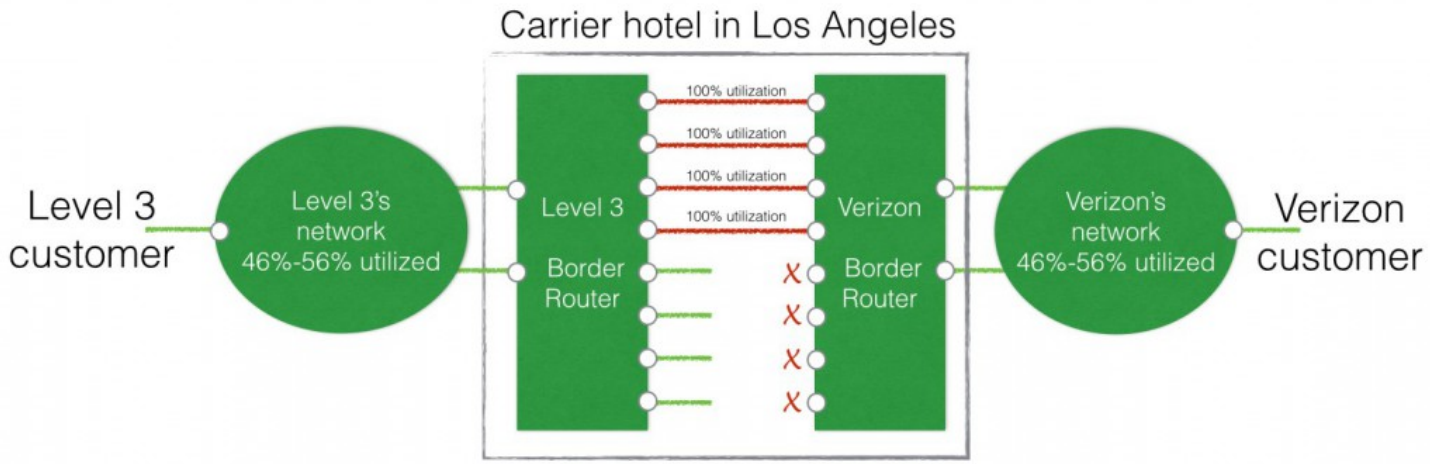
Security Now! #465 - 07-22-14

iOS Surveillance?

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!

- Google Chrome and Firefox updates
- Level3 responds to Verizon's posting
- Microsoft Research says not to use strong passwords?
- Taking another look at "Canvas Fingerprinting"
- Miscellaneous Notes & Updates
- And... To what degree is iOS a Surveillance tool?



Security News:

Chrome drops the other shoe: "[x] Check for certificate revocation option removed!"

Firefox updates to v31: Continually moving forward and maturing

Level3 Responds to Verizon's Network Congestion Chart:

- http://blog.level3.com/global-connectivity/verizons-accidental-mea-culpa/
- Mark Taylor, Vice President of Content and Media.

[SNIP]... So why does Verizon show this red bar? And why do they blame Level 3 and the other network operators contracted by Netflix?

Well, as I explained in my last blog post, the bit that is congested is the place where the Level 3 and Verizon networks interconnect. Level 3's network interconnects with Verizon's in ten cities; three in Europe and seven in the United States. The aggregate utilization of those

interconnections in Europe on July 8, 2014 was 18% (a region where Verizon does NOT sell broadband to its customers). The utilization of those interconnections in the United States (where Verizon sells broadband to its customers and sees Level 3 and online video providers such as Netflix as competitors to its own CDN and pay TV businesses) was about 100%. And to be more specific, as Mr. Young pointed out, that was 100% utilization in the direction of flow from the Level 3 network to the Verizon network.

So let's look at what that means in one of those locations. The one Verizon picked in its diagram: Los Angeles. All of the Verizon FiOS customers in Southern California likely get some of their content through this interconnection location. It is in a single building. **And boils down to a router Level 3 owns, a router Verizon owns and four 10Gbps Ethernet ports on each router. A small cable runs between each of those ports to connect them together.** [SGgrc emphasis added] This diagram is far simpler than the Verizon diagram and shows exactly where the congestion exists.

Verizon has confirmed that everything between that router in their network and their subscribers is uncongested – in fact has plenty of capacity sitting there waiting to be used. Above, I confirmed exactly the same thing for the Level 3 network. So in fact, we could fix this congestion in about five minutes simply by connecting up more 10Gbps ports on those routers. Simple. Something we've been asking Verizon to do for many, many months, and something other providers regularly do in similar circumstances. But Verizon has refused. So Verizon, not Level 3 or Netflix, causes the congestion. Why is that? Maybe they can't afford a new port card because they've run out – even though these cards are very cheap, just a few thousand dollars for each 10 Gbps card which could support 5,000 streams or more. If that's the case, we'll buy one for them. Maybe they can't afford the small piece of cable between our two ports. If that's the case, we'll provide it. Heck, we'll even install it.

But, here's the other interesting thing also shown in the Verizon diagram. This congestion only takes place between Verizon and network providers chosen by Netflix. The providers that Netflix does not use do not experience the same problem. Why is that? Could it be that Verizon does not want its customers to actually use the higher-speed services it sells to them? Could it be that Verizon wants to extract a pound of flesh from its competitors, using the monopoly it has over the only connection to its end-users to raise its competitors' costs?

Microsoft Research -- Stop using strong passwords

- http://www.theguardian.com/technology/2014/jul/16/microsoft-stop-using-strong-passwords-everywhere
- http://research.microsoft.com/pubs/217510/passwordPortfolios.pdf
- Many breathless articles in the press… "Microsoft recommends against always using strong passwords."
- Tons of fancy calculus and graphs to tell us what we already know:
    - Using different strong passwords, without reuse, places a huge burden upon the user.

Brian Krebs: Java Update: Patch It or Pitch It (*Java 7 Update 65*.)

- http://krebsonsecurity.com/2014/07/java-update-patch-it-or-pitch-it/

- **Oracle** today released a security update for its **Java** platform that addresses at least 20 vulnerabilities in the software. Collectively, the bugs fixed in this update earned Oracle's "critical" rating, meaning they can be exploited over a network without the need for a username and password. In short, if you have Java installed it is time to patch it or pitch it.

Tracking people through canvas fingerprinting

- Gizmodo: What You Need to Know About the Sneakiest New Online Tracking Tool
  - http://gizmodo.com/what-you-need-to-know-about-the-sneakiest-new-online-tr-1608455771
  - What do the White House and YouPorn have in common? Their websites both use canvas fingerprinting, a newer form of online tracking designed to make it hard to hide. ProPublica investigated the pervasive shadowing method, developed as an insidious alternative to cookies so websites can keep tabs on where their visitors browse online.

- https://securehomes.esat.kuleuven.be/~gacar/persistent/index.html
  - <quote> By crawling the homepages of the top 100,000 sites we found that more than 5.5% of the crawled sites include canvas fingerprinting scripts. Although the overwhelming majority (95%) of the scripts belong to a single provider (addthis.com), we discovered a total of 20 canvas fingerprinting provider domains, active on 5542 of the top 100,000 sites.

- What IS Canvas Fingerprinting?
- What is it NOT?

- Our results.
  - We exhibit a new system fingerprint based on browser font and WebGL rendering. To obtain this fingerprint, a website renders text andWebGL scenes to a <canvas> element, then examines the pixels produced. Different systems produce different output, and therefore different fingerprints. Even very simple tests|such as rendering a single sentence in a widely distributed system font|produce surprising variation.
  - The new fingerprint has several desirable properties:
    - It is consistent. In our experiments, we obtain pixel identical results in independent trials from the same user.
    - It is high-entropy. In 294 experiments on Amazon's Mechanical Turk, we observed 116 unique fingerprint values, for a sample entropy of 5.73 bits. This is so even though the user population in our experiments exhibits little variation in browser and OS.
    - It is orthogonal to other fingerprints. Our fingerprint measures graphics driver and GPU model, which is independent of other possible fingerprints discussed below.
    - It is transparent to the user. Our tests can be performed, onscreen, in a fraction of a second. There is no indication, visual or otherwise, that the user's system is being fingerprinted.
    - It is readily obtainable. Any website that runs Java-Script on the user's

browser can ngerprint its rendering behavior; no access is needed besides what is provided by the usual web attacker model.

- List of sites using persistent fingerprinting:
  - https://securehomes.esat.kuleuven.be/~gacar/sticky/index.html
- "addthis.com" should be blocked by HOSTS file
  - http://www.addthis.com/privacy/opt-out
- EFF's Privacy Badger
  - https://www.eff.org/privacybadger
  - How is Privacy Badger different to Disconnect, Adblock Plus, Ghostery, and other blocking extensions?

    Privacy Badger was born out of our desire to be able to recommend a single extension that would automatically analyze and block any tracker or ad that violated the principle of user consent; which could function well without any settings, knowledge or configuration by the user; which is produced by an organization that is unambiguously working for its users rather than for advertisers; and which uses algorithmic methods to decide what is and isn't tracking.

    Although we like Disconnect, Adblock Plus, Ghostery and similar products (in fact Privacy Badger is based on the ABP code!), none of them are exactly what we were looking for. In our testing, all of them required some custom configuration to block non-consensual trackers. Several of these extensions have business models that we weren't entirely comfortable with. And EFF hopes that by developing rigorous algorithmic and policy methods for detecting and preventing non-consensual tracking, we'll produce a codebase that could in fact be adopted by those other extensions, or by mainstream browsers, to give users maximal control over who does and doesn't get to know what they do online.

Miscellany

DELL begins accepting payment via BitCoin

- http://en.community.dell.com/dell-blogs/direct2dell/b/direct2dell/archive/2014/07/18/we-re-now-accepting-bitcoin-on-dell-com.aspx
- Partnership with Coinbase.
- BTC's USD been floating around just North of $600.

Particle Fever:

- iTunes $5 to watch // Netflix

"A Better Queue" -- What to Watch?

- Netflix meets "Rotten Tomatoes"
- http://abetterqueue.com/
- Sliders:
  - Tomatometer 0-100% / Minimum Number of Reviews / Years Between...
- 27 category selections

DNS Benchmark:

- GRC's #1 ranked freeware.
- 1,600 downloads/day for nearly 1.5 million total
- From: "Michelle Roberts"
  Subject: DNS Benchmark
  Date: Fri, 18 Jul 2014 07:54:36 -0000

  Thank-you very much for the DNS Benchmark application. My ISP, although pretty fast (a cable provider) was still choppy at times. However, since using your application and switching to the top two DNS servers, my internet experience has been like a dream. I assume I will need to "benchmark" on occasion (say quarterly) to stay in good shape...maybe not since OpenDNS seems to be the top player in my area.

  Thanks again for a very nice application.

SpinRite:

Ben Perrett
Location: Sheffield, England
Subject: A bit confused if you can help!

Hi, I am interested in purchasing SpinRite after listening to Security Now for the last 4 months as I have obviously become accustomed to it's use but never needed it until now.

Within the last 2 week my Macbook Pro 1TB hard drive has developed errors which is causing it to crash more regularly. I have bought a new 1TB drive to sustain my solid state urge but wanted to repair the old drive and bring it back to use.

Would it be possible to correct my old hard drive with SpinRite if I connected it to a Windows machine that had SpinRite installed? Would this method be difficult accomplish in terms of File Systems.

Many thanks in advance. Keep up the great show!

Jonathan Zdziarski Links

Jonathan Zdziarski is a former Research Scientist for McAfee, Inc., and well known outside of work in the iPhone community as “NerveGas”, who has contributed significantly to research into the iPhone and iPod touch.

http://www.zdziarski.com/blog/?p=3441

HOPE X Slides:
http://www.zdziarski.com/blog/wp-content/uploads/2014/07/iOS_Backdoors_Attack_Points_Surveillance_Mechanisms.pdf

iOS Surveillance?

Is iOS a Spying Tool?

HopeX Conference:

- Jonathan Zdziarski / http://www.zdziarski.com/blog/
- Slides: Identifying Back Doors, Attack Points, and Surveillance Mechanisms in iOS Devices.
- http://www.zdziarski.com/blog/wp-content/uploads/2014/07/iOS_Backdoors_Attack_Points_Surveillance_Mechanisms.pdf

Here we go again:

- "Security researcher suggests 600M iOS devices have Apple-created backdoors for data"
  - http://gigaom.com/2014/07/21/security-researcher-suggests-600m-ios-devices-have-apple-created-backdoors-for-data/

- "Researcher Identifies Hidden Data-Acquisition Services in iOS"
  - http://threatpost.com/researcher-identifies-hidden-data-acquisition-services-in-ios/107335

- "Forensic Expert Questions Covert 'Backdoor' Services Included in iOS by Apple"
  - http://www.macrumors.com/2014/07/21/covert-backdoors-ios/

- "Undocumented iOS functions allow monitoring of personal data, expert says"
- "Backdoor" can be abused by gov't agents and ex-lovers to gain persistent access."
  - http://arstechnica.com/security/2014/07/undocumented-ios-functions-allow-monitoring-of-personal-data-expert-says/
  - <quote> Apple has endowed iPhones with undocumented functions that allow unauthorized people in privileged positions to wirelessly connect and harvest pictures, text messages, and other sensitive data without entering a password or PIN, a forensic scientist warned over the weekend.

- Hidden network packet sniffer in MILLIONS of iPhones, iPads Plus Host of Spying tools
  - http://www.theregister.co.uk/2014/07/21/ios_firmware_contains_packet_sniffer_and_host_of_secret_spying_tools/
  - <quote> An analysis of iOS by a security expert digging into claims of the NSA spying on Apple products has revealed some unexplained surveillance tools in the operating system.

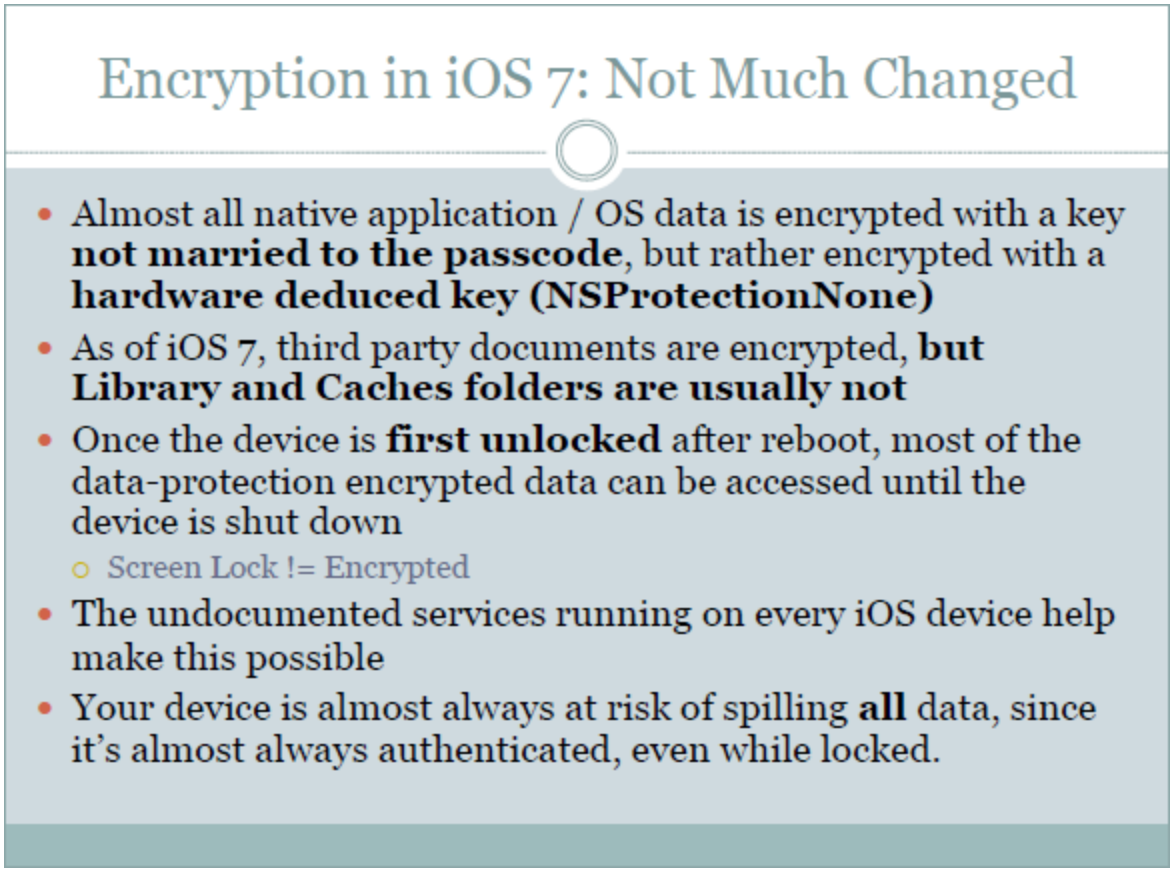
My overall take:

- This sort of ruthless analysis is ALWAYS useful and important for security.

- The nature of the beast (security) is such that well meaning attack is crucial... not only for the achievement of true security, but for the achievement of trust.
  - (Steve Ballmer and XP -- the most secure OS ever.)

- Nothing that was said should take anyone by surprise.
- Jonathan was very careful with his facts.
- I don't think he got anything overtly wrong, yet due to the nature of his presentation, the tone was inherently aimed at frightening us and highlighting weakness.

Slide 10



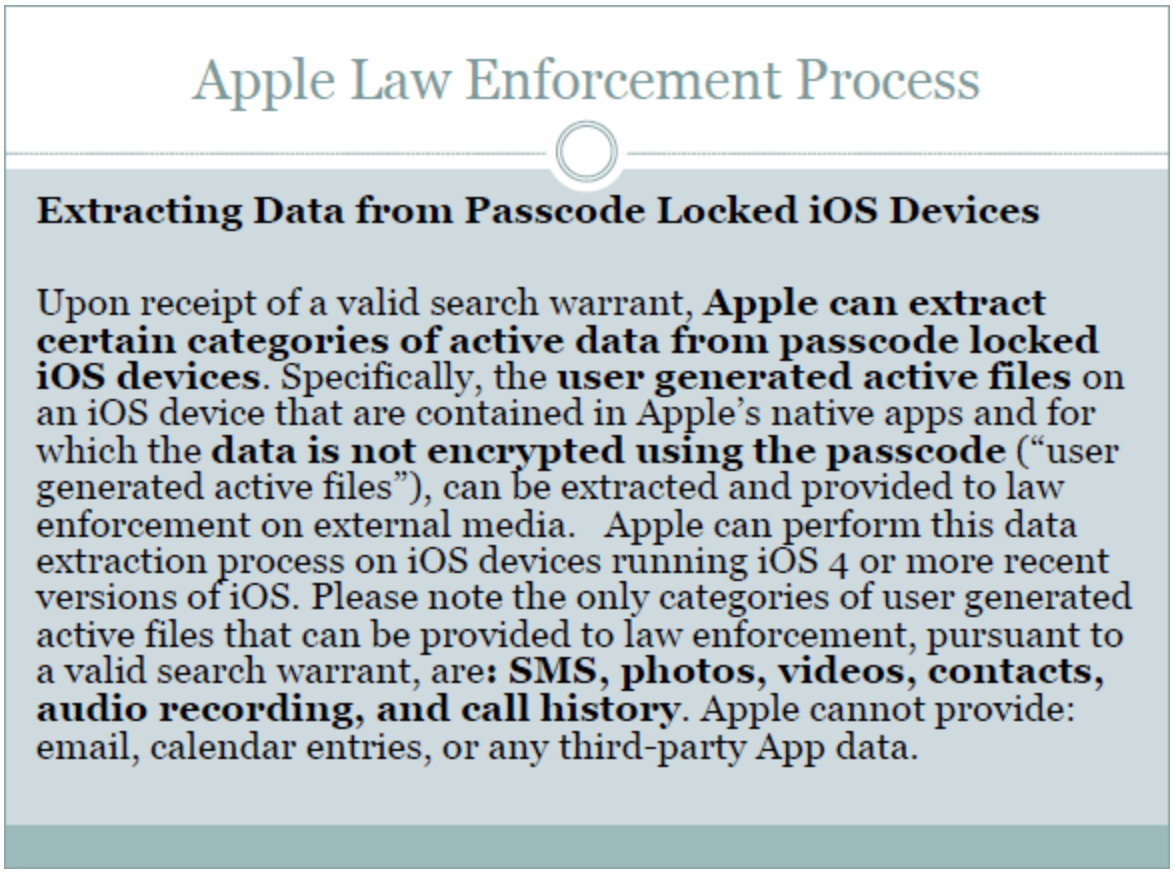
- Yes. And while we're walking upright we're almost always at risk of falling down.
- And, really… "**SPILLING" all data??**

- And all THAT said... he absolutely made some very solid points.
- The iOS attack surface SHOULD always be as minimal as possible.
- Perhaps services such as the pcapd packet capture should not be present in non-developer mode.
- "Developer Mode" should be a more special thing.
- Now that these things HAVE been aired, Apple will need to decide what and where they should and can tighten things down.
- And Apple really DOEs need to respond with more than a canned public relations blurb.

But overall...

This presentation is a beautiful demonstration of the tension -- which is an ongoing theme of this podcast -- which inherently exists between "features and ease-of-use" and security.

Slide 8



Elsewhere Jonathan notes that this is true **ONLY of phones that have been unlocked once since they were powered on or rebooted**. In other words… the iPhone's default file systeem encryption IS absolute -- utterly absolute -- **until** the user places their phone into a mode where it cannot be. (What more could anyone ask?) If the phone is going to be able to operate semi-autonomously in the background to receive eMail, text messages, etc. the lock screen locks the User Interface, not the file system.

"Pairing" is the linchpin...

Jonathan "iOS 7 trust dialog helps, but third party accessories are making people stupid again … and people are naturally stupid too"

Undocumented Services

- Accessed through *lockdownd*, requiring pairing authentication. (Explain Pairing)
- MACTANS talk demonstrated how easy Juice Jacking can be to establish pairing
  - iOS 7 trust dialog helps, but third party accessories are making people stupid again … and people are naturally stupid too
- Law enforcement agencies moving to tablet devices for pairing and acquisition in the field; USB thumb drive to scan computers for pairing records
- Der Spiegel outlined black bag techniques to access a target's computer, where pairing records live

Note: ***"Undocumented Services"*** ?? In a closed system where what's known is almost entirely the result of patient, talented, and truly amazing reverse engineering? Of course it's undocumented… it's closed!

Der Spiegel

- "The documents state that it is possible for the NSA to tap most sensitive data held on these smart phones, including **contact lists**, **SMS traffic**, **notes** and **location information** about where a user has been. In the internal documents, experts boast about successful access to iPhone data in instances where the NSA is able to **infiltrate the computer a person uses to sync their iPhone**. Mini-programs, so-called "scripts," then enable additional access to at least 38 iPhone **features**."

In the internal documents, experts boast about successful access to iPhone data in instances where the NSA is able to infiltrate the computer a person uses to sync their iPhone.

Pairing: the keys to everything ((page 4 & 5))

In order to understand how an attacker could penetrate an iPhone from the owner's desktop computer, it's important to understand how pairing works (A cross-platform software library and tools to communicate with iOS devices natively); A pairing is a trusted relationship with another device, where the client device is granted privileged, trusted access. In order to have the level of control to download personal data, install applications, or perform other such tasks on an iOS device, the machine it's connected to must be paired with the device. This is done through a very simple protocol, where the desktop and the phone create and exchange a set of keys and certificates. These keys are later used to authenticate and establish an encrypted SSL channel to communicate with the device. Without the correct keys, the attempted SSL handshake fails, preventing the client from obtaining privileged access. A copy of the keys and certificates are stored in a single file, both on the desktop machine and on the paired mobile device. The pairing file is never deleted from the device except when the user performs a restore or uses Apple's "Erase All Content and Settings" feature. In other words, every desktop that a phone has been plugged into (especially prior to iOS 7) is given a skeleton key to the phone. This pairing record allows either the desktop, or any client who has copied the file, to connect to the subject's mobile device and perform a number of privileged tasks that can access personal data, install software, analyze network content, and so on. This one pairing file identifies someone as the owner of the phone, and with this file gives anyone trust and access as the device's owner. **There are a few frightening things to know about the pairing mechanism in iOS.** [SGgrc]

Pairing happens automatically, without any user interaction (up until iOS 7), and only takes a few seconds. Pairing can be performed by anything on the other end of the USB cable. The mobile device must either have no passcode, or be unlocked. If the user has "Require Passcode" set to anything other than "Immediate", then it is also possible to pair with the device after it is turned off, until the lock timer expires. So if the user has a device unlocked to play music, and connect it to an alarm clock or a charger running malicious code, whatever it's connected to can establish a pairing record that can later on be used to gain access to the device, at any point in time, until the device is restored or wiped.

While the pairing process itself must take place over USB (Renard), at any time after that, the phone can be accessed over either USB or WiFi regardless of whether or not WiFi sync is turned on. This means that an attacker only needs a couple of seconds to pair with a device, and can then later on access the device to download personal data, or wreak other havoc, if they can reach it across a network. Additionally, an attacker can easily find the target device on a WiFi network by scanning TCP:62078 and attempting to authenticate with this pairing record. As the pair validation process is very quick, sweeping a LAN's address space for the correct iOS device generally only takes a short amount of time.

> **[SGgrc] How Apple would describe the same thing:** Pairing is an important and security-sensitive system which we have made as strong as possible while attempting to strike a balance between users' absolute intolerance for anything getting in their way while still working to protect them as much as possible. To that end, it is IMPOSSIBLE to EVER

> pair wirelessly. Physical USB-cable connection MUST always be present. Since iOS v7, ANY PAIRING also requires that the device be unlocked and the user must acknowledge and accept the pairing request from the physically attached device.

Because of the way WiFi works on these devices, an attacker can take advantage of the device's "known wireless networks" to force a phone to join their network when within range, so that they can attack the phone wirelessly. This is due to iOS' behavior of automatically joining networks whose name (not MAC address) it recognizes, such as "linksys" or "attwifi". It may even be possible for a government agency with privileged access to a cellular carrier's network to connect to the device over cellular (although I cannot verify this, due to the carrier's firewalls).

Essentially, that tiny little pairing record file is the key to downloading, installing, and even manipulating data and applications on the target device. That is why I have advised law enforcement agencies to begin seizing desktop machines, so that they can grab a copy of this pairing record in order to unlock the phone; a number of forensic imaging products (including some I've written), and even open source tools (A cross-platform software library and tools to communicate with iOS devices natively) are capable of acquiring data from a locked mobile device, so long as the desktop's pairing record has been recovered. The pairing record also contains an escrow keybag, so that it can unlock data that is protected by data-protection encryption (Renard). This is good news for the "good" cops, who do crazy things like get warrants; it's very bad for anyone who is targeted by spy agencies or malicious hackers looking to snoop on their data.

[SGgrc]... Yes!... And in the PKI certificate system, a CA's private key is the linchpin to the entire Internet.

Undocumented Services

- Most services are not referenced by any known Apple software (we've looked)
- The raw format of the data makes it impossible to put data back onto the phone, making useless for Genius Bar or carrier tech purposes (cpio.gz, etc)
- The personal nature of the data makes it very unlikely as a debugging mechanism
- Bypassing backup encryption is deceptive
- Services are available **without** developer mode, eliminating their purpose as developer tools

slide 19

com.apple.pcapd

- Immediately starts libpcap on the device
- Dumps network traffic and HTTP request/response data traveling into and out of the device
- **Does not** require developer mode; is active on every iOS device
- Can be targeted via WiFi for remote monitoring
- No visual indication to the user that the packet sniffer is running.

WHY DO WE NEED A PACKET SNIFFER RUNNING ON 600 MILLION PERSONAL IOS DEVICES?

Very dramatic... but remember, NOTHING WORKS unless the bad guys can get the pairing keys from a previously paired device.

slide 38

Invisible Malware

- Installing invisible software that backgrounds is still easy to do in iOS 7
- Apple made a crucial security improvement in iOS 7: prevented socket connections to localhost / local IP
  - Prior to this, I had spyware running invisibly that could dump a phone and send its contents remotely anywhere. (never released for obvious reasons)
- This stopped a number of privately used spyware apps in their tracks; they can not connect to localhost:62078
- Future spyware: phones attacking other phones on the network (zomg zombies)

slide 48

Questions for Apple

- Why is there a packet sniffer running on 600 million personal iOS devices instead of moved to the developer mount?
- Why are there undocumented services that bypass user backup encryption that dump mass amounts of personal data from the phone?
- Why is most of my user data *still* not encrypted with the PIN or passphrase, enabling the invasion of my personal privacy by YOU?
- Why is there still no mechanism to review the devices my iPhone is paired with, so I can delete ones that don't belong?

Summary

- Apple is dishing out a lot of data behind our backs
- It's a violation of the customer's trust and privacy to bypass backup encryption
- There is no valid excuse to leak personal data or allow packet sniffing without the user's knowledge and permission.
- Much of this data simply should never come off the phone, even during a backup.
- Apple has added many conveniences for enterprises that make tasty attack points for .gov and criminals
- Overall, the otherwise great security of iOS has been compromised... by Apple... by design.