Founded 1982
www.rcsi.org

"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

The Rochester Computer Society, Inc.

a computer/tech club open to everyone

MONITOR

Vol. 36, No. 03 March 2018

Tues, March 13, 'The Linux Software Store',
by John Kennedy ("Free-John"),
East-Central Ohio Technology Users Club

Tues, April 10, 'New and/or Obscure Web Browsers, Related Software, and Recent Security Concerns'
by Mark Zinzow

In This Issue

My Take On The Meltdown – Spectre Issues

By Hewie Poplock

The recent revelation of the Meltdown & Spectre vulnerabilities has created a lot of discussions. For the non-techie, it is extremely confusing. Even for the techies, it is confusing. The issue is not a Windows issue, nor a Mac issue, nor a Linux issue, nor a ChromeOS, or an iPad issue. It is not an Intel or an AMD issue. It has to do with the way computer processors (the main chip in all computers, tablets & phones) are all being programmed to speed up computers. This includes almost every computer manufactured in the last 20 years.

All of the operating systems are being patched. All of the security

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, **Virtual Technology Conferences**, ONLINE
presented by APCUG

Saturdays: 5/5, 8/18, 11/3

For Conference Description & Registration Links, go to apcug2.org/category/ **virtual-tech-conference**

---

software (the anti-virus & anti-malware) are being patched to work with the operating system patches and to avoid interfering with the OS.

Because of the patches, every computer tablet, & smartphone may experience some slowdowns. The patches are being rushed out to all computers. While it is actually a CPU chip flaw, the fix seems to be a software one. Eventually, new chips will be designed differently and new computers will regain lost speed.

Some articles that I have read stated that every computer needs to be scrapped and replaced. However, I have not read if there is even a chip that does not operate without the flaw. My hope is that all systems get patched quickly and then the speed issues are addressed fully. It is everyone's responsibility to upgrade their operating system as soon as updates are available to keep their systems as secure as possible, as well as working as intended. Yes, sometimes updates & patches cause new issues, but they too must be addressed.

I am looking for an ideal explanation of the Meltdown & Spectre issues. One that helped me understand was at https://blog.cloudflare.com/meltdown-spectre-non-technical/ and also a 7.5 minute video from Leo LaPorte at TWIT at https://twit.tv/shows/twit-bits/episodes/4665.

Taken from Hewie Poplock's website, https://hewie.net.

Introduction to Personal Digital Security and Privacy

Presented by Robert Hurlbut
Meeting review by John Kinkopf
Member of Danbury Area Computer Society, CT

Our guest speaker at the August general meeting was Robert Hurlbut, an independent software security consultant and co-host of the Application Security Podcast. Robert delivered an excellent talk that covered many aspects of the wide field of software security. An expert in the field, he managed to provide lots of useful information without becoming too technical.

Asked from the audience which anti-virus software he uses, Robert answered rather provocatively: none! Most in the computer security field don't use an anti-virus software . . . . though he keeps Microsoft's Windows Defender on, included with Windows 10. Why? He explained that those in the security field live in a secure way, while anti-virus software usurps elevated privilege of one's system, more than any other application. We don't know if anti-viruses have faults in their code or security issues. And the majority of attacks these days are not the viruses of old, but things like ransomware that anti-viruses can't find, no way.

Updating Windows is essential to combat ransomware, and using Windows 10 over Windows 7 is his recommendation; definitely don't use Windows XP or earlier versions. Where a couple years ago there were 100,000 new virus patterns per year coming out; now it's 200,000 per DAY with which anti-viruses can't keep up. Thus, restrict your machine from executing things without your permission, meaning beware of clicking on things, and don't surf the internet as administrator, but rather in a user account. He also mentioned that there have been recent [but disputed] allegations against Russia-based anti-virus Kaspersky Labs.

Our connected world is a tracked world. Many TVs, home devices, and Echo or Home personal assistants listen to you. Many smart devices are security openings. Stores you enter may try to hook up with your phone's wi-fi to find out things about you. Credit card purchases leave footprints. [Yahoo scans my Trenton Computer Festival emails to pitch me "Meet Trenton Singles" ads. They guess and list my email recipient's phone number ("No, an out-of-state

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.*

friend's church"), and "related contacts" as I compose.]

Private photos that iPhones backed up to the iCloud were obtained by fooling celebrity victims into divulging passwords with phishing emails. [Websites derive revenue from letting Facebook, Twitter, and marketing analysts observe which can be blocked by the NoScript extension for Firefox.]

Showing an RFID shield, Robert told how his Fitbit activity tracker began flashing numbers and making strange noises at the DEF CON hacker convention. Though visitors are warned to turn off any Bluetooth device at hacker conventions, a Fitbit's listen remains on. He's refraining from connecting it to anything until he can test it for tampering on a laptop he can wipe.

Get rid of many routers known to have vulnerabilities. Buy your own wi-fi equipment, using your own router over those an ISP provides, so you're managing your wi-fi instead of them. Use WPA 2 for your home wi-fi encryption; DON'T use WEP.

Virtual Private Networks (VPN)

To provide a secure channel to network servers over the internet, companies commonly use Virtual Private Networks for off-site workers. Phones can also be connected by VPN. Free personal VPNs offer privacy, not anonymity — you pay by providing info of your use that may be sold. Robert advises, nothing is free; don't use a free VPN. Use VPNs when you can, and only reputable pay VPNs [$60-$120/yr]. [Websites rate VPNs.] Robert subscribes to F-secure Freedome; it logs attempts stopped to track you and how much transmitted data was protected; they've been a reputable provider for 25 years. PIA is a VPN recommended by publications as doing minimal logging of the user's IP address and usage. For banking Robert answered that he would use a VPN, but they raise banks' suspicions of your authenticity. Asked about using a VPN to bypass media play geo-restrictions, Robert followed up by email that he once used ExpressVPN, and gave these references:

https://thevpn.guru/how-bypass-geo-restrictions-location-errors/
https://www.bestvpn.com/best-bbc-iplayer-vpn/

Audience members pointed out that governments may require VPNs to provide their logfiles of users. A VPN user in the audience shared that PIA's encryption processing made his battery life prohibitively short, in his experience. OpenVPN is open source; keep its patches up-to-date. OpenVPN how to: https://openvpn.net/index.php/opensource/documentation/howto.html

Browsers > Tor > Tails

Unfortunately, browsers track you. While Apple is good at security, their Safari browser lags; but, at least it excludes Flash, notorious for having security and reliability issues. [July News Flash: Adobe will pull the Flash plug-in in 2020.] Search engine DuckDuckGo.com claims not to track you . . . they say. URLs beginning with https provide improved communication security over http sites.

By relaying online communication through multiple nodes on its volunteer network around the world, free download Tor (The Onion Router) anonymizes a web surfer's identity and point of origin. Once the route for each use is established, one surfs the internet via Tor's modified Firefox browser – during which all other browsers must be closed for Tor's anonymity to be effective. Downsides are that while preserving your web anonymity on your end, many websites recognize Tor exit nodes, and place restrictions. For example, Wikipedia restricts edits made through Tor; BBC blocks its use to access iPlayer. And Tor's practicality is limited by slowed browsing from bouncing communications around multiple anonymizing nodes in world locations of varying internet speeds. Only download Tor from the Tor Project website: https://www.torproject.org

Tor is used to access Tor sites on the dark web which Edge, Google, and Chrome won't. Because it's possible that data may still unmask you, the next step is to use Tor in Tails.

Tails (The Amnesic Incognito Live System) is a live operating system the user boots from a USB drive or DVD for the purpose of having no connection to anything on the PC, say a library PC, just the network. When your session is finished no data is saved, everything is anonymous, and traces are not left when you disconnect. But associating with, for example, your email or Facebook would give you away, of course. As using your home computer would identify you to your ISP. It's better to get a dedicated laptop with completely separate email and other accounts that you never use in ways to identify you. The Tails website: https://tails.boum.org

Passwords

Early August News Flash: Robert Burr, responsible for the 2003 recommendation that secure passwords include upper and lower-case letters, and symbols that render remembering passwords difficult, made the media rounds rescinding the suggestion, or "|\|3\/€R /V\1|\|D." His, and Robert's current thinking is to use long passphrases – passwords composed of words strung together into a nonsense phrase you can remember. [For example, "A wet duck only flies at midnight," "The blue sun melts the wet snow" – from TV's "Get Smart"]

The "Have I Been Pwned?" website is a free service to which one submits their email address. The site, maintained by Australian Troy Hunt, will reply if the account is found among the millions breached, along with when, what, and where it was found, say perhaps in Pastebin, where a lot of stuff happens. You may also sign up for its Notify Me service, to be notified in the event future account compromises are found, for which Pwned needs to save your email. Robert has met Troy; the site gets some financial support but he does this mainly as a labor of love. Website: https://haveibeenpwned.com

A Password Manager (software) helps you manage your passwords with one master password that should be chosen to be especially difficult to crack. Password Managers can also manage security questions. Security question answers you choose need not be truthful, and should not be obvious. The password manager Robert uses is Blur, often recommended in books, which also can create virtual credit cards for you. Blur hasn't shown up in any breaches or other problems, while 1Password and LastPass have had reported security fallibility.

Two-factor authentication (2FA)

An example: Upon entering my account password, YouTube requires that I submit a code sent to my email (or phone). Robert likes it; I feel my YouTube account is more secure. But he thinks that it's crazy to give oft-hacked Yahoo his phone number. The website TwoFactorAuth.org lists whether or not websites support the additional security of 2FA.

Computer Recycling

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

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.

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.

Email

All emails are wide open. [Like my ballot at the Putnam County polling place!] They are transmitted from server to server, where hackers can view them along the hops. Even if you delete an email, the email services have made copies for sending redundancy. Be wary of clicking on email links and attachments. For privacy consider premium email services based outside the U.S. that encrypt. OpenPGP.org can be tried for encryption. A member of the audience reported using it in Gmail. The cable email accounts are worse regarding sharing your email information. Don't ever send forms with your social security number via email. [Send word documents only as PDF files, for with

Word file hidden histories a recipient could work back all your revisions, back to the resume I started writing this review over!]

Credit Cards

Robert said your health care records are worth even more to criminals. Check your credit report annually, at the beginning of the year. A few months later check Experian and Transunion for whether anyone is opening an account in your name. Robert found someone had opened an account under a previous address. One can download them or receive them by regular mail, but don't have the reports sent by email. Consider putting fraud alert and credit freezes on your credit card.

Beware of credit card skimming. July News Flash: wafer-thin "insert skimmers" stealing bank card information at ATMs are proliferating. August News Flash: tiny gas pump skimmers transmitting credit card information, as Robert mentioned, are featured on TV news. Robert mentioned that credit cards with chips are partially better, but not as good as in Europe, where a PIN is required, too. At locations credit card skimmers target, it's better to use a prepaid card or Apple Pay. But Apple Pay's one-time token uses near field communication (one needn't contact, but be in proximity) and there are devices the hacker can use to connect and obtain information.

Iconic hacker Kevin Mitnick advises having someone else buy your debit cards so video cameras don't record that it's your purchase. NSA whistleblower Edward Snowden did this, along with using Tails.

Mobile Security

Update to the latest operating system version and patches. [Ha! Google no longer supports Android versions predating 4.4.] For iOS definitely get the latest version, 10.3.3, which patches a chip vulnerability that was exploited at the Black Hat hacker conference. Passwords or passcodes protect your device. Adjust your permissions per app to, "No, no, no, no." Robert keeps his Uber car service location permission set to Never, except for the few minutes he needs to switch the permission to Always to use the app. Robert answered how to, for an Android phone, go to Application Manager, click on the app, and it should show you the permissions, at least since the 6.0.0 Marshmallow release. Anything version 5 or below, you couldn't do this. For Android, you definitely want an anti-virus. Sync, back-up your data, and install a phone finder app. It is very important to turn off wi-fi and Bluetooth when you're not home or not around trusted endpoints, which is nearly everywhere. Turn them off when they are not needed.

Pineapple is a popular device at the hacker conferences. If your phone has ever been connected by wi-fi it retains that information, and connects when in range to any of them when its wi-fi is on. The Pineapple connects to your phone, without your knowing, by pretending to be one of its former wi-fi connections.

The most secure mobile phones are the basic flip phones, turned off [in an RFID shield]. Tether your mobile phone to a hotspot in lieu of wi-fi or Bluetooth. Law enforcement uses fake cellular towers to spy. [August News Flash: Android messaging apps were found carrying SonicSpy trojanware to spy on audio, take control of phone cameras, and nearly all of a phone's functions.]

Security News Sources

Robert said that he keeps current by following several security news sites on Twitter. KrebsOnSecurity.com is an oft-referenced website, widely sourced when it detailed how customer accounts were hacked though Target's air-conditioner computers. [One can subscribe to his email newsletter.] Robert has Google searches set up to feed emails when certain terms come up such as router or VPN. One audience member subscribes to Wire's news feed, another visits https://www.social-engineer.org .

Books Robert Recommends

**The Complete Privacy and Security Desk Reference: Volume 1: Digital – Michael Bazzell and Justin Carroll
**Hiding from the Internet: Eliminating Personal Online Information – Michael Bazzell
**Personal Digital Security: Protecting Yourself from Online Crime – Michael Bazzell
**The Art of Invisibility – Kevin Mitnick
**How to Be Safe in the Age of Big Brother and Big Data – Kevin Mitnick

From the Danbury Area Computer Society, CT, www.dacs.org, dacseditor@dacs.org.

Can My Computer Be Hacked If It's Turned Off?

Hacking a turned-off computer requires a few mistakes on your part. It's unlikely, but possible.
//
In general, can a PC with no remote software be hacked if it is powered off? The power supply and the Internet cable are still connected to the PC. In my discussions with others, 50% say yes, 50% say no. An Internet search was also divided in response with no agreement.

It's a *very* unlikely scenario that could allow a turned-off computer to be hacked. I'll describe it and show you how to prevent it.

Fifty percent say no?

Welcome to the world of technology, where there are very rarely black-and-white answers. One of my most common phrases (that I get kidded about by my assistants) is: "It depends." There are rarely yes-or-no answers to technological questions. The real answer is usually nuanced and depends on many factors. This happens to be one of them.

Hacking a turned-off computer

The good news is that in general, the answer is "No." Your PC is off; it's not doing anything. Unless you've taken extra steps described below, the PC will not be able to be restarted and hacked from outside if it's turned off, even if you leave it connected to the Internet and to power.

The exception to the rule is a feature that, when enabled, allows a PC to be remotely turned on and booted. In short, the network adapter for the computer is not turned off completely, but instead monitors for specific instructions that tell it to wake up. When those instructions are received, power is restored to the computer and it boots. In such a scenario, if the PC has been configured to respond to the remote requests, then the PC could be turned on and booted remotely. At that point, if the PC did not have appropriate security software installed (say it was not behind a firewall and it did not have anti-malware tools), then it is *conceivable* the PC could be hacked remotely, even though it was powered off.

One caveat: standby

It's not uncommon for a laptop to be placed into standby mode only to wake up on its own a while later. The exact reasons this happens vary — I can't give you a simple explanation. There is a simple work around, though: if you find your laptop waking up on its own, and that concerns you, don't use standby. If it works for you, that's great, but I generally avoid standby for a variety of reasons, including this one.

Allowing remote access

Hacking a turned-off machine is *extremely* unlikely. A lot of things have to line up for it to happen. You have to have this remote power-on ability (Wake on LAN) turned on in the network settings, and most computers do not. In most cases, it's a setting in the UEFI or BIOS you have to turn on yourself. If you haven't turned it on, then it's probably not on. The PC also has to be fundamentally insecure. In other words, it has to be vulnerable to be being hacked when it's running. That's something you can control by putting appropriate security measures into place.

So, as I said, it's possible.
It's just extremely unlikely.

Ask Leo !
By Leo Notenboom, https://askleo.com/
Making Technology Work For Everyone

Are USB Ports Going Away?

All technology changes, and yes, USB ports will someday disappear. "How quickly?" is the real question. I'm not terribly concerned.
//
At least two articles on the future claim that either USB sockets and/or Flash drives will disappear in 5 years or more. I use mine daily. Should I stock up on flash drives while I can? The article(s) in question predict the USB port's demise on two things: cloud storage replacing local, physical storage, and smaller mobile devices that leverage the cloud with no ability to connect to external storage devices.

The problem is, they're absolutely right: much of the technology we take for granted and rely on today will be replaced by something. The question isn't whether it will happen; the question is: when?

The lifespan of USB

To address USB specifically, I don't believe the end is anywhere close to near. Connectors continue to change from time to time, necessitating conversion cables or adapters, and newer versions of the interface continue to get faster and faster, but ultimately, USB has become too ubiquitous for it to disappear any time soon.

USB is the most commonly-used interface for attaching just about anything to your desktop computer, your laptop, and in many cases, your mobile phone. Particularly for mobile phones and small electronic devices, and even some laptops using USB-C, it's also become the most efficient and ubiquitous power-delivery system for recharging device batteries — to the extent that these days, hotels often provide multiple USB ports in your room to recharge portable devices.

I fully expect to be using USB-something well into the next couple of decades. After that, who knows? But I'm not worried about the devices I have today.

The problem with hoarding

On one hand, stocking up on flash drives sounds like a way to prepare for their eventual demise, whenever it happens. There are two problems with that approach. The first is that it'd be the equivalent of stocking up on floppy disks 20 years ago because you heard that the floppy drive was on the way out. Today you've be left with a pile of obsolete disks and very few drives to use them in. If the USB port truly is on the way out in a time frame that will impact you, you might find yourself in a similar situation: plenty of flash drives, and nowhere to use them.

The second problem is that today's "huge" is tomorrow's "tiny". This is particularly true for external memory and disk devices, including CF, SD, and uSD cards as well as USB thumb drives.

Sure, you might stock up on whatever size is popular and cheap today, only to find that in 10 years, it doesn't have anywhere near the capacity required for whatever you'll be using it for then. I've got this fantastic little 32MB (megabyte) compact flash card that was originally primary storage on one of my older digital cameras. I can insert it into my current camera, but it doesn't have the capacity for even a single image.

Rather than hoarding them, better to just buy them as you need them. Your needs, as well as their capacity and speed, will no doubt continue to increase over time.

Obsolescence and betting on the right horse

Product obsolescence is generally market driven. As long as there's a demand, and whatever comes along to replace it doesn't create a more compelling demand, USB should be around for a long time. But in part, it's also a gamble. As I said, someday the USB interface will join the floppy disk as an interesting relic of the past. I think it's a safe bet that USB will be around for a while, but it is just that: a bet. I've certainly seen my share of odd technologies over the years which have not just fallen out of favor, but for all practical purposes just disappeared completely.

The difference that allows me to believe my bet on USB is more secure, or at least longer lasting, is simply ubiquity. Even if I still had it, there's no device that would read the seven-track magnetic tape on which I carefully archived all my university projects. The biggest problem isn't age or even device capability; it's that I used a proprietary, non-standard format. Had it been in a more ubiquitous format, there'd be hope. (And I'd have converted it to a more contemporary format long ago.)

But, yes, technology changes. The good news is, it doesn't happen overnight. That's what's allowed me to carefully copy over my backup CDs of recent years onto more capacious, more easily-accessed (and backed up) hard drives in recent years.

To me, the ultimate irony of all this is that there are solutions to disappearing storage technology like floppy disk and optical (CD) drives no longer built into your computer: external drives connected by — you guessed it — USB. As technologies change, I'm confident that transition-enabling converters and adapters will be part of that change, at least for the most common technologies. And there's no question that USB is common today.

* * * End of article * * *

Raspberry Pi

By Dick Maybach
Brookdale Computer Users' Group, NJ

I introduced the Arduino in my August 2017 article (available at http://www.bcug.com), and this month I'll do the same for the Raspberry Pi. Although the two are both small, inexpensive, single-board devices designed to aid people to learn computer technology, they provide much different experiences. Using the Arduino is like visiting one of our national parks; while you will learn new things, you stay in a familiar environment. In particular, you work on your home computer using your present operating system. Using the Pi is more like touring a foreign country on your own; you are in a new environment with much to learn to become comfortable. In particular, you are using Linux on a completely new PC, and rather than just using applications, much of the time you will be configuring the system, often from the command line. While the rewards of mastering the Pi are greater, so is the effort required to achieve them.

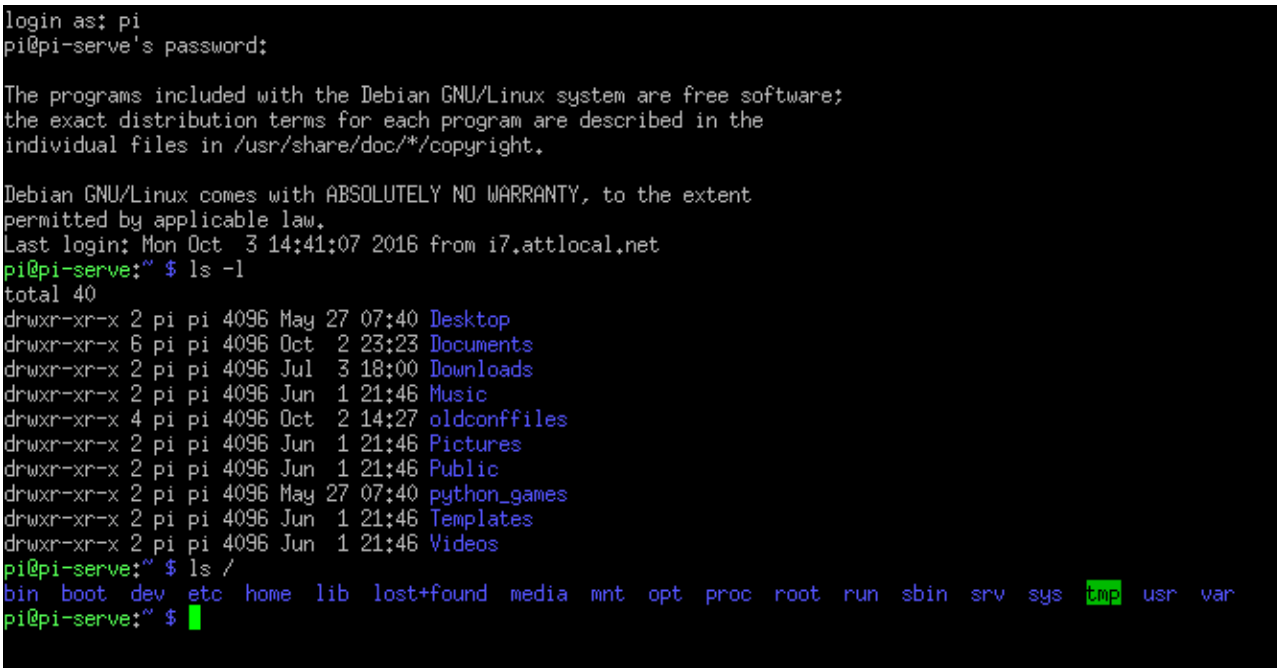
The Raspberry Pi is a single-board computer requiring only a micro SD storage card, display, keyboard, and mouse for a complete desktop system. It normally runs under Linux, and the great majority of applications and activity are based on this operating system. (A smart-phone-like version of Windows has recently become available for it, https://developer.microsoft.com/en-us/windows/iot. Like Linux, it is free, but is far less capable than either Linux or Windows 10 and has far fewer applications and much less activity. However, the download is free, so experimenting with it costs nothing. In the remainder of this article, I'll discuss only the Pi running Linux.) When you enter the Raspberry Pi world, you go back in time to the PC scene of the 1980s. Instead of buying a complete computer, you get parts or kits and build what you want. Those who enjoyed that earlier time will be impressed with how much cheaper, smaller, and more capable the results are. The Pi is a complete computer with network access and applications that include office suites, complex mathematical analysis, graphics, and software design, and you can do anything with it that you now do on your PC. However, it's much slower, so such tasks as complex photographic manipulation aren't practical.

The Pi project began February 2012 with a single model, but in the years since, has evolved into a family, both from the original organization and independents. The Raspberry Pi organization produces the following models.

- The **Pi Zero** is the smallest lightest and cheapest. It's not suitable for use as a PC, but as a component. It features small size and low power consumption, but lacks the interface ports of the other models.
- The **Pi 1 A+** is also intended for use as a component, although unlike the Zero it does have a full-sized USB and an HDMI port.

- The **Pi 1 B+** includes several ports, including four USB, an HDMI, an Ethernet, and a multi-pin general-purpose one. This can function as a PC, although those below are considerably faster. It's been used for media centers, robotics, information displays, and in the International Space Station.
- The **Pi 2** is similar to the 1 B+, but has a faster CPU. It's been used as a desktop PC, media center, web server, and gaming emulator.
- The **Pi 3** is currently the most capable of the family, with the fastest clock speed, the most RAM, the best all-round feature set, including Wi-Fi and Bluetooth. It does consume more power, but it does make a credible PC, although one that is slower than current standards.

When you begin using a Raspberry Pi, you will need to equip it with a mouse, keyboard, and display, and this is surely how you should begin. Alternatively, you could connect it to your network and operate from your PC, which means the Pi doesn't need a display, keyboard, or mouse. You control it either in command-line mode using the secure shell protocol (SSH) or using a remote desktop application to access the graphical interface. My experience is that getting these set up requires some experimentation, so you should wait until you become comfortable with the Pi before you try either. The Screen 1 shows the start of an SSH command-line session. It will look familiar to Linux users.



Screen 1. Controlling a Pi Over a Network Using SSH.

Tidbits of probably useless information

Your body is creating and killing 15 million red blood cells per second!

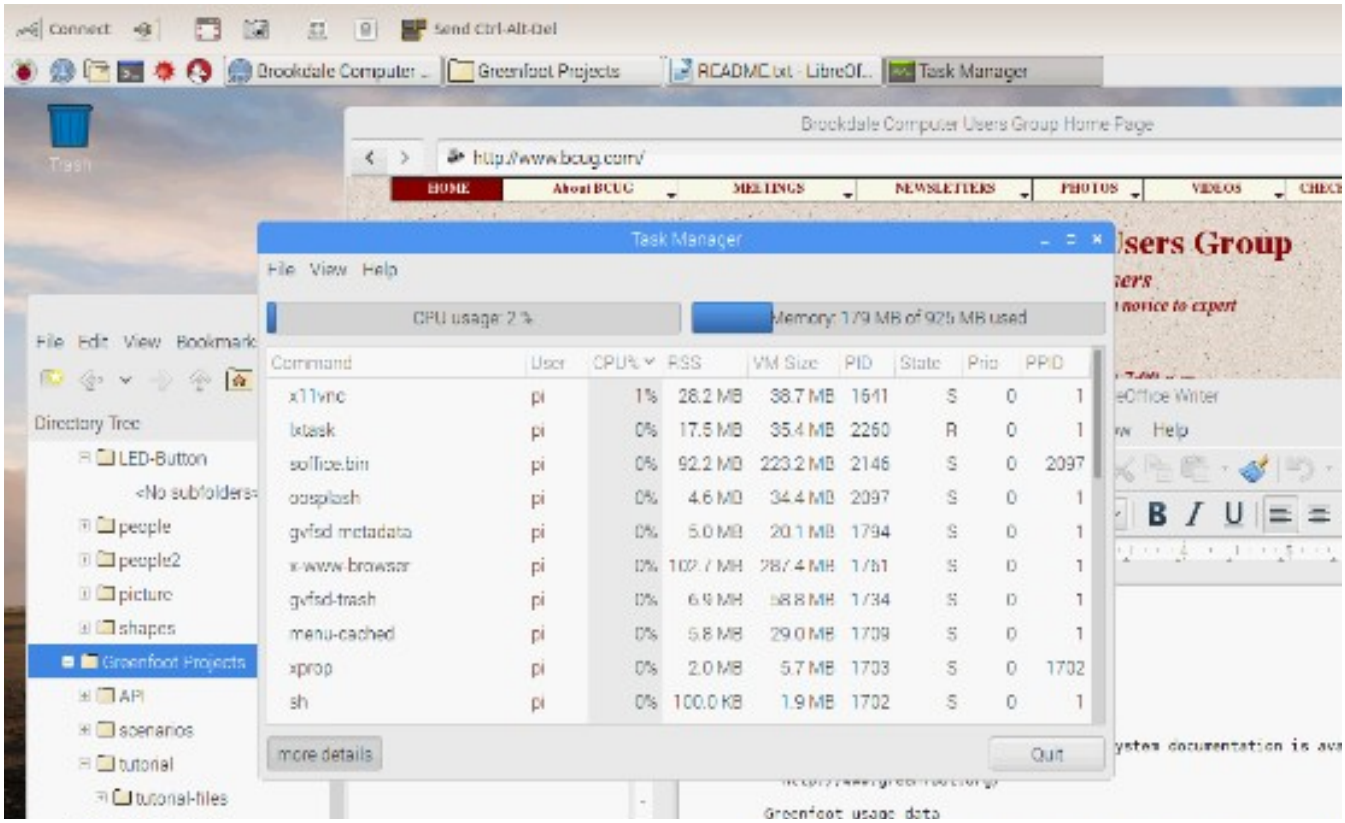
The king of hearts is the only king without a mustache on a standard playing card!

There are no clocks in Las Vegas gambling casinos!

During your lifetime, you'll eat about 60,000 pounds of food, that's the weight of about 6 elephants!

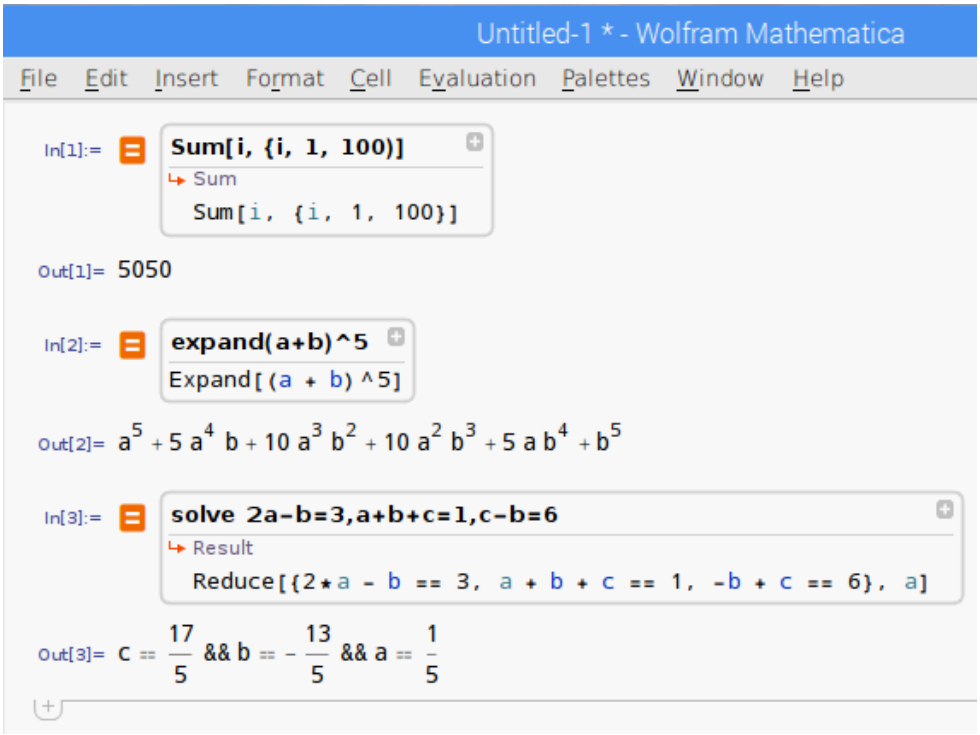
Some ribbon worms will eat themselves if they can't find any food!

Following is a window on my desktop PC; the Pi is across the room and connected by a LAN. Screen 2 is a remote-desktop window on my desktop PC showing the Pi's graphical interface, with three open applications, Web browser, file manager, task manager, and word processor. Normally, you wouldn't put this much load on such a small machine, but I did it here to make the point that it is a complete (although slow) PC.



Screen 2. Controlling a Pi Over a Network Using a Remote Desktop.

The Raspberrian operating system, a variant of Linux available from the Raspberry organization, https://www.raspberrypi.org/, includes the symbolic mathematics program Wolfram Mathematica, https://www.wolfram.com/raspberry-pi/, which is similar to but more sophisticated than wxMaxima, discussed in the July 2017 issue of Bytes (available at http://www.bcug.com). Screen 3 shows three examples of its use, calculating a sum of integers, expanding an expression, and solving a set of three algebraic equations. There is much more to this tool, including plotting and Calculus.



Screen 3. Wolfram Mathematica on a Pi.

Once you have a working PI, what might you do with it? Because it's separate from the PC with your tax returns, family photos, and other valuable data, you can use it as a sandbox where you can experiment without risk.

- **Surf the Internet safely** – if a rogue site does manage to install malware on the Pi, it is still isolated from your main PC. This makes it useful for guest use, especially for those fearless young people. You might even consider setting up a separate e-mail account, just for use while using the Pi, for use when a site demands an e-mail address before letting you have the information you need.
- **Learn to Program** -- The Pi runs on Linux, and one of that operating system's strong points is the wide variety of languages it supports, many with complete development environments. If you manage to make a horrible mistake, the damage is isolated. Consider Scratch if you just want a taste of what programming is or if you want to introduce a young person to it, or Python for a versatile, modern language but less complex than traditional ones, such as c. Python is well supported with many books and on-line communities.
- **Build a Server** -- The Pi's low cost, small size, and low power consumption make it well suited for server duty on your home network. A print server would allow you to share one printer with all your PCs. A file server would allow you to synchronize the contents of selected directories on PCs or would provide a single point for backups. A website server would provide an internal site for sharing information or would give you a place to learn website design. You could keep this simple (HTML only) or could add PHP support or even complete WordPress or Joomla services. Once the site is set up, you can remove its keyboard, mouse, and display. With any of these servers, you are also learning networking.
- **Connect Hardware** -- The Pi has a multi-pin interface to connect external hardware and many expansion boards to make this easier. (While Arduino expansion boards are called shields, those for the Pi are hats.) An Internet search will provide ideas for home control, Internet data collection, weather monitoring, and robotics. You probably don't want to use your home PC for such things, but again, the Pi's small cost, size, and power requirements open up these areas. And if a disaster does strike, you can replace your Pi for about $35.

You can make a Web search for more information, but do check the following.

- The official Raspberry Pi site is http://www.raspberrypi.org/. This is where you get software for it, read news about its development, see what members of its community are doing, and ask for help.
- A free monthly magazine, the MagPI is available at http://www.raspberrypi.org/magpi/. There are over 50 issues available for download, each with news and projects. A printed version is also available, but it's not free.
- There are many dealers for the Raspberry Pi, expansion cards, kits, accessories, books, and suggested experiments. Two popular ones are *Adafruit*, http://www.adafruit.com/, and *Sparkfun*, http://www.sparkfun.com/. You can have at least as much fun poking around these sites as we used to have at computer shows.
- Although the above dealers carry books, you can probably save money by buying them from on-line book dealers such as Amazon, and many large brick-and-mortar bookstores have several publications on the device.

From the September 2017 issue, BUG Bytes, www.bcug.com, n2nd@att.net.

Interesting Internet Finds

Steve Costello, Boca Raton Computer Society

While going through the more than 300 RSS feeds, I often run across things that I think might be of interest to other user group members.

The following are some items I found interesting during the month of October 2017.

Did you know you can "Voice Type" in Google Docs?
https://whatsonmypc.wordpress.com/2017/10/01/google-docs-voice-type/

I did not know this before reading this post, and I am sure not many others do either. No special software needed, but of course, you do need to have a working microphone.

5 Common PayPal Scams and How to Avoid Them
https://www.maketecheasier.com/common-paypal-scams/
If like me you use PayPal, you should read this post and be aware of these common scams as well as others.

How to Use VirtualBox: User's Guide
http://www.makeuseof.com/tag/how-to-use-virtualbox/
I use VirtualBox all the time and have told others about it. For anyone who wants to know more about VirtualBox this is an excellent source.

Android Security 101: How to Secure Your Data Connections & Browse the Web Safely
https://android.gadgethacks.com/how-to/android-security-101-secure-your-data-connections-browse-web-safely-0180466/
Good general advice. Specific apps are suggested but not necessarily the best, though I use the suggested password manager and privacy browser myself, and have for a long time. It really doesn't matter, if you use a good alternative.

Linux For Old Laptops: The 4 Best Linux Distros to Try
https://www.addictivetips.com/ubuntu-linux-tips/linux-for-old-laptops-the-best-linux-distros/
There are many Linux distributions out there. If you have an old laptop lying around, check out this post for four distributions to try if interested in trying Linux out.

The Best Ways to Scan a Document Using Your Phone or Tablet
https://www.howtogeek.com/209951/the-best-ways-to-scan-a-document-using-your-phone-or-tablet/
If you have a smartphone or tablet with you, you also have a portable scanner. Check out this post to learn how to scan documents with Android or iOS devices. It is quick and easy on my Android smartphone.

****

Most Fridays, more interesting finds will be posted on the *Computers, Technology, and User Groups Blog*:
http://ctublog.sefcug.com/tag/interesting-internet-finds/

From the October newsletter, editor@brcs.org, http://ctublog.sefcug.com/.

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

Microfluidics from LEGO bricks

MIT engineers make microfluidics modular using the popular interlocking blocks.

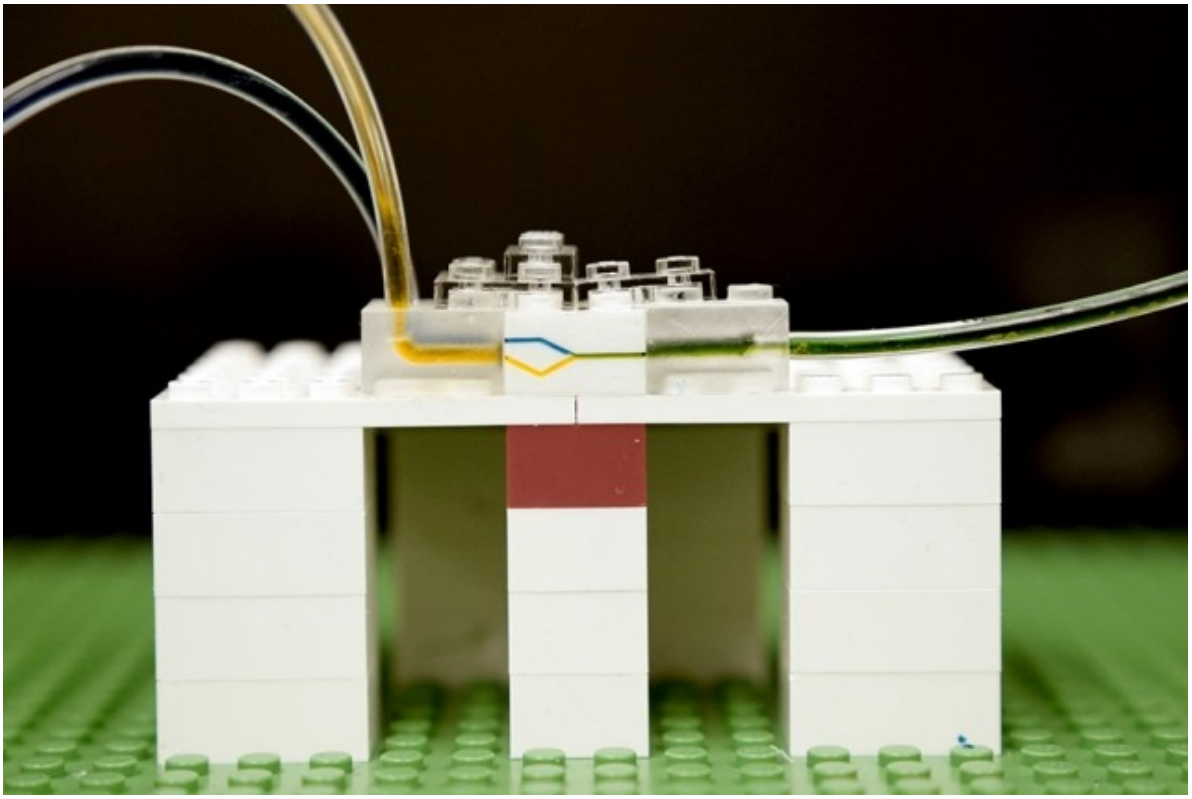
Jennifer Chu | MIT News Office
January 30, 2018

MIT engineers have just introduced an element of fun into microfluidics.

The field of microfluidics involves minute devices that precisely manipulate fluids at submillimeter scales. Such devices typically take the form of flat, two-dimensional chips, etched with tiny channels and ports that are arranged to perform various operations, such as mixing, sorting, pumping, and storing fluids as they flow.

Now the MIT team, looking beyond such lab-on-a-chip designs, has found an alternative microfluidics platform in "interlocking, injection-molded blocks" — or, as most of us know them, LEGO bricks.

"LEGOs are fascinating examples of precision and modularity in everyday manufactured objects," says Anastasios John Hart, associate professor of mechanical engineering at MIT.



Indeed, LEGO bricks are manufactured so consistently that no matter where in the world they are found, any two bricks are guaranteed to line up and snap securely in place. Given this high degree of precision and consistency, the MIT researchers chose LEGO bricks as the basis for a new modular microfluidic design.

In a paper published in the journal *Lab on a Chip*, the team describes micromilling small channels into LEGOs and positioning the outlet of each "fluidic brick" to line up precisely with the inlet of another brick. The researchers then sealed the walls of each modified brick with an adhesive, enabling modular devices to be easily assembled and reconfigured.

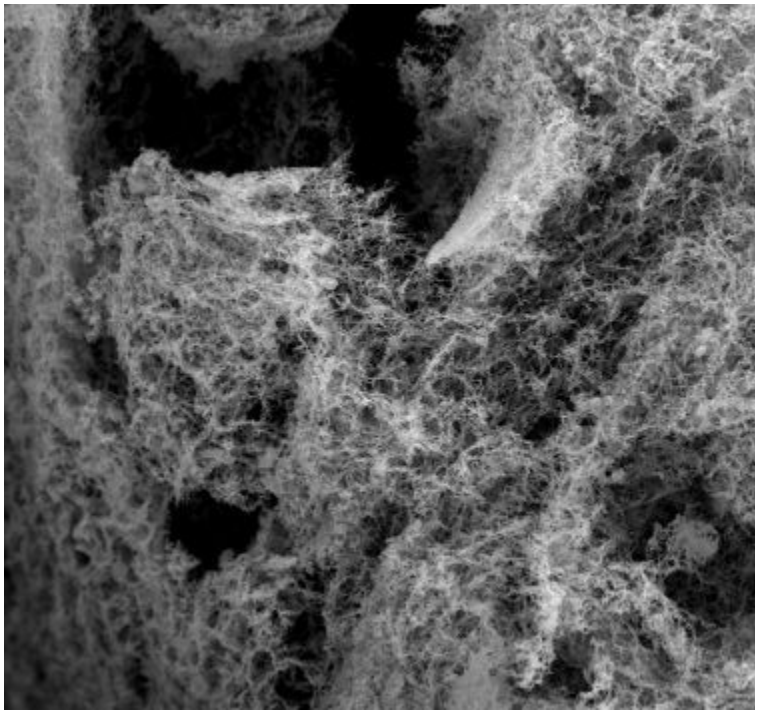
Each brick can be designed with a particular pattern of channels to perform a specific task. The researchers have so far engineered bricks as fluid resistors and mixers, as well as droplet generators. Their fluidic bricks can be snapped together or taken apart, to form modular microfluidic devices that perform various biological operations, such as sorting cells, mixing fluids, and filtering out molecules of interest.

"You could then build a microfluidic system similarly to how you would build a LEGO castle — brick by brick," says lead author Crystal Owens, a graduate student in MIT's Department of Mechanical Engineering. "We hope in the future, others might use LEGO bricks to make a kit of microfluidic tools."

For the rest of this article, go to http://news.mit.edu/2018/microfluidics-lego-bricks-0131.

New Material Efficiently Generates Hydrogen from Water

by Ryan Whitwam



The use of hydrogen as a fuel and energy storage medium has interested scientists for decades, but physics isn't on our side. Generating hydrogen from water requires a lot of power and expensive materials, but researchers from Washington State University may have developed a method that could make it a viable way to store energy cheaply and efficiently.

Many of the technologies we look toward as part of a renewable energy economy are less consistent than traditional means. For example, solar power produces a lot of energy during the day and none at night. It's the same story with wind power — it might provide more power than needed when it's gusty out, but none on a calm day. You need some way to store excess energy for later use, and battery technology comes with its own complications. If you can generate hydrogen, it's an extremely efficient way to store energy. Just pump it into a fuel cell, and you get water and energy. In addition to industrial storage, some vehicles could also be powered by hydrogen fuel cells.

The issue with using hydrogen is that you need a lot of power to split a water molecule (the most common source of hydrogen atoms), and the catalysts needed are expensive. Most methods use either platinum or ruthenium, and they must be replaced frequently as they degrade. As described in a newly published study, the Washington State team used cheap and plentiful nickel and iron to make a water-splitting catalyst.

The team calls its material a "porous nanofoam." It's a bit like a metallic sponge with microscopic holes and tunnels that give it a very large total surface area. That's key to its ability to catalyze the formation of hydrogen and oxygen from water. In testing, the team found this material was even more effective in generating hydrogen than the more expensive catalysts made from precious metal. As for stability, the team reports it showed no drop in functionality after a 12-hour run time.

Most elements of this process are the same we currently use to generate hydrogen, so it's conceivable the nanofoam could be substituted for other catalysts at industrial scale with few changes. However, the Washington State University study only tested the material in a laboratory setting. More research is needed to see how the nanofoam catalyst might work at industrial scale. Until then, don't toss your lithium-ion batteries in the trash.

Editor's note: this article was reported in www.extremetech.com, in February, 2018.