Colleagues,

This week I had the opportunity to attend a career night at UCCS with several of our colleagues. The focus of this night was to engage with the students in the Peak Chaos club and to share with them our experiences and knowledge to help them plan for their future.

When we meet with groups such as this, I’m often struck by how young they all look but then as you engage in a conversation with them you also quickly realize how unbelievably smart many of these young people are. It gives me great hope for the future of our career field. Serving as a mentor for the next generation of cyber professionals doesn’t require a lot of time but it is a wonderful opportunity to share what we have learned over the years so these students can have differing perspectives before they make career choices.

Cyber Professionals

For example, one student really wanted to get into Cybersecurity but felt he wasn’t qualified because he was a Computer Science major and had very little programming experience. Another was an Electrical Engineer and felt they wouldn’t be a good fit for the field either. Here’s the thing about our career field, we all recognize we have a need for people who have technical skill sets. Many times those skill sets will not be 100% aligned with what we perceive to be the model for Cybersecurity Professionals. If we look at our own careers, how many of us were being trained for the roles we are filling now?

The facts are, yes our career field has specific needs but with good mentoring we can take people who may not have the “model” skill set and mold them into highly performing professionals…especially when they

(Continued on page 4)
If You’re Not Paranoid, You’re Crazy

By Walter Kirn, The Atlantic Monthly, November 2015

I knew we’d bought walnuts at the store that week, and I wanted to add some to my oatmeal. I called to my wife and asked her where she’d put them. She was washing her face in the bathroom, running the faucet, and must not have heard me—she didn’t answer. I found the bag of nuts without her help and stirred a handful into my bowl. My phone was charging on the counter. Bored, I picked it up to check the app that wirelessly grabs data from the fitness band I’d started wearing a month earlier. I saw that I’d slept for almost eight hours the night before but had gotten a mere two hours of “deep sleep.” I saw that I’d reached exactly 30 percent of my day’s goal of 13,000 steps. And then I noticed a message in a small window that signaled the app?

Walnuts,” it read. It told me to eat more walnuts.

It was probably a coincidence, a fluke. Still, it caused me to glance down at my wristband and then at my phone, a brand-new model with many unknown, untested capabilities. Had my phone picked up my words through its mic and somehow relayed them to my wristband, which then signaled the app?

The devices spoke to each other behind my back—I’d known they would when I “paired” them—but suddenly I was wary of their relationship. Who else did they talk to, and about what? And what happened to their conversations? Were they temporarily archived, promptly scrubbed, or forever incorporated into the “cloud,” that ghostly entity with the too-disarming name?

It was the winter of 2013, and these “walnut moments” had been multiplying—jarring little nudges from beyond that occurred whenever I went online. One night the previous summer, I’d driven to meet a friend at an art gallery in Hollywood, my first visit to a gallery in years. The next morning, in my inbox, several spam e-mails urged me to invest in art. That was an easy one to figure out: I’d typed the name of the gallery into Google Maps. Another simple one to trace was the stream of invitations to drug and alcohol rehab centers that I’d been getting ever since I’d consulted an online calendar of Los Angeles—area Alcoholics Anonymous meetings. Since membership in AA is supposed to be confidential, these e-mails irked me. Their presumptuous, heart-to-heart tone bugged me too. Was I tired of my misery and hopelessness? Hadn’t I caused my loved ones enough pain?

Some of these disconcerting prompts were harder to explain. For example, the appearance on my Facebook page, under the heading “People You May Know,” of a California musician whom I’d bumped into six or seven times at AA meetings in a private home. In accordance with AA custom, he had never told me his last name nor inquired about mine. And as far as I knew, we had just one friend in common, a notably solitary older novelist who avoided computers altogether. I did some research in an online technology forum and learned that by entering my number into his smartphone’s address book (compiling phone lists to use in times of trouble is an AA ritual), the musician had probably triggered the program that placed his full name and photo on my page.

Then there was this peculiar psychic incursion. One night, about a year before my phone suggested I eat more walnuts, I was researching modern spycraft for a book I was thinking about writing when I happened across a creepy YouTube video. It consisted of surveillance footage from a Middle Eastern hotel where agents thought to be acting on behalf of Israel had allegedly assassinated a senior Hamas official. I watched as the agents stalked their target, whom they apparently murdered in his room, offscreen, before reappearing in a hallway and nonchalantly summoning an elevator. Because one of the agents was a woman, I typed these words into my browser’s search bar: Mossad seduction techniques. Minutes later, a banner ad appeared for Ashley Madison, the dating site for adulterous married people that would eventually be hacked, exposing tens of millions of trusting cheaters who’d emptied their ids onto the Web.

Membership Update

We are currently maintaining our membership level around 380. Please keep those renewals as well as new member referrals coming! Shawn Murray, Glenn York, and I represented the chapter at the ISSA International Conference in Chicago 11-14 November. Lots of good sessions and networking as well a little bit of fun thrown in. There were also a lot of ISSA specific events that gave us a lot of opportunity to “show the chapter flag”. During the Chapter Leaders’ Meeting on Wednesday, the Baltimore Chapter leaders and I presented a status and recommendation briefing to the group. We got quite a bit of feedback; most of it was very positive. Out of that discussion we got a few minor action items to resolve but generally positive support from the ISSA International board. We will need to show that it works to make it a permanent program.

Now, the important news: “Freemium Student” is active as of 22 October and working on the Join Now page!!! The Beta Test program allows Colorado Springs and Baltimore chapters to enroll students as “Freemium Student” members as long as they meet the following criteria:

- Student
- Cybersecurity Degree or Major
- Other Majors Acceptable—Chapter Prerogative on Case by Case Basis (COS policy will be very liberal here)
- Not Fully Employed in Cybersecurity—Up to 24 Hours/Week
- Non-cybersecurity employment is Acceptable for Transitioning Students

Once they are enrolled they will have access to the following benefits at the ISSA International level: No Voting Rights at Intl Level, receive Intl Journal and Newsletter (Electronic Editions), participate in Free ISSA Webinars, and participate in ISSA Special Interest Groups. Since the ISSA-COS board decision for our chapter was to fully integrate the student members as much as possible, they will receive the following benefits at the chapter level: Voting Rights at Chapter Level is up to the Chapter (will have voting rights in ISSA-COS), participate in Chapter Activities (Meetings, Conferences, Training, Etc.), receive Chapter Newsletters (Electronic Editions), participate in Mentoring Programs as Provided by the Chapter, and networking with chapter members—Jobs! The week of 26 Oct I sent out emails to all current and former student members informing them of the program and I’ve been in communication since then. This program is an option for current student members to use at renewal as long as they still meet the criteria. If I missed anyone inadvertently please get in contact with me as soon as possible. Also, to make this work it will be critical for the members to solicit as many students as possible when they have opportunities. I have created a handout with all the information and appropriate links so if anyone needs a copy of that just drop me an email and I’ll send it out. The wider this is disseminated, the more chance we have to make it successful.

Four of our members, Pat Laverty, Mark Spencer, Ryan Schneider and I, supported the UCCS Peak Chaos Career night on October 22. 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. Yes, I provided Freemium handouts to everyone as well as leaving a few with Wayne Havey, their club president.

Melissa Absher has been working getting the mentorship program rolling again with the start of the new school year. She has some great ideas to improve the program from last year. More to follow from her in the near future. One of those improvements is to add 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. If you are interested in being a mentor to either of these groups, please contact either Melissa Absher or me. WE NEED MORE FOLKS TO STEP UP AND BE MENTORS!!! Don’t believe you can’t contribute here. We all have varied backgrounds that can provide different perspectives. Even if you’re not comfortable in signing up to be a one on one mentor, Melissa is coming up with lots of great ideas to allow people to contribute in other mentoring roles too such as group sessions, field trips, etc. Volunteer—we need your help to make our mentoring program successful and it also gives you opportunities to check those “volunteer” boxes required for Senior member and the Fellow programs with ISSA. It’s also a nice bullet to have on your resume if you need one of those.

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.

David Reed
Membership Committee Chairman
dreed54321@comcast.net
When I started with the chapter in the 2002, there were only a few females involved. It is exciting to see those females are still involved. Over the last 13 years the number of females involved has grown. As I was reading the articles in the October 2015 ISSA Journal, I realized there were more articles written by females than male. Our current ISSA International President is female. Andrea Hoy was here in 2014 and spoke at the CSTTF conference and spoke as a speaker for one session. She was also part of women in security panel. I had the opportunity to talk to her one on one and she is just an amazing person. In the chapter we have many amazing females also. If you have not spoken to them about what they have done or are doing, then do that. I think you will be surprise on what they are up to.

During a discussion with another member, I was stating the fact that there are more women involve in the chapter today than when I started. Their comment back to me was that there was still a lot of grey hair man within the chapter. Why is that? Where are the younger men? They are needed too to keep our chapter growing and strong.

As professionals we need to have discussions with all professionals in this field and get them involve. This field is still growing and we require new ideas and viewpoints. I know that I’m not fond of change because it is hard, however I generally find out that change is good. Even though it is still hard, in the end it is better. We are still seeing issues that were present 20 plus years ago. Why can’t we fix the issues such as user error, insecure coding or bad hardware? How come there are professionals thinking that these are new issues? How do we adapt to a generation that grow up with posting everything about their life on line and see nothing wrong with that?

**Upcoming events:**
- 18 Nov – luncheon at The Retired Enlisted Association
- 4 Dec – award luncheon and elections at Antlers Hilton

---

(Continued from page 1)

have a technical acumen and a willingness to learn new things. Why am I spending so much time on this issue? That’s an easy one…there’s a real need for mentors. You may not think you have anything to offer but put yourself in the shoes of the young college student who is unsure about their future…trust me, we all have knowledge that can impact a life in positive ways. If you’re interested in mentoring opportunities, please reach out to Tim Hoffman at tdlis47@hotmail.com or Melissa Absher at Melissa.absher@gmail.com.

Thanks for all you do! Happy Thanksgiving.
Training Team Update

Security+

We completed three very successful Security+ Exam Prep Review Seminars this year, in April, June, and October. We filled every class to the maximum possible, and unfortunately, even had to turn away many more who wanted to attend. Hopefully they’ll register for one of our Security+ Seminars next year. These seminars would not be possible without the exceptional support of our Training Team volunteers, instructors, and our Security+ Lead, Susan Ross. Thanks Susan, for the exceptional job you did this year in planning, organizing, and executing three highly successful seminars! We’re always looking for new members to join us, so if you’re interested in joining our Training Team, please send an email to our Training Team leads at: Training@issa-cos.org.

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/), 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 Training Team leads at: Training@issa-cos.org.

After 10 years, supporting approximately 600 hours of training, Pam Miller is stepping down as our refreshments lead. On behalf of every CISSP and Security+ class, and every student and every instructor, we thank you, Pam for the exceptional job you’ve done all these years. It’s critically important to have refreshments for our seminars, so if you’re interested in volunteering for this role, please contact our Training Team leads at: Training@issa-cos.org.

If you have ideas/suggestions/requests for training initiatives, please email our Training Team leads at: Training@issa-cos.org.
A team of ISSA-COS people represented our chapter at SecureWorld 2015 Denver conference in mid-October. Everyone spent time at our booth, but also made numerous contacts with many companies and organizations potentially interested in becoming a sponsor and/or speaker for our meetings and conferences. The team included Russell Wharton, Thomas Jessop, Calvin Swartz, James Asimah, Chuck Forth, and Suzanne Chance.

The speakers were excellent. Among the topics:

- Just like electronic stock market trading, defense against automated AI malware attacks will also need to be automated because the attacking malware can instantly morph tactics as it sees existing defenses.

- By 2018, AI will reach the capability of a mouse brain, and by 2023 human brain potential may be achieved.

- The OPM breach was the worst hack in U.S. history and captured information on anyone with a TS clearance or below, but excluding SCI. It is believed that China is sitting on the information. The breach occurred because a contractor left credentials on a desk, an opening for the attackers to install an overtly identical program that the contractor continued to use while unaware, leaving the attackers the opportunity to quietly achieve their aims.

- Mobile apps on all mobile platforms except Blackberry, often flashlight apps but not every flashlight app, can contain malware. This raises the issue if Blackberries should be reconsidered in both government and corporate worlds. The malicious apps record every conversation, take photos and videos, as well as gather GPS data, PII, emails, keystrokes, and other information. Because it takes three to six months to determine whether an app is malicious, that leaves a broad time for attackers to continue their agenda undisturbed.

Suzanne

Update Your Profile!

Don’t forget to periodically logon to www.issa.org and update your personal information.
Hackers turning millions of smart CCTV cameras into botnets


Security researchers have spotted that malware is being used to hijack CCTV cameras all over the world into botnets so that hackers can use them to launch Distributed Denial of Service (DDoS) cyber attacks.

According to research firm IHS Technology, in 2014 there were 245 million video surveillance cameras installed and active globally, and of course, most of these devices are now wirelessly connected, which makes them part of the Internet of Things (IoT).

However, while CCTVs might be providing security to physical locations by recording video footage, researchers from Incapsula have discovered that many Linux-based cameras with poor cybersecurity are quietly being hijacked by malware to serve a more sinister purpose.

Malware attacks CCTV cameras running on BusyBox

The researchers discovered that a botnet made up of about 900 CCTV cameras from countries all over the world were repeatedly attacking a "large cloud service, catering to millions of users worldwide". The researchers will not reveal who, but are certain people could imagine a few companies that fitted the bill.

The researchers found that the compromised CCTV cameras were running on Linux together with BusyBox, which is a package of common stripped-down Unix utilities designed for systems with limited resources. The malware attacked by scanning for all network devices running on BusyBox that had failed to secure the telnet protocol, attacking and hijacking them to join the botnet, which then instructed the compromised cameras to send out successive HTTP flooding attacks to a chosen target.

While the compromised cameras were located all over the world, more HTTP flooding attacks originated from hijacked surveillance cameras in India, Peru, Thailand, Vietnam, Egypt, Turkey, Indonesia and Colombia, showing that cybersecurity practices was particularly weak in these nations.

However, the researchers also found a compromised camera down the road from them in a store in California, which showed that anyone could make this mistake. Similar to internet routers, once surveillance cameras are installed and they work, people tend to leave them alone with the same default admin passwords they came out of the box with unless the internet goes down or the camera stops recording, which gives hackers an easy way in.

Cameras hacked by multiple individuals at the same time

Interestingly, the researchers found that the compromised cameras were not just in one single botnet – they had been hacked by multiple individuals and were being instructed to carry out attacks from several different locations in the world at the same time, and all the cameras were different camera models and by different manufacturers.

"We hope our story will raise awareness about the importance of basic security practices—as well as the threat posed by unsecured connected devices. Even as we write this article, we are mitigating another IoT DDoS attack, this time from a network-attached storage (NAS)-based botnet. And yes, you guessed it, those were also compromised by brute-force dictionary attacks," the researchers wrote in a blog post.

Read the rest here:
http://www.ibtimes.co.uk/hackers-turning-millions-smart-cctv-cameras-into-botnets-ddos-attacks-1525736
New Microchip-Enabled Credit Cards May Still Be Vulnerable to Exploitation by Fraudsters

By FBI, October 13, 2015

By October 2015, many U.S. banks will have replaced hundreds of millions of traditional credit and debit cards, which rely on data stored on magnetic strips, with new payment cards containing a microchip known as an EMV chip. While EMV cards offer enhanced security, the FBI is warning law enforcement, merchants, and the general public that no one technology eliminates fraud and cybercriminals will continue to look for opportunities to steal payment information.

Technical Details

With traditional credit cards, the magnetic strip on the back of the card contains static personal information about the cardholder. This information is used to authenticate the card at the point of sale (PoS) terminal, before the purchase is authorized. When a consumer uses an EMV card at a chip PoS terminal, that transaction is protected using the technology in the microchip. Additionally, consumers will be able to continue to use the magnetic strip on the EMV card at retailers who have not yet implemented chip PoS terminals. When the card is equipped with a personal identification number (PIN), which is known only to the cardholder and the issuing financial institution, issuers will be able to verify the user’s identity. Currently, not all EMV cards are issued to consumers with the PIN capability and not all merchant PoS terminals can accept PIN entry. EMV transactions at chip PoS terminals provide more security of consumers’ personal data than magnetic strip PoS transactions. In addition, EMV card transactions transmit data between the merchant and the issuing bank with a special code that is unique to each individual transaction. This provides the cardholder greater security and makes the EMV card less vulnerable to criminal activity while the data is transmitted from the chip enabled PoS to the issuing bank.

Threat

Although EMV cards provide greater security than traditional magnetic strip cards, an EMV chip does not stop lost and stolen cards from being used in stores, or for online or telephone purchases when the chip is not physically provided to the merchant, referred to as a card-not-present transaction. Additionally, the data on the magnetic strip of an EMV card can still be stolen if the merchant has not upgraded to an EMV terminal and it becomes infected with data-capturing malware. Consumers are urged to use the EMV feature of their new card wherever merchants accept it to limit the exposure of their sensitive payment data.

Defense

Consumers should closely safeguard the security of their EMV cards and PINs. This includes being vigilant in handling, signing, and activating a card as soon as it arrives in the mail, reviewing statements for irregularities, and promptly reporting lost or stolen credit cards to the issuing bank. Consumers should also shield the keypad from bystanders when entering a PIN, as PINs are vulnerable to cybercriminals who work to steal these numbers to commit ATM and cash-back crimes.

The FBI encourages merchants to handle the EMV card and its data with the same security precautions they use for standard credit cards. Merchants handling sales over the telephone or via the Internet are encouraged to adopt additional security measures to ensure the authenticity of cards used for transactions. At a minimum, merchants should use secure servers and payment links for all Internet transactions with credit and debit cards, and information should be encrypted, if possible, to avert hackers from compromising card information provided by consumers. Credit card information taken over the telephone or through online means should be protected by the retailer to include encrypting digital information and securely disposing written credit card information.

If you believe you have been a victim of credit card fraud, reach out to your local law enforcement or FBI field office, and file a complaint with the Internet Crime Complaint Center (IC3) at www.IC3.gov.

What is an EMV credit card?

The small gold chip found in many credit cards is most often referred to as an EMV chip. Cards containing this chip are known as EMV cards, as well as “chip-and-signature,” “chip-and-pin,” or “smart” cards. The name “EMV” refers to the three originators of chip-enabled cards: Europay, MasterCard, and Visa. EMV chips are now the global standard for credit card security.
Cautionary Tales from Digital Forensics

By Benjamin Wright, DFI News, October 22, 2015

Just in time for Halloween, Benjamin Wright, a lawyer and senior instructor with the SANS Institute, has pulled together some of the creepiest cases he has collected over the past decade. As these spooky tales demonstrate, technology is quickly changing the legal landscape proving that digital investigators need to take serious precautions when dealing with dangerous cases. For those who dare to continue, be forewarned, the stories you are about to read are true.

Strange Disappearance

What began as a seemingly straightforward case, quickly turned into a horrific nightmare for one lawyer in Florida. A citizen sued the Seminole County Sheriff’s Department after being injured in a shooting involving sheriff deputies. The citizen’s lawyer sent a letter to the department demanding that it preserve all evidence. The Sheriff Department’s in-house lawyer, David Lane, read the letter and gave copies of it to the top supervisors in the department.

Mysteriously, relevant evidence on the laptops owned by the department disappeared—an evil villain erased the hard drives. Gasp!

The judge in the lawsuit learned of this wicked act while Mr. Lane was sitting in the gallery observing the proceedings along with the public (Mr. Lane was not there to make an official appearance or statement). All of a sudden the Judge ordered Mr. Lane to rise from the public gallery and sit on the witness stand! It was a dreadful situation. However, the judge could do this because Mr. Lane, a licensed member of the Florida Bar Association, is also an “officer of the court.”

The judge asked Mr. Lane pointed questions about why he had not done more to protect the evidence on the laptops. After a bone-chilling testimony, the judge concluded Mr. Lane had a direct professional duty to prevent others in the department from erasing evidence from laptops. Because he had failed in that duty, the judge imposed a gruesome and unusual penalty on Mr. Lane. As if this paranormal story could not get any worse, Mr. Lane was required to pay the fine out of his pocket! Now that is scary!

Ghoulish Behavior

If your blood has not run cold yet, consider this next hair-raising case. In a major commercial lawsuit, Coleman (Parent) Holdings, Inc. sued Morgan Stanley (MS) for fraud in connection with the sale of the Sunbeam appliance company to Coleman. MS was required to find and turn over emails as part of “e-discovery” in the lawsuit. MS dribbled out emails over a couple of years, claiming various excuses for not finding and handing all of them over at once.

The judge became suspicious that evil was at play, particularly that the lawyers were helping the client withhold relevant records to drag out litigation. Fearing the worst, the judge took the highly unusual and ghastly step of requiring MS’s lawyers to sit on the witness stand and explain in gruesome detail what they knew about the email records and when they knew it. The situation quickly turned into the lawyers’ worst nightmare because normally everything a lawyer does for a client is confidential under attorney-client privilege.

On the witness stand the lawyers revealed, for the first time in this painstakingly long lawsuit, that MS was technically able to find emails more quickly than it had been claiming! Incensed by this ghoulish behavior, the judge imposed a strategic disadvantage on MS, which contributed to a jury concluding MS owed $1.4 billion. There is more to this gruesome tale, ultimately MS fired its lawyers, claiming they had committed malpractice.

Creepy Confidence

Ready for another spooky story? Consider then the gruesome case involving Scott London, a senior audit partner at KPMG, who miscalculated the ability of regulators to find small-scale insider trading.

As a top auditor, London possessed confidential client information about events like mergers and acquisitions. His decades of experience (and creepy confidence) led him to believe that financial regulators could not find or prosecute small-scale insider trading. His sinister thinking was wrong thanks to advances in technology. Mr. London’s experience from the 1990s was out of date. Unaware his wicked ways could be uncovered, Mr. London fed insider information to his golf buddy, who made small successful bets in the stock markets. Because big data techniques can now be used by regulators to find even small acts of evil—or anomalies—in financial markets, regulators discovered Mr. London’s wicked actions.

Fearing federal regulators, London’s buddy agreed to help them in exchange for leniency. London’s buddy arranged to meet him in a parking lot to hand over an envelope full of cash. At the meeting, the quivering buddy was wearing a wire; the Feds photographed the transaction from a dark distance. Later sentenced to jail, London was shocked to learn the Feds were able to find and track his vile little insider trades.

Canadian military seeks hackers to build exploits and defences against connected car cyberattacks


Canada's military is concerned the advent of connected cars with state-of-the-art computer systems and internet access will see a rise in cyberattacks, and is now looking to hire hackers to help them understand all the ways a car can be hijacked.

Defence Research and Development Canada (DRDC), the Canadian military's research agency, published an official request for interested companies to submit proposals on improving cyber security in automotive systems on Tuesday 6 October, according to the Toronto Star.

"Cyberattacks on information technologies like personal computers and servers usually result mostly in immaterial damages, like the loss, the alteration or the theft of information or money," DRDC wrote in the proposal. "In the case of vehicular systems, cyberattacks are a more important concern since the safety of their users or other users on the road might be at stake."

Up to 100 computers in connected cars today

The researchers stress a car produced in 2014 now includes up to 100 computers – also known as Electronic Control Units (ECU) – running 60 million source lines of code, 145 actuators and 75 sensors. The ECUs exchange up to 25GB of data every hour, but since the car has wireless communication capabilities, this opens up a whole new ballpark of trouble.

The contract up for offer is estimated to be worth CA$620,000 (£311,506, $476,685) and will require the chosen security contractor to be able to exploit and improve software developed by the DRDC that was coded in Python and works on Linux.

"In the last three years, the hacking community has demonstrated many times the possibility to compromise the cybersecurity of cars," the DRDC wrote. "There is a need to study the security of automotive vehicles, including understanding their vulnerabilities and assessing the potential mitigation measures.

"The first need, understanding the problem, requires appropriate tools and methodologies. The second need, studying mitigation measures, implies testing existing technologies and studying upcoming regulations and guidelines."

Hackers can kill engines and hijack steering wheels remotely

There have been several high-profile stories in the media about security researchers demonstrating how easily they can hack into a variety of connected cars.

In particular, Wired's Andy Greenberg allowed hackers Charlie Miller and Chris Valasek to hack into a Ford Escape and a Toyota Prius as the writer drove them around a car park in 2013, deliberately disabling the brakes, commandeering the steering wheel and honking the horn.

Read the rest here:
http://www.ibtimes.co.uk/canadian-military-seeks-hackers-build-exploits-defences-against-connected-car-cyberattacks-1522908
Chinese Tsinghua Plans to Buy SanDisk and Toshiba

By Softpedia, October 8, 2015

The infamous Chinese state-owned mammoth corporation, Tsinghua Unigroup has laid its hungry eyes this time on the veteran, but financially shaky, giants Toshiba and SanDisk.

After attempting to buy American NAND manufacturer Micron in "one gulp" and ending up ultimately being blocked by the U.S. government, Tsinghua isn't done attempting to throw money around in order to forcefully buy precious NAND patents owned by companies like Toshiba and SanDisk.

The move is quite obvious since the Chinese affair didn't work out as planned during talks that targeted buying Micron, deals that ended with the Chinese being unequivocally refused by the always vigilant CFIUS (Committee on Foreign Investment in the United States) and considered the case closed for now.

The main reason why Tsinghua has shifted their interest towards Toshiba and SanDisk, however, is quite simple. These are easy targets to prey, since both deal in NAND flash drive manufacturing and one of them, Toshiba, passes through serious financial woes as a result of major corruption scandal that saw the company's previous CEO being sacked together with its entire upper staff.

As a result, Toshiba announced that it would kill its TV and PC businesses to conserve cash, and is looking for partners in continuing its nuclear contracts with the Japanese state.

Tsinghua pushes onwards with Micron deal as well

Tsinghua, on the other hand, is in the middle of a major Chinese drive of building a solid NAND and DRAM industry on Chinese soil by apparently any means, and sums of money, necessary. Last time Tsinghua held talks with Micron, it offered the staggering sum of $23 billion in order to guarantee an acquisition, but the deal was ultimately shut down by CFIUS once the U.S. government considered the Micron acquisition a matter of national security.

According to DigiTimes, the Chinese continue their efforts to buy the precious know-how that Micron holds by acquiring partial stakes of the company, like it did with HP. If this fails, Toshiba will most likely be their next target.


Watchdog Duo Wants to Move Security Clearance Data Out of OPM

By Camille Tuutti, NextGov, October 9, 2015

After the massive hack that compromised sensitive information of more than 21.5 million former, current and prospective federal employees, the Office of Personnel Management has no business handling security clearance data, according to two members of Congress.

“We strongly believe that security clearance data -- which has been described as the ‘crown jewels’ -- of our national intelligence should not be protected by OPM, which is neither an intelligence agency nor a defense organization,” Reps. Ted Lieu, D-Calif., and Steve Russell, R-Okla., wrote to David Mader, acting deputy director of management at the Office of Management and Budget.

In their Oct. 7 letter, Lieu and Russell said they, along with the House Oversight and Government Reform Committee on which they serve, were “shocked” to hear during congressional hearings that “for years, OPM leadership had ignored warnings from the inspector general of ‘material weakness’ in data security.”

Although the two legislators said they and the committee had “renewed faith” that OPM could revamp its systems under acting Director Beth Cobert’s leadership, the agency itself shouldn’t house sensitive information.

“Simply put, OPM was not designed to house and protect this sensitive data,” wrote the duo, who have since July been working on legislation to move security clearance data out of OPM.

The lawmakers requested a more secure location to store and safeguard security clearance data, and asked for further review of security clearances that would include evaluating methods such as data segmentation and cryptographic hash functions.

Lieu and Russell both have previously criticized OPM’s role in handling security. Russell said the massive hack was “akin to gross negligence.”

Russia Chokes On Tor

By James Dunnigan, Strategy Page, October, 12, 2015

Back in mid-2014 Russia offered a prize of $111,000 for whoever could deliver, by August 20th 2014, software that would allow Russian security services to identify people on the Internet using Tor (The Onion Router), a system that enables users to access the Internet anonymously. On August 22nd Russia announced that an unnamed Russian contractor, with a top security clearance, had received the $111,000 prize. No other details were provided at the time. A year later it was revealed that the winner of the Tor prize is now spending even more on lawyers to try and get out of the contract to crack Tor’s security. It seems the winners found that their theoretical solution was too difficult to implement effectively. In part this was because the worldwide community of programmers and software engineers that developed Tor is constantly upgrading it. Cracking Tor security is firing at a moving target and one that constantly changes shape and is quite resistant to damage. Tor is not perfect but it has proved very resistant to attack. A lot of people are trying to crack Tor, which is also used by criminals and Islamic terrorists as well as people trying to avoid government surveillance. This is a matter of life and death in many countries, including Russia.

Similar to anonymizer software, Tor was even more untraceable. Unlike anonymizer software, Tor relies on thousands of people running the Tor software, and acting as nodes for email (and attachments) to be sent through so many Tor nodes that it was believed virtually impossible to track down the identity of the sender. Tor was developed as part of an American government program to create software that people living in dictatorships could use to avoid arrest for saying things on the Internet that their government did not like. Tor also enabled Internet users in dictatorships to communicate safely with the outside world. Tor first appeared in 2002 and has since then defied most attempts to defeat it. The Tor developers were also quick to modify their software when a vulnerability was detected.

But by 2014 it was believed that NSA had cracked TOR and others may have done so as well but were keeping quiet about it so that the Tor support community did not fix whatever aspect of the software that made it vulnerable. At the same time there were alternatives to Tor, as well as supplemental software that were apparently uncracked by anyone.

Russia may have been encouraged by an Iranians effort in 2011 that came up with a way to detect Tor users, and cut them off from the Internet. For the Iranian censors, that was good enough. This was a blow to American efforts to support the hacker community in keeping the Internet accessible for all users in to countries like Iran, Cuba and North Korea. In Iran the government managed to shut down over 90 percent of Iranians using Tor. But the Tor developers quickly issued a software update that got around the government detection system. Since Iran had developed the detection software internally, rather than buying them from Western suppliers, they kept modifying it to regain the ability to detect Tor. But the Tor developers have been able to respond each time, including another round in this battle in 2014. The Russians appear to believe they can help the Iranian effort with a prize completion.

The U.S. government, despite a long, combative and acrimonious relationship with the hacker and Internet freedom communities, has been funding work on “Internet freedoms programs” that seek to bypass Internet censorship in dictatorships. Thus the American government has provided over $30 million dollars for hackers seeking to create software that will enable people to evade Internet surveillance and censorship.

While this anti-censorship software can also be used by criminals, terrorists and spies, the U.S. government believes that these groups already have access to software that can hide them, and that it’s more important that police states have more reason to pay attention to what their citizens want.

Meanwhile, the American money has funded development of software that makes smart phones safer for users who want to say things to others that their governments disapprove of. All this activity is directed at countries with heavy Internet censorship programs, like China, Burma, Iran, Cuba, Venezuela and several African countries. Russia recently joined this group by placing more restrictions on Russian Internet users and outlawing a lot of anti-government activity.

Some dictatorships have created virtually impregnable Internet controls. This is the case in Cuba and North Korea, where the local Internet is cut off from the global Internet. In effect, the Cuban and North Korean Internet are each restricted to one country, and heavily monitored by the security services. Iran considered that, but decided not to implement an "Iranian Islamic Internet" because the Iranian economy, fueled by huge oil income, has too many useful external contacts. Cutting Iran off from the worldwide web would hurt the economy and cause more unrest.

Read the rest here: http://www.strategypage.com/dls/articles/Russia-Chokes-On-Tor-10-12-2015.asp
You’ve Been Misled About What Makes a Good Password

By Tom Simonite, MIT Technology Review, October 19, 2015

“Password must include upper and lowercase letters, and at least one numeric character.” A common scold dished out by websites or software when you open an account or change a password—and one that new research suggests is misleading.

A study that tested state-of-the-art password-guessing techniques found that requiring numbers and uppercase characters in passwords doesn’t do much to make them stronger. Making a password longer or including symbols was much more effective.

“Attacks are more sophisticated now, and those best practice countermeasures are a little bit out of sync,” says Matteo Dell’Amico, a researcher at Symantec Research. He worked with Maurizio Filippone at the French research institute Eurecom. The pair presented a paper on their work at the ACM Computer and Communications Security conference last week.

Recommendations that we include a mixture of cases, symbols, and numbers in passwords originate in the idea that it reduces the chance of a correct guess by software that systematically tries every combination of characters, says Dell’Amico. Password meters that give feedback on the “strength” of a password work on the same basis.

But the latest password guessing software is smarter than just guessing at random. Instead it is trained using leaked lists of millions of passwords to make guesses that try the passwords—or patterns found in passwords—most commonly used first. Password-guessing software can be used to try to reveal improperly encrypted passwords leaked online, like the 130 million taken from Adobe in 2013, or to directly access password-secured software or devices that don’t limit guessing attempts.

Dell’Amico and Filippone came up with a new way to measure the strength of a password that takes that into account. They trained attack software, used it to generate lists of passwords, and invented a way to use those to assign a kind of “guessability” score to any given password. They used 10 million leaked passwords to train several kinds of attack software and tested their guessability method on another 32 million passwords.

The results show that making a password longer or adding symbols is a better way to strengthen it than by adding uppercase characters or numbers. That’s because people tend to add uppercase characters at the start of passwords and numbers at the end, and password attacking methods can take advantage of that, says Dell’Amico. “Basically you need to make your passwords less predictable,” he says. The new method could be used to create more accurate ways to give people a sense of the strength of a password, says Dell’Amico.

Facial Recognition Remains a Human Penchant, For Now

By Seth Augenstein, Forensic Magazine, October 21, 2015

Computer algorithms have given forensic professionals unprecedented new avenues to investigate criminal cases especially with advanced DNA analysis techniques in the past half-decade. But, there is still no substitute for trained human analysts when it comes to facial recognition, according to a recent international study.

Trained experts beat out both computer algorithms and other people in tests as published in results last month in The Proceedings of the Royal Society B.

The forensic analysts beat out the computers and other people, despite time limits and a lack of specialized tools and labs.

“This study was a first attempt to do a systematic exam of face-recognition expertise within an international group of professionals,” said Alice O’Toole, of the University of Texas, Dallas, one of the authors, in a statement. “At present, computer programs are set only to look at faces, while the people were able to take in other body cues, such as body size, hair and shoulders. That made a big difference.”

The tests were conducted at a conference of the Facial Identification Scientific Working Group in Quantico, in May 2014. Forty-one volunteers attempted their best at facial matching, identification, and other exercises.

The international experts from various agencies achieved near-100 percent accuracy, according to the results.

The examination was undertaken in response to questions posed by a 2009 report from the National Academy of Sciences on multiple disciplines within the forensic sciences.

Read the rest here:
Peterson Air Force Base FBC Tech event and ISSA-COS conference
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:
doncreamrissa@q.com

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

What's the Creepiest Thing Your Computer Has Ever Done?

By Maddie Stone, Gizmodo, October 31, 2015

Whether or not you believe in the supernatural, there’s almost certainly been a moment in your life when you were sure your computer was possessed.

Mine came a few months back. I have a home office, but sometimes when I work late into the evening, I like to move my iMac into the bedroom. That way, after I’m done with work I can just watch Clone Wars reruns in bed until I pass out (don’t judge). Anyway, I’ve just drifted off to sleep this one night, when all of a sudden I’m startled awake by an atrocious noise. As best I can tell, it’s human voices—lots of them—all distorted and babbling at once, like somebody tossed a bunch of English words into a meat grinder and pumped them through a loudspeaker. It’s repulsive and terrifying.

Read the rest here:
http://gizmodo.com/whats-the-creepiest-thing-your-computer-has-ever-done-1739723283