docs-show-a-university-helped-fbi-bust-silk-road-2-child-porn-suspects
- http://motherboard.vice.com/read/academics-livid-concerned-over-allegations-that-cmu-helped-fbi-attack-tor?trk_source=recommended

- The Tor Project Blog: https://blog.torproject.org/blog/did-fbi-pay-university-attack-tor-users
  The Tor Project has learned more about last year's attack by Carnegie Mellon researchers on the hidden service subsystem. Apparently these researchers were paid by the FBI to attack hidden services users in a broad sweep, and then sift through their data to find people whom they could accuse of crimes. We publicized the attack last year, along with the steps we took to slow down or stop such an attack in the future.

  We have been told that the payment to CMU was at least $1 million.

  There is no indication yet that they had a warrant or any institutional oversight by Carnegie Mellon's Institutional Review Board. We think it's unlikely they could have gotten a valid warrant for CMU's attack as conducted, since it was not narrowly tailored to target criminals or criminal activity, but instead appears to have indiscriminately targeted many users at once.

  Such action is a violation of our trust and basic guidelines for ethical research. We strongly support independent research on our software and network, but this attack crosses the crucial line between research and endangering innocent users.

  This attack also sets a troubling precedent: Civil liberties are under attack if law enforcement believes it can circumvent the rules of evidence by outsourcing police work to universities. If academia uses "research" as a stalking horse for privacy invasion, the entire enterprise of security research will fall into disrepute. Legitimate privacy researchers study many online systems, including social networks — If this kind of FBI attack by university proxy is accepted, no one will have meaningful 4th Amendment protections online and everyone is at risk.

  We teach law enforcement agents that they can use Tor to do their investigations ethically, and we support such use of Tor — but the mere veneer of a law enforcement investigation cannot justify wholesale invasion of people's privacy, and certainly cannot give it the color of "legitimate research".

  Whatever academic security research should be in the 21st century, it certainly does not include "experiments" for pay that indiscriminately endanger strangers without their knowledge or consent.

- Matthew Green, Johns Hopkins... on Research Ethics
  http://blog.cryptographyengineering.com/2015/11/why-tor-attack-matters.html
  [snip]

  You might wonder why this is important. After all, the crimes we're talking about are pretty disturbing. One defendant is accused of possessing child pornography, and if the allegations are true, the other was a staff member on Silk Road 2.0. If CMU really did conduct Tor de-anonymization research for the benefit of the FBI, the people they identified were allegedly not doing the nicest things. It's hard to feel particularly sympathetic.

  Except for one small detail: there's no reason to believe that the defendants were the only people affected.

  If the details of the attack are as we understand them, a group of academic researchers deliberately took control of a significant portion of the Tor network. Without oversight from the University research board, they exploited a vulnerability in the Tor protocol to conduct a traffic confirmation attack, which allowed them to identify Tor client IP addresses and hidden services. They ran this attack for five months, and potentially de-anonymized thousands of users. Users who depend on Tor to protect them from serious harm.

  While most of the computer science researchers I know are fundamentally ethical people, as a community we have a blind spot when it comes to the ethical issues in our field. There's a view in our community that Institutional Review Boards are for medical researchers, and we've somehow been accidentally caught up in machinery that wasn't meant for us. And I get this -- IRBs are unpleasant to work with. Sometimes the machinery is wrong.

  But there's also a view that computer security research can't really hurt people, so there's no real reason for [that] sort of ethical oversight machinery in the first place. This is dead wrong, and if we want to be taken seriously as a mature field, we need to do something about it.

  We may need different machinery, but we need something. That something begins with the understanding that active attacks that affect vulnerable users CAN be dangerous, and should never be conducted without rigorous oversight -- if they must be conducted at all. It begins with the idea that universities should have uniform procedures for both faculty researchers and quasi-government organizations like CERT, if they live under the same roof. It begins with CERT and CMU explaining what went on with their research, rather than treating it like an embarrassment to be swept under the rug.

  Most importantly, it begins with researchers looking beyond their own research practices. So far, the response to the Tor news has been a big shrug. It's wonderful that most of our community is responsible. But none of that matters if we look the other way when others in our community fail to act responsibly.

- ArsTechnica Coverage Links:
  - https://nakedsecurity.sophos.com/2015/11/13/tor-project-says-fbi-paid-carnegie-mellon-1m-to-unveil-tor-users/
  - http://arstechnica.com/tech-policy/2015/11/fbi-the-allegation-that-we-paid-cmu-1m-to-hack-into-tor-is-inaccurate/
  - http://arstechnica.com/tech-policy/2015/11/tor-director-fbi-paid-carnegie-mellon-1m-to-break-tor-hand-over-ips/

Firmware reverse engineering at scale!

- Automated Dynamic Firmware Analysis at Scale: A Case Study on Embedded Web Interfaces
- http://arxiv.org/pdf/1511.03609v1.pdf
- French & German researchers
- Created a virtual device environment:
  - Ubuntu 14 VM
    - QEMU
    - Collection of open source exploit kits - Metasploit, Nessus, etc.
- 1925 firmware images from 54 different vendors.
- Important vulnerabilities in 185 firmware images, affecting nearly a quarter of vendors.

Police body cams found pre-installed with notorious Conficker worm.

- One of the world's most prolific pieces of malware is found in cams from Martel.
- http://arstechnica.com/security/2015/11/police-body-cams-found-pre-installed-with-notorious-conficker-worm/
- "Vidshield" Body Worn Police Camera
  - http://www.martelelectronics.com/vidshield-body-worn-police-camera/
  - In Stock now! -- FREE Shipping! (But call for pricing)
  - Five Star Rating (*****) 8 Product Reviews
  - <quote> The Vid-Shield Police body video camera not only records in High Definition but it also shots 12 Mega pixel still images, equivalent to the best digital cameras in the world. The Vid-Shield has the Time/Date Stamp embedded into the video and photos and cannot be tamped with it making it perfect for evidence.
- iPower Technologies
  - http://www.goipower.com/?pageId=40
  - iPower Technologies, a Boca Raton based network integrator, discovered the following security vulnerability in the Martel Frontline Camera with GPS. This product is sold and marketed as a body camera for official police department use. iPower is currently working to develop a cloud based video storage system for government agencies and police departments to store and search camera video.

    During testing and evaluation of the Martel Electronics product, employees discovered that multiple body cameras had been shipped to iPower preloaded with the Win32/Conficker.B!inf worm virus.

    When the camera was connected to a computer, iPower's antivirus software immediately caught the virus and quarantined it. However, if the computer did not have antivirus actively protecting the computer it would automatically run and start propagating itself through the network and internet. iPower staff proceeded to test the virus in a virtual lab environment, and did confirm that the virus was not a false positive. iPower uploaded the files to Virus Total, a web based application designed to test computer files for viruses and the site verified iPower's findings.

In the iPower virtual lab environment, packet captures were also run on the infected PC to view the viruses' network activity using Wireshark. The virus, classified as a worm virus, immediately started to attempt to spread to other machines on the iPower lab network, and also attempted several phone home calls to internet sites.

iPower initiated a call and multiple emails to the camera manufacturer, Martel on November 11th 2015. Martel staff has yet to provide iPower with an official acknowledgement of the security vulnerability. iPower President, Jarrett Pavao, decided to take the story public due to the huge security implications of these cameras being shipped to government agencies and police departments all over the country.

- https://www.virustotal.com/en/file/dfc1f69b3efc968310ed8901eda055ea40fa488059a6a3763c356539820ccc3e/analysis/
  - Win32/Conficker.B!inf
  - 40/54 -- NOT recognized by MalwareBytes or McAfee

- Dan Goodin writing for ArsTechnica:
  Alternately known as Downup, Downadup, and Kido, Conficker took hold in late 2008, a few days after Microsoft issued an emergency patch for a Windows vulnerability that allows self-replicating exploits. Within a few months, Conficker had enslaved as many as 15 million Windows PCs. Its sprawling botnet of infected machines eluded the vigorous takedown efforts of the Conficker working group, which was made up of Microsoft and more than a dozen partners in the security and domain registration industries.

  Conficker was especially hard to contain because it used a variety of advanced methods to self-propagate, including exploiting weaknesses in the Windows autostart feature when users inserted USB drives into their computers. The malware also generated hundreds of pseudo-random domain names each day that infected machines could contact to receive new instructions. The scheme allowed the botnet to survive even when old domain names were turned over to the working group. There are at least five significant variations of Conficker that are denoted with the letters A through E.

  A report that police cameras are shipping with Conficker.B preinstalled is testament to the worm's relentlessness. It's also troubling because the cameras can be crucial in criminal trials. If an attorney can prove that a camera is infected with malware, it's plausible that the vulnerability could be grounds for the video it generated to be thrown out of court, or at least to create reasonable doubt in the minds of jurors. Infected cameras can also infect and badly bog down the networks of police forces, some of which still use outdated computers and ineffective security measures.

WhatsApp's is (at the least) leaking metadata

- http://www.fit.vutbr.cz/research/pubs/index.php?file=%2Fpub%2F10979%2FWhatsApp.pdf&id=10979
- This amounts to an important metadata decryption.
    - (Abstract) WhatsApp is a widely adopted mobile messaging application with over 800 million users. Recently, a calling feature was added to the application and no comprehensive digital forensic analysis has been performed with regards to this feature at the time of writing this paper. In this work, we describe how we were able to decrypt the network traffic and obtain forensic artifacts that relate to this new calling feature which included the:
        - a) WhatsApp phone numbers,
        - b) WhatsApp server IPs,
        - c) WhatsApp audio codec (Opus),
        - d) WhatsApp call duration, and
        - e) WhatsApp's call termination.
    - We explain the methods and tools used to decrypt the traffic as well as thoroughly elaborate on our findings with respect to the WhatsApp signaling messages. Furthermore, we also provide the community with a tool that helps in the visualization of the WhatsApp protocol messages.
    - The communication keys were NOT retrieved, but they speculate that further analysis and reverse engineering may produce additional revelations.

Security Tools

Hardware platform for pfSense:

- http://www.pcengines.ch/

Miscellany

- iPad Pro
    - Two *separate* environments:
        - This is my primary (perhaps only) device
        - This is my secondary (alternative) device

    - The Good:
        - Fast: A more powerful processor
        - Newer keyboard with less shifting is a win!
        - The sound is amazing!
        - Watching video with the screen and sound is great.

    - The Bad:
        - It's too big.
            - Physically cumbersome
            - Poor use of larger screen space except for Web surfing.
            - Room for many more icons.
            - Mail doesn't utilize space... web does

    - Pad's power consumption is WAY up!
        - Fast: A more powerful processor
        - A LOT more screen to backlight.
        - Short battery life compared to smaller ipad.
        - Runs quite hot at full brightness.
        - Reducing brightness to ~50% helps a lot.
        - So power hungry that it's draining even when plugged in!

    - Newer keyboard is so big that one finger typing is difficult.
    - Sound effect volume is very low

    - iOS appears to be collapsing
        - Web Portal login often fails, rebooting fixes for awhile.
        - Safari shows lower page blanking

    - Tip on sidebar access: start way to the left.
        - (Sidebar should have its own MRU)

- Gene Amdahl died last week at age 92. (Blank stares from the TWiT panel)
    - Osbourne?? Anyone??
    - "Daddy! You 3D printed the Save Icon!"

- "Auralux" for iOS (iPhone iPad) and Android
    - by War Drum Studios
    - Description (from the PC version)
    - Auralux (formerly Aurora) is an abstract, essentialized, and simplified real-time strategy game. You have only one type of unit to command and only one type of order to give those units. You and your [automated] opponents start the game with equal resources. Quick reflexes will get you nowhere. The only path to victory is through strategy.

      Auralux features a slow, floating feel and gorgeous minimalistic graphics. The entire world pulses to the rhythm of ambient music, and the player's actions evoke sounds that smoothly coalesce into melody. This game is meant to provide a relaxing, cerebral experience. Every action has its reaction, and every option has its costs. Auralux is a game in which your choices matter.

    - Features:
        - Includes every feature and more from the renowned PC game.
        - Free to try for as long as you like! Simply purchase additional levels for a very low price if you enjoy the game and want more challenges.
        - Gameplay optimized for touch screen devices.
        - Countless hours of gameplay
        - Two available game modes : Normal and Speed Mode, with a secret mode for expert players to unlock!
        - Relaxing, ambient soundtrack brings you into a rhythm and meditative state.
        - Free to install, additional packs available

- Revisiting "Spectre"
    - IMDB of 7.3 vs Skyfall at 7.8
    - http://www.movies.com/movie-news/39spectre39-has-broken-two-guinness-world-records/19522
    - The latest James Bond movie has broken a few box office records since its release, including the one for biggest opening of all time in the UK. But SPECTRE, which also topped the box office in the U.S. over the weekend, has achieved some other feats that don't have to do with theatrical performance.

      The movie officially features the largest film stunt explosion in history, as acknowledged by Guinness World Records. The honor specifically goes to effects supervisor Chris Corbould (who is also an Oscar winner for Inception and nominee for The Dark Knight) for creating the esteemed sequence.

      Taking place in Erfoud, Morocco, the blast had a total yield of 68.47 tonnes of TNT equivalent and was the result of detonating 8,418 litres of kerosene with 33 kg of powder explosives - and it lasted for over 7.5 seconds.

      SPECTRE has broken all the records to become the biggest opening of all time in UK box office history. It also made box office history for the biggest openings in the Netherlands, Finland, Norway, Denmark and Sweden.

- The Good Wife : "Driven" S7 / E7

SpinRite

Simon Guettier <simon@guettier.co.uk>
Location: Waddesdon Village, Buckinghamshire, England, UK
Subject: Spinrite blows away the storm that blew away my PC!
Date: 16 Nov 2015 05:26:07
:
Hi Steve,
This morning I booted my desktop PC and to my alarm it was behaving monstrously at startup, basically just being incredibly sluggish - desktop icons wouldn't appear at all, browser launch took over 5 minutes - nothing worked at all. I was puzzled because the day before I'd done a complete fresh install of Windows and all appeared fine then. When I powered down the PC the night before all had been fine.

Then I remembered that the day before my village had suffered some power glitches. I live in the small village of Waddesdon near Oxford in the UK. We'd had severe storms and, believe it or not, mains power to the village is at least in part still delivered by overhead power lines. In storms the lines get whacked by trees and outages are quite common. The day before there were two actual outages and two instances where the mains voltage dipped alarmingly for 2-3 seconds each time.

My PC was on at the time though I wasn't sitting at it. Could this be the cause of the dreadful slowdown in performance?

"Let's try Spinrite", I thought.

My PC has a 256Gb SSD as the operating system drive and a large 2Tb standard hard drive which serves for data. I ran Spinrite at Level 2 on the SSD - no errors. At this point I almost stopped, thinking that the other 2Tb drive was not really mission critical and shouldn't really affect performance. But - what the hell - I did another Level 2 check which, obviously, took quite a bit longer. I was watching those little blue squares from time to time - no greens or reds. But at one point I did notice that for a while Spinrite took ages before it put a blue square up - for several squares in a row, perhaps 10. Anyway it finished, all normal, no green or red indications.

I wasn't terribly convinced that I'd found the problem as no errors were reported. So you can imagine my surprise on rebooting to find that all was well again and the PC behaved just as it should.

This is the second time Spinrite has rescued me - I managed to rescue a friend's badly corrupted drive where she had many irreplaceable photos of her father who had passed away. So I reckon I've had my money's worth. I look forward to the new version.

With best wishes,
Simon Guettier (PR. GET-EEE-A)
Waddesdon,
England

Encryption: Law Enforcement's Whipping Boy

Troublesome Reporting:

- ArsTechnica:
  <quote> The investigation into last Friday's coordinated terrorist attacks has quickly turned up evidence that members of the Islamic State (ISIS) communicated with the attackers from Syria using encrypted communications, according to French officials. (links to NYT article)

- New York Times:
  <quote> European officials said they believed the Paris attackers had used some kind of encrypted communication, but offered no evidence. “The working assumption is that these guys were very security aware, and they assumed they would be under some level of observation, and acted accordingly,” said a senior European counterterrorism official who spoke on the condition of anonymity to discuss confidential information.

Update from the New York Times:
http://www.nytimes.com/2015/11/17/world/europe/encrypted-messaging-apps-face-new-scrutiny-over-possible-role-in-paris-attacks.html
The New York Times
"Encrypted Messaging Apps Face New Scrutiny Over Possible Role in Paris Attacks"

WASHINGTON — American and French officials say there is still no definitive evidence to back up their presumption that the terrorists who massacred 129 people in Paris used new, difficult-to-crack encryption technologies to organize the plot.

But in interviews, Obama administration officials say the Islamic State has used a range of encryption technologies over the past year and a half, many of which defy cracking by the National Security Agency. Other encryption technologies, the officials hint, are less secure than terrorist and criminal groups may believe, and clearly they want to keep those adversaries guessing which ones the N.S.A. has pierced.

Some of the most powerful technologies are free, easily available encryption apps with names like Signal, Wickr and Telegram, which encode mobile messages from cellphones. Islamic State militants used Telegram two weeks ago to claim responsibility for the crash of the Russian jet in the Sinai Peninsula that killed 224 people, and used it again last week, in Arabic, English and French, to broadcast responsibility for the Paris carnage. It is not yet clear whether they also used Telegram's secret-messaging service to encrypt their private conversations.

Nonetheless, such "end-to-end" encryption technology is now so widespread that the attack has revived vitriolic arguments between American intelligence officials and Silicon Valley. Only weeks ago, the matter appeared settled, at least temporarily, with a decision by President Obama that it would be fruitless for the government to try to compel the technology companies to provide the keys to protected conversations and data.

Apple has already made encryption technology a standard part of its iMessage service, and Apple's chief executive, Timothy D. Cook, has been among the most vocal in defending a technology for which the keys to decode messages are held not by his company but by the users at each end of the conversation.

Any other approach, Mr. Cook has argued to Mr. Obama, would undercut Apple customers' confidence that the most precious data they keep in their phones is safe from garden-variety cybercriminals as well as sophisticated nation states that could gain access to keys via hacking, or lawfully through court order. Mr. Cook argues that investigators have ways to obtain crucial clues from the available "metadata" about who is talking to whom by phone, from information in the Internet cloud — or, security experts have said, by hacking a target's device.

But the speed of the encryption wave has touched off alarm among law enforcement and intelligence officials, who say it significantly increases the chances that they will miss evidence of an impending attack. Prime Minister David Cameron of Britain threatened late last year to ban such technologies, although he soon backed down. France is threatening to insist on access — and if the French do, so will China, many fear, raising questions about whether the same technology used to crack terrorists' communications will be used to crack dissidents' as well.

"I think this is going to open an entire new debate about security versus privacy," said Michael Morell, a former deputy director of the C.I.A., whose book this year, "The Great War of Our Time," traced the efforts, and failures, in tracking terror plots.

"We have, in a sense, had a public debate" on encryption, he said over the weekend on CBS News's "Face the Nation." "That debate was defined by Edward Snowden," the former National Security Agency contractor who revealed much about the agency's efforts to break encryption. Now, he said, a new argument will be "defined by what happened in Paris."

It is also possible the Paris attackers conducted much of their planning face to face, particularly since several lived in the same Brussels neighborhood. But if there was a command center in Syria or elsewhere, some form of communications would have been required.

Just before the Paris attacks, Belgian officials said Islamic State terrorists had been hiding their communication using online gaming tools like Sony's PlayStation 4 to mask their chatter under that of millions of online video war game players who invoke the same language of violent, religious extremists.

Jan Jambon, Belgium's federal home affairs minister, told a public audience last week that "PlayStation 4 is even more difficult to keep track of than WhatsApp," a popular messaging system owned by Facebook.

But if that was the case, it would undermine the argument that end-to-end encryption allowed the Paris terrorism plot to go undetected. While PlayStation and Xbox deploy encryption to protect customers' personal data like credit card information, it leaves their communications open to government interception in ways that WhatsApp and iMessage do not.

So far, Mr. Obama has been reluctant to insist on a back door into the systems. He rejected the argument of the F.B.I. director, James B. Comey, that the United States should require any company that provides encrypted software and hardware to engineer a way for the government, armed with a court order, to get access. That decision came after a year of study led by the White House counterterrorism adviser, Lisa Monaco, and the head of the White House cybersecurity office, Michael Daniel.

The White House ultimately adopted a view put forth by 14 of the world's top cryptographers and computer security experts who wrote, in a white paper, that weakening the encryption of American technology sold by companies like Apple, Google and Facebook would only render confidential data and critical infrastructure more vulnerable to criminals and national adversaries, and push terrorists to adopt encrypted services sold overseas. As a result, when companies like Apple and Facebook are issued court orders to help governments monitor their customers' messages, all they can do is turn over a stream of unintelligible code.

That has inflamed law enforcement officials like Mr. Comey and William J. Bratton, the New York City police commissioner, who told "Face the Nation" on Sunday that encrypting communications in this way had made it impossible for officials to collect warnings on terrorist attacks.

"We, in many respects, have gone blind as a result of the commercialization and the selling of these devices that cannot be accessed either by the manufacturer or, more importantly, by us in law enforcement, even equipped with search warrants and judicial authority," Mr. Bratton said.

Security experts counter that such arguments ignore the fact that even end-to-end encrypted technology leaves a trail of metadata behind that can be used to parse who is talking to whom, when and where. "Encryption is really good at making it difficult to hide the content of communications, but not good at hiding the presence of communications," said Matt Blaze, a computer security expert at the University of Pennsylvania.

Mr. Blaze also noted that the authorities can still read communications if they hack into the target's device, or what security experts call "the end point."

“All the encryption in the world doesn’t help if the end point that holds the keys are compromised,” Mr. Blaze said. “So this idea that encryption make terrorists’ communications go completely dark has a pretty big asterisk next to it.”

Even if Apple and others in the United States were compelled to weaken the encryption in their services, American authorities still would have had no judicial authority over Telegram, the Berlin-based messaging service, recently used by Islamic State terrorists to broadcast their communiqués.

Bruce Schneier:

- "Paris Attacks Blamed on Strong Cryptography and Edward Snowden"
    - https://www.schneier.com/blog/archives/2015/11/paris_attacks_b.html
- Bruce writes: Well... that didn't take long:
    - http://www.dailydot.com/politics/paris-attack-encryption-snowden/
    - (quotes the top of The Daily Dot) As Paris reels from terrorist attacks that have claimed at least 128 lives, fierce blame for the carnage is being directed toward American whistleblower Edward Snowden and the spread of strong encryption catalyzed by his actions.
- (Bruce) "Now the Paris attacks are being used an excuse to demand back doors."
- I was going to write a definitive refutation to the meme that it's all Snowden's fault, but Glenn Greenwald beat me to it.

Glenn Greenwald

- Exploiting Emotions About Paris to Blame Snowden, Distract from Actual Culprits Who Empowered ISIS
- https://theintercept.com/2015/11/15/exploiting-emotions-about-paris-to-blame-snowden-distract-from-actual-culprits-who-empowered-isis/