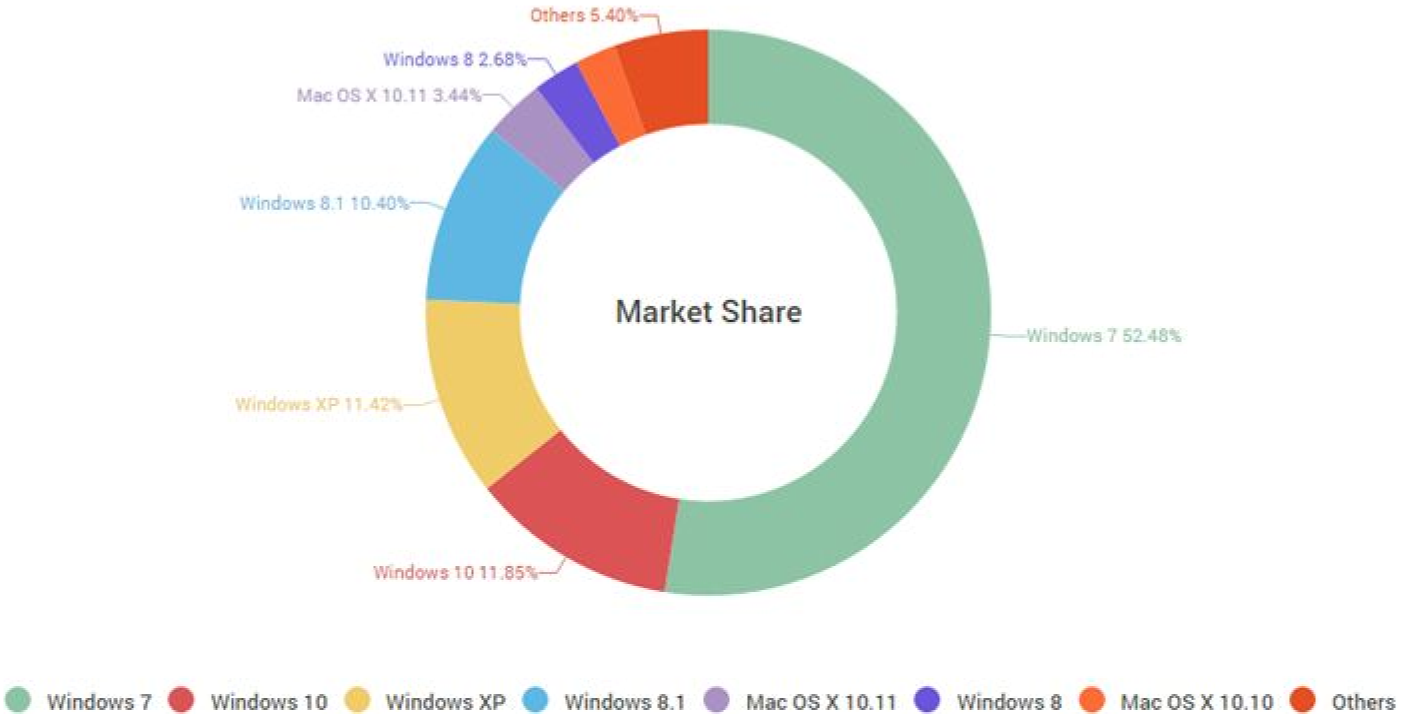
Security Now! #545 - 02-02-16

Three Dumb Routers

This week on Security Now!

- Java finally leaving the browser
- Google's February Nexus Android update
- The ongoing encryption debate
- A bunch of miscellany
- Down into the weeds of consumer router topology
    - (Why no fewer than three dumb routers is sufficient!)

Mac OS X 10.11 at 3.44%, Others at 5.4%, Windows… all the rest:



(Source: http://thehackernews.com/2016/02/windows-10-upgrade.html)

Security News:

"Moving to a Plugin-Free Web" by the Product Management blog of the Java Platform Group
https://blogs.oracle.com/java-platform-group/entry/moving_to_a_plugin_free
By late 2015, many browser vendors have either removed or announced timelines for the removal of standards based plugin support, eliminating the ability to embed Flash, Silverlight, Java and other plugin based technologies.

With modern browser vendors working to restrict and reduce plugin support in their products, developers of applications that rely on the Java browser plugin need to consider alternative options such as migrating from Java Applets (which rely on a browser plugin) to the plugin-free Java Web Start technology.

Oracle plans to deprecate the Java browser plugin in JDK 9. This technology will be removed from the Oracle JDK and JRE in a future Java SE release.

Early Access releases of JDK 9 are available for download and testing at http://jdk9.java.net. More background and information about different migration options can be found in this short whitepaper from Oracle.
http://www.oracle.com/technetwork/java/javase/migratingfromapplets-2872444.pdf

February 1st - Nexus Security Bulletin - February 2016
https://source.android.com/security/bulletin/2016-02-01.html

- 5 "critical" security vulnerabilities
- 4 "high" severity
- 1 "moderate" issue.

Two critical vulnerabilities were found and fixed in the Broadcom WiFi driver that could be exploited by attackers to perform Remote Code Execution (RCE) on affected Android devices when connected to the same network as the attacker.

The vulnerabilities (CVE-2016-0801 and CVE-2016-0802) can be exploited by sending specially crafted wireless control message packets that can corrupt kernel memory, potentially leading to remote code execution at the kernel level.

The security advisory says: "These vulnerabilities can be triggered when the attacker and the victim are associated with the same network. This issue is rated as a Critical severity due to the possibility of remote code execution in the context of the kernel without requiring user interaction."

Two critical security vulnerabilities were also found and fixed in Mediaserver (re: Stagefright).

The recently discovered flaws (CVE-2016-0803 and CVE-2016-0804) in Mediaserver could enable remote code execution (RCE) on affected Android devices through email, web browsing, or MMS files when processing media files.

Also, a separate elevation of privilege (CVE-2016-0810) flaw was also found in Mediaserver that could be exploited to gain elevated capabilities, including Signature or SignatureOrSystem permissions privileges, that aren’t accessible to third-party apps.

On schedule, Windows 10 Upgrade moves from “Optional” to “Recommended” Update

- http://betanews.com/2016/02/01/microsoft-makes-windows-10-a-recommended-update-for-windows-7-and-8-1-users/
- http://thehackernews.com/2016/02/windows-10-upgrade.html
- http://www.zdnet.com/article/microsoft-starts-pushing-windows-10-as-a-recommended-update/

Mary Jo Foley:
In October 2015, Microsoft officials outlined a schedule for stepping up the company's push to get Windows 7 and Windows 8.1 users to move to Windows 10.
"As we shared in late October on the Windows Blog, we are committed to making it easy for our Windows 7 and Windows 8.1 customers to upgrade to Windows 10. We updated the upgrade experience today to help our customers, who previously reserved their upgrade, schedule a time for their upgrade to take place," said a company spokesperson.

Matt (@madwallsecurity)
2/1/16, 6:23 AM
@SGgrc U keep talking about Apple being able 2 do "safe" warrant access crypto. What about all the others that can't, but would have to?

Via Private DM:
The U.S. might have laws preventing unreasonable search, but a lot of countries in which Apple does business have no such protections. If you make the phone technically accessible to U.S. authorities, you make it technically accessible to every country's authorities.

Miscellany

Mark Russinovich's "TCP View" (Windows Only)
https://technet.microsoft.com/en-us/sysinternals/tcpview.aspx
And tcpvcon: Tcpvcon usage is similar to that of the built-in Windows netstat utility:

```
Usage: tcpvcon [-a] [-c] [-n] [process name or PID]
-a    Show all endpoints (default is to show established TCP connections).
-c    Print output as CSV.
-n    Don't resolve addresses..
```

Zeo Sleep Manager Pro

- https://www.grc.com/zeo.htm
- Zeo: December 29th 2003 - early 2013
- Zeo, Inc., formerly Axon Labs, a private company founded by four Brown University students.
- A Smart alarm clock
- A "Pod dock"
- The Sleep Manager Pro
- "ZeoBand" http://zeoband.com/

Why has SyFy suddenly become good?
Wired interviewed SyFy's Bill McGoldrick
http://www.wired.com/2015/12/geeks-guide-syfy-scifi/
(SyFy got a new Head of Programming)

This past week Syfy premiered Childhood's End, a six-hour adaptation of Arthur C. Clarke's classic first contact novel. The show is part of an ambitious new slate of book-to-TV adaptations being overseen by Bill McGoldrick, Syfy's new head of original programming. And while Hollywood is known for misguided rewrites of sci-fi classics, McGoldrick was determined to create a faithful adaptation of Clarke's novel.

McGoldrick said: "We all just wanted to honor the book and really give him the recognition that he was just so prescient, because all of the themes and all of the things he was writing about are so valid today."

For years Syfy has tried to broaden their appeal beyond science fiction fans, populating the channel with ghost hunters, pro wrestlers, and low-budget creature features like Sharknado and Mansquito. And while that did pull in new viewers, it also alienated sci-fi fans. McGoldrick was brought in with a clear mandate: lure the fans back with smart, ambitious shows. Adapting classic books is part of that plan.

McGoldrick said: "We want to honor that core fan base that is passionate about the material. We're really trying to focus on that core audience, and I think the way to do that is to respect the stuff they really liked in the first place."

One thing fans are passionate about is space opera shows like Farscape, Firefly, and Battlestar Galactica. But in recent years Syfy simply lacked the budget to create those kinds of shows.

McGoldrick said: "If you don't have the budget to go up into space and try to make that feel authentic, you might have to do some things that don't play to the core as much as sci-fi fans would like."

But things have changed. The success of core genre shows like HBO's Game of Thrones and AMC's The Walking Dead have persuaded Syfy's parent company, Comcast, to invest big in the channel. That means new Syfy shows like Childhood's End and The Expanse are full of gorgeous visuals and jaw-dropping special effects. McGoldrick promises that future book adaptations, which include classic works will have a similar focus on quality.

"The wallet will open for the right show, and that's what makes it so exciting to have this job right now," he says.

Temperfect Mug Update #34 (Kickstarter)
2016: The Year of the Fire Monkey / "For backers only"

January saw much progress on the Temperfect mug project. Things are coming together. A number of sourcing sub-projects were concluded successfully, loose ends were tied, and all mug parts and supplies from several factories were brought together in one place for the culmination of the made-in-China phase of this project: the "stuffing" of the shipping container arranged by our sourcing agency to bring everything to the US.

Early in the month we wrapped up the trials and final adjustments to the lid mold, which was the last tool to be finished, and all the lids for our Kickstarter rewards got made on time. All the plastic and rubber parts are now molded, inspected, consolidated and ready to go into the container: these are the lids, gaskets, sleeves, feet and shutter pivots that dress the stainless steel mug bodies.

And the bodies? Most of the parts for those were made during my last trip to the factory in December. Forty-five bodies were assembled without trouble and finished and looked good before I left. Then later in December the factory had a problem that required a large number of these assemblies to be scrapped (they were not strictly following the work instructions, the problem reported in last month's update). In January the factory started to have other difficulties with the assembly, it seems because a machine was mal-adjusted. After some time they found a solution and were able to rework the parts and get back on track with production.

...

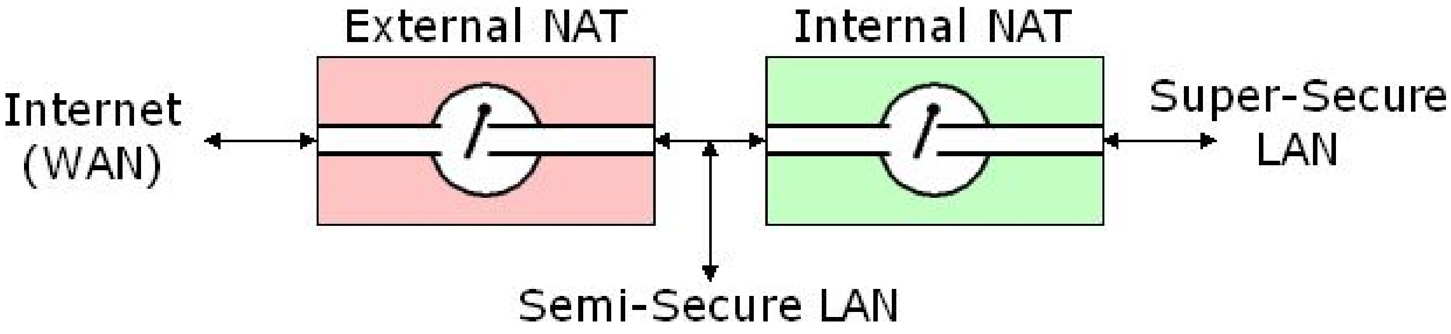
We do know we won't be getting the shipment out of China before Chinese New Year. Elvis has left the building: the workers are heading home to celebrate, and there's no one there to finish and pack and ship our mugs. They'll be back February 19th.

SpinRite

Dennis Stephens (@ParkerTechGuy)
2/1/16, 5:27 PM
@SGgrc System I use for my job, work from home died, ran my copy of SpinRite overnight, no errors reported, system booted fine #Happy

Three Dumb Routers

- Menu: Research / General / NAT Router Security
- https://www.grc.com/nat/nat.htm


External NAT
Internal NAT
Internet
(WAN)
Super-Secure
LAN
Semi-Secure LAN