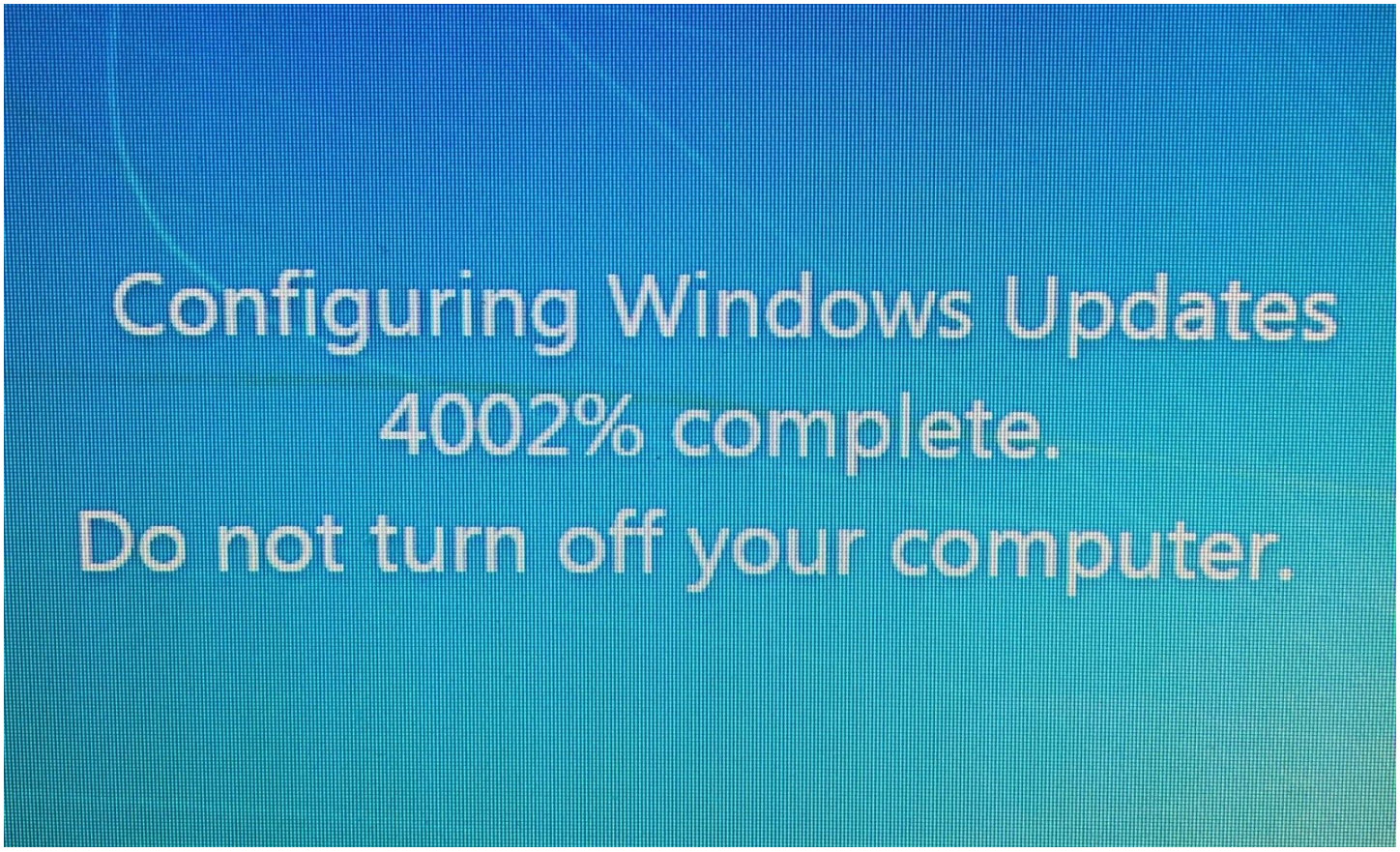
Security Now! #584 - 11-01-16

Q&A #242

This week on Security Now!

- An oh-so-subtle side-channel attack on Intel processors,
- The quest for verifiable hacker-proof code (which oh-so-subtle side-channel attacks on processors can exploit anyway!)
- Another compiler optimization security gotcha,
- The challenge of adding new web features without opening routes of exploitation,
- Some good news about the DMCA,
- Matthew Green and the DMCA,
- The MPAA and RIAA keep pushing the limits and threatening the Internet,
- The secure ProtonMail service feels the frightening power of skewed search results,
- Regaining control over Windows 10 upgrade insistence,
- A 0-day vulnerability Google revealed before Microsoft has patched it,
- A bit of errata, miscellany…
- And as many listener feedback questions and answers as we have remaining time for in a two-hour podcast!



Well played, Patch Tuesday… well played.

Next Week on Security Now

The Windows "Atom Bomb" Exploit and Attack.
Windows "Atom Bombing" is performed **only** by using long-established features present in every Windows operating system… mainly the global "Atom Table." There is no need to exploit an operating system bug or vulnerabilities... so there's nothing to patch, and Microsoft cannot, at this point, significantly change or remove these longstanding features.

Security News

Speaking of Windows and Updates...

- I noticed after last week's podcast that my Windows machine had the preview for November's update as an "optional" update.
- "October, 2016 Preview of Monthly Quality Rollup for WIndows 7 x64 based systems.

Tweet by Victor van der Veen (Project lead at UV Amsterdam)

- https://twitter.com/vvdveen/status/791643123432693760
- Victor is the project lead on the UV Amsterdam group who did DRAMMER.
- "This so cool, your explanation of Drammer is absolutely perfect!
  I just fell in love with your show :-)"

Tweet by Victor van der Veen (@vvdveen) 10/25/16, 6:20 AM

- We now know that LPDDR4 RAM is also vulnerable.
- ArsTechnica's Dan Goodin tweeted: "Bit flips on Google Pixel XL, One Plus 3, Galaxy Note 7 (...)"

An Oh-So-Subtle side-channel attack on Intel processors

- http://www.electronicproducts.com/Programming/Software/Flaw_in_Intel_chips_makes_users_more_susceptible_to_malware_attacks.aspx
- http://arstechnica.com/security/2016/10/flaw-in-intel-chips-could-make-malware-attacks-more-potent/
- Researchers at UC Riverside and the State University of New York at Binghamton, have devised a robust technique to bypass the important protections provided by ASLR. If left unfixed (and it's unclear how to fix this), it could render malware attacks much more potent.
- Review: ROP - Return Oriented Programming and the need for ASLR.
    - Implementation mistakes have been found and exploited, such as kernel code which inadvertently exposes its own address in returned parameters.

- Described in research presented a few weeks ago, Tuesday, Oct. 18 at the IEEE/ACM International Symposium on Microarchitecture, titled: Jump Over ASLR: Attacking Branch Predictors to Bypass ASLR

- The researchers demonstrated the technique on a computer running a recent version of Linux on top of a Haswell processor from Intel. By exploiting a flaw in the CPU's performance accelerating branch predictor, the demonstration application developed by the researchers was able to identify the memory locations where specific chunks of code resided.
- The technique also operates within the virtualized environments common in cloud-based computing and hosting.
- The new technique exploits collisions in the branch target buffer table to figure out the addresses where specific code chunks are located.

Verifiable hacker-proof code

- https://www.quantamagazine.org/20160920-formal-verification-creates-hacker-proof-code/
- Title: "Hacker-Proof Code Confirmed"
- Subtitle: "Computer scientists can prove certain programs to be error-free with the same certainty that mathematicians prove theorems. The advances are being used to secure everything from unmanned drones to the internet."

- <QUOTE> In the summer of 2015 a team of hackers attempted to take control of an unmanned military helicopter known as Little Bird. The helicopter, which is similar to the piloted version long-favored for U.S. special operations missions, was stationed at a Boeing facility in Arizona. The hackers had a head start: At the time they began the operation, they already had access to one part of the drone's computer system. From there, all they needed to do was hack into Little Bird's onboard flight-control computer, and the drone was theirs.

  When the project started, a "Red Team" of hackers could have taken over the helicopter almost as easily as it could break into your home Wi-Fi. But in the intervening months, engineers from the Defense Advanced Research Projects Agency (DARPA) had implemented a new kind of security mechanism — a software system that could not be commandeered. Key parts of Little Bird's computer system were unhackable with existing technology, its code as trustworthy as a mathematical proof. Even though the Red Team was given six weeks with the drone and more access to its computing network than genuine bad actors could ever expect to attain, they failed to crack Little Bird's defenses.

  Kathleen Fisher, a professor of computer science at Tufts University and the founding program manager of the High-Assurance Cyber Military Systems (HACMS) project, said: "They were not able to break out and disrupt the operation in any way. That result made all of DARPA stand up and say, oh my goodness, we can actually use this technology in systems we care about."

  The technology that repelled the hackers was a style of software programming known as formal verification. Unlike most computer code, which is written informally and evaluated based mainly on whether it works, formally verified software reads like a mathematical proof: Each statement follows logically from the preceding one. An entire program can be tested with the same certainty that mathematicians prove theorems.

The 15th International Conference on Cryptology and Network Security

- http://cans2016.di.unimi.it/program
- Amid presentations titled:
    - Diversity Within the Rijndael Design Principles for Resistance to Differential Power Analysis
    - Efficient Implementation of Supersingular Isogeny Diffie-Hellman Key Exchange Protocol on ARM
    - Signer-Anonymous Designated-Verifier Redactable Signatures for Cloud-Based Data Sharing
    - Efficient and Secure Multiparty Computations Using a Standard Deck of Playing Cards

- When Constant-Time Source Yields Variable-Time Binary: Exploiting Curve25519-donna Built with MSVC 2015

- Curve25519 was presented in 2006 by Bernstein with security in mind. This curve naturally provides state-of-the-art timing-attack protection. Particularly the implementation avoids input-dependent branches, input-dependent array indices, and other instructions with input-dependent timings.

- Google's Adam Langley implemented a constant-time ECDH, in C, using Bernstein's Curve25519, calling this version "Donna."

- "Although the computation of the scalar multiplication should be time-constant, we spotted some timing differences depending on the value of the key."

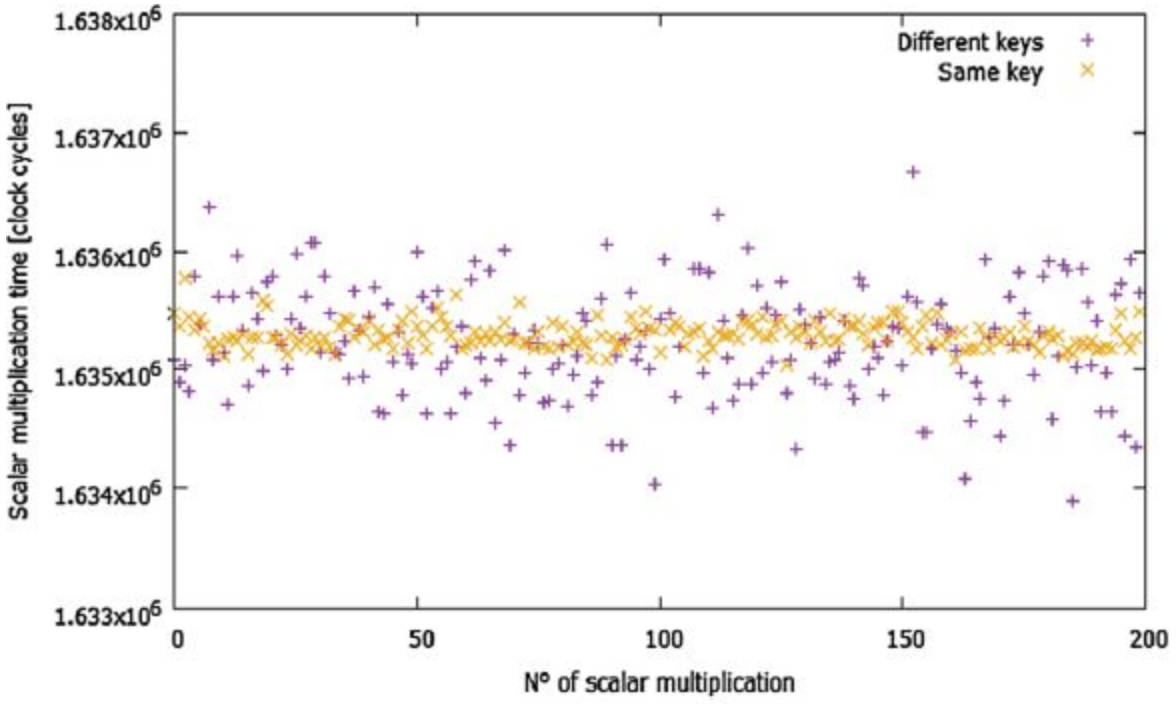
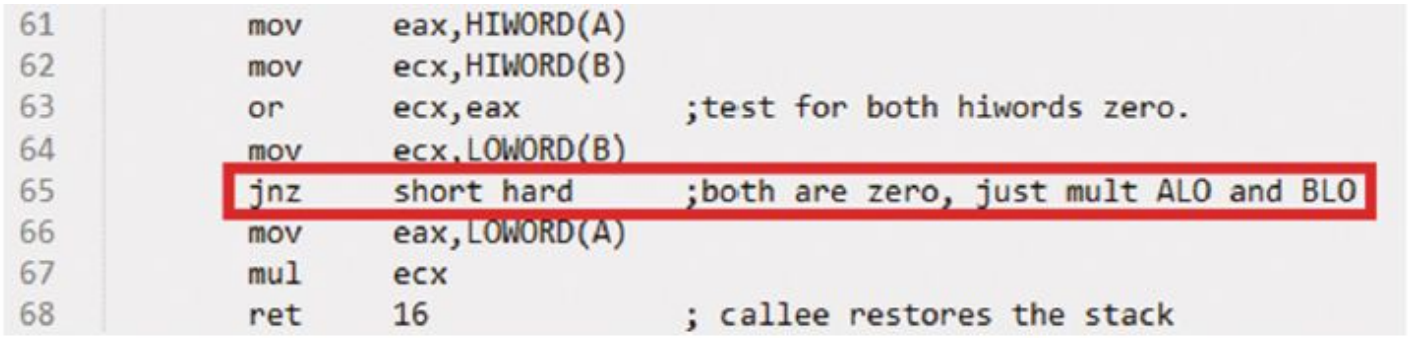


Fig. 1. Computation times depending on the key.

- After a careful analysis of the binary code, the observed timing leakage appeared to be coming from the assembly function llmul.asm found in the Windows runtime library1. The function llmul.asm is called to compute the multiplication of two 64-bit integers. It contains a branch condition which causes differences in execution time (see Fig. 2, line 65). If both operands of the multiplication have their 32 most significant bits equal to 0 then the multiplication of these words is avoided as the computation is correctly judged to be 0.



```
61      mov     eax,HIWORD(A)
62      mov     ecx,HIWORD(B)
63      or      ecx,eax         ;test for both hiwords zero.
64      mov     ecx,LOWORD(B)
65      jnz     short hard      ;both are zero, just mult ALO and BLO
66      mov     eax,LOWORD(A)
67      mul     ecx
68      ret     16              ; callee restores the stack
```

Fig. 2. Part of the code of the Microsoft *llmul* function with incriminating line

- Visual Studio breaks constant-time code…

Mozilla removing web content access to battery state information

- https://bugzilla.mozilla.org/show_bug.cgi?id=1313580
- Mozilla's Chris Peterson:
- https://groups.google.com/forum/#!msg/mozilla.dev.platform/5U8NHoUY-1k/9ybyzQIYCAAJ
- What is the use case for the Battery Status API [0], navigator.getBattery()?
    - Can we remove the Battery API or perhaps restrict it to non-web content like browser extensions or privileged web apps?
    - Chrome and Firefox support the Battery API, but neither Edge nor WebKit have signaled an intent to implement it [3].

- In theory, web developers would use the Battery API to save document data before the battery dies, to ease off heavy computation when the battery is low, or to implement the Firefox OS settings app. The real world use cases, however, seem to be fingerprinting users [1] and inflating Uber prices for desperate users with low batteries [2]. Can anyone point to a real website using the Battery API for a legitimate purpose?

  The BATTERY_STATUS_COUNT probe [4] reports over 200M battery API calls for Firefox 49. The USE_COUNTER2_DEPRECATED_NavigatorBattery_PAGE probe [5] reports that 6% of web pages use the Battery API, IIUC. That seems surprisingly high given the few legitimate use cases. (Could that counter be inadvertently triggered by web content that simply enumerates the navigator object's properties without actually calling navigator.getBattery()?)

  I have a patch that makes the Battery API chrome-only and fixes the web-platform tests.

- The thread continues with a bunch of back and forth.
- There's some commentary about having previously reduced the reporting resolution to reduce but not eliminate the tracking specificity.
- This stuff is difficult.
    - The Web standards folks add stuff that they think is cool.
    - The Browser guys want to be fully standards compliant, so they implement it.
    - The Real World folks realize they have a new tracking hook.
    - The Browser guys realize their nifty new feature is being abused to reduce their users' privacy…
- Now what do they do?
  (It's never easy to remove things that some people may need, want, or depend upon.)

DMCA updated to allow security research

- http://www.theregister.co.uk/2016/10/28/toaster_penetration_testing_green_lighted/
- The exemptions cover:
    - The use of recorded and streaming video in educational and documentary contexts.
    - The use of electronic literary works in conjunction with assistive technologies.
    - Jailbreaking phones and tablets to enable interoperability or remove unwanted software.
    - Efforts to access automobile software.
    - Efforts to make non-functioning video games accessible.
    - Efforts to bypass 3D printer materials controls.
    - Efforts by patients to access data in personal medical devices.
    - Attempts to reverse-engineer software for security research.

- Security researchers must still abide by the Computer Fraud and Abuse Act.
- The terms of the exemption specify that reverse-engineering or deobfuscating code must be "carried out in a controlled environment designed to avoid any harm to individuals or the public."
- Furthermore, any information gained from such activity must be used to promote the security of the type of device on which the code runs or the security of the people using the device. And the fruits of such research must be maintained in a way that avoids facilitating copyright infringement

Crypto guru Matt Green asks courts for DMCA force field so he can safely write a textbook

- http://www.theregister.co.uk/2016/09/30/green_asks_protection_from_dmca_lawsuits/
- by Ian Thomson
- Assistant Professor Matthew Green has asked US courts for protection so that he can write a textbook explaining cryptography without getting sued under the Digital Millennium Copyright Act.

  Green, who teaches at Johns Hopkins University in Maryland, is penning a tome called Practical Cryptographic Engineering that examines the cryptographic mechanisms behind the devices we use every day, such as ATM machines, smart cars, and medical devices. But this could lead to a jail sentence if the manufacturers file a court case using Section

1201 of the DMCA.

Section 1201 prohibits the circumvention of copyright protection systems installed by manufacturers, and comes with penalties including heavy fines and possible jail time. As such, the Electronic Frontier Foundation (EFF) has taken up Green's case, and that of another researcher, to try to get the provision ruled illegal by the courts.

EFF staff attorney, Kit Walsh, said: "If we want our communications and devices to be secure, we need to protect independent security researchers like Dr Green."

So the EFF has decided to support two actions against the DMCA: Green and the case of another researcher who wants to make an open-source computer that would allow commercial videos to be edited. EFF is hoping that these test cases can bring down Section 1201, and hopefully the entire DMCA.

- (God bless the EFF!)

"MPAA and RIAA's Anti-Piracy Plans Harm The Internet" - TorrentFreak

- https://torrentfreak.com/mpaa-and-riaas-anti-piracy-plans-harm-the-internet-161027/
- The MPAA and RIAA continue pushing back against even proper use of the Internet.
- The Internet Infrastructure Coalition (I2Coalition) -- a group which includes Amazon, Google, Dreamhost, GoDaddy, Plesk, Rackspace, Tucows, Verisign and many more -- is urging the U.S. Government not to blindly follow the RIAA and MPAA's input regarding online piracy threats. The group warns that the future of the Internet is at stake.
- The problem is, the copyright stake holders are broadening their attacks beyond specific sites, such as The Pirate Bay, to include technologies and technology providers which they claim threaten their rights.
- For example, this year the MPAA and RIAA identified domain name registrars as possible piracy facilitators.

- In addition, several "rogue" hosting providers were mentioned, as well as CDN provider Cloudflare.

- For example, the MPAA characterizes Cloudflare as a service that creates "obstacles to enforcement" as it helps pirate sites to "hide."

- I2Coalition also argues that the submissions show a misinterpretation of the obligations domain name registrars have under the Registrar Accreditation Agreement (RAA).

- The MPAA and RIAA would like domain registrars to suspend domain names that are merely ACCUSED of copyright infringement. But most refuse to do so without a court order. Rightfully so, according to I2Coalition: "The vilification of technology and misconstruing of the RAA have one goal in common: forcing Internet infrastructure companies to act as intermediaries in intellectual property disputes. This is not the answer to intellectual property infringement, is not the purpose of the Special 301 process, and proposals to expand the use of these companies as intermediaries are misguided."

How Google almost killed ProtonMail

- https://protonmail.com/blog/search-risk-google/
- "Search Risk – How Google Almost Killed ProtonMail"

- The short summary is that for nearly a year, Google was hiding ProtonMail from search results for queries such as 'secure email' and 'encrypted email'. This was highly suspicious because ProtonMail has long been the world's largest encrypted email provider.

  When ProtonMail launched in Beta back in May 2014, our community rapidly grew as people from around the world came together and supported us in our mission to protect privacy in the digital age. Our record breaking crowdfunding campaign raised over half a million dollars from contributors and provided us with the resources to make ProtonMail competitive against even the biggest players in the email space.

  By the summer of 2015, ProtonMail passed half a million users and was the world's most well known secure email service. ProtonMail was also ranking well in Google search at this time, on the first or second page of most queries including "encrypted email" and "secure email". However, by the end of October 2015, the situation had changed dramatically, and ProtonMail was mysteriously no longer showing up for searches of our two main keywords.

  Between the beginning of the summer and the fall of 2015, ProtonMail did undergo a lot of changes. We released ProtonMail 2.0, we went fully open source, we launched mobile apps in beta, and we updated our website, changing our TLD from .ch to the more widely known .com. We also doubled in size, growing to nearly 1 million users by the fall. All of these changes should have helped ProtonMail's search rankings as we became more and more relevant to more people.

  In November 2015, we became aware of the problem and consulted a number of well known SEO experts. None of them could explain the issue, especially since ProtonMail has never used any blackhat SEO tactics, nor did we observe any used against us. Mysteriously, the issue was entirely limited to Google, as this anomaly was not seen on any other search engine.

- All throughout Spring 2016, we worked in earnest to get in touch with Google. We created two tickets on their web spam report form explaining the situation. We even contacted Google's President EMEA Strategic Relationships, but received no response nor improvement. Around this time, we also heard about the anti-trust action brought forward by the European Commission against Google, accusing Google of abusing its search monopoly to lower the search rankings of Google competitors. This was worrying news, because as an email service that puts user privacy first, we are the leading alternative to Gmail for those looking for better data privacy.

- In August, with no other options, we turned to Twitter to press our case. This time though, we finally got a response, thanks in large part to the hundreds of ProtonMail users who drew attention to the issue and made it impossible to ignore. After a few days, Google informed us that they had "fixed something" without providing further details. The results could be immediately seen.

Retaking control of updates in Windows 10

- http://techgage.com/article/taking-back-control-of-windows-10-updates/

- Father Robert reverted to Win7 after his machine forced an update in the middle of a podcast.

- The only robust way to fix Win10's insistence upon updating is through Group Policy:

- Win10 Home won't have gpedit.msc.

- GPEDIT.MSC
    - Computer Configuration > Administrative Templates > Windows Components > Windows Update
    - In the right panel are a list of settings.
    - We want: Configure Automatic Updates.
    - Double click it to open up its settings.
    - There are four different "levels" which can be set. We want Level2 - Notify for download and notify for install.
    - Be certain to select "enabled" to enable the policy override.
    - Apply, OK and close Group Policy.

Google: Disclosing vulnerabilities to protect users

- https://security.googleblog.com/2016/10/disclosing-vulnerabilities-to-protect.html
- On Friday, October 21st, we reported 0-day vulnerabilities — previously publicly-unknown vulnerabilities — to Adobe and Microsoft. Adobe updated Flash on October 26th to address CVE-2016-7855; this update is available via Adobe's updater and Chrome auto-update.

  After 7 days, per our published policy for actively exploited critical vulnerabilities, we are today disclosing the existence of a remaining critical vulnerability in Windows for which no advisory or fix has yet been released. This vulnerability is particularly serious because we know it is being actively exploited.

  The Windows vulnerability is a local privilege escalation in the Windows kernel that can be used as a security sandbox escape. It can be triggered via the win32k.sys system call NtSetWindowLongPtr() for the index GWLP_ID on a window handle with GWL_STYLE set to WS_CHILD. Chrome's sandbox blocks win32k.sys system calls using the Win32k lockdown mitigation on Windows 10, which prevents exploitation of this sandbox escape vulnerability.

  We encourage users to verify that auto-updaters have already updated Flash — and to manually update if not — and to apply Windows patches from Microsoft when they become available for the Windows vulnerability.

Errata

Tweet by Darko Vrsic
Hi Steve! In SN you said any unpatched web facing Linux server is vulnerable to Dirty COW exploit. Isn't it only locally exploitable?
Tweet by Jeff Bearer
@SGgrc really got his description of dirty cow wrong. Like super extra wrong. It's not remotely exploitable.

Miscellany

Peter Hamilton's "A Night Without Stars"
A good conclusion to "The Faller" saga. I LOVE Hamilton's Commonwealth... but, overall, I thought this was not as wonderful as the Pandor's Star / Judas Unchained pair.

The second season "Humans" has started
But the U.S. doesn't get it until February, 2017 on AMC.
Season 2 introduces Carrie-Anne Moss (The Matrix) as AI expert Dr. Athena Morrow.
Season 2 picks up a few months after the final episode of first series, and finds Niska still at an unknown location, with the consciousness code still on her. Laura and Joe are working on their marriage issues, while Mia, Leo and Max are soul-searching. Breakthrough AI research is underway in the United States, but the motives behind it may be questionable.

Blue Sky Department: If Diamonds Are Forever, Your Data Could Be, Too.
http://www.nytimes.com/2016/10/27/science/diamonds-data-storage.html

SpinRite

Hi Steve, A SpinRite story for you with a punch line:

My story begins when I advised my dad to give your product a try on a failing drive in his laptop. Sadly it was so far gone mechanically that it wasn't any help, though he was able to eventually get the data off. He was frustrated, and decided to give his license to me. Fast forward a few months and a friend of mine in Colorado has started having troubles saying his system was getting blue screens on boot with the error mentioning: "This was probably caused by the following module: hal.dll."

After looking up that dll, I found it's the Hardware Abstraction Layer module. Not good. I sent my friend a copy of the Spinrite ISO and walked him through setting up a bootable CD. After that, I got him set with running a scan over a drive. The next I heard from him, the system was running again without any problems, so whether you like it or not, Steve, you can now say of SpinRite: "So easy, a stoner can do it."

- Matthew Olmsted, Davis, CA