Colleagues,

Great news...this week Chinese President Xi Jinping said that China and the United States could work together to address cyber crimes. Wow, that was easy...if only all problems could be solved so easily. Okay, despite our hopeful thinking we all know that’s not the end of the Chinese cyber threat. For this reason and many more, the importance of maintaining our respective skill sets cannot be emphasized enough. Your chapter board understands that and it is one of the reasons we are working so hard to introduce speakers on different topics. In a career field such as ours, some people still find it very easy to rest on yesterday’s knowledge, and the fact of the matter is that if you want a job where you can learn something and apply it the same way for the next 20 years then cyber security is probably not the career field you want to be in. In our career field we have to be continually on top of the latest threats and current attack vectors, and we want to ensure that you are receiving information on current tools and receiving the knowledge to combat those threats. If you have topics you would like to see a presentation on let us know, and we’ll find a person or organization that can speak to that topic.

In October we’re going to give you more opportunities to expand your knowledge base by hosting two (2) Cyber Focus days. The first one will be at Peterson AFB on 27 Oct and the second one will be at Ft. Carson on 28 Oct. The agendas are still being worked but there will be several speakers at each event and opportunities to earn continuing education credits. Watch for more information coming out soon.

(Continued on page 9)
Crystal knows best ... or too much? The disconcerting new email advice service


Do your emailed attempts at sarcasm routinely backfire? Do you never know when to sign off with “x”, or go in with an emoji? Is your judgment of basic etiquette lacking? Then you might be in the target audience for Crystal, a new tool that bills itself as the “best improvement to email since spellcheck”, and is elsewhere described as “somewhere between a horoscope and a Myers-Briggs profile” and “walking the line between innovative and super creepy”.

Crystal creates a unique profile for anyone with a LinkedIn account, explaining how to speak, email, work with or sell to them most effectively. With disconcerting specificity, it tells you the “words, phrases, style and tone you should use to reach the recipient in the way that they like to communicate, rather than your own” – even their tolerance for sarcasm and emoticons.

It builds this profile from what it can glean about them online: their public Facebook or blog posts, their tweets and the other bits and pieces we all leave like a trail of breadcrumbs behind us as we go about our business on the internet.

For a sum, Crystal will even draft emails to people you’ve never met, using a tone and language that their online presence suggests will resonate with them.

“Elle is naturally stoic and methodical about decisions, but is willing to take a risk if it is backed up by enough logic,” it tells me about myself, somewhat hesitantly. Despite the 49,300 tweets attached to my name, Crystal’s “accuracy confidence” is just 47%, acknowledging that it found “limited data ... but enough to analyse”.

Pressing on, Crystal recommends that someone setting out to email me would be best to do so in “three sentences or less” (...fewer?), and should eschew exaggeration and “sarcastic remarks” in favour of using “data to prove a point”.

Its assessment of me is eerily accurate: I am a cyborg, incapable of humour, emotion and empathy, and consequently intolerant of all demonstrations of them by others. I’m a little surprised that it didn’t mention the fact I never blink and am comprised mostly of scrap metal, but I guess that’s what the 53% of wiggle room allows for.

In fact, I’d say the 47% accuracy figure is about right. Though I am not quite as robotic as Crystal suggests, I am a fairly to-the-point person and, though I delight in rambling, expressive emails from friends – even those that dip into metaphor – I’d be less enthusiastic to receive one from a stranger.

I think twice before giving third parties access to my inbox but, intent on seeing how deep the rabbit hole went, I installed the Crystal Gmail extension. The add-on makes suggestions in real time as you type.

I went to compose an email to my friend Craig, an early adopter who made me aware of the service when he tweeted a screenshot of his profile that said empathy “did not come naturally” to him as though it were something to be proud of – a fact that probably tells you more about him than Crystal can.

“Be logical,” Crystal urged me before I’d typed a single word. “I Changes,” it flashed after I’d written just five: “Hi Craig, how’s it going”?

“Craig wants to read a thoughtful, interesting message with casual language that gives him something to be curious about,” it said (Crystal’s emphasis). “Consider leaving out the friendly but unnecessary phrase how’s it going or ask a more specific question.”

I’d never felt performance anxiety when it came to writing an email before, but then I’d never been told that I must interest my correspondent “on an intellectual or personal level”. Big Brother has never felt quite so immediate – or judgmental.

“Read the rest here: http://www.theguardian.com/media/2015/may/19/crystal-knows-best-or-too-much-the-disconcerting-new-email-advice-service"
We are currently maintaining our membership level around 380. Please keep those renewals as well as new member referrals coming! We’re working closely with ISSA International about the pilot test of the “Freemium” student sponsorship program. We’re at the “how do we actually implement” phase of the discussion. We’ve been working with the database/website developer for ISSA International to figure out the actual mechanics of making this work. They have gotten some initial work done and in test. We are providing feedback and after some modifications and further tests we expect this to be available within the next couple of weeks. So, we’re getting close! That will definitely help our numbers as we get some new student members enrolled. I will be presenting our Freemium program status to the Chapter Leaders’ summit as part of the ISSA International Conference. As one of the “guinea pig” chapters (Baltimore is the other one) we will begin putting together our chapter implementation plan to get it off the ground as soon as the website functionality is finalized. I have sent out a couple of emails to students so far that I’m aware of. I intend to reach out to as many student members as possible over the next few weeks. However, I will ask that all current student members who are coming up for renewal to drop me an email (address below) that includes your name, membership number, expiration date and student status (currently enrolled and graduation date) so I can get this resolved for folks as quickly as possible. We’ve got lots of upcoming activities and we want to ensure everyone stays informed of everything. That information will also let me prioritize some test cases as we get the ISSA International program off the ground. More information will be published about this great opportunity for our chapter as it becomes available.

We will be supporting the UCCS Peak Chaos Career night on October 22. It will be held at 7:30 PM at UCCS in Osborne A208. This is the same location as last year when we supported also supported their meeting. It was a great opportunity to interact with students. We got to share our backgrounds and careers as well as representing ISSA. It was very successful for both their club and the chapter. Last year we were able to represent the broad range of cybersecurity here in the Springs—Government, military, contractors, and commercial. If you can support this meeting at UCCS please let me know as soon as possible and I will coordinate with everyone who volunteers. My email address is at the bottom of this article.

Melissa Absher has been working getting the mentorship program rolling again with the start of the new school year. There will be a mentoring kickoff meeting for mentors October 20 from 4:00-5:30pm. More to follow on that in the near future. In addition, we are working on a separate mentoring program for entry level professionals. This coincides with several initiatives that ISSA International is trying to work to get their Cybersecurity Career Lifecycle program off the ground. Again, more to follow soon. If you are interested in being a mentor to either of these groups, please contact either Melissa Absher or me.

Last, and of course not least, I’d like to welcome those new members on behalf of the Chapter! When you’re participating in Chapter activities, please take a moment to introduce yourself to members of the board, me, and other members. Don’t forget to identify yourself as a new member and feel free to ask for help or information.

Thanks for joining the Chapter and don’t forget to look for opportunities to lend your expertise to improve the Chapter. We’re always open to new ideas and suggestions.

David Reed
Membership Committee Chairman
dreed54321@comcast.net

<table>
<thead>
<tr>
<th>New Members</th>
</tr>
</thead>
<tbody>
<tr>
<td>September</td>
</tr>
<tr>
<td>Kimberly Han</td>
</tr>
<tr>
<td>Janis Fleming</td>
</tr>
<tr>
<td>Michelle Barnett Griffin</td>
</tr>
<tr>
<td>James Fredette Jr.</td>
</tr>
<tr>
<td>Thomas P. Karmondy</td>
</tr>
</tbody>
</table>
A Note from our VP

The end of the calendar year is coming quickly. Secure World is being held in Denver on the 15th. There are two free passes left if someone wants to volunteer to help with our table. Then there is the CyberGirlz even on the 24th. This is an opportunity for the women in the chapter to encourage young females into the cyber security world. Instead of a conference at UCCS we are partnering with Federal Business Council (FBC) and their Tech Fair. The first Tech Fair will be on Peterson Air Force Base on the 27th and the second is at Fort Carson on the 28th. We will need volunteers for both of these events. There will be a luncheon on Nov 18th and our December award luncheon on the 4th.

I want to say a special thank you to all that have volunteered this year especially the training team. Without your help the chapter could not be as successful as it is. The training team had to update both Security + and CISSP slides year before teaching the classes. They did a great job and several people have passed the exams.

Cindy

Upcoming Events:

  
- ISSA-COS will have a table on **Oct 15** – need volunteers to staff the table – coordinate with Chuck Forth or Pat Laverty

- **Oct 24** – CyberGirlz event at Fox Meadow Middle School *(see page 5)* – if anyone is attending please contact Cindy Thornburg.

- **Oct 27** – Peterson Air Force Base FBC Tech event and ISSA-COS conference

- **Oct 28** – Fort Carson FBC Tech even

- **Nov 18** – Lunch meeting at TREA
Regis University in cooperation with Harrison School District presents CyberGirlz

Event location:
Fox Meadow Middle School, Harrison School District, Colorado Springs, CO

All middle & high school girls are HIGHLY ENCOURAGED to register.

To provide opportunities and address the need to support women going into the cybersecurity and technology fields

Training workshops to introduce girls to tools and technology: After school computing workshops will be conducted starting in mid-September leading up to the 24 Oct event.

CyberGirlz Event Schedule 24 Oct

8:50 AM Registration (Continental Breakfast) 11:50 AM Networking Lunch & Resource Fair
9:00 AM Welcome 1:00 PM Intro to CTF (Capture the Flag), Team Formation
9:30 AM Presentation: Keynote, Women in Computing and Technology 1:30 PM Closing Comments and Departure
9:45 AM Panel Discussion (Woman in Cyber Futures) Lecture and Q & A
Wireless Hacking In Flight: Air Force Demos Cyber EC-130

By Sydney J. Freedberg Jr., Breaking Defense, September 15, 2015

Matthew Broderick in his basement, playing Wargames over a landline, is still the pop culture archetype of a hacker. But as wireless networks became the norm, new-age cyber warfare and traditional electronic warfare are starting to merge. Hackers can move out of the basement to the sky. In a series of experiments, the US Air Force has successfully modified its EC-130 Compass Call aircraft, built to jam enemy transmissions, to attack enemy networks instead.

“We’ve conducted a series of demonstrations,” said Maj. Gen. Burke Wilson, commander of the 24th Air Force, the service’s cyber operators. “Lo and behold! Yes, we’re able to touch a target and manipulate a target, [i.e.] a network, from an aircraft.”

What’s more, Wilson told reporters at the Air Force Association conference here, this flying wireless attack can “touch a network that in most cases might be closed” to traditional means. While he didn’t give details, many military networks around the world are deliberately disconnected from the Internet (“air-gapped”) for better security. You can try to get an agent or dupe to bring a virus-infected thumb drive to work, as reportedly happened with Stuxnet’s penetration of the Iranian nuclear program, but that takes time and luck.

You unlock a lot more virtual doors if you can just hack a network wirelessly from the air. Israeli aircraft using BAE’s Suter system reportedly did just this to Syrian air defenses in 2007’s Operation Orchard, and the Navy is interested in the capability, but this is the first I’ve heard an Air Force general discuss it. Digital AESA radar can do much the same thing, as we’ve reported about the F-35.

“That doesn’t mean that we may not still try to touch a target through a traditional networking set of capabilities, but to be able to go and use the other domains [e.g. from the air] I think is really the future,” Wilson said.

The big picture here is not any one aircraft, but the ability to attack a single target simultaneously in multiple ways from multiple domains. That’s both high explosives and hacking, coming from cyberspace, from electromagnetic signals propagating through air and space, and — if you bring in the other services — from the sea and land as well. “In the past those have been fairly separate,” Wilson said. “What we’re seeing today is a power of being able to integrate those.”

Read the rest here:

Update Your Profile!
Don’t forget to periodically logon to www.issa.org and update your personal information.
At least 81% of major healthcare or health insurance companies had a data breach in the past two years

By Jennifer Abel, Consumer Affairs, September 4, 2015

A recent report by auditing service KPMG confirms what most Americans probably suspected already: personal data held by hospitals and health insurance companies is extremely insecure. Indeed, KPMG says that 81 percent of hospitals and health insurance companies suffered a data breach in the past two years.

"Extremely hackable" health care system

The hackability of American health care won’t surprise anyone who’s paid attention. Consider this partial sampling of hacks dating back only to summer 2014: that August, the for-profit hospital network Community Health Systems admitted that Chinese hackers had breached their network and stolen confidential data on more than 4.5 million patients. The following February, the Anthem health-insurance network admitted that hackers had stolen up to 80 million medical records dating back to 2004.

In March, Premera Blue Cross admitted to a breach compromising 11 million medical and financial records dating back to 2002. CareFirst Blue Cross/Blue Shield admitted to a hacking in May: “only” 1.1 million records were compromised that time. In mid-July, the UCLA Health System admitted that 4.5 million patient records were at risk from a hacking UCLA had discovered two months earlier.

In May – around the same time that the UCLA hacking occurred, though two months before any affected patients were notified of it, Larry Ponemon, of the Ponemon Institute, and Rick Kam, of ID Experts, co-wrote an article for the Dark Reading security blog suggesting outright that “escalating cyberattacks threaten U.S. healthcare systems … Imagine a hostile nation-state with your psychiatric records. Or an organized crime ring with your child’s medical file. Or a disgruntled employee with your medical information.”

And stealing medical or financial records isn’t the worst thing hackers might do to hospital patients, either. Early last month, the Food and Drug Administration issued an alert advising hospitals and medical centers to stop using a certain model of wireless-connected intravenous pump because hackers could exploit a security vulnerability to remotely seize control of a patient’s IV; it would allow hackers to make potentially fatal alterations to the amount or type of drugs administered.

Matter of national security

Such anecdotes arguably painted a bleak-enough picture of American medical cybersecurity, even before KPMG released its report with that dismal 81-percent statistic.

Greg Bell, KPMG’s Cyber US Leader, said “These are all incidents where they have determined they lost data. This wasn’t just a malware or a virus infection – it actually went to exfiltration.”

To produce the report, which is available as a .pdf file here, KPMG analyzed a survey of 223 senior security or technology executives from health care organizations with more than $500 million in annual revenues. “Apart from typical financial fraud, there is also the possibility of medical insurance fraud, or, in the case of providers, attacks on computer-controlled medical devices. As this is the largest part of the U.S. economy and a safeguard of peoples’ well-being, healthcare is a matter of national security,” KPMG explained in the report's executive summary.

Yet despite such high stakes, “the healthcare sector lags in terms of its preparedness for cyber threats…. In terms of technical capabilities, the healthcare industry is behind other industries in protecting its infrastructure and electronic protected health information.”

Read the rest here:
Ouroboros, one of the world’s most sophisticated hacking groups with close ties to the Russian government, has been accused of hijacking unencrypted commercial satellite communications. They use hidden receiving stations in Africa and the Middle East to hide their Control & Command servers and mask attacks on Western military and governmental networks.

The group which created the advanced malware known as “Snake” or “Turla” was exposed last year as having mounted aggressive cyber espionage operations against Ukraine and a host of other European and American government organizations over nearly a decade.

In a report by Kaspersky released on Wednesday, they said they had identified a new “exquisite” attack channel being used by the group that was virtually untraceable. The need for hackers to communicate regularly with machines they have compromised allows security researchers to trace back the hackers’ Command & Control servers.

“This method makes it almost impossible to discover the physical location of these C&C servers,” said Stefan Tanase, senior security researcher at Kaspersky. “Safe to say this is the ultimate level of anonymity that any cyber espionage group has reached in terms of hiding its origins.”

The Ouroboros satellite hack exploits the fact that most satellite communications being sent from satellites back to earth are unencrypted, and so can be spoofed. The process is laid out by Kaspersky in a large illustration and follows a number of steps.

First, the Ouroboros malware sends out a request for instructions. Normally such a request goes straight to a C&C server, and is traceable. Ouroboros instead sends the request to an unwitting decoy server, because the hackers have identified it as a satellite communications user.

The request from Ouroboros is then automatically routed via a commercial satellite and beamed to earth towards the location of the decoy. Once the decoy server receives the request for instructions, it discards it, because the request is meaningless to it.

But the satellite will have beamed the request over a large geographical area. A hidden receiver anywhere in the area, planted by Ouroboros’ operators, can then pick up the unencrypted request. The receiver then issues a reply to Ouroboros, disguised as a communication returning from the decoy.

This way, any defender looking to trace communications from Ouroboros back to its controllers will lose the trace from the point at which the data becomes a signal beamed from a satellite, effectively breaking any direct digital link.

Ouroboros’ handlers are using satellite operators in the Middle East and Africa. Finding the receivers depends on the size of the dish, but it’s a needle in a haystack because the area could be tens of thousands of square kilometers.

“The receivers do not necessarily cost much themselves but finding a physical location for these indicates that there is some kind of extensive logistical support network,” Kaspersky said. Such operations point to a state intelligence service, he added.

For the moment, satellite operators are powerless to prevent the hackers from routing requests through their networks until they encrypt all of their downstream communications, which would cost hundreds of millions in new satellite arrays.

Read the rest here:
https://blog.knowbe4.com/expert russians hackers use satellites to hide amazing exploits
Training Team Update

**CISSP**

We completed the 2015 CISSP Exam Prep Review Seminar, and already know that at least one of our students passed the exam! This year’s seminar would not have been possible without the amazing support from our Training Team volunteers. They spent countless hours developing new slides, and sample questions, for each of the eight new (ISC)² Common Body of Knowledge domains. Over 900 slides were developed to cover the requisite material and ensure our students receive the most current and complete information possible to help prepare them for the CISSP exam. Three other ISSA Chapters requested copies of our slides due to their inability to accomplish what our Training Team volunteers did. A huge THANK YOU goes out to every one of them for their time/efforts in developing slides, reviewing our draft slides for accuracy and completeness, providing refreshments for our students and instructors, and for teaching the material!

**Security+**

We’ve completed two very successful Security+ Exam Prep Review Seminars so far this year, one in April and one in June, with our final Security+ Seminar scheduled later this month. These seminars would not be possible without the exceptional support of our Training Team volunteers. Nearly 200 slides required a complete review and update to incorporate the new CompTIA 401 exam objectives to ensure our students receive the most complete and current information possible. A huge THANK YOU goes out to everyone who helped develop/update the slides, organize the seminars, provide refreshments for the students and instructors, and for teaching the material!

Our final Security+ Exam Prep Review Seminar for 2015 is scheduled for 17 Oct, at Colorado Technical University (CTU). We already have at least 10 students registered for the class, with less than two weeks remaining to sign up. If you’re interested in attending, or have any questions, please send an email to our Chapter Training leads at: [Training@issa-cos.org](mailto:Training@issa-cos.org), or sign up at the EventBrite site: [https://www.eventbrite.com/e/security-exam-prep-seminar-tickets-18708131525](https://www.eventbrite.com/e/security-exam-prep-seminar-tickets-18708131525).

**CEU/CPE Ideas**

Do you know there are numerous free or low cost CEU and CPE options available? Check out the ISSA-COS web page ([http://www.issa-cos.org/](http://www.issa-cos.org/)), Training Classes, “On-Line Training” link for suggested sites.

**Volunteer Opportunities**

Looking for a volunteer opportunity? Looking for a way to share your knowledge/expertise? Looking for a way to earn CompTIA CEUs or (ISC)² CPEs? We’re always looking for members to teach one or more of the Security+ or CISSP domains. We provide the slides, but you can modify them as you see fit as long as your changes remain consistent with the official CompTIA or (ISC)² criteria. If you would like to volunteer to teach one of the Security+ or CISSP domains, or if you have questions, please contact our Chapter Training leads at: [Training@issa-cos.org](mailto:Training@issa-cos.org).

*If you have ideas/suggestions/requests for training initiatives, please email our Training leads at: Training@issa-cos.org.*

(Continued from page 1)

This month I really want to highlight our chapter’s training team that is doing amazing work. Over the past several months they revamped the entire CISSP course, adjusting material to meet the new ISC² requirements. I can tell you that we have been contacted by several chapters requesting our training material, and we’re happy to brand and share it. This highlights that we are once again leading the way and making a difference for ISSA and chapters around the nation. We have outstanding volunteer members willing to give a little, or in some cases a lot, of their time so that we can teach current CISSP, as well as Security+, material to our training attendees. Our chapter thanks all of you who are taking the time to make a difference for our chapter by serving on our training team...it is people like you that make our chapter so special.

We are always looking for more volunteers to work on committee’s or to help in some small way, so if you have some time to give and want to get involved to help your chapter move forward please reach out to us. Thanks for all you do.

Pat
Once seen as bulletproof, 11 million+ Ashley Madison passwords already cracked

By Dan Goodin, ArsTechnica, Sep 10, 2015

When the Ashley Madison hackers leaked close to 100 gigabytes' worth of sensitive documents belonging to the online dating service for people cheating on their romantic partners, there seemed to be one saving grace. User passwords were cryptographically protected using bcrypt, an algorithm so slow and computationally demanding it would literally take centuries to crack all 36 million of them.

Security researcher could only crack weak passwords—just 0.0668% of trove.

Now, a crew of hobbyist crackers has uncovered programming errors that make more than 15 million of the Ashley Madison account passcodes orders of magnitude faster to crack. The blunders are so monumental that the researchers have already deciphered more than 11 million of the passwords in the past 10 days. In the next week, they hope to tackle most of the remaining 4 million improperly secured account passcodes, although they cautioned they may fall short of that goal. The breakthrough underscores how a single misstep can undermine an otherwise flawless execution. Data that was designed to require decades or at least years to crack was instead recovered in a matter of a week or two.

The cracking team, which goes by the name "CynoSure Prime," identified the weakness after reviewing thousands of lines of code leaked along with the hashed passwords, executive e-mails, and other Ashley Madison data. The source code led to an astounding discovery: included in the same database of formidable bcrypt hashes was a subset of 15.26 million passwords obscured using MD5, a hashing algorithm that was designed for speed and efficiency rather than slowing down crackers.

The bcrypt configuration used by Ashley Madison was set to a "cost" of 12, meaning it put each password through $2^{12}$, or 4,096, rounds of an extremely taxing hash function. If the setting was a nearly impenetrable vault preventing the wholesale leak of passwords, the programming errors—which both involve an MD5-generated variable the programmers called $loginkey$—were the equivalent of slashing the key in a padlock-secured box in plain sight of that vault. At the time this post was being prepared, the blunders allowed CynoSure Prime members to positively crack more than 11.2 million of the susceptible passwords.

Read the rest here:

Ashley Madison password crack could spell trouble across the Internet

By Dan Goodin, ArsTechnica, Sep 10, 2015

Now that a hobbyist team has uncovered programming errors that make more than 15 million of the Ashley Madison account passwords orders of magnitude faster to crack, it will be only a matter of time before a large percentage of them are available to hackers everywhere. And given how rampant password reuse is, the tsunami-sized torrent is sure to affect accounts all over the Internet.

As Ars chronicled in a 2012 feature headlined Why passwords have never been weaker—and crackers have never been stronger, it's not unusual for Twitter, Amazon, and online services to monitor large leaks and require password changes for affected users. As we reported:

In late 2010, Sean Brooks received three e-mails over a span of 30 hours warning that his accounts on LinkedIn, Battle.net, and other popular websites were at risk. He was tempted to dismiss them as hoaxes—until he noticed they included specifics that weren't typical of mass-produced phishing scams. The e-mails said that his login credentials for various Gawker websites had been exposed by hackers who rooted the sites' servers, then bragged about it online; if Brooks used the same e-mail and password for other accounts, they would be compromised too.

The warnings Brooks and millions of other people received that December weren't fabrications. Within hours of anonymous hackers penetrating Gawker servers and exposing cryptographically protected passwords for 1.3 million of its users, botnets were cracking the passwords and using them to commandeer Twitter accounts and send spam. Over the next few days, the sites advising or requiring their users to change passwords expanded to include Twitter, Amazon, and Yahoo.

Read the rest here:
Windows 10 Worst Feature Now Installing On Windows 7 And Windows 8

By Gordon Kelly, Forbes, September 6, 2015

Last week came the warning, now comes the roll out. The most criticised aspect of Windows 10 is coming to Windows 7 and Windows 8 after Microsoft released upgrades which enable the company to extensively track what users are doing. The releases bring good and bad news...

**The Bad News**

The three updates in question – KB3075249, KB3080149 and KB3068708 (which replaces KB3022345) – all add “customer experience and diagnostic telemetry” to Windows 7 and Windows 8. This is shorthand for monitoring how you use Windows and sending that data back to Microsoft HQ for evaluation.

Worse still software specialist site gHacks, which first discovered the tracking, notes these updates will ignore any previous user preferences:

“These four updates ignore existing user preferences stored in Windows 7 and Windows 8 (including any edits made to the Hosts file) and immediately starts exchanging user data with vortex-win.data.microsoft.com and settings-win.data.microsoft.com.”

**The Good News**

Now they have been launched the positive news is KB3075249 and KB3080149 have been classed as 'Optional' in Windows Update. This means they won’t install without Windows 7 and Windows 8 users giving them express permission to do so (a key difference to Windows 10).

On the flip side KB3068708 is classified as ‘Recommended’ which means Windows 7 and Windows 8 PCs with Windows Update set to automatic will install it by default. That said for the update to appear in the first place you will need to be a participant in Microsoft’s Customer Experience Improvement Program, an opt-in program which already has you agreeing to send user data to the company.

As PCWorld notes, unfortunately CEIP members who now feel uncomfortable about being a part of the program will have to jump through hoops to get out of it:

“Most programs make CEIP options available from the Help menu, although for some products, you might need to check settings, options, or preferences menus. Some pre-release products that are under development might require participation in CEIP to help ensure the final release of the product improves frequently used features and solves common problems that exist in the pre-release software.”

PCWorld also confirms gHacks observation that KB3075249, KB3080149 and KB3068708 all bypass user privacy settings in the Windows hosts file, so the easiest option for Windows 7 and Windows 8 users is to uninstall and then hide it.

This can be done by following these instructions...

To Uninstall the updates in Windows 7 and Windows 8:

- Go to Control Panel
- Go to Programs
- Go to Uninstall or change a program and locate them by name
- Double click on each update to uninstall it or right click on the update and choose uninstall

To hide the updates so they won’t install in future:

- Go to Control Panel
- Go to System and Security
- Go to Windows Update
- Go to Check for updates
- Find them in pending updates, right click on each and select ‘Hide’

**The Future With Microsoft**

Of course the bigger question than how to deal with these individual updates, is what the future holds for Microsoft customers on all versions of Windows.

Read the rest here:
Fake recruiters on LinkedIn are targeting infosec pros

By V.P. Prabhakaran, LinkedIn, September, 4, 2015

Unfortunately due to legal risk, Cisco has stopped providing letters of volatility. I am hearing rumors this will become more and more common from other manufactures as well. This is the guidance we have been given by the Cisco legal team.

"There's a group of fake recruiters on LinkedIn mapping infosec people's networks. Not sure what their goal is yet, just a heads-up to others," Yonathan Klijnsma, a threat intelligence analyst working at Dutch infosec firm Fox-IT, warned via his Twitter account.

"They will approach you by sending a general recruiter message with a profile picture of an attractive woman," he then explained their modus operandi. "The job will be relative to your job. They will 'scout' a few people (besides you). After about a week they stop sending out new requests, the profile picture is removed and a bit later their name is changed (making it hard to find these people back in your list if its big). In about a month the accounts disappear, not sure if on purpose."

F-Secure's Sean Sullivan dug a bit into these recruiters' company's - Talent Src or Talent Sources - online presence and found an official website that provides no useful information and a skimpy Twitter account that has last been updated in January (likely on the date when it was set up).

On LinkedIn, the accounts of the apparently fake Talent Src recruiters note that each one is dedicated to recruiting specific specialists working in a variety of security niches (automotive security, mobile security, etc.).

Also, a reverse image search for each of the images used on the profiles reveals that they have been taken from legitimate LinkedIn and Instagram accounts, and were simply flipped.

Read the rest here:

Your identity is sold for $1 in the Dark Web

By Charlie Osborne, Cnet, September, 4, 2015

Stolen data is a hot commodity in the Internet underground -- but how much it goes for might be a surprise.

Data breaches are becoming a weekly part of the news cycle, and so common that the idea of our data being lost by companies which collect it, while still distressing, is not as much of a surprise as it used to be. The recent Ashley Madison and Hacking Team data breaches reveal just how damaging these kinds of cyberattacks can be, with millions of user accounts compromised, intellectual property leaked and the private details of both user and executive spewed onto the web.

In Trend Micro's new report, dubbed "Understanding Data Breaches," (http://www.trendmicro.co.uk/) the security firm explores who is most often targeted in data breaches, how they take place, and what happens to data once it leaves corporate networks.

Using the Privacy Rights Clearinghouse (PRC)'s Data Breaches database, Trend Micro found that hacking or malware was behind only 25 percent of data breach incidents from 2005 to April this year. Insiders are also a common reason for data loss, as well as the use of physical skimming devices and the loss or theft of devices including laptops, flash drives and physical files were also found to be the root cause of damaging data breaches.

But what happens to this data afterwards can often be lost in the news. While sensitive, stolen information used in identity theft can cause heartache for victims, for those who trade in this data, personal information can be sold at a pittance. Unintended disclosure, through mistakes or negligence, is also a reported reason for information to end up in the wrong hands.

Payment service providers are a hot target for hackers these days, with an increase in card-related data breach reports of 169 percent over the past five years. Cybercriminals can steal data through card skimming, making a rub off cards, rigging ATMs with skimmer devices or cameras and modifying point-of-sale (PoS) terminals. Interestingly, hardware keyloggers installed on cash registers have also entered as a data theft tactic.

Read the rest here:
NIST Releases Draft Framework to Help ‘Cyber Physical Systems’ Developers

By Chad Boutin, NIST, September 18, 2015

Unmanned vehicles, “intelligent” buildings, your cell phone, the fitness bracelet on your wrist—all of these are cyber-physical systems (CPS). Today the National Institute of Standards and Technology (NIST) has released a draft CPS Framework document intended to help manufacturers create new CPS that can work seamlessly with other such smart systems that bridge the physical and computational worlds.

NIST is requesting public comments within the next 45 days on the Draft Framework for Cyber-Physical Systems, (http://www.cpspwg.org/Portals/3/docs/CPS%20PWG%20Draft%20Framework%20for%20Cyber-Physical%20Systems%20Release%200.8%20September%202015.pdf) which was developed in partnership with industry, academic and government experts in the NIST CPS Public Working Group (CPS PWG). According to NIST’s David Wollman, the framework is intended to provide a methodology for understanding, designing and building CPS including those with multiple applications.

“Creating a complex device involves a lot of people with varying interests and concerns, from the designers to the engineers to the safety testers,” says Wollman, who co-chairs NIST’s Cyber-Physical Systems Public Working Group. “What the framework provides is an organized treatment of these concerns so the group can address and manage them all effectively. It will prompt them to think of concerns they may not be aware of, and support understanding and integration of different CPS.”

While the field is still new, a common characteristic of CPS is the tight integration of physical and computing devices—such as movement sensors that inform your fitness bracelet how far you have walked, or the computer controlling the transmission and antilock brakes in your car. Whatever the purpose of a given CPS, the draft framework outlines the common attributes that its subparts share with other CPS devices and systems, and indicates what it must do to interact successfully with the broader CPS environment.

The draft document reflects more than a year’s effort by the public working group, which includes a few hundred members drawn primarily from industry, academia and government. The draft framework is available for download from the group’s website (http://cpspwg.org/) which has a template for submitting comments.

Wollman says the framework is likely to undergo a second draft release for further public comment before a final version is published.

This article appears at:
http://www.nist.gov/el/nist-releases-draft-framework-cyber-physical-systems-developers.cfm?

Fake Anti-Forensic Malware Widens Cyber-Skills Gap

By Tara Seals, Information Security Magazine, September 8, 2015

The rise of attacks that use file-less malware and other anti-forensics measures is creating a greater-than-ever skills gap in the cybersecurity industry.

Increasingly, bad actors are using techniques that leave little trace on physical disks. And unfortunately, the white hats aren’t keeping up: There’s a shortage of digital forensics practitioners able to investigate these types of offensives.

According to Alissa Torres, founder of Sibertor Forensics and former member of the Mandiant Computer Incident Response Team (MCIRT), “Attackers know how forensics investigators work and they are becoming increasingly more sophisticated at using methods that leave few traces behind—we are in an arms race where the key difference is training.”

In the last year, Torres said that she has seen a rise in file-less malware, which exists only in volatile memory and avoids installation on a target’s file system.

“Five years ago, to see sophisticated anti-analysis and acquisition techniques in the wild was like seeing a unicorn but that is no longer the case,” she said. “As techniques for detecting trace artefacts on a compromised system have improved, the more sophisticated attackers have adapted quickly.”

The SANS Institute estimates that possibly one in four digital forensics and incident response (DFIR) professionals has the level of training to successfully analyze the new types of self-defense techniques that include more sophisticated rootkit and anti-memory analysis mechanisms.

Read the rest here:
One of the scariest parts of the massive cybersecurity breaches at the Office of Personnel Management just got worse: The agency now says 5.6 million people's fingerprints were stolen as part of the hacks.

That's more than five times the 1.1 million government officials estimated when the cyberattacks were initially disclosed over the summer. The total number of those believed to be caught up in the breaches, which included the theft of the Social Security numbers and addresses of more than 21 million former and current government employees, remains the same.

OPM and the Department of Defense were reviewing the theft of background investigation records when they identified additional fingerprint data that had been exposed, OPM said in a statement.

Breaches involving biometric data like fingerprints are particularly concerning to privacy experts because of their permanence: Unlike passwords and even Social Security numbers, fingerprints cannot be changed. So those affected by this breach may find themselves grappling with the fallout for years.

"The fact that the number [of fingerprints breached] just increased by a factor of five is pretty mind-boggling," said Joseph Lorenzo Hall, the chief technologist at the Center for Democracy & Technology. "I’m surprised they didn’t have structures in place to determine the number of fingerprints compromised earlier during the investigation."

Lawmakers, too, were upset about the latest revelation. "OPM keeps getting it wrong," said Rep. Jason Chaffetz (R-Utah). "I have zero confidence in OPM’s competence and ability to manage this crisis."

As fingerprints increasingly replace passwords as a day-to-day security measure for unlocking your iPhone or even your home, security experts have grown concerned about how hackers might leverage them.

But federal experts believe the potential for "misuse" of the stolen fingerprints is currently limited, according to OPM, but that could "could change over time as technology evolves." It also said an interagency working group including experts from law enforcement and the intelligence community will review ways that the fingerprint data could be abused and try to develop ways to prevent that from happening.

"If, in the future, new means are developed to misuse the fingerprint data, the government will provide additional information to individuals whose fingerprints may have been stolen in this breach," OPM said.

OPM says it is still in the process of notifying everyone caught up in the breach. But they will be offered free identity theft and fraud protection services, the agency said.

China is widely suspected of being behind the breaches, perhaps as part of move to build a massive database on Americans. But U.S. government officials have so far declined to publicly blame the nation for the cyberattacks. Chinese President Xi Jinping is currently visiting the U.S. and described China as a strong defender of cybersecurity and a victim of hacking itself during a speech in Seattle on Tuesday.

The hacks sparked an outcry on Capitol Hill where lawmakers criticized the government's response and said the agency should have done more to protect the information in the first place. Some called for the firing of OPM director Katherine Archuleta, who eventually resigned in July.

One lawmaker criticized OPM for releasing the new information during the Pope's visit to Washington: "Today's blatant news dump is the clearest sign yet that the administration still acts like the OPM hack is a PR crisis instead of a national security threat," said Sen. Ben Sasse (R-Neb.) in a statement.

Cisco Router Break-Ins Bypass Cyber Defenses

By Eric Auchard, Reuters, September 16, 2015

Security researchers say they have uncovered clandestine attacks across three continents on the routers that direct traffic around the Internet, potentially allowing suspected cyberpers to harvest vast amounts of data while going undetected.

In the attacks, a highly sophisticated form of malicious software, dubbed SYNful Knock, has been implanted in routers made by Cisco, the world's top supplier, U.S. security research firm FireEye said on Tuesday.

Routers are attractive to hackers because they operate outside the perimeter of firewalls, anti-virus, behavioral detection software and other security tools that organizations use to safeguard data traffic. Until now, they were considered vulnerable to sustained denial-of-service attacks using barrages of millions of packets of data, but not outright takeover.

"If you own (seize control of) the router, you own the data of all the companies and government organizations that sit behind that router," FireEye Chief Executive Dave DeWalt told Reuters of his company's discovery.

"This is the ultimate spying tool, the ultimate corporate espionage tool, the ultimate cybercrime tool," DeWalt said.

The attacks have hit multiple industries and government agencies, he said.

Cisco confirmed it had alerted customers to the attacks in August and said they were not due to any vulnerability in its own software. Instead, the attackers stole valid network administration credentials from targeted organizations or managed to gain for themselves physical access to the routers.

"We've shared guidance on how customers can harden their network, and prevent, detect and remediate this type of attack," Cisco said in a statement.

Cyberspies Seen As Responsible

Altogether FireEye's computer forensic arm Mandiant has so far found 14 instances of the router implants in India, Mexico, Philippines and Ukraine, the company said in a blog post at bit.ly/1ObMm7u. It added that this may be just the tip of the iceberg in terms of yet-to-be-discovered attacks.

Because the attacks actually replace the basic software controlling the routers, infections persist when devices are shut off and restarted. If found to be infected, FireEye said basic software used to control those routers would have to be re-imaged, a time-consuming task for technicians.

Hitherto, infections of commercial routers, while not unknown, have largely remained theoretical threats, DeWalt said, as distinct from routers consumers use at home, which according to media reports have been hit by malware in recent years.

Read the rest here:
http://www.reuters.com/article/2015/09/16/us-cybersecurity-routers-cisco-systems-idUSKCN0RF0N420150916

Survey Finds People Hate Passwords, Go Figure

By Catalin Cimpanu, Softpedia, August 31, 2015

A survey carried out on 522 respondents highlights the current hatred people have for passwords and their openness to implementing simpler, yet safer authentication systems.

The survey, released by mobile authentication platform LaunchKey, shows that 84% of survey takers would be open to the idea of doing away with passwords, and three-quarters of all respondents see alternative identity verification systems like facial recognition, retinal scans, and fingerprints as more secure.

In 2015, password reuse is still a problem

The hatred for passwords can be seen in the fact that 52% of all users answered they have less than 10 passwords in use, hinting at heavy password reuse in their daily life, to which over 68% admitted.

Additionally, only 22% claim they can always remember all their passwords, 31% said they usually use the "lost password" links, while over 46% have to write them down somewhere.

Asked bluntly what frustrates them the most about passwords in general, most users said that they hate being required to choose passwords in complex formats (eg: Password123$%!) and being forced to change passwords at regular intervals.

Probably this explains why 2 out of 5 respondents acknowledged they were the victim of a data breach in the past.

The LaunchKey study also highlighted that most people don't trust online retailers with their passwords while banking and financial institutes are at the opposite side of the spectrum.

Two-Factor Authentication does not appeal to the masses

When it came to 2FA (Two-Factor Authentication), 53% admitted to not knowing what it is, while from the people that knew, 20% refused to activate it, 16% use it for sensitive accounts, and only 9% chose to enable it when available.

Read the rest here:
Forcing Suspects to Reveal Phone Passwords is Unconstitutional, Court Says

By David Kravets, Arstechnica, September 24, 2015

The Fifth Amendment right against compelled self-incrimination would be breached if two insider trading suspects were forced to turn over the passcodes of their locked mobile phones to the Securities and Exchange Commission, a federal judge ruled Wednesday.

"We find, as the SEC is not seeking business records but Defendants' personal thought processes, Defendants may properly invoke their Fifth Amendment right," US District Judge Mark Kearney of Pennsylvania wrote.

The decision comes amid a growing global debate about encryption and whether the tech sector should build backdoors into their wares to grant the authorities access to locked devices. Ars reported today that an Obama administration working group "considered four backdoors that tech companies could adopt to allow government investigators to decipher encrypted communications stored on phones of suspected terrorists or criminals."

Without this capability, the authorities are trying to get suspects to cough up their passwords instead. The Supreme Court has never ruled on the constitutionality of the issue. There's been a smattering of varying court rulings nationwide on the topic. In 2012, a federal appeals court said that forcing a child-porn suspect to decrypt password-protected hard drives would amount to a Fifth Amendment violation.

In the latest case, the SEC is investigating two former Capital One data analysts who allegedly used insider information associated with their jobs to trade stocks—in this case, a $150,000 investment allegedly turned into $2.8 million. Regulators suspect the mobile devices are holding evidence of insider trading and demanded that the two turn over their passcodes.

The decision was going on a fishing expedition:

Here, the SEC proffers no evidence rising to a "reasonable particularity" any of the documents it alleges reside in the passcode-protected phones. Instead, it argues only possession of the smartphones and Defendants were the sole users and possessors of their respective work-issued smartphones. SEC does not show the "existence" of any requested documents actually existing on the smartphones. Merely possessing the smartphones is insufficient if the SEC cannot show what is actually on the device.

Read the rest here:

Online security braces for quantum revolution

By Chris Cesare, Nature, September 8, 2015

It is an inevitability that cryptographers dread: the arrival of powerful quantum computers that can break the security of the Internet. Although these devices are thought to be a decade or more away, researchers are adamant that preparations must begin now.

Computer-security specialists are meeting in Germany this week to discuss quantum-resistant replacements for today's cryptographic systems—the protocols used to scramble and protect private information as it traverses the web and other digital networks. Although today's hackers can, and often do, steal private information by guessing passwords, impersonating authorized users or installing malicious software on computer networks, existing computers are unable to crack standard forms of encryption used to send sensitive data over the Internet.

But on the day that the first large quantum computer comes online, some widespread and crucial encryption methods will be rendered obsolete. Quantum computers exploit laws that govern subatomic particles, so they could easily defeat existing encryption methods.

"I'm genuinely worried we're not going to be ready in time," says Michele Mosca, co-founder of the Institute for Quantum Computing (IQC) at the University of Waterloo in Canada and chief executive of evolutionQ, a cyber-security consulting company.

Read the rest here:
http://www.nature.com/news/online-security-braces-for-quantum-revolution-1.18332?
Request for Chapter Presenters

We are looking for members to present at both the lunch and dinner meeting. The presenter has about 40 minutes to give the presentation and answer questions. This could be one slide with a situation identified and audience will then discuss possible solutions or a how-to presentation with a demonstration afterwards. The below listed are topics that have been suggested as areas of interest from our members. Please send an email to either, Pat Laverty (plaverty1961@gmail.com) and/or myself, Cindy Thornburg (thornbuc@aol.com) with topic to be presented, and we will connect with you for your availability. We would like the topic to be presented at both meetings however we do understand that may be difficult to accomplish.

- Cyber Security Laws in Colorado
- Interior Protection
- Building in Resiliency
- Ethics
- Intrusion Detection/Prevention Systems – configuration and how to review
- Making the Business Case for Security – how to
- Hacking – how to
- Application Security Scanning
- COMPTIA CE Cycles & Fee Structure
- A Summary and Rating of available Certifications
- A Survey of current IA Incidents We Should Know About (heartbleed) and What They Mean for the State of Our Industry
- Latest Innovations in Network Management Systems
- Real World Case Studies
- Threat Overview – Real World
- Legal Issues in Information Systems
- Asymmetric Warfare – what is it
- Spear Phishing – what is it and demonstration
- Prevention of Cyber Bullying
- Best Practices for Backing Up & Archiving Corporate Data
- When to Maximize or Minimize Your Cyber Footprint/Persona
- Threat Structuring
- Security Modeling – how to
- Data Flow Control
- Trusted Software Development – how to
- Risk Management Framework and what does it mean
- Case Study of Breaches – how they happen and how to prevent
- Security Architecture Development – ‘Building it In’
- ‘Mobile’ Security Management
- Bring Your Own Device (BYOD)
- Biometric Security and Privacy
- Hacking Back

Thank you!

Cindy
ISSA photos are courtesy of our Chapter Photographer Warren Pearce.
The Information Systems Security Association (ISSA)® is a not-for-profit, international organization of information security professionals and practitioners. It provides educational forums, publications, and peer interaction opportunities that enhance the knowledge, skill, and professional growth of its members.

The primary goal of the ISSA is to promote management practices that will ensure the confidentiality, integrity, and availability of information resources. The ISSA facilitates interaction and education to create a more successful environment for global information systems security and for the professionals involved. Members include practitioners at all levels of the security field in a broad range of industries such as communications, education, healthcare, manufacturing, financial, and government.

Article for the Newsletter?
If you would like to submit an article...

Are you a budding journalist? Do you have something that the Colorado Springs ISSA community should know about? Tell us about it!

We are always looking for articles that may be of interest to the broader Colorado Springs security community.

Send your article ideas to Don Creamer at: doncreamer-issa@q.com

Ensure that “Newsletter” is in the subject line.
Looking forward to seeing you in print!

Struck By a Duck: The Strangest Codes in the US Medical Billing System

By Kate Knibbs, Gizmodo, October 2, 2015

When you go to the doctor, there’s a medical code that determines how your treatment gets billed. Getting treated for urban rabies? Well, that’s distinct from woods-based sylvatic rabies, and your invoice will reflect that. Until today, the system in the US was the same one we used in the 1970s. But there’s a new catalog of ailments, and some of it is weird as hell.

Doctors in the US will now bill according to the International Classification of Diseases, Tenth Revision (ICD-10). The updated code is an exhaustive malady roadmap for medical billing. Some of it is the same as the old code—a horrifying array of fevers and motorcycle collision injuries. But now there are 68,000 new and oddly specific ways to describe how screwed your health is.

Here are some of the strangest entries in ICD-10:

Read the rest here: