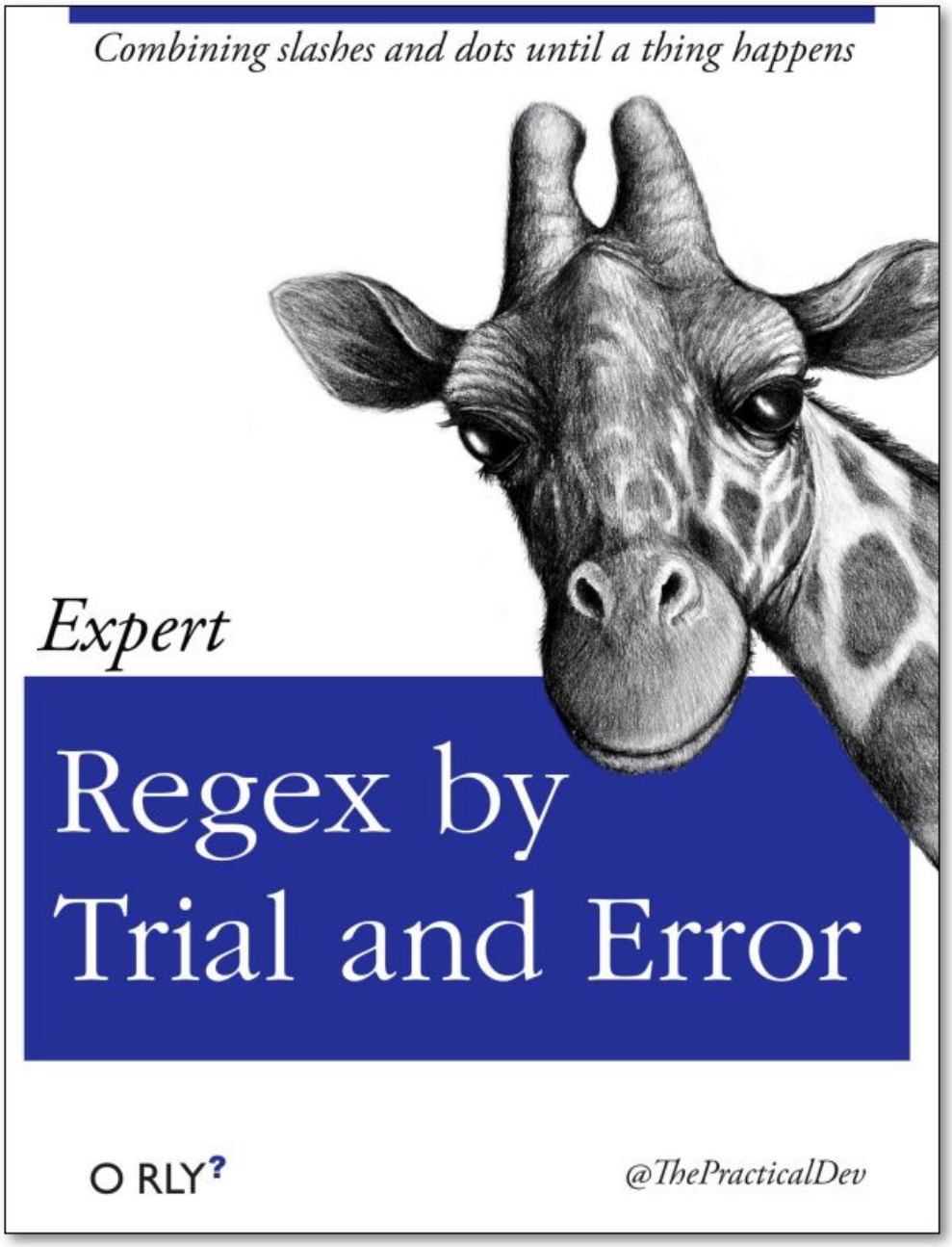
Security Now! #577 - 09-13-16

Q&A #239

This week on Security Now!

A bit of Flip Feng Shui follow-up, Apple's announcements, Android's rough week, Wireless device privacy leakages, some fun miscellany, and ten questions, comments, and observations from our terrific listeners.



Security News

Flip Feng Shui follow-up: VU Amsterdam's security research group led by Prof. Herbert Bos

- Ben Gras @bjg
  @SGgrc As one of the authors, thank you for your knowledgeable & detailed exposition! We're honored by it & your kind words! cc @vu5ec

- Thank you again for your Flip Feng Shui coverage. Because of more recent coverage I am a bit of an expert on how well our work is understood and I don't hesitate to rate your coverage at a 95-percentile rating for expertise and quality of exposition . We also loved your appreciative words of course, so full marks, thank you so much! I'm also a big fan of the show so it's just joy all round here.

The Apple iOS 7 -- and product spread

- More memory, faster processor, terrific camera,
- Just like with Windows... people are hanging back because what they already have is working just fine.
- TIP: Want to determine your ISP's true downstream bandwidth? Update several iOS devices at the same time. Apple's CDN WILL deliver at very high speed. I pinned my download at 100mbps by updating my phone and five iPads simultaneously.

Android has another bad week

- Google has releases fixes for Nexus users.
- OEM partners have received the code, but unknown when, or in some cases if, they will have patches available. And older phones that are no longer supported will never receive these updates.
- The most worrisome vulnerability was reminiscent of the many troubles with the Stagefright module because a maliciously formatted JPEG image could be used to compromise the recipient device's security.
- An exploit would leverage some mishandling of the JPEG images EXIF header data.
- The second vulnerability was disclosed by researcher Mark Brand, allowing attackers to execute malware or escalate local privileges on vulnerable phones. Google has stated that the exploit was for research purposes, and could not be used in real world attacks unless the intruder found it and modified it.
- However... the Google Play store HAS been hosting malicious apps which leveraged these vulnerabilities.
- ArsTechnica reported that: malicious apps were downloaded as many as 2.5 million times from Google's official Play Marketplace.
- http://arstechnica.com/security/2016/09/two-critical-bugs-and-more-malicious-apps-make-for-a-bad-week-for-android/
- http://blog.checkpoint.com/2016/09/08/calljam-android-malware-found-on-google-play/

Bluetooth presence and location leakage

- http://arstechnica.com/information-technology/2016/09/hands-on-blue-hydra-can-expose-the-all-too-unhidden-world-of-bluetooth/
- Sean Gallagher, for ArsTechnica, writes:
  My new neighbor was using AirDrop to move some files from his phone to his iMac. I hadn't introduced myself yet, but I already knew his name. Meanwhile, someone with a Pebble watch was walking past, and someone named "Johnny B" was idling at the stoplight at the corner in their Volkswagen Beetle, following directions from their Garmin Nuvi. Another person was using an Apple Pencil with their iPad at a nearby shop. And someone just turned on their Samsung smart television.

  I knew all this because each person advertised their presence wirelessly, either over "classic" Bluetooth or the newer Bluetooth Low Energy (BTLE) protocol—and I was running an open source tool called Blue Hydra, a project from the team at Pwnie Express. Blue Hydra is intended to give security professionals a way of tracking the presence of traditional Bluetooth, BTLE devices, and BTLE "iBeacon" proximity sensors. But it can also be connected to other tools to provide alerts on the presence of particular devices.

  Despite their "Low Energy" moniker, BTLE devices are constantly polling the world even while in "sleep" mode. And while they use randomized media access control (MAC) addresses, they advertise other data that is unique to each device, including a universally unique identifier (UUID). As a result, if you can tie a specific UUID to a device by other means, you can track the device and its owner. By using the Received Signal Strength Indication (RSSI), you can get a sense of how far away they are.

  That information can be used, for good or ill, to generate movement data about the people who carry those devices—and to watch for devices that appear when they shouldn't. Pwnie's Rick Farina told Ars, as he gave us a walk-through of the tool: "I have an alert set up for when my mother-in-law's car pulls into range. It gives me about a 30-second warning."

- Note: The tradeoff between absolute privacy and features is a problem with all of our wireless technologies. WiFi similarly blabs about who it is, where it's been, and who it knows. We want the convenience of having everything "just work" -- when things "pair" instantly and easily, everyone cheers. But forgotten is the nature of the underlying interchange, and in many cases beacons broadcasting, the presence and identity of its owner.

Miscellany

A Loud Sound Just Shut Down a Bank's Data Center for 10 Hours

- http://motherboard.vice.com/read/a-loud-sound-just-shut-down-a-banks-data-center-for-10-hours
- NG Bank’s main data center in Bucharest, Romania, was severely damaged over the weekend during a fire extinguishing test.

- Inert fire-suppression gas, under very high pressure, pinned the needles at 130db, of sound monitoring gear.
- Damaged drives and knocked the banks operations offline for ten hours.
- Storage researchers at IBM have written: “The HDD can tolerate less than 1/1,000,000 of an inch offset from the center of the data track—any more than that will halt reads and writes. Early disk storage had much greater spacing between data tracks because they held less data, which is a likely reason why this issue was not apparent until recently.”
- (A pre-SpinRite utility I wrote realigned a drive's heads.)

You know you're in trouble when... Headlines read: "How to tell an explosive Galaxy Note 7 from a non-explosive one."

- Or worse: "Samsung Galaxy Note 7 explodes in New York, burns six-year-old boy"
- http://arstechnica.com/gadgets/2016/09/samsung-galaxy-note-7-explodes-boy/
- Fire was strong enough to set off homeowner's smoke detectors.
- The New York Post wrote in their coverage with the headline: Recalled Samsung phone explodes in little boy’s hands: "The boy had been using the device at his family home when it "suddenly burst into flames. He was rushed to hospital with burns to his body."

BlazingDB (http://blazingdb.com/)

- BLAZING GPU DATABASE
- A modern data warehouse. / High performance SQL on petabyte scale needs.
- BlazingDB heavily uses specialized, massively parallel co-processors... specifically graphics processors (GPUs).
- BlazingDB's software uses graphics processing units to perform complex operations on enterprise-scale databases, completing those operations between 5 and 140 times faster.
- Written in C/C++
- C/C++ is a low level language, with very granular control of hardware (memory, processors, etc.). C/C++ is our dedication to delivering massive scale and hyper speed for our customers.

Errata -- Correcting the Record:

- Doom was MOSTLY 'C', not Assembler:
- From: "James Boer"
  Subject: DOOM trivia
  Kirkland, WA

  Just FYI, Doom was written in C, with some small portions of rendering code in assembly. Even so, you're correct that it was masterfully coded. Doom was partially what convinced me to become a professional video game programmer.

  Doom was not the first pseudo-3D rendered game, nor was it the first shareware game. What made it unique, among a few other details, was that it was one of the first games that could render reasonably complex world geometry using the entire screen on a 486-class machine, and of course, for the stunningly visceral game play.

In case you're wondering why I call it "pseudo-3D", that's because it's not true 3D rendering (like Quake), and is sometimes referred to as "2.5D".

You can see the code here: https://github.com/id-Software/DOOM

SpinRite

Paul in Worthing, UK shares his recent SpinRite success wit SSD's...
Steve,

I cannot remember how I came across SpinRite - think it may have been at v5 back then.

I assumed when I switched my system drives to SSD that I would be using SpinRite a lot less - I used to have the habit of running SpinRite regularly on my system drives every few months, or if the system started to slow. It always was great, and I have recovered drives that blue screened or failed to start completely...

I built a new machine last year using a SANDISK SSD, I chose an enterprise version with a 10-year guarantee because as a commercial photographer I need speed but value reliability even above speed. It was great, SANDISK dedicated software allowed me to monitor it and run a TRIM command. I had a big project running (layered photoshop files sized between 3 and 7 GB on disk) and the system slowed, particularly on start up, BUT some days it was fine -fast and no problems. Sandisk emailed to tell me I should update the firmware (but backup everything on the disk first...) and also update the dedicated SanDisk SSD Dashboard software. First I updated the SanDisk SSD Dashboard software and it FAILED COMPLETELY it just destroyed the existing working version. No worries just 'roll back' the system (I use Farstone recovery software). No good, install the old version of SSD Dashboard, another no - OK I should have downloaded and copied it like I always used to but these days you don't need to do you? By this time I am tearing what is left of my hair out so of course I started thinking 'what I need is SpinRite for SSD'.

To cut a long story short I dug around the Internet and discover that SpinRite can help SSDs. OF COURSE IT DID! It found one defective and unrecoverable sector close to the beginning of the drive and two further ones that it recovered. Rebooted the machine and since then the machine has been running like lightning again.

I, for one, know that SpinRite is one of the most cost effective software purchases I have ever made. I look forward to its future fixing BOTH my spinning and my non-spinning mass storage.

Thanks for your great software and the Security Now! show