The PULP

Newsletter of the Hartford User Group Exchange

http://www.huge.org Volume 35 Issue -- 06

June 21st General Meeting:

Geek Toys

Rev. Fleming Hall
2533 Main Street,
Glastonbury, CT

Q&A Session: 7 PM–7:15PM
Meeting starts at: 7:15PM

Member of apcug

An International Association of Technology & Computer User Groups

Contents	Page

The **PULP** is published monthly by and for members of the Hartford User Group Exchange, Inc. (**HUGE**). **HUGE** is a nonprofit organization whose aim is to provide an exchange of information between users of personal computers. The **PULP** is not in any way affiliated with any computer manufacturer or software company. Original, uncopyrighted articles appearing in the **PULP** may be reproduced without prior permission by other nonprofit groups. Please give credit to the author and the **PULP**, and send a copy to **HUGE**. The opinions and views herein are those of the authors and not necessarily those of **HUGE**. Damages caused by use or abuse of information appearing in the **PULP** are the sole responsibility of the user of the information. We reserve the right to edit or reject any articles submitted for publication in the **PULP**. Trademarks used in this publication belong to the respective owners of those trademarks.

MEETING LOCATIONS

Rev. Fleming Hall
2533 Main Street,
Glastonbury, CT

From The Editor

by Stuart Rabinowitz

This month is the semi-annual visit to "What to get the Geek in your life". That includes yourself.

In the news: Cracker Jack has replaced the iconic physical prizes with QR codes to play games on your phone/tablet.

The Panama Papers data breach is now searchable online Look up your 'favorite' rich person. But if you want to be a bit safer: Put your data in space .Cloud Constellation is planning a set of petabyte data centers on satellites called SpaceBelt. You would need a new communication center(s).

A Russian hacker has shared Millions of stolen email credentials online. BTW, most appear to be old and not in use. A different (?) hacker is selling 167 million LinkedIn user records.

Viv, the new voice assistant from the creators of Siri has been introduced. Researchers have begun to 'teach' computers to translate human languages accurately.

Lenovo Solution Center (LSC) software has a major security risk. A patch is available. A similar problem exists with other PC manufacturers.

100 thieves stole $12.7 million from ATMs in 2.5 hours

"Weasel pops Large Hadron Collider". Yes, a weasel knocked out the Large Hadron Collider.

Face recognition app FindFace may make you want to take down all your online photos. It boasts of a 70% accuracy, as in snap a photo of a stranger and then find out who that person is via their social media profile

Researchers are working toward an effective small scale microbial fuel cells for energy generation using urine.

Both the FCC and FTC have opened inquiries into smartphone security updates (or lack of).

Think you have privacy on the internet? Twitter location data reveals users' homes and workplaces.

The latest BackBlaze survey claims to know who makes the most reliable hard drive. Hitachi has tracked at just about 1 percent failure. Also, generally speaking, stay away from the 3 TB drives.

A U of Michigan, biomedical engineer has developed a 3D printed splint that absorbs into the body over time. The technique has already saved one life.

Send your comments to editor@huge.org

Until next month…Happy computing!!

Stuart Rabinowitz, Editor

Here is the appropriate copyright citation and a link to the full text. articles from "Tidbits"

http://creativecommons.org/licenses/by-nc-nd/3.0/

A Little Computer Quiz

1 We (should) all know "WOPR" (think Global Thermonuclear War), but what was the name of the first computer based war-game and when was it developed?

2 In 1954 where did programmers develop the first computer based blackjack program?

3 Who developed the first computer based game and when?

4 In 1947 a patent was filed for a "cathode ray tube amusement device", what game did it play?

5 With another homage to "WOPR", who developed the first computer tic-tac-toe game and when?

May Quiz Answers

1 This past April, 2016 marked the anniversary of the birth of the first mainframe affordable to smaller companies, What was it?
A The IBM System/360 was announced on April 7, 1964

2 What was the initial cost?
A Monthly rental of the base model was $2,700. The typical config was $115,000. Purchases were in the $133,000 to $5,500,000

3 What was the initial speed of the base model (in terms of additions/second)?
A 33,000 for the base model up to 25 times that for top of the line

4 As we all know the key to be able to use the computer is the software. So how many lines of code came with the initial system release?
A Initially it came with !,000,000 lines of code and grew to about 10 times that. By contrast the IBM 1401 (the competition) came with 100,000 lines

5 This computer has also appeared in several movies and TV shows including one fairly recent & popular series, which one?
A The advertising agency in "Mad Men" leased one in season 7. It also appeared in "The Doll Squad" & "The Girl Most Likely…"

Why Your Bits Might Be Flipped (and What to Do about It)

---

by Joe Kissell: <jk@alt.cc>, @joekissell
article link: <http://tidbits.com/e/16467>

While working on my latest book, "Are Your Bits Flipped?," I spent lots of time thinking about the widespread phenomenon of technology misconceptions. Hardware and software have seen incredible advances in recent years, and we've all become more accustomed to products that would have seemed magical just decades ago. At the same time, basic misunderstandings about technology are rampant, with results that range from comical to tragic. I'd like to offer a few reflections on why that may be and what to do about it.

<http://tid.bl.it/flippedbits-tidbits>

At a dinner party with some casual acquaintances, a guy asked me what I do for a living. I replied that I write books about technology. I mentioned a few of the topics and suggested that he might find them useful.

"I hope your books aren't the kind that try to explain how things work," he said, wrinkling his nose. "I don't have time for that, and I'm not interested. Just tell me what to click — that's all I care about."

I took a deep breath and paused to think about how to reply diplomatically. I said that my books usually do have lots of explicit, step-by-step instructions but that they also provide background explanations so that people who want to know what's going on behind the scenes can learn more. That clearly wasn't good enough for him, and he became defensive when I gently suggested that a little bit of behind-the-scenes information could never hurt.

I quickly changed the subject. But I felt sad, because this fellow's attitude made him prone to mistakes and ensured that he'd forever be relying on friends, technicians, and authors like me to figure things out for him and solve his problems.

Nobody is going to force you to understand the inner workings of your Mac or iPhone, an app or cloud service, or any other technology you might encounter. But however much you may try to distance yourself from the mysterious contents of the black box, your brain will automatically and involuntarily create a mental model that you'll rely on to predict future behavior and make decisions. The further that model is from reality, the greater the chance you'll experience confusion and frustration.

For example, suppose you use Gmail, and you notice that the Web sites you visit often have ads for exactly the products you've been discussing with a family member by email. Maybe that strikes you as mysterious or even suspicious, and you unconsciously form the opinion that someone at Google must be reading your email and actively passing along your interests to advertisers. That is, shall we say, a highly inaccurate description of what actually occurs. But if you've never looked into the details behind the technology, you might become excessively paranoid (or, at the other extreme, excessively trusting), and that can affect the way you use email, browse the Web, respond to advertising, and choose which products to buy.

More often than not, the initial flawed assumption is pretty tiny. Metaphorically speaking, it's nothing more than a "flipped bit" — a one that should be a zero or vice-versa — but it can lead the brain down the garden path to an elaborate misconception. For as long as I've been working in technology (over two decades), my mission has been to help people notice and eliminate these errors and thereby become smarter about how they use their tools.

And this is what I have to say to anyone whose brain has led them astray: It's not your fault (Fair warning: that video clip has some profanity).

<https://www.youtube.com/watch?v=GtkST5-ZFHw>

You know the old story about the guy whose computer had a broken "cup holder," but it was actually the CD-ROM tray. Or people who see the message "Press any key" but get stuck and call tech support because they can't find the Any key. There are countless tales like these, and when we hear them, we all laugh and roll our eyes, baffled that anyone could be that stupid.

<http://mistupid.com/people/page032.htm>

But stupidity isn't the right diagnosis. Rather, the people who create products have a set of assumptions, but the people who buy and use those products don't necessarily share the same assumptions; they have different mental models. If stupidity is indeed at work, one could just as easily say it was stupid of designers and engineers not to put themselves in the position of their customers and imagine what things would look like from their perspective.

Some of us may have more experience than others, or mental models that are more likely to match those of product designers, but anyone can experience a misconception about technology. If you have a bit flipped, it's not your fault. But if you have the opportunity to correct a flipped bit, you should take it!

In my opinion, the people who develop technology and the people who use it should be willing to meet each other halfway. You shouldn't have to be a technology expert to use a computer or smartphone, but on the other hand, following a policy of willful ignorance does no one any good. By all means, complain about foolish design choices, but also, read the manual. Urge developers to make their products "just work," but also, take responsibility for understanding how they're intended to be used.

There's no shame in not knowing something, or in being honestly mistaken. But being willing to learn more — to eliminate incorrect assumptions and improve your mental models — is a virtue.

Whenever I write a TidBITS article or a Take Control book, I start with the assumption that I understand the subject matter pretty well and end with the assumption that I've explained it clearly. Both assumptions are often wrong! Like everyone, I sometimes get my bits flipped. Tech reviewers and commenters point out factual errors that slipped past me, while editors and readers tell me when my explanations baffled them, despite my best efforts. Although I may grumble or gripe, I do my best to accept these corrections with equanimity. They're learning experiences. They mean I've just gotten a tiny bit smarter, and when I next revise the article or book, it'll be that much better.

Whether as technologists or as consumers, we can all benefit from examining our assumptions from time to time. The more willing we are to acknowledge our flipped bits and improve our understanding, the better our relationship with technology (and with other people) will be.

In that spirit, I invite you to take a look at "Are Your Bits Flipped?." Let me be candid: if you're a dyed-in-the-wool "just tell me what to click" person, this book is not for you. It's not a how-to book, like most Take Control titles. Instead, it's a series of essays about common tech misconceptions, inspired by my FlippedBITS series of TidBITS articles. For each myth or misunderstanding, it explains what's really going on in a friendly, down-to-earth way. Not only will it help to set your brain on the straight and narrow, it will also help you understand what may have led some of those bits to flip in the first place and learn what you can do to avoid future misunderstandings. I hope you find it both entertaining and educational — and I'll eagerly await your corrections.

<http://tid.bl.it/flippedbits-tidbits>
<http://tidbits.com/series/1285>

---

read/post comments:
<http://tidbits.com/e/16467#comments>
tweet this article: <http://tidbits.com/t/16467>

Make Sure You're Getting OS X Security Data
---

by Adam C. Engst: <ace@tidbits.com>, @adamengst
article link: <http://tidbits.com/e/16377>
9 comments

A few weeks ago, Josh Centers wrote about an update to OS X 10.11 El Capitan's System Integrity Protection that broke Ethernet for many Mac users briefly, before Apple pushed out a second update to resolve the problem (see "El Capitan System Integrity Protection Update Breaks Ethernet," 29 February 2016). Josh's article confused me for a bit, because the problem revolved around El Capitan's Incompatible Kernel Extension Configuration Data file, but I could find no evidence of it being installed on either my iMac or MacBook Air.

<http://tidbits.com/article/16296>

Discussion in the comments on that article and on TidBITS Talk revealed the answer: I had not selected the "Install system data files and security updates" checkbox in the App Store pane of System Preferences.

<http://tidbits.com/resources/2016-03/App-Store-prefs-before.png>

(No time to read more of this article right now? Just make sure that checkbox is selected and get on with your life. We now return the rest of you to the regularly scheduled explanation of what's going on.)

Why had I avoided such an important-sounding checkbox? Because Apple messed up the interface here in a big way. The top enclosing checkbox is clear: "Automatically check for updates." Everyone should have that checked. The next one isn't as simple: "Download newly available updates in the background." That's fine in most cases, but if you give network-connected presentations or are in bandwidth-constrained situations where Internet use without your knowledge might be problematic, turn it off. However, note what the interface says next: "You will be notified when the updates are ready to be installed." Great! That's exactly what I want to have happen — updates will be downloaded in the background and then I'll be notified and get to choose when to install.

It would seem that the next three checkboxes are related, but that's where Apple messed up. The next two — "Install app updates" and "Install OS X updates" — sound like "Install system data files and security updates," but they work differently. When selected, those first two checkboxes tell the App Store app to install app and OS X updates automatically; if you leave them deselected, you're instead notified of updates and given the opportunity install to them manually at a convenient time.

In contrast, if you fail to select "Install system data files and security updates," you won't be notified of these critical background security-related updates. These are not the same as Apple's foreground updates with names like "Security Update 2016-002" — they fall into the "OS X updates" category.

So what are they? TidBITS Talk member Al Varnell, who works in the security community, shared what he knows in the discussions there, but warns that the information is incomplete because Apple has avoided documenting these systems due to the security implications. These critical background updates include at least the following:

* Core Suggestions Configuration Data
* CoreLSKD Configuration Data
* Gatekeeper Configuration Data
* Incompatible Kernel Extension Configuration Data
* MRT Configuration Data
* XProtectPlistConfigData

I assume some of these files contain information used by security processes, as outlined in this Apple support article. Gatekeeper enables OS X to avoid opening applications that aren't signed. MRT likely stands for "Malware Removal Tool" since it appeared around the time of the MacDefender malware (see "Apple Responds to Increasingly Serious MacDefender Situation," 25 May 2011) — Apple's Security Update 2011-003 could detect and remove MacDefender. And XProtect is part of OS X's File Quarantine feature, which scans downloaded files for malware and blocks Web plug-ins with known vulnerabilities like Flash and Java. Incompatible Kernel Ex-

tension Configuration Data helps OS X disable old kernel extensions that may cause crashes, but it's unclear what Core Suggestions Configuration Data and CoreLSKD Configuration Data contain. (You might also see Chinese Word List Update; I presume that's not security-related.)

<https://support.apple.com/en-us/HT201940>
<http://tidbits.com/article/12199>
<https://support.apple.com/en-us/HT202225>

Apple needs to push out updates to these files based on new threats —

if Apple's engineers become aware of a new piece of malware, OS X's security systems need to know about it as soon as possible to protect Mac users around the world. Disabling the "Install system data files and security updates" checkbox is, frankly, a terrible idea — it's not installing code, and barring a mistake like Apple made in accidentally adding the Ethernet kernel extension to the Incompatible Kernel Extension Configuration Data file, it's unlikely that allowing this security-related data to be updated could cause many problems.

So if you've deselected "Install system data files and security updates," turn it back on and wait a day or two for Software Update to notice and update everything.

<http://tidbits.com/resources/2016-03/App-Store-prefs-after.png>

If you don't want to wait, select that checkbox and then issue this command in Terminal.

```
sudo softwareupdate --background-critical
```

To verify that the updates have taken place, look in the Software > Installations category in System Information (as explained in "El Capitan System Integrity Protection Update Breaks Ethernet") — click the Date Installed column header twice to sort with the newest installations at the top.

<http://tidbits.com/resources/2016-03/System-Information-installations.png>

For those who are constitutionally opposed to automatic updates, this is how you can get these critical background updates manually: select the checkbox, run the softwareupdate command above, verify that the updates have taken place, and then deselect the checkbox again.

It's worth noting that, despite Apple's policy of releasing security updates only for the current version of OS X and two versions prior, the company continues to update these security data files all the way back to 10.6 Snow Leopard, when the File Quarantine feature made its debut.

Regardless, Apple should clarify the importance of this checkbox by rewording it to something like "Install critical anti-malware definitions and system data." Having it selected is presumably already the default, but wording like that should prevent unwitting users from disabling it. Plus, if that checkbox is not selected, Software Update should notify the user about each individual update, just like any other OS X update.

---

read/post comments:
<http://tidbits.com/e/16377#comments>
tweet this article: <http://tidbits.com/t/16377>

Restricting Your Cell Carrier's Use of Your CPNI Data

---

by Adam C. Engst: <ace@tidbits.com>, @adamengst

article link: <http://tidbits.com/e/16345>

4 comments

I recently received a message from AT&T, my cellular service provider, alerting me to the fact that I could restrict AT&T from using my "customer proprietary network information" (CPNI) within the AT&T family of companies for AT&T's own marketing purposes. The message was plainly written yet utterly inscrutable. For instance, it defines CPNI as including:

"the types of telecommunications and interconnected VoIP services you currently purchase, how you use them and the related billing for those services. CPNI does not include your telephone number, your name, or your address."

<http://tidbits.com/resources/2016-03/ATT-CPNI-notice.png>

It's reassuring to know that CPNI does not include your telephone number, name, or address, but the phrase "how you use them" is as clear as mud. In its CPNI privacy policy, AT&T provides a little more information, such as the fact that "calling details" are also part of CPNI.

<http://www.att.com/gen/privacy-policy?pid=2566>

Confused, I turned to Geoff Duncan, who has written extensively on telecommunications and data privacy issues for TidBITS over the years. He explained that CPNI originally referred to anything that might appear on your bill, but now varies widely by service and carrier. With cellular carriers, it might include your data plan and usage, device info, location history, Web browsing history, and even demographic information.

What is CPNI used for? AT&T says that it "does not sell CPNI to unaffiliated third parties," and another page about CPNI clarifies just which companies qualify as being able to use this information — there are a lot:

"The AT&T family of companies are those AT&T companies that provide communications-related products and/or services, including the AT&T local and long distance companies, AT&T Corp., AT&T Long Distance, AT&T Internet Services, AT&T Mobility and other subsidiaries or affiliates of AT&T Inc. that provide, design, market or sell these products and/or services."

<http://www.att.com/gen/privacy-policy?pid=22561>

Geoff said that the FCC's original regulatory framework was intended to prevent two practices. The first is uncompetitive upselling, which could happen if a telco used its CPNI to tweak pricing for additional services for a particular customer in ways that competitors couldn't match, for instance. The second, "pretexting," prevents CPNI from being purchased by an outside party that would then pretend to be the phone company in order to get a customer to disclose or do something they wouldn't otherwise.

<https://www.fcc.gov/consumers/guides/protecting-your-telephone-calling-records>

The most recent changes to the CPNI legislation were back in 2007, but Geoff said that AT&T started notifying customers about the company's use of CPNI in 2012. Indeed, when I searched through my email archives on "CPNI," there was just one hit, an identically worded message from AT&T, sent in August 2012.

Are there any actual abuses of CPNI? Yes. Additional research revealed, among many other stories at the Electronic Privacy Information Center (EPIC), that in 2014 Verizon paid a $7.4 million fine for using CPNI for marketing purposes without informing customers. Worse, AT&T had to pay a $25 million fine in 2015 for disclosing personal information (and misusing CPNI data) for almost 280,000 of its U.S. customers, thanks to crooks paying off employees in three AT&T call centers in Mexico, Colombia, and the Philippines to unlock stolen and/or grey market phones.

<https://epic.org/privacy/cpni/>
<https://apps.fcc.gov/edocs_public/attachmatch/DA-14-1251A1.pdf>
<https://apps.fcc.gov/edocs_public/attachmatch/DOC-332911A1.pdf>

It's important to realize that restricting a carrier from using your CPNI doesn't prevent it from being collected, so opting out might not prevent such information from being swept up in data breaches like AT&T's, but it certainly can't hurt. Regardless, the fact that the FCC felt it was important to require telcos to offer such an opt-out makes me think it's worth doing.

Restricting AT&T from using CPNI isn't difficult, but it does require information you may not have handy. Follow these steps (or you can use a voice-response system at 800-315-8303 or talk to a person at 800-288-2020):

1. Go to http://att.com/ecpnioptout. (Amusingly, the link underneath the associated text in the email message used a tracking link, which makes me wonder if a click on it would become part of my CPNI.)

<http://att.com/ecpnioptout>

2. Enter your account number or customer ID and billing ZIP code, select Restrict Use of My CPNI, and click Submit.

The tricky part here is getting your account number, which is most easily found on your bill or by logging in to AT&T's site and looking in your profile. AT&T says it's also available on the CPNI notice, which isn't true — you can see my notice above, and there's no ID on it.

<http://tidbits.com/resources/2016-03/ATT-CPNI-opt-out.png>

What about other carriers and other types of personal information that's gathered and potentially shared or sold? A page in the MIT Information Systems & Technology Knowledge Base offers links to opt out of these and other programs at AT&T, Verizon Wireless, and Sprint. I'd encourage everyone to explore those links — I discovered that although our phone numbers were opted out of AT&T's "External Marketing & Analytics Reports," they were still set to receive "Relevant Advertising — Wireless," whatever that is. MIT's page says that T-Mobile does not sell CPNI, which seems to match with T-Mobile's CPNI page.

<http://kb.mit.edu/confluence/pages/viewpage.action?pageId=152570432>
<http://www.t-mobile.com/Company/PrivacyResources.aspx?tp=Abt_Tab_CPNI>

Personally, I'm not particularly perturbed to have my information used when businesses offer me products or services. However, if this information is so valuable, why do companies get to collect it (from services we're paying for!) and use it for free? Wouldn't it be interesting to put personal information into a marketplace, where you would get to say for what purposes it could be purchased, and for how much? Some Italian researchers did a study on the economics of personal data back in 2014, and there's even a firm called Handshake aiming to do this, but it has been in closed beta since 2013, which isn't a good sign. Still, food for thought...

<https://www.technologyreview.com/s/528866/researchers-test-personal-data-market-to-find-out-how-much-your-information-is-worth/>
<http://handshake.uk.com/>

---

read/post comments:
<http://tidbits.com/e/16345#comments>
tweet this article: <http://tidbits.com/t/16345>

PULP Staff

Editor Stuart Rabinowitz

Distribution George Carbonell

Membership: Anyone may become a member. Dues are $12 per year and includes a one-year subscription to The Pulp. Meeting topics, times and places can be found on page 1 of this issue.

Officers & SIG Leaders

Leader:	George Carbonell	860 568–0492	george.carbonell@comcast.net
Secretary:	Stuart Rabinowitz		
Treasurer:	Charles Gagliardi	860 233 6054	epencil@aol.com
Director at Large:	Phil Manaker	860 659-4584	amanaker@earthlink.net
Director at Large:	Ted Bade	860 643-0430	tbade@cox.net
Director at Large:	Stuart Rabinowitz	860 633–9038	s.e.rabinowitz@att.net
Web Manager:	Bob Bonato		bob@bonatodesign.com
Membership:	Richard Sztaba		richer1@aol.com
Integrated SIG:	Stuart Rabinowitz		

		June	2016			
			1 1867 the typewriter first described	2	3	4 1979 VisiCalc demo'd
5	6	7	8 1979 The Source goes online	9	10	11
12	13	14	15	16 1911 CTR (IBM to be) founded	17	18
19	20	21 ***General Meeting*** ***7 PM***	22	23 Alan Turing birthday	24	25
26	27	28 Tau Day	29	30		