SIM2K
Adapting Technology to Your Business Needs

1•18
Information you can use

SIMformation

Intel Reveals Serious Chip Flaw

Researchers from Google, academia and cybersecurity firms discovered two flaws in computer chips that affect nearly all modern computers and devices with Intel chips made in the past 20 years. Officials at Intel revealed that Google first alerted it to the vulnerability, and Google has published a detailed rundown of the exploits.

Intel and other companies were scrambling to fix the problem before word got out, the New York Times reports, but news of the vulnerability was reported by The Register on January 2, so the companies and researchers rushed to release information about it the next day. SIM2K put information on this issue on our Facebook page and website immediately upon receiving this news.

The vulnerabilities allow an attacker to compromise the privileged memory of a processor by exploiting the way processes run in parallel. They also allow an attacker to use JavaScript code running in a browser to access memory in the attacker's process. That memory content could contain key strokes, passwords, and other valuable information. Researchers are already showing how easy this attack works on Linux machines, but Microsoft says it has "not received any information to indicate that these vulnerabilities have been used to attack customers at this time."

There are two flaws that researchers have uncovered:

• "Meltdown" is a flaw that affects laptops, desktop computers and servers with Intel chips and could let hackers steal data, such as passwords saved in Web browsers. Microsoft Corp, Apple Inc and Linux, the three major operating systems, are all issuing updates, though the Apple and Microsoft have not said precisely when.

• "Spectre" affects chips in smartphones and tablets, as well as computer chips from Intel and Advanced Micro Devices Inc. Hackers can trick apps into leaking sensitive information.

Spectre is less dangerous than Meltdown, but will be more difficult to patch. Consumers should check with their device maker and operating system provider for security updates and install them as soon as possible.

Google said Android phones with the most recent security updates are protected, and users of popular web services like Gmail are also safe. Chromebook users on older versions will need to install an update whose release date has not been set. Chrome web browser users are expected to receive a patch Jan. 23.

Researchers say an update is in the work for Apple laptops and desktops, but it is not yet clear whether the company's iPhones and iPads are at risk.

Major cloud services aimed at business customers – including Amazon Web Services, Google Cloud Platform and Microsoft Azure – say they have already patched most of their services and will fix the rest soon.

Protecting a Windows PC is complicated right now, and there's still a lot of unknowns. Microsoft, Google, and Mozilla are all issuing patches for their browsers as a first line of defence. Firefox 57 (the latest) includes a fix, as do the latest versions of Internet Explorer and Edge for Windows 10. Google says it will roll out a fix with Chrome 64 which is due to be released on January 23rd. Apple has not commented on how it plans to fix its Safari browser or even macOS. Chrome, Edge, and Firefox users on Windows won't really need to do much apart from accept the automatic updates to ensure they're protected at the basic browser level.

For Windows itself, this is where things get messy. Microsoft has issued an emergency security patch through Windows Update, but if you're running third-party anti-virus software then it's possible you won't see that patch yet.

A firmware update from Intel is also required for additional hardware protection, and those will be distributed separately by OEMs. It's up to OEMs to release the relevant Intel firmware updates, and support information for those can be found at each OEM support website. If you built your own PC you'll need to check with your OEM part suppliers for potential fixes.

If you own a Windows-powered PC or laptop, the best thing to do right now is ensure you have the latest Windows 10 updates and BIOS updates from Dell, HP, Lenovo, or one of the many other PC makers. The industry is waiting for Microsoft or Intel to create a simple tool (they have a PowerShell script right now) to check protection for both the firmware and Windows updates, but until such a tool is available users will need to manually check or get familiar with PowerShell. Of course, SIM2K can assist with the PowerShell scripting.

These steps only currently provide protection against Meltdown, the more immediate threat of the CPU flaws. Spectre is still largely an unknown, and security researchers are advising that it's more difficult to exploit than Meltdown. The New York Times reports that Spectre fixes will be a lot more complicated as they require a redesign or the processor and hardware changes, so we could be living with the threat of a Spectre attack for years to come.

As more information and patches are released for these chip issues, SIM2K will continue to provide clients with updates and take appropriate actions to help protect your IT infrastructure. If you have questions, please let us know.

What's The Buzz on Blockchain?

Blockchain, perhaps best known for underpinning its better-known progeny, Bitcoin, is a rapidly evolving technology that remains something of a mystery for IT shops and in boardrooms. The distributed ledger technology seemed to take off in 2017, with everyone from IBM to J.P. Morgan and countless smaller companies rushing to embrace it. Other firms hammered IT vendors with questions about the technology and how it could be used.

Deciding when and why your company might want to roll out a blockchain transactional ledger remains something of a risky move; many early adopters could wind up spending a lot of time and money on something that ultimately provides them with little to no benefit, according to a new report from the Everest Group.

Banking and financial services were the first to embrace blockchain ledgers – no surprise given that their core business functions are ideally suited to its distributed nature, transparency and immutability as a system of record. In addition, those same industries have to rely on establishing trust between transaction participants, an often time-consuming and high-friction process due to central administration, a large number of intermediaries, and regulatory oversight that can sometimes span continents. Even so, significant business benefits can be achieved with relatively simple, non-disruptive blockchain implementations, Everest Group Research said in its report.

Rather than jumping into the deep end, IT experts suggest setting up a pilot program to test if Blockchain will be a boon to the company. Blockchain pilot programs can be inexpensive and easy to set up, especially given the growing number of Blockchain-as-a-Service offering that include cloud-based infrastructure and easy-to-integrate APIs.

Initial costs, however, can also be high due to the scarcity of knowledgeable Blockchain developers, a lack of any "best practices" standards, IT infrastructure costs (such as server nodes) and lack of reusable components.

While market hype is now drawing in companies, enterprises should not rush into blockchain implementations, as "a partially-informed decision could result in costly mistakes, potentially destroying any organizational appetite for this powerful technology," according to the Everest Group. Companies should also develop a market intelligence team to track innovations in the blockchain ecosystem and follow what industry peers are doing. With those building blocks in place, companies can then conduct proof-of-concepts and real-world pilots to explore blockchain's potential and build up internal expertise in the technology.

Digital currency continues to be the "Wild West" of IT, as it has both legitimate uses but also is the currency of ransomware. Just beware of any "sounds too good to be true" situations here - it probably is.

New Phone from Zultys

Zultys is pleased to announce the immediate availability of the advanced ZIP 47G IP phone. The ZIP 47G is targeted at the busy professional looking for an attractive phone packed with features.

The features of ZIP 47G include:

- 4.3" hi-resolution color display
- Dual Gigabit Ethernet ports
- 10 LCD labelled programmable keys
- Bluetooth headset support with optional adapter
- Wi-Fi network support with optional adapter
- Full duplex speakerphone
- Electronic Hook Switch (EHS) support

The ZIP 47G supports up to 27 LCD labelled soft keys, plus wired and wireless headsets with optional Electronic Hook Switch (EHS) support. The ability to utilize Bluetooth headsets and leverage Wi-Fi network connectivity enhances the deployment flexibility of the ZIP 47G.

The phone is fully compatible with Zultys' MXIE and ZAC Unified Communication applications, allowing users to manage calls and messages directly from their computer and even receive instant messages on their phones.

The Zip 47G is compatible with the Zultys MX 12 release and later, so should be good for use for most of our current SIM2K client Zultys installations, if they are looking to upgrade their handsets. For any other company looking for a new unified communications solution in 2018, please contact SIM2K to learn more about the Zultys VOIP solution, and the power of MXIE, the desktop client, to help you manage your calling and to take advantage of the advanced options Zultys provides, yet at an economical price.

SIMformation is the monthly newsletter from SIM2K. Information presented here is designed to inform you of trends in the business world affecting information technology. For questions or comments, write SIM2K, 6330 E. 75th St., Suite 336, Indianapolis, IN 46250. Call us at (317) 251-7920 or e-mail sales@sim2k.com. Visit us at www.sim2k.com.

Google to Dump Chrome and Android?

You may have heard that Google is preparing a new unified operating system to replace Chrome OS (the operating system that powers Chromebooks) and Android (the operating system that powers most smartphones). Facts and forecasts are often packed together to persuade you of the premise that Google intends to replace Chrome OS and Android, and soon.

Google is in fact working on an open-source operating system called Fuchsia. Unlike Google's other operating systems (Chrome OS and Android), Fuchsia isn't based on Linux, but on a kernel called Zircon, which was originally intended to serve as a "real-time OS," meaning an embedded systems OS. However, the code also shows that Fuchsia could theoretically run on any kind of device, including internet of things appliances, traffic lights, ATMs, smartwatches, smartphones, tablets and desktops — devices Android, and also get Android running on Chromebook-like devices.

According to an unsupported set of predictions, Fuchsia will replace Android Wear, Android and Chrome OS, but run existing apps designed for those platforms. In other words, future Android phones would ship with Fuchsia instead of Android, and Chromebooks would ship with Fuchsia instead of Chrome OS. That would spell the end of Chrome OS and Android as we know them and usher in a single-platform app to run across all platforms.

The replacement of Chrome OS and Android with Fuchsia implies the termination of Chrome OS and Android. This is simultaneously the most common and also the least likely prediction. Chrome OS devices are on the rise in enterprises and increasingly dominant in the education market. Chrome OS is the most Google-y of operating systems because it's based on a cloud-first model. It's arguably the most secure business-friendly client platform on the market, and for the same reason. A great many OEMs are happily building Chrome OS devices. Google has no incentive to take risks with Chrome OS.

Android is now the world's biggest operating system. Close to 2 billion people use Android, and the Play Store is approaching 3 million Android apps, far more than Apple's App Store. But wait, you might say. If Fuchsia runs either Chrome OS or Android apps flawlessly out of the box (or both), then killing off these operating systems would be fine, right? The answer is yes.

But launching a new operating system of any kind is a difficult feat. Creating a new operating system that's ready for public use takes many years. And making one that runs apps from two distinct operating systems takes longer still. So even if Fuchsia is released as a general-purpose or mobile operating system, it wouldn't replace Chrome OS or Android for many years. They would co-exist. So as Mark Twain said, "rumors of my death are greatly exaggerated." Don't expect Chrome or Android to disappear.

"Random Tid-Bytes"

Dual-Screen Phones to Replace Laptops?

Phones have on-screen keyboards. Laptops have clamshell designs. The next-generation enterprise mobile device will have both. A dual-screen clamshell mobile device makes sense. *(Like they did a decade ago? ed.)* Smartphone makers want to maximize screen real estate. This form factor doubles it to the size of a small tablet. Tablet makers want portability. The dual-screen clamshell mobile enables a tablet to be folded in half and put into a pocket. Above all, dual-screen clamshell mobiles are super flexible. They could potentially be used in eight different "modes": Phone; Laptop; Book; 2-screen Single User; Tablet, Single-user Tent; Dual User Tent; and Smartphone. While there will be a market for very high-end tablets like the iPad Pro, or very low-end tablets like the Amazon Fire line, the midrange of the market will be gutted by dual-screen, clamshell smartphones, because they'll also serve as tablets when users need one. The coming year will usher in the first serious dual-screen clamshell phones — and perhaps begin to usher tablets right out the door.

Net Neutrality Update

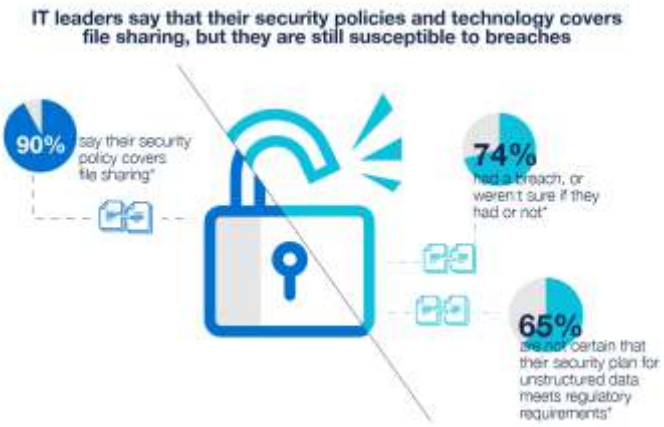
As discussed in last month's SIMformation, the FCC did take action to repeal the Obama Administration's rules on Net Neutrality. This has touched off a firestorm of protests from people who believe this means the end of the Internet. Proponents point out the Internet existed just fine up until two years ago when the Net Neutrality regulations were invoked, so this basically returns the Internet right back where it has "always been." So far, no ISP has made an effort to segment web traffic or to charge extra for streaming particular content, so the Internet continues as it always has. SIM2K will continue to watch for any movement in this arena and will advise you if any actions will impact our business users.

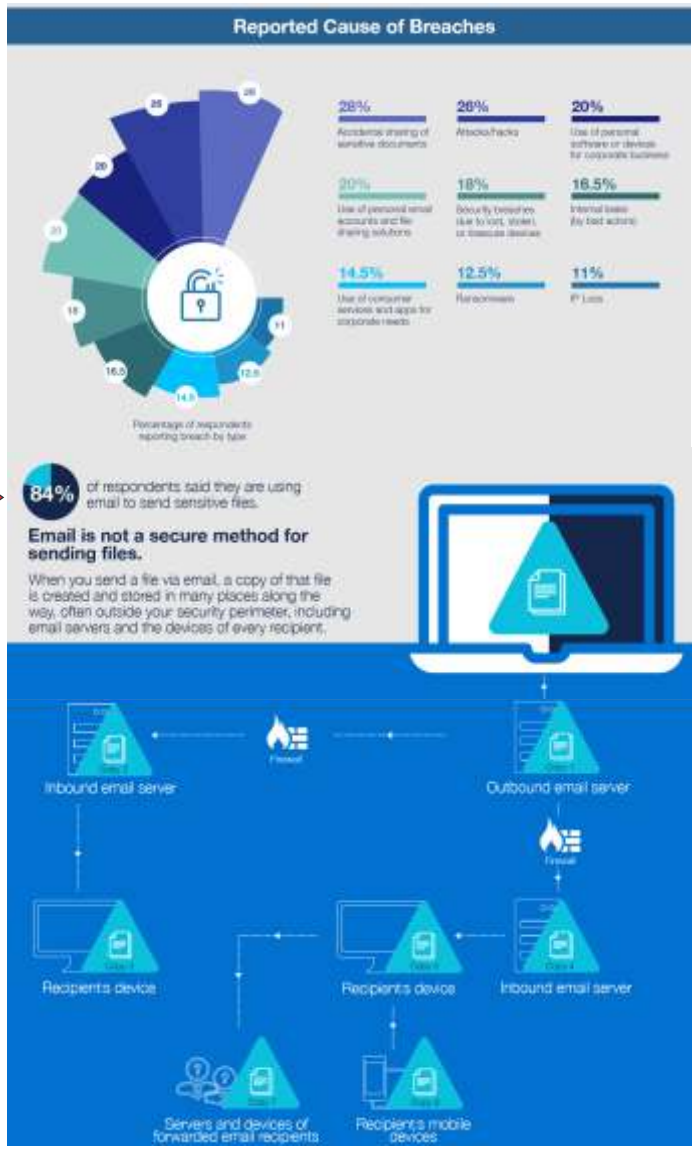
Microsoft Issue Buggy Patches (again)

Microsoft has admitted up to a couple of the known bugs in the December 2017 Windows10 version 1709 cumulative update, KB 4054517 – in particular, the stall at 99% download, and the completely bogus warning that the patch had failed to install with error 0x80070643. Sadly, several other problems with KB 4054517 have not been acknowledged. In addition, there are also problems going back to the November Patch Tuesday security update for Excel 2016, KB 4011220, which throws a "Cannot run the macro" warning, and for this month's Patch Tuesday security fix for Microsoft Exchange, KB 4045655. The Dec. 12 Exchange Server patch is an even bigger mess, which is "great" considering this patch was issued as a necessary bug fix from an earlier patch. This update affected Exchange services and failed to install some updates without notification to the user that the update failed. Microsoft says it is working on fixes for all these issues from last months' failed updates. If you are a SIM2K Critical Updates client, we are aware of these issues and stopped any of the updates at this time until the "fix is in." If you do your own updates, you should be aware of these problems and await Microsoft's next attempt to get it right.

File Sharing Leads to Security Issues

A recent study commissioned by Blackberry has found significant security gaps in the financial services industry. However, these practices are also prevalent in other industry groups and the results shed light on a real potential for information leaks.





If you are using e-mail as your primary method of file sharing in your company, you might need to re-consider this practice as it is not secure. SIM2K can help you devise a better solution that will still give employees access to critical documents but in a manner that ensures the integrity of that document and also to make sure only those authorized to see that information can actually access it. Call us for more details on security for your company.

Blackberry study as appearing in Computerworld 12/16/17

SIM2K
6330 E 75th St., Suite 336
Indianapolis, IN 46250
317.251.7920 • 800.746.4356
www.sim2k.com • sales@sim2k.com