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

PATACS Posts

Newsletter of the Potomac Area Technology and Computer Society

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

HTTPS and Digital Communications Security

How it works and why it is useful to you

By John Krout

Potomac Area Technology and Computer Society (PATACS)

This article was inspired by a question asked during the very illuminating presentations at the PATACS/OPCUG meeting on March 16, 2019.

One presentation during that meeting introduced the basic purposes of Virtual Private Networks. Another, by an Apple employee, included a question from the audience pertained to how passwords are sent in encrypted form using a web browser and HyperText Transfer Protocol – Secure (HTTPS).

An important question asked during that second presentation was: **why is HTTPS secure when the encryption key is sent to my browser unencrypted?**

That core of the question was revealed during the meeting over a period of time. The answer at the time was not terribly detailed, which was no fault of the presenter. It takes time to explain how HTTPS works.

This article is my attempt to flesh out the answer for everyone.

This information is not specific to Apple, however; it applies to all browsers on all operating systems. It turns out that **two different but related encryption keys** are involved, a relatively new approach invented by three Massachusetts Institute of Technology (MIT) professors.

These days, all the work of encryption and decryption is handled by your computer. That includes management of the relevant keys. You are not required to type in a long encryption key.

Here is some necessary background on how HTTPS accomplishes its secure communications.

THE MAN IN THE MIDDLE

An important security concern is known as a **Man in the Middle attack**.

The Internet routes messages more or less at random through many intermediate servers between your Internet Service Provider (ISP) and any company that supplies a web site to the public. The path through intermediate servers can vary to some extent each time you click on a link. Most of those intermediate servers do not belong to the web site that you are using.

Somebody with access to one of those intermediate servers could install message-trap software to copy every email passing through that one server. That somebody is known as a **Man in the Middle**. The astute Man in the Middle could analyze those emails, find your ID and password for, say, your bank, and use those to log into the bank system and drain your account.

Assuming The Man in the Middle found your email ID and password, that bad apple could also

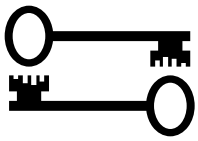
(Continued on page 2)

(Continued from page 1)

write emails using your account, and send fake responses to your friends and acquaintances, possibly including computer malware.

Man in the Middle attacks have existed for ages. Telegraph operators could receive messages intended for other recipients. Analog landlines could be tapped easily by anyone who understood the technology and could access a specific landline set of wires. Unencrypted cordless phones could be picked up by anyone with a receiver tuned to an appropriate frequency.

RSA AND ASYMMETRIC KEY ENCRYPTION



Back around 1980, an MIT professor named Ron Rivest decided to look into encryption methods that could be used to prove that a message **undeniably originated** from a particular sender and was **undeniably intended** for a particular recipient. The goal was to prove those two facts to a neutral, dispassionate third party, meaning a judge.

This is not an insignificant issue. Communications and agreements are the foundation of modern commerce and most of life's relationships. And a very common defense in many court cases is denial of agreement: *No I did not say that* is perhaps one of the most commonly uttered phrases in court.

Rivest, along with MIT professors Shamir and Adelman, came up with **asymmetric key encryption**, meaning that two related keys were involved: a public key and a private key, working as a pair.

Here is the most important behavior of asymmetric key encryption. Something encrypted with a private key could be decrypted only with the paired public key. Something encrypted with a public key could be decrypted only with the paired private key.

The idea is that each owner of a pair of related keys keeps one key private, and provides the related public key to others. You will see some examples discussed below.

At the time, the MIT professors aimed strictly to make email far more secure than it was. The web did not exist at the time. However, when the web became popular, key pairs became very important for web commerce, as you will learn below.

The three MIT professors were named as inventors of a US patent 4,485,829 for their asymmetric key encryption algorithm. That patent was issued in 1983, and the patent expired in 2000. The three professors creates a company, RSA Security; the name was the initials of the three founders. That company commercialized their security algorithm, and that company eventually spun off another, called Verisign. Both were quite successful. In effect, the professors created the entire security basis for web commerce.

Verisign and other companies sell public/private key pairs. To create more key pairs, the companies use server farms to find prime numbers to use for creation of key pairs.

The keys are very large numbers, hundreds of binary digits. What makes the encrypted data secure is that the keys are so long that computer attempts to decrypt without knowing the keys would take a very long time, trying many possible keys. This is called a **brute force attack**.

The inventors use the term **computationally infeasible** to describe that long time, meaning finding the decryption would take so long that the cost of computer time would exceed the value of the encrypted email information.

Since the asymmetric key pair approach was introduced back in the early 1980s, computers became faster. Personal computer Central

(Continued on page 3)

(Continued from page 2)

Processing Units (CPUs) in that time ran at low megahertz speeds, and now run at low gigahertz speeds, roughly five hundred times faster.

As a result of the evolution of CPU power, ensuring that decryption would still be computationally infeasible means that key length must continue to grow. Both trends continue: faster computers and longer encryption keys. It is a never-ending battle.

HOW HTTPS USES KEY PAIRS

The secure form of the World Wide Web, called HTTPS, is based on encryption and decryption using key pairs. The secure form of web pages is used when the Uniform Resource Locator (URL) starts like this: `https://`

The S following the P indicates Secure.

Credit: Wikimedia.org CCSA-4.0

To achieve that security, when your browser accesses an HTTPS web server, the web server sends to your browser a **digital certificate** containing the public key, issuing certificate authority (CA) and expiration date of a key pair owned by the web company.

For instance, CNN.com owns key pairs, Google.com owns key pairs, Amazon.com owns key pairs, your bank and your stock brokerage and your credit card company own key pairs, and so forth.

As the questioner at the PATACS meeting correctly noted on March 16, 2019, the public key is sent unencrypted. Read on to understand why, nonetheless, that unencrypted public key stymies the Man in the Middle, even when that person intercepts the unencrypted public key.

Here's how HTTPS works with web browsers like Chrome, Firefox, Edge, Safari et cetera.

After your browser receives the public key from the web server, your browser uses that public key for two purposes.

First, each subsequent web page sent from the same web server is encrypted with the private key paired with the public key in the digital certificate. So the browser decrypts each web page using the public key.

The Man in the Middle could decrypt those next pages also, if the server administered by the Man in the Middle received both the digital certificate and the subsequent web pages.

Second, each subsequent URL that you click on, and each field you fill out such as ID and password, credit card details, et cetera, is encrypted by your browser using the public key, and sent back to the web server. The web server decrypts those URLs and data using its paired private key.

The Man in the Middle can possibly receive those encrypted URLs and encrypted data. **However, the Man in the Middle cannot decrypt the URLs and data**, because the Man in the Middle does not have the private key, only the public key.

Web browsers on modern personal computers and even tablets and smart phones do all of this HTTPS encryption and decryption automatically,

(Continued on page 4)

(Continued from page 3)

and so quickly that the encryption and decryption duration simply is not noticed by you.

You might get the impression there are literally hundreds of thousands of public keys, and millions of encrypted HTTPS pages and data submissions, moving across the World Wide Web on a daily basis. That is correct.

Your own web browser may be using several certificates concurrently, if you have a tab open for say Google, CNN.com, Amazon, and your email service.

But wait, there is more.

Although most key pairs have an expiration date roughly 3 years from the date of purchase, some of the biggest, busiest web sites might use a particular key pair only for one day, and then use a new one on the next day. This is to avoid any security compromise by web site employees, the risk of which grows over time.

THE REPLAY ATTACK, DEFEATED

The Man in the Middle might just recognize that certain encrypted data is an encrypted ID and encrypted password. This would allow the Man in the Middle to compose a bogus login message containing the same encrypted ID and the encrypted password.

This is known as a **Replay Attack**. Replay attacks no longer happen very often. Here is the reason.

The secure web server sends you not only its public key but also frequently sends a block of data to append to your ID and your password before each are encrypted. That block is called a **Nonce**. Its contents are irrelevant, **except that your browser can use any nonce only one time**. When your web browser sends something including the encrypted nonce back to the web server, then the web server sends a web page including a different nonce to your web browser, to be used for the next encrypted data you send, such as a URL.

Even if the same Man in the Middle receives both the public key and each nonce, that man in the middle does not have the private key and cannot decrypt what your browser sends back, and so cannot separate the encrypted nonce from your encrypted ID or encrypted password.

And the nonce is single-use. If the Man in the Middle does a simple replay attack, sending the encrypted ID+nonce and the encrypted password+nonce, the web server will simply reject it since the same nonce has been used previously by you.

This is why many web server login sequences now collect IDs and passwords on separate web pages. That way, one nonce value is used for encrypting the ID, and a different nonce is used for encrypting the password. I noticed that AOL switched to this separate page approach sometime in 2018, several months after Verizon forced me to switch from the Verizon.net email server to the email server of Verizon's subsidiary AOL.

Additionally the server path between your browser and the web server may change between sending the encrypted ID and sending the encrypted password. Path fluctuation reduces the chance that both will flow through the server used by the Man in the Middle.

All of that makes life for the Man in the Middle very unprofitable.

THE SPOOFING ATTACK, DEFEATED

In the age of the web, The Man in the Middle has also sometimes chosen to attack your web browser, rather that the web server. Here is how that used to happen.

(Continued on page 5)

(Continued from page 4)

Assuming HTTPS is not in use, the basic attack is that the Man in the Middle sees your uploaded URL, receives the web page sent back to you from the web server, modifies that response web page to include illicit links, and downloads it to your web browser. That is known as a **spoofing attack**.

The contents of that bogus web page might include links to web sites that download tracker cookies, or web sites that download malware to your computer.

HOW GOOGLE USES HTTPS

Google.com is an example of a popular web site now using HTTPS instead of HTTP.

Google's search results pages were once widely subject to spoofing attacks, simply because the pages include so many links to other web pages. The spoofing attacker always found a bounty of links to alter in the search results.

Today, Google uses HTTPS. When you load the Google home page, your browser receives the Google public key and a nonce.

When you send a search term to Google, your browser encrypts your search string and the nonce, using the public key sent from Google. In response, the results pages sent by Google to you are encrypted using Google's private key, so your browser uses the public key to decrypt the results pages. Google also sends a different single-use nonce, so the secure process can repeat.

The use of the pair of encryption/decryption keys proves to you that the search was performed by Google and the response web page was sent to you by Google, the only web service able to decrypt your search term. The use of the pairs of keys also proves that the results were returned by Google.

Spoofing attacks also are eliminated. If the Man in the Middle also received the public key from Google, then the Man in the Middle can decrypt the search result page. However, the Man in the Middle cannot encrypt bogus hacked search results to send to you, since the Man in the Middle does not have the private key owned by Google and needed to encrypt search results.

In the bad old days before Google.com adopted HTTPS, spoofing attacks worked. Those were documented often enough that Google.com adopted HTTPS to stop spoofing attacks.

Google does not want its reputation to be sullied by those spoofing attacks. Neither does Amazon, CNN.com, or just about any other web site that appeals to large public audiences.

ABOUT THE AUTHOR: John Krout has been writing about creative uses of personal computers and related technology since the early 1980s. He lives in Arlington VA and spent most of his career as a C and C++ software engineer, helping create major systems for federal agencies. He recently retired after being a tech writer for a major vendor of automated fingerprint identification hardware, supporting a federal agency system using that hardware.

Making Windows 10 Look and Act Like Windows 7

by Tom Burt
Vice-President, Sun City Summerlin Computer Club
Gigabyte Gazette, January 2020 issue
www.scscc.club
tomburt89134 (at) cox.net

Microsoft ended support for Windows 7 on Tuesday, January 14th. After that date, there will be no further updates, bug fixes or security patches for Windows 7. The short-term consequences of the end of support are minimal: Windows 7 and installed applications will continue to work. Over time, however, as hackers discover new security flaws to exploit, Windows 7 will become less secure. So, it's time to think about moving to Windows 10, which has a more secure core design and still has support.

(Continued on page 6)

(Continued from page 5)

Another concern for Windows 7 users is that it's no longer available. If your current Windows 7 PC's hardware finally gives up the ghost and can't be repaired at a reasonable cost, your only option will be to buy a new Windows 10 PC via the retail market.

Coming from Windows 7, you may initially find Windows 10's user interface unappealing or difficult to navigate—especially the Settings interface. Our article this month will offer some ways to set up Windows 10 so that it looks and acts much like Windows 7. This can help with easing the transition to using the native Windows 10 user interface. For small businesses, this could afford a big saving on retraining staff accustomed to using Windows 7. We'll also talk about some ways to get applications written for Windows 7 to run on Windows 10. This can be critical if the support for that application has gone away – a not uncommon occurrence with "free" programs downloaded over the years.

Helpful Articles

Here are some links to helpful articles I found while researching for this month's article. I'll be highlighting a few of the items these articles offered.

https://www.howtogeek.com/277448/how-to-make-windows-10-look-and-act-more-like-windows-7/

https://www.theguardian.com/technology/askjack/2019/jun/06/how-can-i-make-windows-10-look-more-like-windows-7

https://www.windowscentral.com/top-10-ways-make-windows-10-more-windows-7

https://www.digitaltrends.com/computing/how-to-make-windows-10-look-like-windows-7/

Classic Shell

One of the biggest differences between Windows 7 and Windows 10 is the Windows Start menu. Classic Shell is a free program that you can download and install to give you a variety of Start Menu styles, including that of Windows 7. You can find the download link at

http://www.classicshell.net/

The original author has placed the program in the public domain on GitHub.com, but you can still download his final version from the above site.

Classic Shell was originally built when Windows 8 was released; Windows 8 had NO Start Menu. It is compatible with Windows 8, 8.1 and 10. The articles above also offer a link where you can get an image file of the Windows 7 Start orb to be used with Classic Shell.

File Explorer

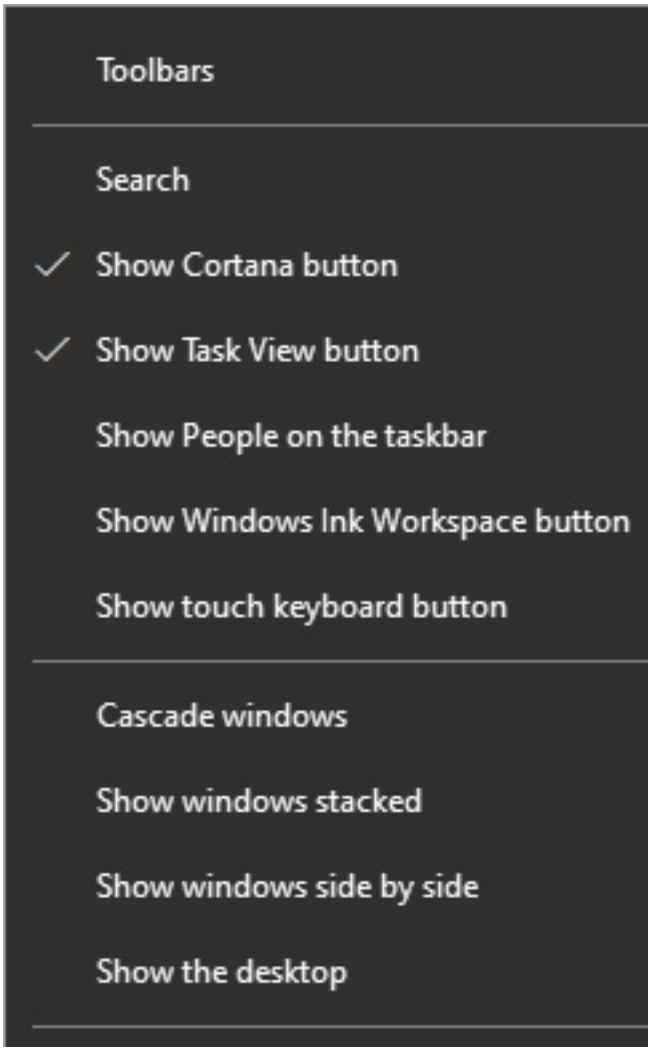
The Windows 10 File Explorer features the tabbed "ribbon" interface, which differs from Windows 7's Windows Explorer, which featured a "menus and toolbar" interface. I didn't find File Explorer that different and like the way it presents the user interface in the ribbon. But, for a closer recreation of Windows Explorer, the "Classic Shell" setup includes "Classic Explorer", which allows you to get a highly customized File Explorer, including making it look and act like the Windows Explorer.

Task Bar

The Windows 10 Task Bar includes the Search box, the "Talk to Cortana" icon and the "Task View" icon. These are not present in Windows 7. To remove them, right-click on an open spot on the Task Bar to display a pop-up menu.

Uncheck the "Show Cortana button" and "Show

(Continued on page 7)



(Continued from page 6)

Task View button" to remove those from the Task Bar.

If you hover over the Search item, a submenu slides out with toggle options to "Show search box", "Show a search icon" or completely Hide the search.

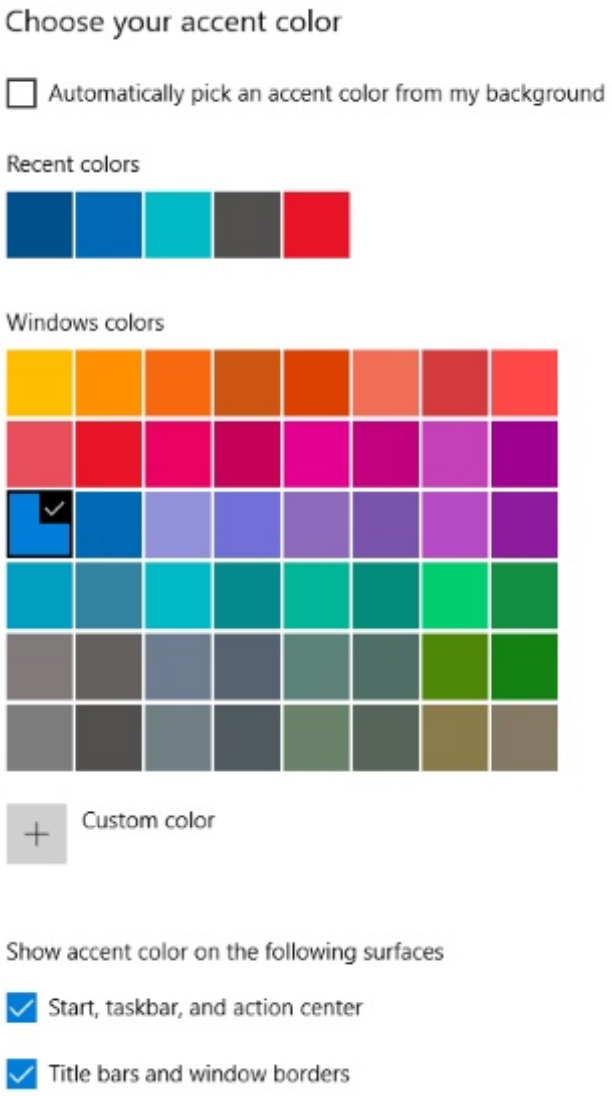
You can also click "Taskbar Settings" to go to an extensive page of other Task Bar settings.

Title Bar Colors

In Windows 10's default color scheme, window title bars are colored white, making it difficult to see which Window has the focus to the mouse and keyboard. To add some color to title bars and other UI elements, you can go to Start > Settings > Personalization > Colors. This will display a page of color settings.

This screenshot shows the key parts for changing the color of various window and screen elements.

Uncheck (if checked) the "Automatically pick an accent color from my background" checkbox.



Select a pleasing accent color from the palette or click the + for a custom color. Check or uncheck the boxes for where the accent color should be used.

This tip can be handy even if you don't use any of the others.

(Continued on page 8)

(Continued from page 7)

Program Compatibility

A separate concern from making Windows 10 look like Windows 7 is getting older programs that ran on your Windows 7 system to run on Windows 10. This can be a challenge for programs whose authors are no longer in business. Windows 10 provides options to run a program in "compatibility" mode and/or Administrator mode.

The best way to do this is to start by creating a desktop shortcut to the program. In File Explorer, browse to the program's .exe file [*Ed.* You need to make sure "Show Extensions" is checked in the File Explorer "View" Tab settings], right-click and, in the popup menu that appears, hover over "Send to" and then, in the secondary menu that appears, click "Desktop (create shortcut)". See the following screenshot. Rename the desktop shortcut to something meaningful to you.

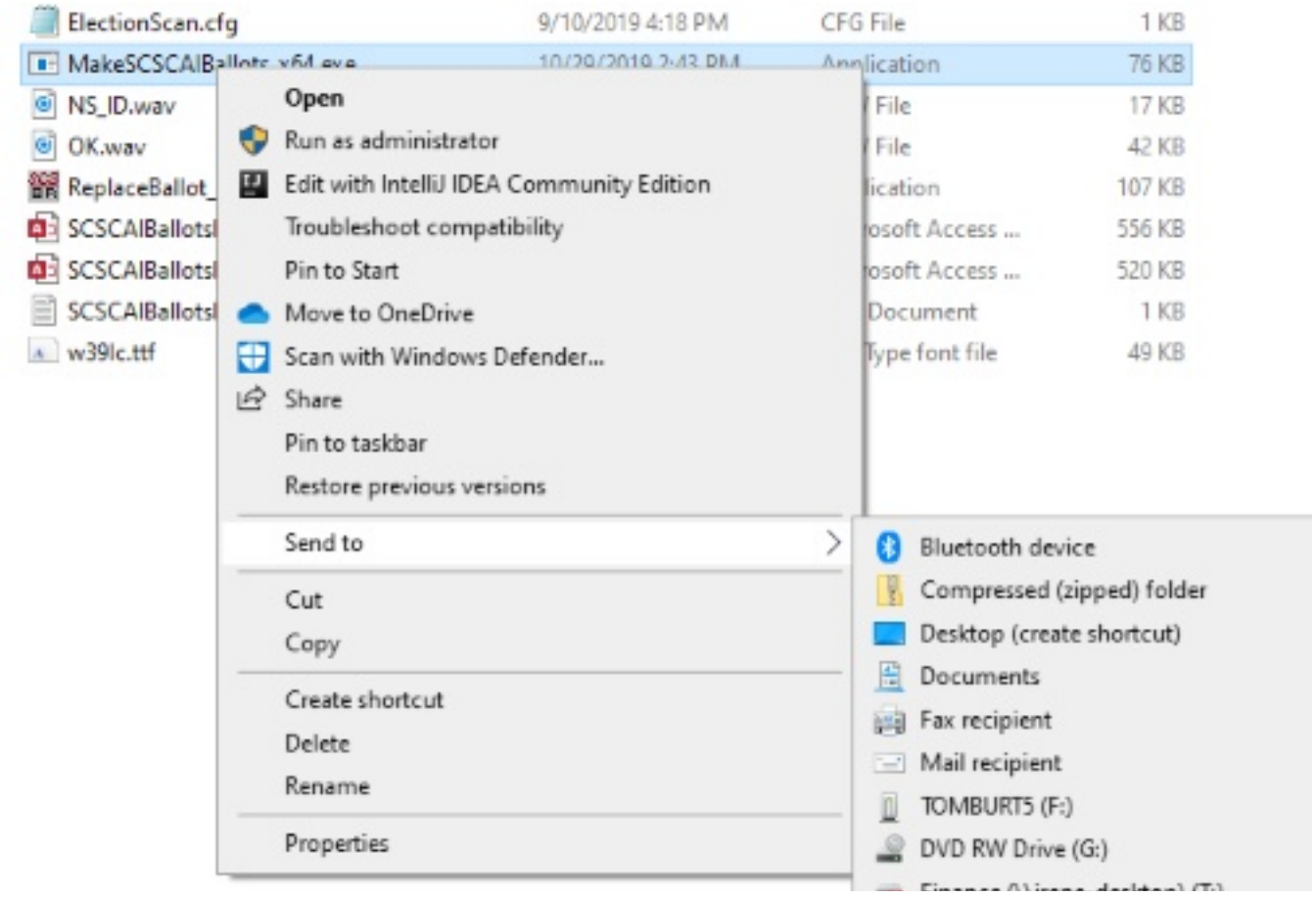
Next, right-click the shortcut and choose Properties from the popup menu. In the Properties dialog, click the "Compatibility" tab. Check the box for "Run this program in compatibility mode for:"

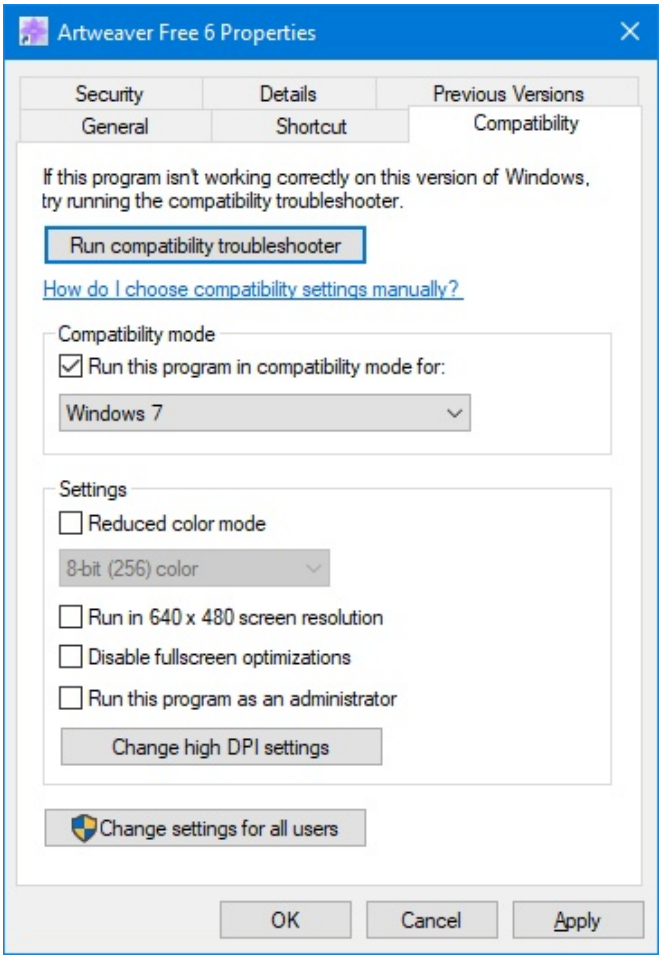
In the dropdown, choose "Windows7".

You can also click the "Shortcut" tab and then click the "Advanced" button. A small dialog will display with a checkbox for "Run as administrator" [*Ed.* Run as Administrator selection is also on the "Compatibility" Tab]. Try checking this box if the program still doesn't run properly with Windows 7 compatibility selected.

When done with setting Properties, click "OK". Then double click the shortcut to run the program. Hopefully, it will launch and run normally.

(Continued on page 9)





(Continued from page 8)

Some Windows 7 utility programs, especially those with accompanying drivers, may not run, even with compatibility mode.

Creating a Windows 7 Virtual Machine

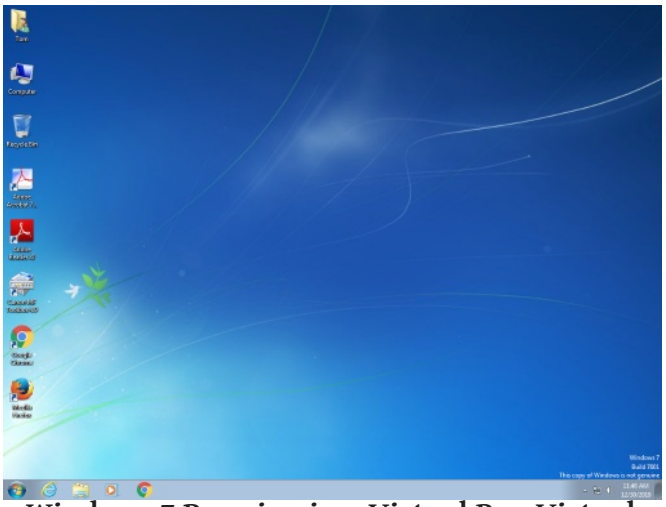
If a program still fails to run on Windows 10 after you've tried Windows 7 compatibility mode and Run as administrator, you may want to try setting up a Windows 7 virtual machine. This requires a fair bit of technical skill, so I recommend visiting the SCSCC Tuesday Repair Lab team for help. Also, check out my "Virtual Machine Primer" seminar handout at https://www.scscc.club/smnr/Virtual_Machine_Primer.pdf.

The most universal virtual machine utility is the free Oracle Virtual Box, which runs on Windows 10 Home or Pro, macOS and Linux. You can download Virtual Box at https://www.virtualbox.org/.

A virtual machine is a software/hardware emulation of a PC (the Guest) that runs as an application on a real PC (the Host). The Guest operating system and its applications run in the virtual machine and are unaware that they are running in a virtual environment. The virtual machine can be "booted" when needed and "shut down" when not needed. The virtual machine has a virtual hard drive, which is a single large file on the Host PC.

The general approach is to capture a snapshot of your Windows 7 PC's C: drive and system partitions and use that snapshot to create the virtual hard drive file.

That virtual hard drive file is attached as the boot drive of a virtual machine configured to emulate a Windows 7 PC. Once this is done, you can "boot" the virtual machine and it will virtually start Windows 7 from the attached virtual C: drive. Your virtual machine will then be running your former Windows 7 PC and its applications.



Windows 7 Running in a Virtual Box Virtual Machine on Windows 10

The easiest way to make a snapshot of your Windows 7 PC's C: drive and system partitions is to create a backup image using Macrium Reflect or Acronis True Image. That image can then be

(Continued on page 10)

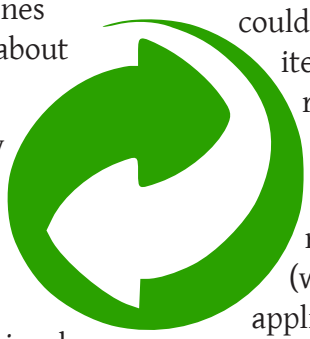
(Continued from page 9)

restored to the empty virtual C: drive of the Windows 7 virtual machine. Once the restore is done, the virtual machine will be able to boot up and the same Windows 7 and applications that you had on the original PC.

Is "Refurbished" Worth the Price?

News and/or Opinion from Paul Baecker
Newsletter Publisher & Editor
Sterling Heights Computer Club
October 2019 issue, WYSIWYG
www.sterlingheightscomputerclub.org
newsletter (at) sterlingheightscomputerclub.org

I recently went shopping for a cable modem to eliminate the rental cost of the one supplied by my ISP. After doing some online research, I decided on a capable Arris model and found it at a local retailer. The store had some new ones but also had some refurbished ones for about half the price of the new ones.



I thought to myself, well, they've simply been returned by shoppers who had changed their minds because they didn't like the color or style, and the units were probably basically unused. I inquired and learned that they had previously been used in a business somewhere (how would the salesman know?). So next I thought, well, do I want to save a few bucks by buying this so-called refurbished unit? Surely the items would have been repaired (if necessary) and tested by an Original Equipment Manufacturer (OEM) facility so that they operated as though they were new, even if they did have some wear marks on them. A no brainer to save the money, right?

But for whatever reason, I got a bit more inquisitive and asked about to what extent these items were refurbished. To the original manufacturer's specifications? In this case, nope. Well, then, surely the store could vouch for the level of refurbishment done by the third party. Nope again. I learned that there are businesses that exist to refurbish electronic products to their own specifications, and they are not necessarily noted as to their relationship to the product's original specs. My excitement in getting a great deal was gradually waning. Finally, the store rep tells me that they offer a 14-day return on a purchase of this item, but no warranty beyond that return option. I eventually passed on this offer. I figured that with my luck, the item would last past those 14 days, but die too soon thereafter.

I also checked the details on the web site of a popular online retailer of computers and accessories. I found similar statements about refurbished products being refurbished to the specs of the refurbishing organization. Some refurbished items came with warranties, some could be warranted at extra cost, and some items were 'as is' (such as demos) with no right to complain after the purchase.

So, what this adventure taught me is to carefully vet the retailer of any refurbished item you're considering (whether electronics, furniture, appliances, etc.) and carefully study the purchase agreement and any (often hidden) disclaimers that apply to the purchase.

A definition I found online for the term "refurbish" is "to brighten or freshen up."

Yikes!!!

This is an online article about doing your homework when shopping for refurbished products.

https://lifehacker.com/when-should-i-buy-refurbished-electronics-5885492

You can snag discounts as high as 50% off on smartphones, tablets, computers and associated devices when looking for a refurbished unit, but you've got to do your homework.

Review: MailWasher Pro

Another Level of Protection

By Jim Fromm
Editor/Webmaster, MOAA-The TUG, HI
October 2019 issue, The TUG newsletter
www.the-tug.org
editor (at) the-tug.org

Our September meeting was mostly Q&A; one of the questions received via email was about MailWasher Pro. I am going to save some keyboard clicks and refer to it as MWP. It is a utility that lets you look at the headers of all the emails in all of your mailboxes before downloading. It is very useful if you have multiple mailboxes. I have 12 email addresses, (don't ask), and eliminates the ads, solicitations, requests from Amazon for reviews, etc. before they ever make it into my mail program. Besides saving space, it decreases the chance of getting bit by malware. Here's a portion of the opening screen.

You have three immediate choices. Check for new mail, Wash (delete) mail and Select the mail program you want to use. Messages are listed in order received (default) or you can click on the title bar to separate them to your liking. Clicking on the box in the Delete column will select those emails for deletion. When you've finished picking the ones you don't want, click on the bar of soap icon. They will be deleted from the listing—but—like a bad penny, they are not completely gone. The messages are moved to the Recycle bin and will remain there until you clean it out.

If you want to recover one, or more, of those in the Recycle bin, merely right click on the email and select Restore. You'll need to have designated an email address to send them to. They will be sent to that address and show up in MWP again.

After you've decided which ones go and which ones stay, click on Mail Program. Your designated mail program will launch and download the mail into their respective Inboxes.

- If you've signed up for a number of ezines that you no longer want and have been unable to unsubscribe, click the box in the delete column.
- If you receive emails urging you to verify your subscription, for which you've never signed up, click the box.
- If you get email from companies offering you discounts on products that you're never going to buy, click the box.

Simple as that.

You can mark messages as spam and block them via sender, and even domain.

Avoid viruses, spam, junk mail and other pesky emails with MWP. Works with all email programs. I use Outlook 2019. Set-up is easy; MWP will import the settings for your existing email accounts.

Now, here comes the part that will turn some of you penny pinchers off. MWP is not free. The initial one-year subscription costs $29.96 and can be used on three computers, including your mobile devices. Renewals are $24.95 per year, three computers. I just renewed with a 2-year renewal for $43.16. I've been using MWP since version 1, they are now into version 7.

Hooray! There is a free 30-day trial version. You can use it with full functionality for thirty days and then subscribe or take your chances and do without it.

Travel to https://www.firetrust.com/products/mailwasher-pro# to get the trial version or pay to help the authors.

PATACS Membership

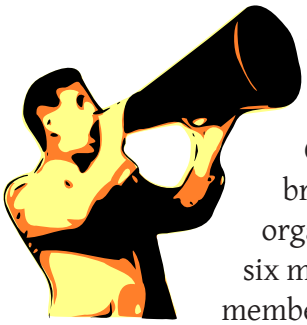
PATACS memberships are now available via electronic payment for US $30 per year. Payment may also be made via check or cash at our meetings.

Benefits include:

- Eligibility for door prize drawings,
- Monthly download of the full color, PDF-format PATACS Posts newsletter,
- Optional monthly US Mail delivery of the B&W print edition of the newsletter,
- Access to the PATACS email list (see below),
- Access to our membership database for noncommercial use,
- Members may place classified ads in the newsletter at no charge.

The time, effort, and money saved from your association with PATACS will quickly exceed the nominal annual dues.

Apply for or extend your membership at https://www.patacs.org/membershippat.html. You may also use the membership application to update your membership contact information.



Special Membership Promotion

Current members who bring a new member to the organization will receive a six month extension of their membership. New member is defined as someone who has not been a member in the thirty-six months prior to month of received application. The new member should list your name as the 'source' of their membership on the application form (pick up at meetings or download from https://www.patacs.org/membershippat.html).

Help Wanted: Meeting Speakers

Finding presenters for our meeting programs is difficult—your help in the effort to enhance the value we all receive from PATACS membership would be greatly appreciated!

Please consider speaking to your friends at an Arlington or Fairfax meeting. We'd love to feature your take on a smart phone or tablet app. A presentation on these or other topics of interest to you would undoubtedly be welcomed by your PATACS colleagues. We have space in our schedule for 15, 30, 60 and 75 minute discussions —what are you waiting for?

We also have ready-made paragraphs you could use in e-mail communications to help us find speakers. Contact: director2(at)patacs.org

PATACS Meetings Archive

Did you know that videos and presentation slides of most PATACS meetings are available on the PATACS website's 'Recent Meetings' page?

Go to https://www.patacs.org/recmtgspat.html and scroll down for links.

Shopping on Amazon.com? Don't Forget PATACS!

If you shop online at Amazon.com, don't forget to start each session by clicking the Amazon link on the PATACS home page, then continue shopping on Amazon as usual. Doing so earns PATACS a 4 to 6.5% commission on your purchase at no additional cost to you.

Thank you for supporting your user group!

PATACS Email Discussion List

Join the PATACS members-only email list to discuss tech topics of mutual interest, ask and answer questions, share resources, convey news, and increase our sense of shared community with fellow members.

(Continued on page 13)

(Continued from page 12)

Email sent to the list email address and replies are distributed to all list subscribers. Participation requires a valid PATACS member email address and your current email program (e.g. Microsoft Outlook, Mozilla Thunderbird, Google Gmail webmail).

Due to changes at Yahoo! Groups that hosted the original "PATACS-B" email list, PATACS rehosted the email list on the Groups.io service. All PATACS members should have received an email invitation to register a Groups.io subscription to the PATACS email list.

If you are a PATACS member and did not receive an invitation by email, review the information at https://groups.io/g/patacs and click on the "Join This Group" button.

If you do not receive email from patacs@group.io after joining, check the spam folder in your email program and ensure your email program does not block this email address.

APCUG Resources

PATACS is a member of the Association of Personal Computer User Groups (APCUG), a worldwide organization that helps technology user groups by facilitating communications between member groups and industry vendors.

Archived APCUG Presentations

Presentation PDFs and handouts can be found at: https://apcug2.org/category/virtual-tech-conference/.

Online Workshops

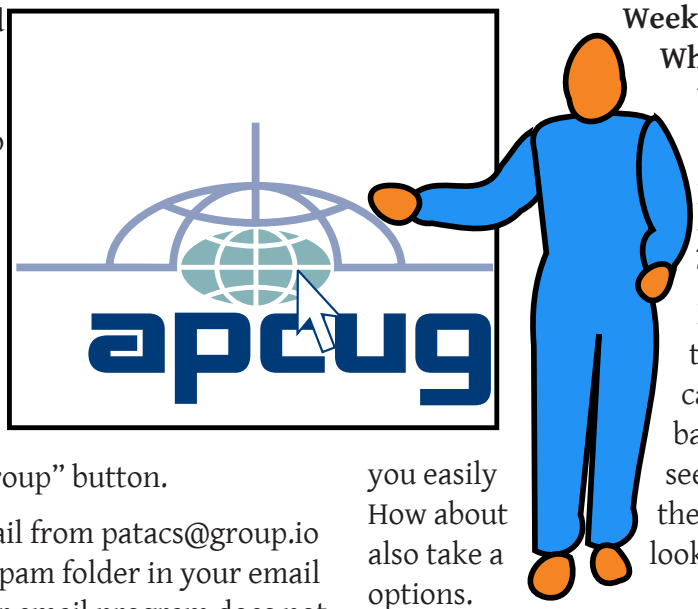
APCUG is pleased to announce online workshops during the Summer and Fall.

Getting to Know Windows from an Insider's Point of View

The second Wednesday of the month at 9 am PT, 10 am MT, 11 am CT, 12 pm ET

Moderator: Bill James, APCUG Advisor, Region 8

The four 2-hour workshops will be on how to get the best out of Windows 10. There will be how-tos, hands-on demos, and discussion with ample time for Q&A.



Week 1 (May 13, 2020): What's new with Windows 10, the 2004 Spring feature update.

Have you customized your Start menu, Taskbar, and Notifications? What are those Hidden Icons? How can I immediately get back to my Desktop? Can you easily see your mouse pointer? How about the Display text size? We'll also take a look at the powerful Search options.

Week 2 (June 10, 2020): Settings

We'll explore the many options you can change to make your computer more secure. Do you know how much RAM you have? What version of Windows? What about the Security & Update area, do you take a look at every once in a while? Do you check your custom settings after the Spring and Fall Feature update?

Week 3 (July 8, 2020): File Explorer

Back-in-the-day, Bill Gates told us to think of our hard drive as a file cabinet and to organize our files. File Explorer is our handy file cabinet. We'll dig into File Explorer to see how it can help us with our daily life with our computer. Have you added the helpful checkbox?

(Continued on page 14)

(Continued from page 13)

Week 4 (August 12, 2020): Edge

It's now a Chromium-based browser. It brings a lot of new features to the table. We will explore all of them and find out if it is the best browser. We'll also learn how to earn $$ by using Bing.

We will use the same Zoom password encrypted meeting URL for each workshop. You will receive the URL after you have registered by completing this form.

Judy Taylour will be the contact point for these workshops and will be available to assist you in connecting to the Zoom sessions.

The registration list will be used to identify everyone in the Waiting Room before being admitted to the session.

Home Automation for Seniors

The second Wednesday of the month at 9 am PT, 10 am MT, 11 am CT, 12 pm ET.

Week 1 (September 9, 2020): Why do I need it?

The next series of workshops will begin by explaining why home automation is important to Seniors, including what products are on the market, costs, security, and some real-world testimonials.

Week 2 (October 14, 2020): Where do I start?

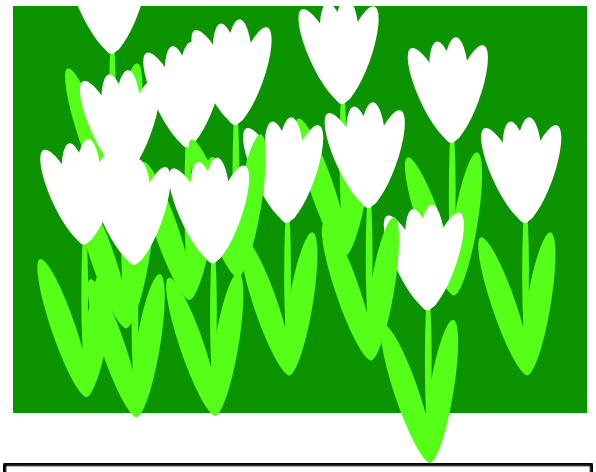
In the second week, we will talk about how to go about planning your home automation project and best practices.

Week 3 (November 11, 2020): Lights, doorbells, locks, and cameras

In the third week, we will talk about applications using lights, doorbells, locks, and cameras.

Week 4 (December 9, 2020): Doing It Myself vs Having It Done

Lastly, we will talk about the benefits of making it a Do It Yourself project or having a professional install.



Credit: https://xkcd.com/2304/, CC BY-NC 2.5

 PATACS Information Monthly Circulation: 100

PATACS, Inc. 201 S. Kensington St. Arlington VA 22204-1141

Club Information call: 703-370-7649 Web Site: www.patacs.org

Posts is an official publication of the Potomac Area Technology and Computer Society (PATACS), a Virginia membership corporation, a tax exempt organization under section 501(c)(3) of the Internal Revenue Code. Contributions are gratefully received and tax deductible. We encourage our members to organize small topic-specific meetings at your choice of time/place. For further information or suggestions chat with any officer or director. Tech clubs often have Special Interest Groups (SIGs) on topics such as photography, Windows, Apple products/services, genealogy, financial applications, and much more. SIGs offer members the opportunity to find others with similar interests and increase knowledge in specific areas. We are very fortunate to have members with many skills they generously share.

OPCUG / PATACS Saturday Meeting Information and Agenda

12:30 – Social time in Coffee Room / Annex

1:00 – 1:05: TA-1: Meeting Start – Introductions, Announcements

Please silence phones.

1:05 – 1:19: Q&A – detailed responses may be deferred to post-meeting communication.

1:20 – 1:50: 'Learn in 30' Presentation

1:50 – 2:00: Break in Coffee Room / Annex

2:00 – 3:20: Featured Presentation

3:20 – Door Prize Drawings (usually 3) for each group. Eligibility—group members only.

3:30 – Adjourn

Expect some flexibility in scheduled times. Order may be varied to accommodate scheduling needs of our valued presenters.

In June and December, a PC Clinic / Tech Help session is run concurrently with the meeting from 1 PM in the Annex.

See: https://www.patacs.org/clinicpat.html

With the concurrence of presenters, meeting sessions are webcast using the Zoom.us cloud meeting service.

Dues-paid members may 'attend' from remote locations, using the meeting number information provided on the PATACS website.

Please see:
https://www.patacs.org/mtgdetpat.html#3rdsat

For more information about using Zoom, see
https://www.patacs.org/zoom.html

PATACS, Inc.
201 S Kensington St
Arlington VA 22204-1141

FIRST CLASS MAIL

AFFIX
FIRST
CLASS
POSTAGE

TEMP-RETURN SERVICE REQUESTED

April 2020 PATACS Event Calendar

www.patacs.org | 703-370-7649

Sun	Mon	Tue	Wed	Thu	Fri	Sat
			1 7-9pm General Meeting, Online	**2**	**3**	**4** Hug a Newsperson Day
5 National Flash Drive Day	**6**	**7**	**8** Love the Internet Day 7-9pm Online Meeting	**9**	**10** Safety Pin Day	**11**
12	**13**	**14** Fractal Appreciation Day	**15**	**16**	**17**	**18** 1:00-3:30pm General Meeting, Online
19	**20** 7-9pm PATACS Board Meeting, Online	**21** National Library Day	**22** 7-9pm Technology & PC Help Desk, Online	**23** Int'l Girls in Information and Telecom Technologies Day	**24**	**25** June Newsletter Articles Due
26	**27** Morse Code Day	**28**	**29**	**30**		

Arlington: Carlin Hall Community Center
5711 4th Street South
Arlington VA 22204

Fairfax: Osher Lifelong Learning Institute
4210 Roberts Road
Fairfax VA 22032