Security Now! #598 - 02-07-17

Two Armed Bandits

This week on Security Now!

Speak of the devil... printers around the world get hacked!, Vizio's TVs really were watching their watchers, Windows has a new 0-day problem, Android's easy-to-hack pattern lock, an arsonist's pacemaker rats him out, a survey finds that many iOS apps are not checking TLS certificates, the courts create continuing confusion over eMail search warrants, a blast from the past: SQL Slammer appears to return, Cellebrite's stolen cell phone cracking data begins to surface, some worrisome events in the Encrypted Web Extensions debate, Non-Windows 10 users are not alone, a couple of questions answered, my report of a terrific Sci-Fi series, a bit of other miscellany... and a fun story about one armed bandits being hacked by two armed bandits.

What users see when an important security warning appears:

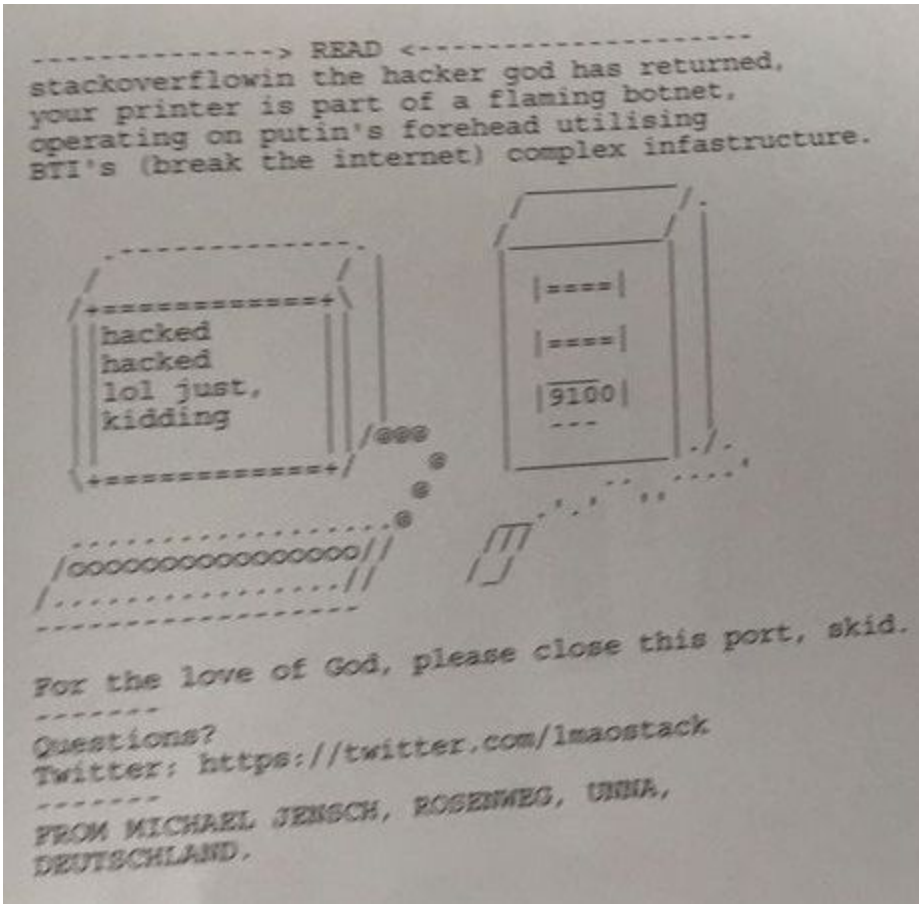
Security News

More than 150,000 Internet-facing printers were scanned, located, and used.

- Following up from last week's "Traitors in our Midst"...

- Some reporting of this erroneously indicated that publicly exposed printers had been enslaved into a Botnet.

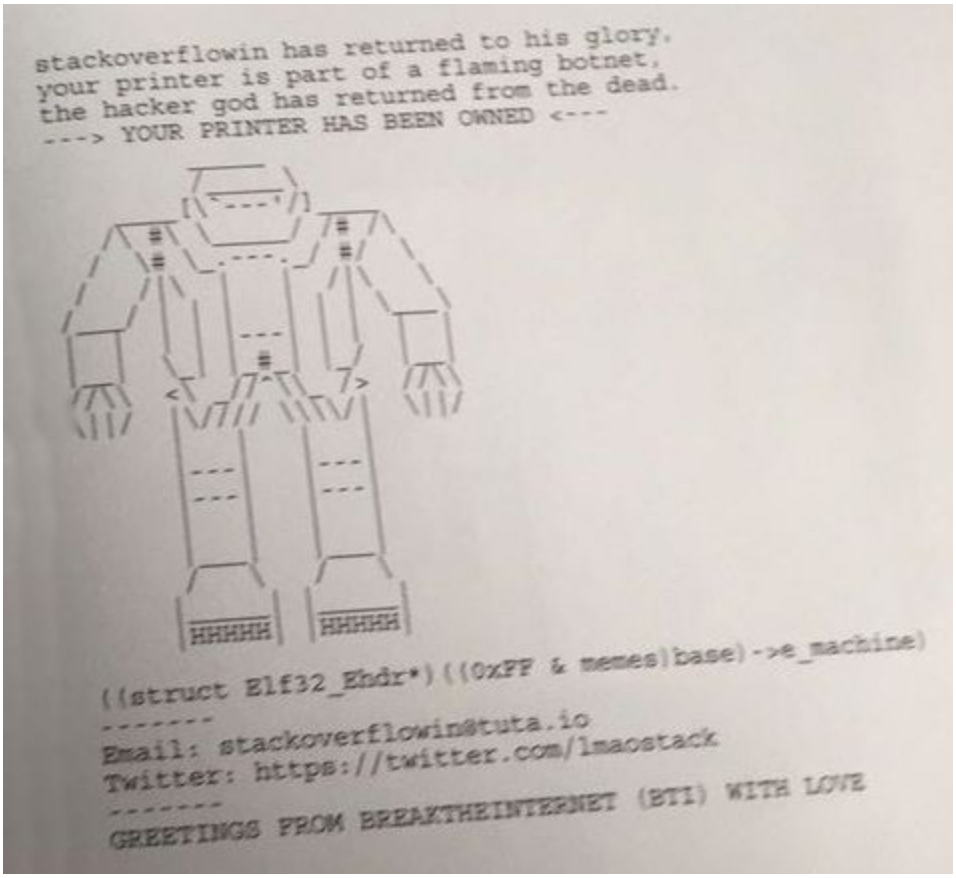
- A Hacker who calls himself "Stackoverflowin" wrote a script to scan the Internet for printers publicly exposing their IPP (Internet Printing Protocol) ports, LPD (Line Printer Daemon) ports, and port 9100.



- Priscilla (@PrissSoares_) 2/3/17, 10:07 AM
  The printer for our POS systems at work got hacked lmao pic.twitter.com/ZHX2PVIaC0

- UPNP: Remember... if your router has UPNP enabled, your printers (or anything else on your network for that matter, can have surreptitiously punched a hole through your border router's stateful NAT firewall to make itself "available" to anyone on the public Internet in the world.

- Today a warning message gets printed. Tomorrow??



- Ports:
  - IPP: Port TCP/631
  - LPD: Port TCP/515
  - RAW: Port 9100

- Coverage:
  - https://www.bleepingcomputer.com/news/security/a-hacker-just-pwned-over-150-000-printers-left-exposed-online/
  - http://www.bbc.com/news/technology-38879671

What Vizio was doing behind the TV screen | Federal Trade Commission

- Federal Trade Commission:

  Consumers have bought more than 11 million internet-connected Vizio televisions since 2010. But according to a complaint filed by the FTC and the New Jersey Attorney General, consumers didn't know that while they were watching their TVs, Vizio was watching them. The lawsuit challenges the company's tracking practices and offers insights into how established consumer protection principles apply to smart technology.

  Starting in 2014, Vizio made TVs that automatically tracked what consumers were watching and transmitted that data back to its servers. Vizio even retrofitted older models by installing its tracking software remotely. All of this, the FTC and AG allege, was done

without clearly telling consumers or getting their consent.

What did Vizio know about what was going on in the privacy of consumers' homes?

On a second-by-second basis, Vizio collected a selection of pixels on the screen that it matched to a database of TV, movie, and commercial content. What's more, Vizio identified viewing data from cable or broadband service providers, set-top boxes, streaming devices, DVD players, and over-the-air broadcasts.

Vizio captured as many as 100 billion data points each day from millions of TVs.

Vizio then turned that mountain of data into cash by selling consumers' viewing histories to advertisers and others.

[The FTC writes] And let's be clear: We're not talking about summary information about national viewing trends. According to the complaint, Vizio got personal. The company provided consumers' IP addresses to data aggregators, who then matched the address with an individual consumer or household.

Vizio's contracts with third parties [DID] prohibit the re-identification of consumers and households by name, but allowed a host of other personal details – for example, sex, age, income, marital status, household size, education, and home ownership. And Vizio permitted these companies to track and target its consumers across devices.

Vizio [hid] its tracking functionality behind a setting called "Smart Interactivity." But the FTC and New Jersey AG say that the generic way the company described that feature – for example, "enables program offers and suggestions" – didn't give consumers the necessary heads-up to know that Vizio was tracking their TV's every flicker... AND the "Smart Interactivity" feature didn't provide the promised "program offers and suggestions."

The complaint alleges that Vizio engaged in unfair trade practices that violated the FTC Act and were unconscionable under New Jersey law. The complaint also alleges that Vizio failed to adequately disclose the nature of its "Smart Interactivity" feature and misled consumers with its generic name and description.

To settle the case, Vizio has agreed to stop unauthorized tracking, to prominently disclose its TV viewing collection practices, and to get consumers' express consent before collecting and sharing viewing information. In addition, the company must delete most of the data it collected and put a privacy program in place that evaluates Vizio's practices and its partners.

The order also includes a $1.5 million payment to the FTC and an additional civil penalty to New Jersey for a total of $2.2 million.

- Coverage:
  - https://www.ftc.gov/news-events/blogs/business-blog/2017/02/what-vizio-was-doing-behind-tv-screen
  - https://arstechnica.com/tech-policy/2017/02/vizio-smart-tvs-tracked-viewers-around-the-clock-without-consent/
  - https://www.engadget.com/2017/02/06/vizio-smart-tv-viewing-history-settlement-ftc/
  - http://www.androidcentral.com/vizio-fined-22-million-ftc-way-they-collect-your-data

- Jeff Wilson (@jeffwilsontech) 2/6/17, 2:17 PM
  @SGgrc Steve Consumer space is resembling enterprise IT space...we need home LAN micro-segmentation in wake of Vizio revelations!

Microsoft Unpatched 0-Day Windows SMB Flaw:

- Security researcher Laurent Gaffie gave Microsoft 90-days to patch a flaw he found in Windows client processing of SMB (Server Message Block - Windows File and Printer Sharing) protocol handling.

- Microsoft didn't provide any patch for it. (Perhaps they will next Tuesday?)

- Microsoft's response, as reported by TheHackerNews, was:
  "Windows is the only platform with a customer commitment to investigate reported security issues, and proactively update impacted devices as soon as possible. We recommend customers use Windows 10 and the Microsoft Edge browser for the best protection."

- So Laurent went public, releasing a Python Proof of Concept (PoC).
  https://github.com/lgandx/PoC/blob/master/SMBv3%20Tree%20Connect/Win10.py

- US-CERT warns that the vulnerability could do more than crash a system... it could also be exploited to execute arbitrary code with Windows kernel privileges.

- It affects Windows 10 and v8.1 client systems and Windows Server 2012 & 2016.

- The vulnerability is a "malicious server" denial of service where, when an innocent Windows client connects to a malicious SMB server, the server can return a malformed structure to crash the client.

- As we know... crashes have a nasty habit of becoming remote code execution vulnerabilities.

- The concern is, SMB is deeply ingrained and integrated into Windows and there are all sorts of ways to get Windows to "reach out" to local AND remote SMB servers.

- In the past we've seen exploits where visiting a webpage can cause Internet Exploder to create an outbound SMB connection for perfect user fingerprinting.

- At the router: Block TCP ports 139 & 445, and UDP ports 137 & 138.

- Coverage:
  - https://www.kb.cert.org/vuls/id/867968
  - http://www.ghacks.net/2017/02/03/smb-zero-day-affecting-windows-8-10-and-server/
  - http://thehackernews.com/2017/02/windows-smb-0day.html

Obvious in retrospect: That Android 3x3 grid sequence lock is trivial to crack...

- University of Lancaster researchers captured video footage of people unlocking their phones from 30 feet, without the screens visible, were able, with 95% accuracy, deduce the sequence.

- In a study of 120 unique patterns, 95% could be determined in 5 or fewer attempts.

- They write: "The size of the screen or the position of the pattern grid on the screen does not affect the accuracy of our attack. And what's more, complex patterns do not provide stronger protection over simple patterns under our attack."

- Abstract
  Pattern lock is widely used as a mechanism for authentication and authorization on Android devices. This paper presents a novel video-based attack to reconstruct Android lock patterns from video footage filmed using a mobile phone camera. Unlike prior attacks on pattern lock, our approach does not require the video to capture any content displayed on the screen. Instead, we employ a computer vision algorithm to track the fingertip movements to infer the pattern. Using the geometry information extracted from the tracked fingertip motions, our approach is able to accurately identify a small number of (often one) candidate patterns to be tested by an adversary. We thoroughly evaluated our approach using 120 unique patterns collected from 215 independent users, by applying it to reconstruct patterns from video footage filmed using smartphone cameras. Experimental results show that our approach can break over 95% of the patterns in five attempts before the device is automatically locked by the Android operating system. We discovered that, in contrast to many people's belief, complex patterns do not offer stronger protection under our attacking scenarios. This is demonstrated by the fact that we are able to break all but one complex patterns (with a 97.5% success rate) as opposed to 60% of the simple patterns in the first attempt. Since our threat model is common in day-to-day life, this paper calls for the community to revisit the risks of using Android pattern lock to protect sensitive information.

- Research Paper:
  - https://drive.google.com/file/d/0B8ehxKOxGuQfTTBQa1FrbW9hZlE/view

- Coverage:
  - http://www.businessinsider.com/lancaster-university-researchers-crack-android-lockscreen-patterns-video-computer-vision-algorithm-2017-1
  - http://www.research.lancs.ac.uk/portal/en/publications/-(9d47cd22-a76a-4cf0-b35c-aaf8f1a2f102).html

NetworkWorld: "Cops use pacemaker data to charge homeowner with arson, insurance fraud"
"Police called pacemaker data an 'excellent investigative tool' that provided 'key pieces of evidence' to charge a man with arson and insurance fraud."

If you are dependent upon an embedded medical device, should the device that helps keep you alive also be allowed to incriminate you in a crime? After all, the Fifth Amendment of the U.S. Constitution protects a person from being forced to incriminate themselves.

Nonetheless, that's what happened after a house fire in Middletown, Ohio.

WCPO Cincinnati caught video of the actual fire, as well delivered news that the owner's cat died in the fire. As a pet owner, it would be hard to believe that a person would set a fire and leave their pet to die in that fire. The fire in question occurred back in September 2016; the fire department was just starting an investigation to determine the cause of the blaze.

A month later, 59-year-old homeowner Ross Compton was arrested and charged with felony aggravated arson and insurance fraud. The cause of the fire was still undetermined, but it had resulted $400,000 in damages to the house and contents of the 2,000-square-foot home.

Fire investigators knew there had been "multiple points of origin of the fire from the outside of the residence." At the time, the police cited inconsistencies in Compton's statements when compared with the evidence from the fire.

There were additional "conflicting statements" given to the 911 operator; Compton had said "everyone" was out of the house, yet the 911 operator also heard him tell someone to "get out of here now." In the 911 call published by WLWT5, an out-of-breath Compton claimed he had "grabbed a bunch of stuff, threw it out the window." He claimed to have packed his suitcases, broken the glass out of bedroom window with his walking stick, and tossed the suitcases outside.

Compton also told the dispatcher he had "an artificial heart."

After this, things really get interesting because police investigators used data from Compton's electronic heart device against him. Isn't that self-incrimination? Can a person "plead the Fifth" when it comes to self-incriminating data collected from their medical device?

Police set out to disprove Compton's story about the fire by obtaining a search warrant to collect data from Compton's pacemaker. WLWT5 reported that the cops wanted to know "Compton's heart rate, pacer demand and cardiac rhythms before, during and after the fire."

On Friday, Jan. 27, the Journal-News reported that court documents stated: "A cardiologist who reviewed that data determined 'it is highly improbable Mr. Compton would have been able to collect, pack and remove the number of items from the house, exit his bedroom window and carry numerous large and heavy items to the front of his residence during the short period of time he has indicated due to his medical conditions.'"

Middletown Police said this was the first time it had used data from a heart device to make an arrest, but the pacemaker data proved to be an "excellent investigative tool;" the data from the

pacemaker didn't correspond with Compton's version of what happened. The retrieved data help to indict Compton.

Lt. Jimmy Cunningham told WLWT5, "It was one of the key pieces of evidence that allowed us to charge him."

It's worth noting that gasoline was also found on various pieces of Compton's clothing. Could police have indicted him without using the data from his pacemaker against him?

Coverage:

- https://jonathanturley.org/2017/02/04/pacemaker-data-used-to-charge-alleged-arsonist/
- http://www.networkworld.com/article/3162740/security/cops-use-pacemaker-data-as-evidence-to-charge-homeowner-with-arson-insurance-fraud.html

At least 76 apps in the iOS App Store fail to check the identity of TLS connection certificates.

- Will Strafach, the president of the Sudo Security Group, posted his group's research findings on Medium, yesterday.

  He writes:

  During the development of our web-based mobile app analysis service verify.ly, it was essential to have a clear understanding of the most common security issues which plague mobile applications today. Automatically scanning the binary code of applications within the Apple App Store en-masse allowed us to get a vast amount of information about these security issues.

  I will present some findings within this post which I believe to be in the public interest, related specifically to iOS applications which are vulnerable to silent interception of (normally) TLS-protected data while in use. Our system flagged hundreds of applications as having a high likelihood of vulnerability to data interception, but at this time I will be posting details of the connections and data which I was able to fully confirm as vulnerable using a live iPhone running iOS 10 and a "malicious" proxy to insert an invalid TLS certificate into the connection for testing.

- Highlights:

  - During the testing process, I was able to confirm 76 popular iOS applications allow a silent man-in-the-middle attack to be performed on connections which should be protected by TLS (HTTPS), allowing interception and/or manipulation of data in motion.

  - According to Apptopia estimates, there has been a combined total of more than 18,000,000 (Eighteen Million) downloads of app versions which are confirmed to be affected by this vulnerability.
  - For 33 of the iOS applications, this vulnerability was deemed to be low risk (All data confirmed vulnerable to intercept is only partially sensitive analytics data about the

device, partially sensitive personal data such as e-mail address, and/or login credentials which would only be entered on a non-hostile network).

- For 24 of the iOS applications, this vulnerability was deemed to be medium risk (Confirmed ability to intercept service login credentials and/or session authentication tokens for logged in users).

- For 19 of the iOS applications, this vulnerability was deemed to be high risk (Confirmed ability to intercept financial or medical service login credentials and/or session authentication tokens for logged in users).

- The App Transport Security feature of iOS does not and cannot help block this vulnerability from working.

- Within the "Solving the Problem" section, I present a simple short-term mitigation to this vulnerability class which any end user will be able to make use of.

- The low risk apps were posted. The medium and high risk are currently withheld pending responsible disclosure process.

- Why can't Apple, their App Transport Security (ATS) and iOS simply enforce certificates?

  This class of vulnerability poses a complex problem, as application developers are the only ones who can fully mitigate it. It is derived from networking-related code within iOS applications being misconfigured in a highly unfortunate manner. Due to this, Apple's "App Transport Security" mechanism will see the connection as a valid TLS connection, as it must allow the application to judge the certificate validity if it chooses to do so. There is no possible fix to be made on Apple's side, because if they were to override this functionality in attempt to block this security issue, it would actually make some iOS applications less secure as they would not be able to utilize certificate pinning for their connections, and they could not trust otherwise untrusted certificates which may be required for intranet connections within an enterprise using an in-house PKI. Therefore, the onus rests solely on app developers themselves to ensure their apps are not vulnerable.

- Workaround: Disable WiFi during sensitive transactions.

  There is a short term trick which can be used to mitigate this type of vulnerability. The vulnerability is very likely to only be exploited if your connection is flowing over Wi-Fi (whether you've joined a public Wi-Fi network, or a determined attacker has force-joined your mobile device onto a rogue network without your knowledge). Therefore, if you are in a public location and need to perform a sensitive action on your mobile device (such as opening your bank app and checking your account balance), you can work around the issue by opening "Settings" and turning the "Wi-Fi" switch off prior to the sensitive action. While on a cellular connection the vulnerability does still exist, cellular interception is more difficult, requires expensive hardware, is far more noticeable, and it is quite illegal (within the United States). Therefore, it is much less plausable for an attacker to risk attempting to intercept a cellular data connection.

- Companies:

    - If you offer an application in the iOS App Store, consider analyzing builds prior to App Store submission using our verify.ly service. This class of vulnerability and all other possible "low hanging fruits" (vulnerabilities discoverable to a determined attacker who commits 24 hours total analysis time) can be fully detected by performing an automated scan of the binary code and giving you an easy to read report outlining any and all flagged issues, ensuring your customer data is safe.

- https://verify.ly/
  verify.ly allows you to scan the binary code of an iOS application to produce a human readable report detailing all detected common security issues and a breakdown of all useful security related information pertaining to the app. The app scan is performed in seconds using our proprietary automated static analysis engine, yielding actionable information regarding the security of the scanned mobile application. No source code required.

- Features
    - Detects all common CWEs and mobile OWASP Top 10 issues within an app.
    - Detects hardcoded sensitive content that is easy to re-construct (API keys/ secrets, encryption keys, passwords, and more).
    - Detects any use of Malicious, Private, or Risky APIs.
    - Detects issues related to SSL/TLS validation.
    - Detects issues with sensitive data-at-rest stored non-securely.
    - Checks code hashes against database of known malicious code.
    - Generate easy-to-read report explaining issues and displaying relevant data in a high level manner, to ensure readability by the widest (and potentially nontechnical) audience.

- Pricing:
    - Professional plan: $100/mo. (Single user account)
    - Small Business: $500/mo. (10 users/account)
    - Enterprise: .....

- Coverage:
    - https://medium.com/@chronic_9612/76-popular-apps-confirmed-vulnerable-to-silent-interception-of-tls-protected-data-2c9a2409dd1#.lytzmp1ch
    - https://arstechnica.com/security/2017/02/dozens-of-popular-ios-apps-vulnerable-to-intercept-of-tls-protected-data/

Last Friday, a U.S. judge ruled that Google, unlike Microsoft, must turn over foreign emails.
[Edited from Reuter's reporting]

A U.S. judge has ordered Google to comply with search warrants seeking customer emails stored outside the United States, diverging from a federal appeals court that reached the opposite conclusion in a similar case involving Microsoft.

U.S. Magistrate Judge Thomas Rueter in Philadelphia ruled on Friday that transferring emails from a foreign server so FBI agents could review them locally as part of a domestic fraud probe did not qualify as a seizure.

The judge said this was because there was "no meaningful interference" with the account holder's "possessory interest" in the data sought.

"Though the retrieval of the electronic data by Google from its multiple data centers abroad has the potential for an invasion of privacy, the actual infringement of privacy occurs at the time of disclosure in the United States," Rueter wrote.

Google replied in a statement, Saturday: "The magistrate in this case departed from precedent, and we plan to appeal the decision. We will continue to push back on overbroad warrants."

The ruling came less than seven months after the 2nd U.S. Circuit Court of Appeals in New York said Microsoft could not be forced to turn over emails stored on a server in Dublin, Ireland that U.S. investigators sought in a narcotics case.

That decision last July 14 was welcomed by dozens of technology and media companies, privacy advocates, and both the American Civil Liberties Union and U.S. Chamber of Commerce.

A few weeks ago, on Jan. 24, 2017, the same appeals court voted not to revisit the decision. The four dissenting judges called on the U.S. Supreme Court or Congress to reverse it, saying the decision hurt law enforcement and raised national security concerns.

Both cases involved warrants issued under the Stored Communications Act, a 1986 federal law that many technology companies and privacy advocates consider outdated.

In court papers, Google said it sometimes breaks up emails into pieces to improve its network's performance, and did not necessarily know where particular emails might be stored.

Relying on the Microsoft decision, Google said it believed it had complied with the warrants it received, by turning over data it knew were stored in the United States.

Google receives more than 25,000 requests annually from U.S. authorities for disclosures of user data in criminal matters, according to Rueter's ruling.

http://mobile.reuters.com/article/idUSKBN15J0ON

- SN Podcast Listener takeaway:
  - If you want to securely exchange messages -- TNO:
  - Write them in a simple editor.
  - Encrypted them yourself with a high-entropy key that you share through some out-of-band means with the receiving party.
  - And send the encrypted binary blob however you choose to that party.

From the "Blast from the past Dept": SQL Slammer Comeback | Check Point Blog

- Starting on November 28th and running through December 4th, 2016, Check Point has observed a huge spike in long-dead SQL Slammer work traffic.

- SQL Slammer (predates the Security Now podcast)
  - 14 years ago, back in 2003, many web servers using the SQL database were misconfigured to expose the standard SQL query port 1434 to the public Internet.

  - The worm exploited a buffer overflow in Microsoft SQL Server 2000 and MSDE 2000 by sending a maliciously crafted UDP packet to port 1434.

  - This would instantly infect the server with the worm code and cause it to begin sending out copies of the attack packet to random Internet IPs.

  - It was a mess!

- Now, Check Point writes:
  More than a decade later, Slammer is hitting again. During a routine analysis of global data collected by Check Point ThreatCloud, we detected a massive increase in the number of attack attempts between November 28 and December 4, 2016, making the SQL Slammer worm one of the top malware detected in this timeframe:

- http://blog.checkpoint.com/2017/02/02/sql-slammer-comeback/

- "Worm Watch 2003"
  - https://www.grc.com/worms/25-01-03.htm

Some of those 900GB of phone hacking tools allegedly stolen from Cellebrite are starting to appear.

- Last month we covered the new of this alleged mega-hack of Cellebrite.

- In the hacker's README, they/he notes much of the iOS-related code is very similar to that used in the jailbreaking scene populted by a community of iPhone hackers that typically breaks into iOS devices and release its code publicly for free.

  Jonathan Zdziarski, a forensic scientist, agreed that some of the iOS files were nearly identical to tools created and used by the jailbreaking community, including patched versions of Apple's firmware designed to break security mechanisms on older iPhones. A number of the configuration files also reference "limera1n," the name of a piece of

jailbreaking software created by infamous iPhone hacker Geohot. He said he wouldn't call the released files "exploits" however.

Zdziarski also said that other parts of the code were similar to a jailbreaking project called QuickPwn, but that the code had seemingly been adapted for forensic purposes. For example, some of the code in the dump was designed to brute force PIN numbers, which may be unusual for a normal jailbreaking piece of software.

Zdziarski noted: "If, and it's a big if, they used this in UFED or other products, it would indicate they ripped off software verbatim from the jailbreak community and used forensically unsound and experimental software in their supposedly scientific and forensically validated products."

- Coverage:
  - https://motherboard.vice.com/en_us/article/hacker-dumps-ios-cracking-tools-allegedly-stolen-from-cellebrite
  - https://www.schneier.com/blog/archives/2017/02/hacker_leaks_ce.html

Worrisome movement in the Encrypted Web Extensions (EME) standardization process

- TechDirt: "The Codification Of Web DRM As A Censorship Tool"

  The ongoing fight at the W3C over Encrypted Media Extensions -- the HTML5 DRM scheme that several companies want ensconced in web standards -- took two worrying turns recently.

  Firstly, Google slipped an important change into the latest Chrome update that removed the ability to disable its implementation of EME, further neutering the weak argument of supporters that the DRM is optional.

  But the other development is even more interesting -- and concerning: Dozens of W3C members -- and hundreds of security professionals -- have asked the W3C to amend its policies so that its members can't use EME to silence security researchers and whistleblowers who want to warn web users that they are in danger from security vulnerabilities in browsers.

  So far, the W3C has stonewalled on this. This weekend, the W3C executive announced that it would not make such an agreement part of the EME work, and endorsed the idea that the W3C should participate in creating new legal rights for companies to decide which true facts about browser defects can be disclosed and under what circumstances.

  One of the major objections to EME has been the fact that, due to the anti-circumvention copyright laws of several countries, it would quickly become a tool for companies to censor or punish security researchers who find vulnerabilities in their software. The director of the standards body called for a new consensus solution to this problem but, unsurprisingly, "the team was unable to find such a resolution."

  So the new approach will be a forced compromise of sorts in which, instead of attempting

to carve out clear and broad protections for security research, they will work to establish narrower protections only for those who follow a set of best practices for reporting vulnerabilities. In the words of one supporter of the plan, it "won't make the world perfect, but we believe it is an achievable and worthwhile goal."

But this is not a real compromise because by working to determine where the line should be drawn, it creates an implicit presumption that there is a line to be drawn. Having a policy is a tacit endorsement of the use of DRM for censoring security researchers -- to whatever degree. Because the argument is not about to what degree such use is acceptable, but whether such use is appropriate at all.

- Our take: If responsible disclosure is criminalized, it will be forced underground. Disclosures will sctill likely be made, but made anonymously and publicly, creating reputation damage for companies who COULD have fixed those problems before disclosure, and endangering end users who will be using products with publicly known and not-yet-patched products.

- Coverage:
    - https://www.techdirt.com/articles/20170201/14285436609/codification-web-drm-as-censorship-tool.shtml

The woes of Windows 10

- The Economist:
  Despite its having been available for 18 months, three out of four PC owners have not bothered to upgrade their computers to the latest version of Microsoft's operating system, Windows 10.

  More than 700 million of the world's 1.5 billion or so computers continue to run on Windows 7, a piece of software three generations old. A further 300 million users have stuck with other versions—half of them stubbornly (and rashly) clinging to 16-year-old Windows XP that Microsoft pensioned off three years ago.

  The business world has been even more recalcitrant. In a recent study by Softchoice, an info-tech consultancy, corporate computers were found to be running a whole gamut of legacy versions of Windows. Fewer than 1% of them had been upgraded to Windows 10.

- http://www.economist.com/news/science-and-technology/21715831-why-so-many-pc-users-are-refusing-upgrade-windows-10-woes-windows-10

garrettbane (@garrettbane) 2/2/17, 2:33 PM
@SGgrc how will LogMeIn and Citrix merger affect LastPass, based on what we know so far?

Quick Q's:

- Passeride (@Passeride) 2/1/17, 4:21 AM
  @SGgrc Thoughts on salting PW hashes with characters in username randomly deterministically selected based on unhashed password?

- Matt Clare (@Mattclare) 2/3/17, 7:02 AM
  @SGgrc SN question: Why do botnets prefer IRC?
  Tor hidden to much work?
  XML too fancy?
  iding in plane site safer?
  Listener since ep -1

Miscellany

"The Expanse" series (season 2) resumed last Wednesday.

(Michael) M.D. Cooper's "Intrepid Saga"
- http://www.aeon14.com/
- Participates in the "Kindle Unlimited" plan... so no charge for avid readers.
- Four Books:
  - Outsystem https://www.amazon.com/dp/B008GZ8HEM/
  - A Path in the Darkness https://www.amazon.com/dp/B00R53GJVO/
  - Building Victoria https://www.amazon.com/dp/B01FWZ5HRS/
  - Destiny Lost https://www.amazon.com/dp/B01M29901Q/

NaturalSleep - packaged Healthy Sleep Formula
- http://www.healthysleepnow.com/sn.html

Morgan Speck (@morganspeck) 2/6/17, 1:50 PM
- @hover You did everything for me automatically.
  I see now why @SGgrc was raving about how great you all are. Thanks!

- (I just moved "BeyondRecall.com" from Network Solutions to Hover.)

SpinRite

- Arcane Code (@arcanecode) 2/1/17, 6:09 AM
  Not much longer for #SpinRite to run on this laptop. Crossing my fingers @SGgrc !

- pic.twitter.com/JZE0y3oBEh

- Arcane Code (@arcanecode) 2/1/17, 9:29 AM
  YAY! #SpinRite fixed my hard drive, my laptop now works without the hard drive constantly churning. Thanks @SGgrc

Two Armed Bandits

https://www.wired.com/2017/02/russians-engineer-brilliant-slot-machine-cheat-casinos-no-fix/

In early June 2014, accountants at the Lumiere Place Casino in St. Louis noticed that several of their slot machines had—just for a couple of days—gone haywire. The government-approved software that powers such machines gives the house a fixed mathematical edge, so that casinos can be certain of how much they'll earn over the long haul—say, 7.129 cents for every dollar played. But on June 2 and 3, a number of Lumiere's machines had spit out far more money than they'd consumed, despite not awarding any major jackpots, an aberration known in industry parlance as a negative hold. Since code isn't prone to sudden fits of madness, the only plausible explanation was that someone was cheating.

Casino security pulled up the surveillance tapes and eventually spotted the culprit, a black-haired man in his thirties who wore a Polo zip-up and carried a square brown purse. Unlike most slots cheats, he didn't appear to tinker with any of the machines he targeted, all of which were older models manufactured by Aristocrat Leisure of Australia. Instead he'd simply play, pushing the buttons on a game like Star Drifter or Pelican Pete while furtively holding his iPhone close to the screen.

He'd walk away after a few minutes, then return a bit later to give the game a second chance. That's when he'd get lucky. The man would parlay a $20 to $60 investment into as much as $1,300 before cashing out and moving on to another machine, where he'd start the cycle anew. Over the course of two days, his winnings tallied just over $21,000. The only odd thing about his behavior during his streaks was the way he'd hover his finger above the Spin button for long stretches before finally jabbing it in haste; typical slots players don't pause between spins like that.

On June 9, Lumiere Place shared its findings with the Missouri Gaming Commission, which in turn issued a statewide alert. Several casinos soon discovered that they had been cheated the same way, though often by different men than the one who'd bilked Lumiere Place. In each instance, the perpetrator held a cell phone close to an Aristocrat Mark VI model slot machine shortly before a run of good fortune.

By examining rental-car records, Missouri authorities identified the Lumiere Place scammer as Murat Bliev, a 37-year-old Russian national. Bliev had flown back to Moscow on June 6, but the St. Petersburg–based organization he worked for, which employs dozens of operatives to manipulate slot machines around the world, quickly sent him back to the United States to join another cheating crew. The decision to redeploy Bliev to the US would prove to be a rare misstep for a venture that's quietly making millions by cracking some of the gaming industry's most treasured algorithms.

From Russia With Cheats

Russia has been a hotbed of slots-related malfeasance since 2009, when the country outlawed virtually all gambling. (Vladimir Putin, who was prime minister at the time, reportedly believed the move would reduce the power of Georgian organized crime.) The ban forced thousands of

casinos to sell their slot machines at steep discounts to whatever customers they could find. Some of those cut-rate slots wound up in the hands of counterfeiters eager to learn how to load new games onto old circuit boards. Others apparently went to Murat Bliev's bosses in St. Petersburg, who were keen to probe the machines' source code for vulnerabilities.

By early 2011, casinos throughout central and eastern Europe were logging incidents in which slots made by the Austrian company Novomatic paid out improbably large sums. Novomatic's engineers could find no evidence that the machines in question had been tampered with, leading them to theorize that the cheaters had figured out how to predict the slots' behavior. "Through targeted and prolonged observation of the individual game sequences as well as possibly recording individual games, it might be possible to allegedly identify a kind of 'pattern' in the game results," the company admitted in a February 2011 notice to its customers.

Recognizing those patterns would require remarkable effort. Slot machine outcomes are controlled by programs called pseudorandom number generators that produce baffling results by design. Government regulators, such as the Missouri Gaming Commission, vet the integrity of each algorithm before casinos can deploy it.