Security Now! #575 - 08-30-16

Pegasus & Trident

This week on Security Now!

- Dropbox and Opera handle incidents responsibly, while a Chinese certificate authority could not have been more irresponsible.
- Facebook and WhatsApp announce an information sharing arrangement.
- The FBI discloses election site hacking.
- Tavis prepares DashLane and 1Password vulnerability disclosures.
- From the fringe: the threat of autonomous weapon systems and WiFi router radio wave spying.
- One erratum, a bit of miscellany, and a deep look into what was behind last week's emergency iOS update to v9.3.5
- A discussion of last week's puzzler… and another intriguing one for this week.

Security News

DropBox Password Reset

- Hi Steve,

  We're reaching out to let you know that if you haven't updated your Dropbox password since mid-2012, you'll be prompted to update it the next time you sign in. This is purely a preventative measure, and we're sorry for the inconvenience.

  To learn more about why we're taking this precaution, please visit this page on our Help Center. If you have any questions, feel free to contact us at password-reset-help@dropbox.com.

  Thanks,
  The Dropbox Team

- If you signed up for Dropbox prior to mid-2012 and haven't changed your password since, you'll be prompted to update it the next time you sign in. We're doing this purely as a preventive measure, and there is no indication that your account has been improperly accessed. We're sorry for the inconvenience.

  Our security teams are always watching out for new threats to our users. As part of these ongoing efforts, we learned about an old set of Dropbox user credentials (email addresses plus hashed and salted passwords) that we believe was obtained in 2012. Our analysis suggests that the credentials relate to an incident we disclosed around that time.

  Based on our threat monitoring and the way we secure passwords, we don't believe that any accounts have been improperly accessed. Still, as one of many precautions, we're requiring anyone who hasn't changed their password since mid-2012 to update it the next time they sign in.

  We have dedicated security teams that work to protect our services and monitor for compromises, abuse, and suspicious activity. We've implemented a broad set of controls including independent security audits and certifications, threat intelligence, and bug bounties for ethical hackers. In addition, we build open source tools such as zxcvbn, use bcrypt password hashing, and offer Universal 2nd Factor authentication to all users.

Opera server breach incident

- https://www.opera.com/blogs/security/2016/08/opera-server-breach-incident/
- Affected 1.7 million (0.5%) of Opera's user base of 350 million users who use the inter-browser Sync service.
- <OPERA:> Earlier this week, we detected signs of an attack where access was gained to the Opera sync system. This attack was quickly blocked. Our investigations are ongoing, but we believe some data, including some of our sync users' passwords and account information, such as login names, may have been compromised.

Although we only store encrypted (for synchronized passwords) or hashed and salted (for authentication) passwords in this system, we have reset all the Opera sync account passwords as a precaution.

We have also sent emails to all Opera sync users to inform them about the incident and ask them to change the password for their Opera sync accounts. In an abundance of caution, we have encouraged users to also reset any passwords to third party sites they may have synchronized with the service.

To obtain a new password for Opera sync, use the password resetting page.

Chinese CA WoSign faces revocation after possibly issuing fake certificates of Github, Microsoft and Alibaba

- http://www.percya.com/2016/08/chinese-ca-wosign-faces-revocation.html
- One of the largest Chinese root certificate authority WoSign issued many fake certificates due to an vulnerability. WoSign's free certificate service allowed its users to get a certificate for the base domain if they were able to prove control of a subdomain. This means that if you can control a subdomain of a major website, say percy.github.io, you're able to obtain a certificate by WoSign for github.io, taking control over the entire domain.

- Many of their certs have been found in the wild for Github, Alibaba, and Microsoft.

- After the vulnerability was disclosed to them, WoSign never reported this misuse to root programs as required. And WoSign's audit report didn't include such misuse either.

- Outraged commentators have stated that WoSign lacks the security knowledge needed for operating a CA. In an online thread discussing potential sanction against WoSign, WoSign stated that:

    - For incident 1 - mis-issued certificate with un-validated subdomain, total 33 certificates. We have posted to CT log server and listed in crt.sh, here is the URL. Some certificates are revoked after getting report from subscriber, but some still valid, if any subscriber think it must be revoked and replaced new one, please contact us in the system, thanks.

- I think we REALLY need to rethink our current "trust everyone" (trust WoSign) policy.
- What we need is something to audit our actual certificate usage and, after a month or two, lock it down and make additional certs available selectively.

Facebook and WhatsApp

- http://www.independent.co.uk/life-style/gadgets-and-tech/news/facebook-is-going-to-start-taking-user-data-from-whatsapp-a7209221.html
- http://www.independent.co.uk/life-style/gadgets-and-tech/news/whatsapp-facebook-terms-private-data-sharing-opt-out-how-to-a7210841.html
- When WhatsApp was purchased by Facebook, it assured its users that their data would remain private:

<quote> “Respect for your privacy is coded into our DNA, and we built WhatsApp around the goal of knowing as little about you as possible”.

- But that appears to be no longer so clear. It has recently announced that it will be making a change to those policies, allowing it to hand over information about its users to parent company WhatsApp.

- The new changes to the terms and conditions allow Facebook to see the phone number that people use with their WhatsApp account. That gives them a way of tracking people that is shared across the two sites, helping Facebook gather data for ads.

- Two ways to prevent this:
    - The first way works if you haven’t accepted the new terms which will pop-up when you open WhatsApp. If you haven’t, when that happens, don’t click “agree” – instead navigate to the smaller “read more” option, and uncheck the box that says “Share my WhatsApp account information with Facebook”.

    - If you already accepted those new terms, you can still opt out within 30 days by opening the Settings menu in WhatsApp and selecting the Account tab. There you’ll find a “share my account info” button that you can uncheck to revoke your previously given permission.

- WhatsApp says that the forthcoming information sharing is meant only to help improve the ads on Facebook. If so, the only consequence might be that the ads you see on the network might be slightly less relevant.

FBI says two sates election systems were attacked and hacked.

- https://s.yimg.com/dh/ap/politics/images/boe_flash_aug_2016_final.pdf
- https://www.yahoo.com/news/fbi-says-foreign-hackers-penetrated-000000175.html

- The FBI has uncovered evidence that foreign hackers penetrated two state election databases in recent weeks, prompting the bureau to warn election officials across the country to take new steps to enhance the security of their computer systems.

- FBI Cyber Division issued a potentially more disturbing warning, titled “Targeting Activity Against State Board of Election Systems.” The alert, labeled as restricted for “NEED TO KNOW recipients,” disclosed that the bureau was investigating cyberintrusions against two state election websites this summer, including one that resulted in the “exfiltration,” or theft, of voter registration data.

- The bulletin does not identify the states in question, but sources familiar with the document say it refers to the targeting by suspected foreign hackers of voter registration databases in Arizona and Illinois.

- In the **Illinois** case, officials were forced to shut down the state’s voter registration system for 10 days in late July, after the hackers managed to download personal data on up to 200,000 state voters.

- The **Arizona** attack was more limited, involving malicious software that was introduced into its voter registration system but no successful exfiltration of data resulted.

- FBI Bulletin:
  - In late June 2016, an unknown actor scanned a state's Board of Election website for vulnerabilities using Acunetix, and after identifying a Structured Query Language (SQL) injection (SQLi) vulnerability, used SQLmap to target the state website. The majority of the data exfiltration occurred in mid-July. There were 7 suspicious IPs and penetration testing tools Acunetix, SQLMap, and DirBuster used by the actor, detailed in the indicators section below.
  - Contains lots of good technical detail from the server logs, including the IP addresses used for the remote web queries.
  - The FBI bulletin also contains a bunch of very good remediation steps for all other election boards.

Google's Tavis Ormandy, last Friday evening at 9:31pm tweeted in reply to a tweet from "SwiftOnSecurity"

- "I hadn't even heard of TrueKey, I have upcoming DashLane and 1Password vulnerabilities. There's a lot of scary garbage."

FROM THE FRINGE…

Lethal Autonomous Weapons Systems
https://www.buzzfeed.com/sarahatopol/how-to-save-mankind-from-the-new-breed-of-killer-robots
https://people.eecs.berkeley.edu/~russell/research/LAWS.html
Stuart Russell, a U.C. Berkeley computer science professor known for his contributions to the field of artificial intelligence writes:

A very, very small quadcopter, one inch in diameter can carry a one- or two-gram shaped charge. You can order them from a drone manufacturer in China. You can program the code to say: "Here are thousands of photographs of the kinds of things I want to target." A one-gram shaped charge can punch a hole in nine millimeters of steel, so presumably you can also punch a hole in someone's head. You can fit about three million of those in a semi-tractor-trailer. You can drive up I-95 with three trucks and have 10 million weapons attacking New York City. They don't have to be very effective, only 5 or 10% of them have to find the target.

There will be manufacturers producing millions of these weapons that people will be able to buy just like you can buy guns now, except millions of guns don't matter unless you have a million soldiers. You need only three guys to write the program and launch them. So you can just imagine that in many parts of the world humans will be hunted. They will be cowering underground in shelters and devising techniques so that they don't get detected. This is the ever-present cloud of lethal autonomous weapons. They could be here in two to three years.

Tinfoil Hat Time: "All the Ways Your Wi-Fi Router Can Spy on You"

- Yet another means for data exfiltration??
- http://www.theatlantic.com/technology/archive/2016/08/wi-fi-surveillance/497132/

All the Ways Your Wi-Fi Router Can Spy on You (It can even be trained to read your lips.)

City dwellers spend nearly every moment of every day awash in Wi-Fi signals. Homes, streets, businesses, and office buildings are constantly blasting wireless signals every which way for the benefit of nearby phones, tablets, laptops, wearables, and other connected paraphernalia.

When those devices connect to a router, they send requests for information—a weather forecast, the latest sports scores, a news article—and, in turn, receive that data, all over the air. As it communicates with the devices, the router is also gathering information about how its signals are traveling through the air, and whether they're being disrupted by obstacles or interference. With that data, the router can make small adjustments to communicate more reliably with the devices it's connected to.

But it can also be used to monitor humans—and in surprisingly detailed ways.

As people move through a space with a Wi-Fi signal, their bodies affect it, absorbing some waves and reflecting others in various directions. By analyzing the exact ways that a Wi-Fi signal is altered when a human moves through it, researchers can "see" what someone writes with their finger in the air, identify a particular person by the way that they walk, and even read a person's lips with startling accuracy—in some cases even if a router isn't in the same room as the person performing the actions.

Several recent experiments have focused on using Wi-Fi signals to identify people, either based on their body shape or the specific way they tend to move. Earlier this month, a group of computer-science researchers at Northwestern Polytechnical University in China posted a paper to an online archive of scientific research, detailing a system that can accurately identify humans as they walk through a door nine times out of ten.

The system must first be trained: It has to learn individuals' body shapes so that it can identify them later. After memorizing body shapes, the system, which the researchers named FreeSense, watches for people walking across its line of sight. If it's told that the next passerby will be one of two people, the system can correctly identify which it is 95 percent of the time. If it's choosing between six people, it identifies the right one 89 percent of the time.

The researchers proposed using their technology in a smart-home setting: If the router senses one person's entry into a room, it could communicate with other connected devices—lights, appliances, window shades—to customize the room to that person's preferences.

FreeSense mirrored another Wi-Fi-based identification system that a group of researchers from Australia and the UK presented at a conference earlier this year. Their system, Wi-Fi ID, focused on gait as a way to identify people from among a small group. It achieved 93 percent accuracy when choosing among two people, and 77 percent when choosing from among six. Eventually, the researchers wrote, the system could become accurate enough that it could sound an alarm if an unrecognized intruder entered.

Something in the way? No problem. A pair of MIT researchers wrote in 2013 that they could use a router to detect the number of humans in a room and identify some basic arm gestures, even through a wall. They could tell how many people were in a room from behind a solid wooden door, a 6-inch hollow wall supported by steel beams, or an 8-inch concrete wall—and detect messages drawn in the air from a distance of five meters (but still in another room) with 100 percent accuracy.

(Using more precise sensors, the same MIT researchers went on to develop systems that can distinguish between different people standing behind walls, and remotely monitor breathing and heart rates with 99 percent accuracy. President Obama got a glimpse of the latter technology during last year's White House Demo Day in the form of Emerald, a device geared towards elderly people that can detect physical activity and falls throughout an entire home. The device even tries to predict falls before they happen by monitoring a person's movement patterns.)

Beyond human identification and general gesture recognition, Wi-Fi signals can be used to discern even the slightest of movements with extreme precision.

A system called "WiKey" presented at a conference last year could tell what keys a user was pressing on a keyboard by monitoring minute finger movements. Once trained, WiKey could recognize a sentence as it was typed with 93.5 percent accuracy—all using nothing but a commercially available router and some custom code created by the researchers.

And a group of researchers led by a Berkeley Ph.D. student presented technology at a 2014 conference that could "hear" what people were saying by analyzing the distortions and reflections in Wi-Fi signals created by their moving mouths. The system could determine which words from a list of lip-readable vocabulary were being said with 91 percent accuracy when one person was speaking, and 74 percent accuracy when three people were speaking at the same time.

[FINALLY, A BIT OF SANITY] I asked the lead researcher behind WiKey, Kamran Ali, whether his technology could be used to secretly steal sensitive data. Ali said the system only works in controlled environments, and with rigorous training. "So, it is not a big privacy concern for now, no worries there," wrote Ali, a Ph.D. student at Michigan State University, in an email.

But as Wi-Fi "vision" evolves, it may become more adaptable and need less training. And if a hacker is able to gain access to a router and install a WiKey-like software package—or trick a user into connecting to a malicious router—he or she can try to eavesdrop on what's being typed nearby without the user ever knowing.

Since all of these ideas piggyback on one of the most ubiquitous wireless signals, they're ripe for wide distribution once they're refined, without the need for any new or expensive equipment. Routers could soon keep kids and older adults safe, log daily activities, or make a smart home run more smoothly—but, if invaded by a malicious hacker, they could also be turned into incredibly sophisticated hubs for monitoring and surveillance.

- What's the reality of such technology?

Errata

- **218 vs 2^18 -- iMessage attack.**

Miscellany

Another terrific "Two & Three Dumb Routers" configuration guide

- http://nerdcave.littlebytesofpi.com/router-configuration/
- (And recorded on the linkfarm page for posperity.)

Willie Howe (@WillieHowe) / 8/28/16, 9:07 AM

- @SGgrc: One of your other subscribers wanted me to share my YouTube channel for Ubiquiti products with you. http://youtube.com/williehowe

- Topics:
  - Public WiFi Security (#1-#5) - Putting It All Together
  - EdgeMax EdgeOS v1.9
  - Blocking traffic at the EdgeRouter
  - UniFi Beta Rate Controls
  - EdgeRouter Local Traffic Blocking
  - EdgeRouter - Multiple WAN (Internet) IP Addresses

Intel Developer Forum – Not Much 3D XPoint Progress

- http://thememoryguy.com/intel-developer-forum-not-much-3d-xpoint-progress/
- We just had the 2016 Intel Developer Forum... and where was XPoint memory one year later??
- Jim Handy: "Intel Developer Forum – Not Much 3D XPoint Progress"
- A layered memory system:
  - XPoint offers another layer: Denser than DRAM, faster than Flash.
  - The Optane XPoint SSD's latency was about seven microseconds compared to 85 microseconds for the flash SSD.
- Jim: "Intel really needs for 3D XPoint Memory to work. Without it, the performance of future computing platforms won't scale with processor upgrades. In other words, when a higher-performance processor is plugged into the system that system's performance won't improve because the rest of the system will bog the processor down. The new 3D XPoint Memory is the key to prevent this from happening. Without it, Intel will be unable to migrate customers to increasingly more powerful processors that sell for higher prices and reap higher margins for Intel.

  This is a tough spot for both companies, and there are no indications of any pending breakthrough that will improve the situation. About all we can do is watch from the sidelines with the hopes that Intel and Micron will overcome their technical problems and get back on track."

- Super capacitors / Next generation battery technologies.
  - Note: About batteries: maintaining a less-than-fully-charged is definitely best.
    - Lenovo 3rd-generation X1 Carbon noticed that t was always plugged-in...
  - Those LiIon explosions occur after over-charging.
  - When a fast-charged NiCad battery's terminal voltage drops, it's done. Li-Ion has no such "end of charge" indication.

Halt and Catch Fire - Season #3 has resumed

- Predominantly character-driven, set in a nominally historical but fictional techie setting... but not particularly compelling characters.

SpinRite

- PGP ID 0x01086FDA (@cristianrasch)
  .@SGgrc thank you for supporting Wine as a valid #SpinRite platform. Just purchased my copy which it's currently hard at work :)

Pegasus & Trident

Steve Gibson @SGgrc (Last Thursday at 3:06pm)…

- Apple recently pushed an "emergency" update for all iOS devices.
  It has been used against "targeted victims", but could see wider use now.

Exploit discovery timeline:

- On the morning of August 10, 2016, Ahmed Mansoor, an internationally recognized human rights defender, blogger, and member of Human Rights Watch's advisory committee, received an SMS text message that appeared suspicious. The next day he received a second, similar text. The messages promised "new secrets" about detainees tortured in UAE prisons, and contained a hyperlink to an unfamiliar website. The messages arrived on Mansoor's stock iPhone 6 running iOS 9.3.3.
- Rather than clicking on the message's provided link, Mansoor forwarded both messages to Citizen Lab researchers for investigation. Mansoor had reason to be concerned about unsolicited messages because during all of the past five years he has been targeted with spyware attacks, starting with the FinFisher spyware in 2011 and Hacking Team spyware in 2012.
- Two days later, on August 12, 2016, Citizen Lab brought Lookout into the loop for their reverse engineering and technical analysis skills.
- Three days later, realizing the emergency implied by what they had discovered, on August 15, 2016 Apple was brought in and up to speed.
- And just 10 days later, on August 25, 2016, Apple released iOS v9.3.5 to patch and close the three, separate, previously unknown, 0-day vulnerabilities which were being exploited by this targeted cyberweapon.

The malware has been in operation for well over a year, which has enabled it to develop a degree of software maturity, and as a result it is capable of exploiting multiple iOS versions. An excerpt from the embedded magic table that maps addresses in the kernel shows that the exploit supports versions of the phone from the iPhone 4s up to the iPhone 6s Plus.

Lookout Security published an in-depth technical analysis:

This is an in-depth technical analysis of a targeted espionage attack being actively leveraged against an undetermined number of mobile users around the world. Lookout researchers have done deep analysis on a live iOS sample of the malware.

Citizen Lab's investigation linked the software and infrastructure to that of NSO Group which offers a product called Pegasus solution.

Pegasus is professionally developed and highly advanced in its use of zero-day vulnerabilities, code obfuscation, and encryption. It uses sophisticated function hooking to subvert OS- and application-layer security in voice/audio calls and apps including remotely accessing text messages, iMessages, calls, emails, logs, and more from apps including Gmail, Facebook, Skype, WhatsApp, Viber, Facetime, Calendar, Line, Mail.Ru, WeChat, Surespot, Tango, Telegram, and others. It steals the victim's contact list and GPS location, as well as personal, Wi-Fi, and router passwords stored on the device.

The iOS version of the attack uses what we refer to as Trident, an exploit of three related zero-day vulnerabilities in iOS, which Apple patched in iOS 9.3.5, available as of the publishing of this report.

The attack is very simple in its delivery and silent in delivering its payload. The attack starts when the attacker sends a website URL (through SMS, email, social media, or any other message) to an identified target. The user only has to take one action--click on the link. Once the user clicks the link, the software silently carries out a series of exploits against the victim's device to remotely jailbreak it so that the espionage software packages can be installed. The user's only indication that anything happened will be that the browser closes after the link is clicked.

To accomplish this, after jailbreaking the user's phone, the spyware does not download malicious versions of these apps to the victim's device, but rather it compromises the original apps already installed on the device. This includes pre-installed apps such as Facetime and Calendar and those from the official App Store. Usually, iOS security mechanisms prevent normal apps from spying on each other, but spying "hooks" can be installed on a jailbroken device.

Pegasus takes advantage of both the remote jailbreak exploit and a technique called "hooking." The hooking is accomplished by inserting Pegasus' dynamic libraries into the legitimate processes running on the device. These dynamic libraries can be used to hook the apps using a framework called Cydia Mobile Substrate, known to the iOS jailbreak community, and which Pegasus uses as part of the exploit.

A user infected with this spyware is under complete surveillance by the attacker because, in

addition to the apps listed above, it also spies on:

- Phone calls
- Call logs
- SMS messages the victim sends or receives
- Audio and video communications that (in the words a founder of NSO Group) turns the phone into a "walkie-talkie"

Access to this content could be used to gain further access into other accounts owned by the target, such as banking, email, and other services he/she may use on or off the device.

The attack is comprised of three separate stages that contain both the exploit code and the espionage software. The stages are sequential; each stage is required to successfully decode, exploit, install, and run the subsequent stage. Each stage leverages one of the Trident vulnerabilities in order to run successfully.

STAGE 1 Delivery and WebKit vulnerability: This stage comes down over the initial URL in the form of an HTML file (1411194s) that exploits a vulnerability (CVE-2016-4655) in WebKit (used in Safari and other browsers).

STAGE 2 Jailbreak: This stage is downloaded from the first stage code based on the device type (32-bit vs 64-bit). Stage 2 is downloaded as an obfuscated and encrypted package. Each package is encrypted with unique keys at each download, making traditional network-based controls ineffective. It contains the code that is needed to exploit the iOS Kernel (CVE-2016-4656 and CVE-2016-4657) and a loader that downloads and decrypts a package for stage 3.

STAGE 3 Espionage software: This stage is downloaded by stage 2 and is also based on the device type (32-bit vs 64-bit). Stage 3 contains the espionage software, daemons, and other processes that are used after the device has been jailbroken in stage 2. Stage 3 installs the hooks into the applications the attacker wishes to spy on. Additionally, stage 3 detects if the device was previously jailbroken through another method and, if so, removes any access to the device that the jailbreak provides, such as via SSH. The software also contains a failsafe to remove itself if certain conditions are present.

The third stage deploys a number of files deployed in a standard unix tarball each with its own purpose. The devious one that caught my eye was:

• ca.crt - root TLS certificate that is added to keystore.

The attack works on iOS up to v9.3.4 and the developers maintain a large table in their code that attacks all iOS versions from 7.0 up to and including iOS 9.3.3. While the code investigated did not contain the appropriate values to initially work on iOS 9.3.4, the exploits we investigated would still work, and it is trivial for the attackers to update the table so that the attack will work on 9.3.4.

One other unique property of this attack is that standard jailbreak detections fail to report that the device has been exploited. The attack and installation of the spying software is designed to be as silent as possible to the target.

Pegasus is well designed in terms of its modularity and efficiency. For example, the kernel exploits call upon magic tables for each of the platforms that map out kernel memory for each version and phone model.

The code is extremely modular, relative to other malware our researchers have encountered. We found common libraries and common formats with similar naming conventions. Unlike most malware authors, the code in Pegasus is clean and efficient, with evidence of professional and careful design. We see evidence of a robust quality assurance process for their development: even their first stage exploit contains both debugging and QA-specific functions of the type one would expect from an enterprise-class software development organization.

The TRI-dent vulnerabilities:

CVE-2016-4655: Memory Corruption in Safari WebKit
A memory corruption vulnerability exists in Safari WebKit that allows an attacker to execute arbitrary code. Pegasus exploits this vulnerability to obtain initial code execution privileges within the context of the Safari web browser. This vulnerability is complex and Lookout continues to work on analyzing this vulnerability and will publish additional findings as they become available.

CVE-2016-4656: Kernel Information Leak Circumvents KASLR
Before Pegasus can execute its jailbreak, it must determine where the kernel is located in memory. Kernel Address Space Layout Randomization (KASLR) makes this task difficult by mapping the kernel into different and unpredictable locations in memory. In short, before attacking the kernel, Pegasus has to find it. The attacker has found a way to locate the kernel by using a function call that leaks a non-obfuscated kernel memory address in the return value, allowing the kernel's actual memory location to be mapped.

CVE-2016-4657: Memory Corruption in Kernel leads to Jailbreak
The third vulnerability in Pegasus' Trident is the one that is used to jailbreak the phone. A memory corruption vulnerability in the kernel is used to corrupt memory in both the 32- and 64-bit versions. The exploits are performed differently on each version. This vulnerability is complex and Lookout continues to work on analyzing this vulnerability and will publish additional findings as they become available.

Jailbreak Persistence

Once the kernel has been exploited, both exploits perform similar tasks to prepare the system to be jailbroken:

- Disable kernel security protections including code signing
- Remount the system partition
- Clear the Safari caches (to help cover their tracks)
- Write the jailbreak files (including the main loader as /sbin/mount_nfs)

Last Week's and This Week's Puzzlers

The Puzzler of Last Week:
Q: "Why do we use primes?"
A: The best way to explain it is that the security of prime number based public-key encryption depends upon a one-way (Trapdoor) function... meaning that it's easy to do, but intractable to "undo" in the other direction. When you're describing this to your non-techie friends, use the analogy of a padlock. It's easy to close, but opening it requires a key.

Two large prime numbers satisfy this requirement because multiplying is easy. But then the security entirely depends upon not being able to undo it. So... if the numbers being multiplied were NOT prime -- if they had multiple smaller divisors, then the problem is MUCH easier to solve, since the smaller factors could be found and removed, reducing the size/length of the remainder, and eventually decomposing the multiplication. :)

The Puzzler for This Week: I received a tweet from someone who had a tricky problem.

A family of network connected embedded-style devices having unalterable firmware is hard wired to make TLS connections to a server at this person's publicly available FQDN. But the firmware only understands how to verify SHA-1 hash certificate signatures. The server these devices are connecting to is currently SHA-1, but as we know, when it expires, it will be impossible to get Symantec/Verisign, or any other CA, to sign an SHA-1 for a standard public FQDN. Is there ANYTHING this company can do, any trick that can be played externally, to satisfy the needs of this unmodifiable hardware??