Founded 1982
www.rcsi.org

The Rochester Computer Society, Inc.
a computer/tech club open to everyone

MONITOR

Vol. 35, No. 12 December 2017

"Your Computer User Group of the Air", Saturdays from 12:00 pm to 2:00 pm with Nick Francesco, Dave Enright, and Steve Rae. Broadcasting on JAZZ 90.1 FM from Rochester, NY.
Call 966-JAZZ (585-966-5299) or 800-790-0415

The RCSI '**Monitor**' newsletter can be found in most public libraries in Monroe County. *Free* copies can also be found in the following computer stores: Microworx, Just Solutions, TSC Electronics, and Pod Computers. Digital copies may be obtained from **www.rcsi.org** or my cloud storage at **http://tinyurl.com/tonydel-rcsi-newsletters/**.

Some Past Presentations:
Open Source and Free Software
Protecting Your Identity
Keeping Mobile Devices Secure
3D Printing, ENABLE project
Flash Drives-Not Just for Storage
Features, Mac OS X & Windows
Tablets, the Programs and Uses
Personal Finance Software
Amazing Browser Tips
Linux is Like Cars
Close up Photography

Member of apcug An International Association of Technology & Computer User Groups

Next Future Meeting
Tues, Jan 9, 2018
6:30 pm, Help's Half Hour
7:00 pm, Main Meeting and Presentation

In This Issue

Don't Get Hacked! Time to Get Serious About Password Safety	Brandpoint
Educating My Phone - Graduating to a Smartphone	Greg Skalka
How Can a Hacker Try All Possible Passwords If Systems Block the Login Attempts?	Ask Leo!
How Long Do Solid State Drives Really Last?	Michael Crider
Musings of an Apple Tyro	Lorrin R. Garson
Keep Your Wi-Fi off KRACK	Larry Greenemeier
Brain-controlled drones are here: What's coming in the next five years?	ScienceDaily
New technology to dramatically speed up home broadband	techxplore.com

Brandpoint, 10/17

Don't get hacked! Time to get serious about password safety

Top tips for locking down your online security .

We all know hiding your house key under the doormat is a terrible idea, but we do it anyway because it's a convenient backup. When it comes to safeguarding passwords, especially in a family setting, people often choose convenience over safety.

As families manage their digital information and online accounts, many end up opting for that less secure key-under-the-doormat solution. People are already sharing passwords, and their methods of sharing are not always the best. Some 41 percent of adults with online accounts admit to

Special Interest Group

Linux Sig

The workshop is the **third Saturday of each month**, at Interlock Rochester, 1115 East Main St. www.interlockroc.org

Enter through door #7 on the end of building, near *Comics Etc* and Goodman St. Find 'Interlock' on the intercom directory to get buzzed in and go upstairs to suite #200. We have experts on hand to fix problems and answer questions about Linux and FOSS (free and open source software). Bring your system in so we can help you get the most out of it. Hope to see you there.

Free, online
Virtual Technology Conferences,
presented by APCUG

Check back, next month
for the 2018
conference dates

---

sharing passwords with friends and family, according to an Americans and Cybersecurity survey by Pew Research Center. Yet, 90.8 percent of respondents say they know that having strong passwords helps them better protect their families.

Consider the number of security breaches that continue to make national news:
* In 2016, we learned the Yahoo data breach compromised 1 billion accounts.
* In that same month, we learned 167 million email addresses and passwords were stolen from LinkedIn.
* In September 2017, a security breach at Equifax was reported, exposing Social Security numbers and other personal data of 143 million users, which is nearly half the U.S. population.

Now more than ever, it's clear how important it is to protect our personal information online. According to a Verizon 2017 Data Breach Investigations Report, 81 percent of data breaches involve weak, reused or stolen credentials. That's significantly higher than the 63 percent it was in 2016.

"If you were to dig into the reasons behind these repeated, overly simple, shared passwords, it's actually pretty understandable as to how this happens," according to LastPass Senior Director of Product, Steve Schult. "The average person has some 200-plus logins. If you were to give each its own strong, unique password, that's way too many for one person to keep track of and remember, let alone all the other family members that might also use some of those accounts."

But there's no need to trade security for the convenience of digital access. With a password manager designed for individual or family use, you can create those strong passwords for all the accounts you and your family use, and store them within a secure vault that's accessed by a single master password only you know. These digital lockboxes protect your information under multiple layers of security, making it impossible for digital thieves to hack and access.

If you're debating whether to make the switch to a digital password manager, here's a few ways it can improve your family's online security and help stop the struggle with passwords.

Create rock-solid passwords: Most password managers offer a secure password generator that allows you to set and create a long, strong and unique password for every online account. You can create a password up to 100 characters long, including numbers and symbols. Another way to do it is by using the "passphrase" approach, meaning string together words that create a phrase. Be sure to steer clear of birthdays, anniversaries, street names and other specific personal details that can be found through a simple social media search.

Secure more than just passwords: There's an endless number of passwords and sensitive information you can store in your password manager, including banking logins, passport and license numbers, shopping accounts, email and social media passwords and more. By storing all of this information in your secure vault, you'll always have access to the information whenever and wherever you may need it.

Safely share passwords with family members: One benefit of a password manager that's designed for family use is that it lets you safely and conveniently store passwords and valuable documents in folders for flexible sharing with others in the family. LastPass Families includes unlimited shared folders, which means you can create multiple folders and store an endless number of passwords and share with those in your family. For example, you could put your banking account password into one folder and share access with your spouse, have another folder for your favorite streaming services and securely share access with the whole family. All the while, you can keep your personal accounts private.

RCSI Officers

Pres: Steve Staub 429-9877
srstaub1@rochester.rr.com
VP: Mark S. Lawson . . . 544-5377
mslawson51@peoplepc.com
Treas: Dennis P. McMahon
. 235-1260
denmac733@gmail.com
Secretary: www.rcsi.org
Help's Half Hour . . Jan Rothfuss

Board Members at Large

Bob Avery 385-4491
webmaster@rcsi.org, 9/20
Jan Rothfuss 347-6020
jan_rothfuss@hotmail.com, 9/19
Tony Dellelo 734-6149
tonydel@techie.com, 9/18

Standing Committees

Linux SIG: . . . Carl Schmidtmann
unixgeek@faultline.com
Programs: . . . . . Tony Dellelo
Webmaster: . . . . . Bob Avery
Membership: . . . . . Steve Staub
Monitor editor: . . . . . Tony Dellelo

Planning Meeting

Held on 1st Tuesday of each month at 7 pm, at St. John's Meadows, Briarwood building.

Newsletter Printing

The newsletter was printed at St John's/Chestnut Court by the printing group, with the help of Don Wilder (computer and printer operator). *We will try and print on the 1st or 2nd* ***Thursday morning,*** *following the monthly meeting.*

Use it as a teaching moment: Have a talk with your kids about how passwords are the keys to our digital lives, and how good password habits help protect everything from personal details to finances. Show them how to build a good password, and how tools like a password manager can create a safe way to access and share accounts. It's an important life skill that will help them protect themselves for years to come.

Plan for the digital afterlife: When there's a death or serious emergency, it turns out that state and federal laws, along with service agreements, can block your family from getting access to your online accounts. With a password manager that allows emergency access, family members can get into your password vault and have access to whatever they need.

If you're interested in learning more about LastPass or LastPass Families, visit LastPass.com.

President's Corner
by Greg Skalka, President
Under the Computer Hood User Group, CA

Educating My Phone - Graduating to a Smartphone

Though I have built many computers over the years, and used and experimented with lots of technology, for the longest time I have resisted getting the one tech item that now seems to be pervasive in our society - a smartphone. I've had mobile phones, but only "dumb" cell phones. I've had flip phones that could only place voice calls, and a slide phone that allowed talking and texting, but until recently I'd resisted getting a phone that provided access to the Internet. Now at last I am "graduating" to a true smartphone.

Now I'm not opposed to technology. I am an electrical engineer by profession, and currently work for a company designing digital radio systems that may be used to connect cell phone towers to the phone network. I have used computers since before the original IBM PC-XT. I have owned and used all manner of computers, laptops, tablets, Chromebooks, music players, GPS receivers and digital cameras and video recorders. I pay for a mobile phone plan that covers three smartphones (my wife and daughter have iPhones, my son has a Google Nexus), but I've never graduated from my dumb phone. Until now.

There are a lot of reasons I've held back until now. I'm pretty value-conscious (some would say cheap) and for a long time I felt having a smartphone was not worth the cost - mainly in the cost of the phone plan. When data plans were around $40 a month, and my home broadband internet service was about the same, it made me wonder why I had to pay twice; once to have Internet access at home, and again to have it away from home. The phones themselves are what I would consider pretty pricey as well. While none of the computers that I use today (desktop or laptop) cost me more than $500, this appears to be about the median price for smartphones.

While the capabilities of smartphones are impressive, the cultural phenomenon of the smartphone is not (at least to me). I really would like to be able to access the internet from practically anywhere, and look with a bit of envy at those searching the web and getting real-time traffic information while out and about. To scan a product bar code in a store and then search the web for additional information, alternatives and better pricing is very powerful. I don't feel a great need to have my emails with me wherever I go, however; I think being able to communicate via text messaging is plenty good.

For all the good that smartphones represent, I believe there definitely is a dark side. It seems almost everyone has a smartphone, and many can't seem to put them down. Opioid drugs are very useful in pain treatment, but when abused, they can be very addictive, and ultimately destructive. I see the same things in smartphones - a great and useful tool that has the potential for great abuse. Now maybe great abuse on an individual scale is uncommon, but I worry what these devices are doing to our society. I all too often see families seated at a table in a restaurant, with each family member devoting their full attention to their own smartphones rather than each other. My wife suffers from motion sensitivity and so does the driving whenever we travel together; this gives me the opportunity to observe the drivers in the cars around us. I've found it is not unusual to see half of those drivers holding their phones while driving, presumably talking, texting or worse. Unlike laptop computers, smartphones have had traffic deaths attributed to their use, and laws enacted to hopefully prevent their use in situations like driving, where the distraction could be dangerous.

While I was concerned about the added cost, part of my reluctance to getting a smartphone was my desire to not risk becoming "one of them", those zombie-like people that can't put their phones down. I never want to ignore those I am with in deference to these little electronic gizmos, or risk stepping out in front of an oncoming car because I've tuned out everything but that little device in my hand. Stephen Hawking and Elon Musk are smart guys, and they have both expressed concerns about the potential threat to the human race that artificial intelligence could pose if its development continues. In the same way, I fear we are well on our way to trading away our humanity for these addictive little handheld screens.

So, what made me change my mind and submit to the dark side of smartphones? Is it similar to the argument that "it's not guns that kill people, but people that kill people"? I do hope (and believe) I can ignore their siren song and not use a smartphone in an overtly antisocial manner.

In the end, several factors conspired to put a smartphone in my hand (unlike my slide phone, it is too big for my pocket). Though my slide phone served me well for many years, it has started to become unreliable. Though its built-in camera is poor by current digital camera standards, I found it very handy simply because it was almost always with me. I became dependent on its ability to photograph store product tags for items I wanted to research, and send photos of what I'm doing to my kids. Recently, however, it had started to fail me, more often than not taking photos that look like they were taken in Andy Warhol mode (colorful and cartoonish). Finally, attempts to use the phone camera were greeted with the screen message "Camera not available". It was not the lack of the Internet; it was the lack of a camera that pushed me over the edge.

At the same time, I found that phone plans have changed, with data included in our current T-Mobile family plan for each of us, whether we were using it or not. With extra charges for data overages replaced with data throttling when your monthly limit was reached, my concerns over an increasing bill were eliminated. I had been reluctant to change to a smartphone as I thought it would result in a bigger bill due to adding a data plan for it. As it turned out, I had been entitled to use over 2 GB of mobile data all along (and had only been using a few MB of data sending photos with my slide phone). I had the power to have a smartphone all along; all I had to do was click my heels

Computer Recycling

Some Residential Drop off Locations: **Call first**, to find out what is accepted, especially for 'tube type' tvs or monitors.

Pod Computers accepts most electronic waste (no tv's or crt's), located at 1925 South Ave, the wedge where South Ave and East Henrietta Rd meet. 244-2240.

Monroe County *ecopark* (Cathode Ray Tube TVs and monitors - $10 each credit/debit card only) 10 Avion Drive Rochester, NY 14624 Phone: (585) 753-7600 (Option #3)

Best Buy stores accept most electronic waste (CRT and some other TVs include a fee of $25 each)

Maven Technologies offers *free* residential drop off, 9:00 am – 4:00 pm (M-F), 1450 Lyell Avenue, Rochester, NY. The processing center is located on the NW corner of Lyell and Mt Read, behind the 'strip mall'. Go to the customer entrance. 458-2460.

together in the T-Mobile store (so to speak).

With my slide phone broken and data available in my phone plan, the only remaining issue to graduating to a smartphone this June was the device. Since my needs were modest, I expected the price to be modest as well. I consulted with my son, also an electrical engineer, on his choice for a smartphone, but found he had just copied a more knowledgeable friend when he bought his Google Nexus off the web. I looked on Amazon for unlocked smartphones and found promising candidates in the $120 to $170 price range, but concerns about being able to use these on our plan had me look at the T-Mobile web site. The best candidate seemed to be a Samsung Galaxy J3 Prime, which could be bought outright for $150.

Heading with my wife to the T-Mobile store (the phone account is in her name), I felt kind of like a vegan heading to In 'N' Out for a Double-Double, or a diabetic heading to the candy store. Like the recipient of a mail-order bride, I was filled with both excited anticipation and apprehension. Having a smartphone would allow me to do many things I had only dreamed of, like get answers to questions myself when out, rather than have to ask my wife to look things up on her phone. I could get apps and do fun things like check on traffic and control lights at home. Having a smartphone might change me, however. I might become antisocial. I'd have to find a way to carry this larger object and avoid breaking it or losing it. Would I be satisfied with what I had or want more?

At the T-Mobile store, I was able to have my contacts and my few feeble photos transferred from my slide phone to my new smartphone. They took out the 16GB micro SD card from my old phone and put it in my new phone, but I immediately began plotting to get a much larger SD card for the smartphone. I looked at cases for my new phone at the T-Mobile store but they all seemed expensive. I was able to get a nice case with belt clip (my initial experiment with carrying the phone) for a lot less. I didn't take the phone out much until I'd gotten the case, as I was concerned about damaging it. This caution proved to be justified, as I've already dropped the smartphone in the Fry's parking lot once (but the case protected it).

Now I've moved into the 21st century, joining the over 3 billion humans that use smartphones. The phones may be smart - let's hope all the users remain so.

From the July 2017 issue of Drive Light, www.uchug.org, president@uchug.org.

Ask Leo !

By Leo Notenboom, https://askleo.com/

Making Technology Work For Everyone

How Can a Hacker Try All Possible Passwords If Systems Block the Login Attempts?

Some hackers just go for the low-hanging fruit and try the most common passwords, and there is one scenario where brute force works very well.

//

I understand that my password, especially if it's not very strong, can likely be figured out by a computer driven program using trial and error. For example, all permutations, combinations of numbers, letters and special characters. What I don't understand is this – wouldn't a hacker, be it a person or a machine, have to actually try each and every one of these computer derived guesses on the sign-in screen of the website that they are trying to access to see if they get lucky? My experience tells me that after just a few failed attempts at entering a password, the website will not allow any more tries. So how in the heck are they able to try out all of the thousands of possible passwords that he comes up with?

What you've described is called a "brute force attack", and you're quite right; it's a rare system that allows such an attack to proceed past the first few errors.

However, hackers have other options.

Simple brute force

As you said, this type of attack involves the hacker trying to log in using your user ID with every possible password in turn.

Most good systems note that the same person has tried to log in unsuccessfully too many times and lock the account, either for a few minutes or an extended period of time. A brute force attack is most often attempted using a

computer, so locking the account for just a few minutes makes even the fastest automated attack impractical.

But to be honest, even when systems are operating at full speed, the log-in process is usually slow enough on its own to make this type of brute force attempt impractical anyway.

Not surprisingly, it's not what hackers do. If they're going to attack by simply logging in, they'll stack the deck instead.

Targeted brute force

You've probably seen those reports that come out every year revealing the top 100 most popular passwords. We use it as an example of how awful these popular passwords really are.

Don't use them.

But those lists are just the top 100. Hackers can and do "stack the deck" by taking the top 1,000 or 10,000 or 100,000 passwords and trying them in order of popularity. Given how many people use bad passwords, it's worth the hackers' time to try them, even if there are periodic delays.

Just the top 1,000 passwords tried against a large number of accounts will probably get them access to a surprisingly and depressingly large number of accounts.

But there's a very practical and reasonable way for hackers to try *every* possible password. They do it by stealing user account databases.

How passwords are stored

We need to focus on an important definition before we proceed.

I've talked and written before about how most services store your password. They create what's called a *hash* of the password.

Think of a hash as a kind of a one-way encryption that can't be undone. You can create a hash from a password, but you can't get the password from the hash. And it's statistically impossible for two passwords to generate the same hash.

When you set your password, the service creates the hash associated with it and stores the hash, not your actual password.

When you log in, the service again creates the hash of whatever you typed in as your password. It compares this hash with the hash it created when you set your password. If those two hashes match, then you must have typed in the same password this time as you did when you created the password in the first place.

In other words, if the hashes match, you typed in the right password, and the system allows you to log on.

Databases of passwords

Now that we've seen how passwords are stored, we can look at how hackers leverage that approach to their advantage.

You've probably heard about various data breaches at large companies. A hacker gets in and gains access to things they're not supposed to.

One of the goals of most of these breaches is to get a copy of the user account database. That's the list of user IDs *and password hashes*. Once they have a copy of that database, they can go to work.

Later, on their own computers, and at *extremely* high speed, they literally try every possible password. With each attempt, they create the hash; then they see if it's in the database they just stole. If it is, they now know the password for the user account that had that hash; it's the password that created the hash like they just did.

This is where password length and complexity come into play.

It's currently feasible to try all possible eight-character passwords in a short amount of time. That's why **most industry experts now say 12 characters is the new *minimum* length of a password**. The amount of time required to try them all increases exponentially each time you add a character to the length. It's just not practical for hackers to try all possible 12-character passwords today. It would take years, even with the best equipment.

So, yes, there are absolutely scenarios where hackers can and do try all possible passwords. They just don't do it by trying to log in with each one. Using those stolen user account databases, they work *offline* to figure out your password's hash. When they later arrive at the log-in screen, they know exactly what to type in, and only need one try to get into your account successfully.

It all comes down to good passwords

The lesson here, of course, is to choose long, complex passwords. The longer the better, in fact. I now use passwords with 20 random characters whenever I can. I let LastPass create and remember them for me.

Yes, it's possible that even those can be compromised by malware such as keyloggers, which is why I also advise adding two-factor authentication to your important accounts. With two-factor authentication enabled, even knowing the password isn't enough to get in.

* * * * * * SOFTWARE and HARDWARE * * * * * *

How-To Geek

How Long Do Solid State Drives Really Last?

by Michael Crider

When large-scale flash storage first came to the consumer market as an alternative to conventional hard drives, the biggest concern (aside from price) was longevity. Tech fans had a pretty good idea of the general reliability of hard drives, but SSDs were still something of a wild card.

But years later, the market for SSDs has matured considerably, and we've got a lot more data on…well, data. The good news is that SSDs are probably much more reliable than you think, and certainly at least as good as hard drives in terms of data retention and failure rates. The bad news is that SSDs tend to fail more often with age, and not with extended data reading and writing, as formerly predicted.

That means that you're no more likely to lose data with an all-flash setup versus a standard hard drive…but that it's still essential to keep a data backup of important files.

Before we go on to some of the testing, it's important to get a quick primer on some of the more technical terms associated with SSDs:

- **MLC and SLC**: Multi-Level Cell memory is cheaper and slower, generally found on consumer-grade SSD

drives. Single-Level Cell memory in enterprise and enthusiast-grade SSDs is faster and technically less prone to data loss.

- **Memory Block**: a portion of the physical memory on a flash drive. A "bad block" is inaccessible or poorly accessible to your computer, causing a lower-than-reported level of available storage and potential read and write errors for files and software.
- **TBW**: Terabytes Written. The total amount of data written and re-written to a drive over its lifetime, expressed in terabytes.

With that in mind, let's answer this question.

How Long Will They Last?

SSD vendors tend to rate the reliability of their drives on three factors: standard age (like any warranty), total terabytes written over time, and the amount of data written to the drive per specific amount of time, like a day. Obviously measuring by these three different standards will return different results based on methodology. And the very fact that there are three extremely loose standards for "wear" on a digital component should illustrate something to the end user: accurately predicting how long it will take a specific SSD to fail is more or less impossible. We can only give a very vague point of maximum possible data retention, after which using the drive will put you in danger of immediate loss of data and computer operation.

There have been several recent studies trying to determine a more precise lifespan for solid state memory. A few of the more well-known ones include:

A joint study between Google and the University of Toronto, **covering drive failure rates on data servers.** The study concluded that the physical age of the SSD, rather than the amount or frequency of data written, is the prime determiner in probability of data retention errors. It also determined that SSD drives were replaced at Google data centers far less often than conventional hard drives, at about a one to four ratio. But it wasn't all positive in favor of SSDs: they experienced higher uncorrectable errors and bad blocks at a much higher rate than hard drives over the four-year testing period. **Conclusion**: in a high-stress, fast-read environment, SSDs will last longer than hard drives, but be more susceptible to non-catastrophic data errors. Older SSDs are more prone to total failure regardless of TBW or DWPD.

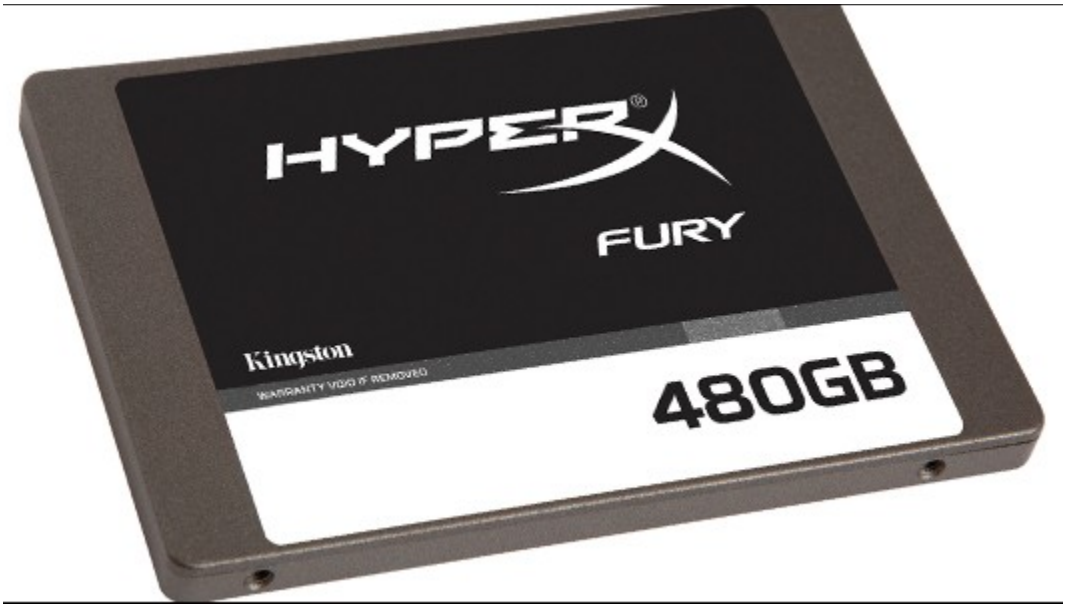
The Tech Report's study **on longevity between major brands.** Among six brands of SSDs tested, only the Kingston, Samsung, and Corsair high-end drives managed to survive after writing over 1000 terabytes of data (one petabyte). The other drives failed at between 700 and 900 TBW. Two of the failed drives, Samsung and Intel, used the cheaper MLC standard, while the Kingston drive is actually the same model as the one that survived, only tested with a similar methodology. **Conclusion**: a ~250GB SSD can be expected to die sometime before one petabyte written—though two (or perhaps three) of the models exceeded that mark, it would be wise to plan a

contingency in case your specific drive under-performs, even if it uses more expensive SLC memory.

Larger capacity SSDs, due to having more available sectors and more "room" to use before failing, should last longer in a predictable manner. For example, if a 250GB Samsung 840 MLC drive failed at 900 TBW, it would be reasonable to expect a 1TB drive to last for considerably longer, if not necessarily all the way to a massive 3.6 petabytes written.

Facebook publicly published an internal study **of the lifespan of SSDs used in its corporate data centers.** The findings were focused on the environmental conditions of the data centers themselves—for example, they came to the fairly obvious conclusion that extended proximity to high heat was damaging to an SSD's lifespan. But the study also found that if an SSD doesn't fail after its first major detectable errors, then it's likely to last far longer than overly cautious software diagnostic software. Contradicting Google's joint study, Facebook found that higher data write and read rates can significantly impact the lifespan of a drive…though it isn't clear if the latter was controlling for the physical age of the drive itself. **Conclusion**: except in cases of early total failure, SSDs are likely to last longer than indicated by early errors, and data vectors like TDW are likely to be overstated by software measurement because of system-level buffering.

You Don't Need to Worry



So taking all of this data in at once, what overall conclusion can we draw? Looking at these studies consecutively, it might seem like your SSD will burst into flames after a year or two. But keep in mind, two of the studies were on enterprise-class data centers, reading and writing data more or less constantly every day for years, and the consumer-oriented study was done specifically to stress test drives with constant use. In order to reach a petabyte of total written data, the average consumer would have to use his or her computer more or less nonstop for a decade, maybe even multiple decades. Even gamers or "power users" will probably never reach the stated maximum amount of data written for a drive under its warranty.

In other words: You'll probably upgrade your entire computer before your SSD fails.

Now, it's still possible for your SSD to fail in terms of its electronic components, just like any computer part. And your SSD's likelihood of data retention failure seems to go up the longer it's used. Since that's true, it's always wise to keep your critical data backed up to an external drive and (if possible) to a remote location as well. But if you're worried about your SSD failing at any moment, or being less reliable than your trusty old hard drive: don't.

Article was reprinted from the **www.howtogeek.com** website and was written in September, 2017.

The Demise of Windows Vista

On April 11th, Microsoft stopped all support for Windows Vista. This means no more security or online technical content updates from Microsoft. See http://bit.ly/2n5zJDv and http://bit.ly/2mzztJh. If you are still using Vista… you know the old saw about skating on thin ice. Microsoft will cease support for Windows 7 (Service Pack 1) on January 14, 2020; see http://bit.ly/2ngOvba.

Aging Mac Computers

In the last year or so, Apple has largely focused on the iPhone, iPad and Apple Watch—not Mac computers. Shown in Table 1 are the number of days (also expressed in years) since various models of Apple computers have been refreshed. This is as of March 18, 2017. Hopefully we will soon see this situation remedied. Apple computers are falling behind. See https://imac.macrumors.com.

Table 1: Time (days and years) Since Last Refreshed

Computer Model	Number of Days	Number of Years
iMac	523	1.4
MacBook Air	741	2.0
Mac Mini	885	2.4
Mac Pro	1,187	3.3

Interestingly, Seamus Bellamy, writing in *PC World,* has decided to abandon his Mac for a PC (see http://bit.ly/2nvWwGH; see also http://bit.ly/2mSYhPG). One of his numerous complaints is Apple's aging computers. See Seamus' article in *PC World* entitled "Switching from Mac to PC: Choosing a laptop"; see http://bit.ly/2nze9W4. Bear in mind *PC World* is generally more favorable toward Microsoft than Apple. It will be interesting to see how this plays out.

Update to macOS Sierra

In early March macOS Sierra 10.12.4 beta 5 was released to developers and public beta testers. Changes to Siri,

Dictation, and Apple's PDF API are expected. Night Shift, which is currently available on iOS devices, will be introduced to Mac computers. Night Shift, which adjusts the color of display after sunset reducing bright blue light that can adversely impact human circadian rhythms and make it harder to sleep, will be introduced to Mac computers. Other changes can be expected but this will not be a major OS update.

MacBook Pro Battery Stamina

Apple claims the battery in this laptop will last up to 10 hours (see http://apple.co/2nza3Ag), but there has been grumbling that it doesn't last anywhere near that long. It turns out that with intensive GPU/CPU use the battery lasts around 80 minutes. For details, see http://bit.ly/2jKUzmm.

Google Chrome

If you use the Chrome Browser, look at http://bit.ly/2kAoYom. This article in *PCWorld* is entitled "10 Frustrating Google Chrome Irritations and How to Fix Them". But there's more than that—there are workarounds on how to mitigate some of these limitations.

Quantum Computers

Quantum computing is in the news these days. What is it, other than being mysterious and quirky? In classical computing a "bit" can have two states: "0" or "1"… "yes" or "no", "on" or "off", etc. In quantum computing, a "qbit" (aka "qubit") can have three states "0", "1" and "0 and 1" simultaneously. Quantum computing is based on quantum mechanics that began with Albert Einstein, Max Planck and other giants of physics in the early 1900's. Why does it matter? Quantum computing has enormous potential for drug design, weather forecasting, communications, "big data" analysis, traffic control and other areas that require massive computer power. The March 11th-17th issue of *The Economist* features quantum computing (p.11 and the special section following p. 44, entitled "Here, there and everywhere"). Also see, as examples, http://bit.ly/2nr7PTL, http://bit.ly/2mvYKnq, and http://bit.ly/2mMANdw. Don't expect to have a quantum computer on your desktop or in a tablet anytime soon, but you don't need it for surfing the Web, email and controlling your garage door.

One Bit on One Atom

On current hard disk drives it takes about 100,000 atoms to store one bit of information. Scientists at IBM's Almaden Lab in San Jose, California have achieved the ultimate. They have managed to store one bit of data on a single magnetized atom of Holmium (Ho). Don't expect to buy a disk drive using this technology at Micro Center anytime soon. It's strictly experimental. See http://bit.ly/2mxDA9A.

Ransomware on Dramatic Rise

According to articles from *PC World* (see http://bit.ly/2mC6tBw) and *CIO* (see http://bit.ly/2mQ1g9O), Ransomware attacks rose from 3.8 million in 2015 to 638 million in 2016. The article in *PC World* contains good advice on how to prevent such attacks and what to do if you get hit.

KrebsOnSecurity

From time to time I have commented on KrebsOnSecurity (https://krebsonsecurity.com/) as an excellent source for information on current security issues. It makes for chilling reading, but I strongly recommend periodic reading of this Web site.

Article was taken from the May 2017 issue, PATACS Posts, www.patacs.org, newslettercolumnist@patacs.org.

Keep Your Wi-Fi off KRACK

By Larry Greenemeier

It seems every week we find out that someone broke into a big company's databases—like the recent Equifax data breach—and made off with millions of credit card numbers, passwords and other valuable info. And now a new kind of worry: someone could hijack your wireless home network and steal your info from under your nose.

That's the possibility raised by a couple of cybersecurity researchers from the Catholic University of Leuven in Belgium. The problem, they say, is a flaw in the very protocol meant to make wi-fi secure. That protocol is called Wi-Fi Protected Access II, WPA2. And WPA2's weakness could allow an attacker within physical range of your wi-fi network to make a copy of that network that they could then control. The researchers call their approach a key

reinstallation attack, or KRACK.

It's important to know that a KRACK attack remains a hypothetical for now. The scientists realized the threat while investigating wireless security. They'll present this research on November 1st at the Computer and Communications Security (CCS) conference in Dallas and in December at the Black Hat Europe conference in London.

In their KRACK scenario, wireless devices would be fooled into connecting to the bogus network. And the attacker would be able to access all of the info that devices send and receive while connected to that network—even if that info has been encrypted. Android and Linux would be especially vulnerable because of how their encryption keys are configured.

One measure of protection against such an attack would be to make sure that you've installed the most up-to-date versions of your apps, browsers and wireless router software. Updated software is most likely to include the security patches needed to avoid falling victim to a KRACK attack. Because chances are that KRACK won't remain simply a proof-of-concept for long.

Editor's note: the above text is a transcript of this podcast, dated October 19, 2017 and reported in Scientific American.

* * * * * * * TECH CORNER * * * * * * *

Science Newsletter

Brain-controlled drones are here: What's coming in the next five years?

Single unmanned autonomous vehicles (UAVs) directed by joysticks, radio controllers, and mobile phones are already accomplishing a variety of useful tasks, such as aerial photography and security patrols. But using multiple drones requires multiple human operators, and this presents a coordination problem.

Now a single operator using emerging human-brain interfaces can control a swarm of drones, making possible new classes of applications, according to Panos Artemiadis, director of the Human-Oriented Robotics and Control (HORC) Lab at Arizona State University.

Artemiadis thinks it is likely that drone swarms using human-brain interface mechanisms will, in the next three to five years, make inroads where individually controlled UAVs cannot. Here are a few of the drone applications that are now within reach:

Search and Rescue Missions

Humans will collaborate with swarms of robots in search and rescue scenarios. The brain-robot interface enables control of many robots at the same time, and it scales the ability of a robotic team to cover larger areas in less time. If the controller detects something in the video stream that warrants closer surveillance, the swarm can be directed to close in on that area.

Fire Fighting

Armed with infrared imaging equipment, a drone swarm can be used to track the spread of a forest fire over large areas in real time, allowing firefighters to adjust their plans accordingly. The human controller can follow a reported change in weather conditions, such as a shift in wind direction, with a swarm of drones to determine if the fire has jumped to a new area.

Agriculture Analysis

Teams of drones will oversee and analyze large agricultural fields -- creating topographic maps for soil analysis and irrigation planning. In addition to being outfitted with cameras, aerial drones will use sensors to identify necessary irrigation adjustments and scanners that can identify crop infections or infestations. Some drone systems are already being used for crop spraying -- swarms will be able to accomplish the task more quickly and efficiently.

Entertainment

As drones enter the entertainment arena, we will begin to see mind-controlled drone swarms for events. For example, a single person could operate a fleet of drones shooting photos and videos at an outdoor concert or sports venue, narrowing in on spectator activities for display on the Jumbotron. And while Lady Gaga's Super Bowl drones

were controlled by a central computer (and filmed in advance of the show), smaller swarms can be managed by a single human for smaller light displays or to drop gifts (t-shirts or CDs, for example) into a crowd.

Cyber-physical surveillance systems

Understanding brain-drone interfaces allows building cyber-physical surveillance systems that combine human intuition and experience with the sensing capabilities of multiple drones. This would allow more efficient and accurate surveillance systems than what is now available -- especially for large, security sensitive events like bowl games, marathons and political rallies.

Editors note: taken from Arizona State University (ASU). "Brain-controlled drones are here: What's coming in the next five years?". ScienceDaily, 29 September 2017.

New technology to dramatically speed up home broadband

Provided by University College London (UCL)

Slow Internet speeds and the Internet 'rush hour' - the peak time when data speeds drop by up to 30% - could be history with new hardware designed and demonstrated by UCL researchers that provides consistently high-speed broadband connectivity.

The new receiver technology enables dedicated data rates at more than 10,000 megabits-per-second (Mb/s) for a truly super-fast, yet low-cost, broadband connection to every UK home.

"UK broadband speeds are woefully slow compared to many other countries, but this is not a technical limitation. Although 300 Mb/s may be available to some, average UK speeds are currently 36 Mb/s. By 2025, average speeds over 100 times faster will be required to meet increased demands for bandwidth-hungry applications such as ultra-high definition video, online gaming, and the Internet of Things", explained lead researcher Dr Sezer Erk?l?nç (UCL Electronic & Electrical Engineering).

"The future growth in the number of mobile devices, coupled with the promise of 5G to enable new services via smart devices, means we are likely to experience bandwidth restrictions; our new optical receiver technology will help combat this problem."

For the study, published today in *Nature Communications* and funded by the EPSRC UNLOC Programme and Huawei Technologies, scientists from the UCL Optical Networks Group and the University of Cambridge developed a new, simplified receiver to be used in optical access networks: the links connecting internet subscribers to their service providers.

To maximise the capacity of optical fibre links, data is transmitted using different wavelengths, or colours, of light. Ideally, we'd dedicate a wavelength to each subscriber to avoid the bandwidth sharing between the users. Although this is already possible using highly sensitive hardware known as coherent receivers, they are costly and only financially viable in core networks that link countries and cities. "Their cost and complexity has so far prevented their introduction into the access networks and limits the support of multi Gb/s (1 Gb/s=1000 Mb/s) broadband rates available to subscribers," said co-author and Head of the Optical Networks Group, Professor Polina Bayvel (UCL Electronic & Electrical Engineering).

The new, simplified receiver retains many of the advantages of coherent receivers, but is simpler, cheaper, and smaller, requiring just a quarter of the detectors used in conventional receivers.

Simplification was achieved by adopting a coding technique to fibre access networks that was originally designed to prevent signal fading in wireless communications. This approach has the additional cost-saving benefit of using the same optical fibre for both upstream and downstream data.

"This simple receiver offers users a dedicated wavelength, so user speeds stay constant no matter how many users are online at once. It can co-exist with the current network infrastructure, potentially quadrupling the number of users that can be supported and doubling the network's transmission distance/coverage," added Dr Erk?l?nç.

The receiver was tested on a dark fibre network installed between Telehouse (east London), UCL (central London) and Powergate (west London). The team successfully sent data over 37.6 km and 108 km to eight users who were able to download/upload at a speed of at least 10 Gb/s. This is more than 30 times faster than the fastest broadband available in the UK, today.

"BT Openreach recently announced that fibre access is a key focus and must improve. With high-capacity broadband a priority for the UK government, we will be working to reduce the electrical power requirements of this technique to make this commercially viable in the nearest future. We believe that it has real potential to provide high-speed broadband connectivity to every home, which will support the growing digitally enabled economy in the years to come," concluded Professor Bayvel.

More information: M. S. Erkılınç et al, Bidirectional wavelength-division multiplexing transmission over installed fibre using a simplified optical coherent access transceiver, *Nature Communications* (2017). DOI: 10.1038/s41467-017-00875-z.

Editor's note: this article was copied from the https://techxplore.com website, October 19, 2017.

Help's Half Hour

by Jan Rothfuss

Q: A member's keyboard is wireless. Last tried Alt-F4 and it no longer communicates.
A: Keyboards can fail.

Q: Octo 375 . Once logged in, the remote keyboard no longer works. He then must use the on-screen keyboard.
A: Likely there is a corrupt user file. It was suggested that he create a new user account. This may then be able to use the keyboard. If this does not work, you may have to install a fresh copy of Windows.