Colleagues,

As I write this we are 5 days removed from our Cyber Focus Day and 3 weeks away from our Professional Networking event so there is a lot going on. Our Cyber Focus Day (CFD) went very well and we’ve received a lot of good feedback that we will consider when planning for future events. For those who stood in lunch for a while, sorry about that…we will work with event staff to ensure that doesn’t happen again! I think overall the event was a big success for our chapter and I really appreciate those who stepped up to help the event run smoothly.

When I showed up 90 minutes before the conference was to start there was already a host of chapter members there setting things up and preparing to check people in. Events as big as this wouldn’t happen without the collective efforts of our chapter members so thank you for stepping up.

The planning for the Professional Networking event is well underway.

Cindy and I are working closely with Russ and James, our Members-At-Large to ensure this event meets chapter members’ professional needs. We’re still clarifying some of those needs so if you have ideas please let us know.

Periodically I like to take a step back and analyze what all is going on in the chapter and where we’re headed. We’ve made some big changes in the past 15 months such as partnering with the Federal Business Council to plan our conferences, conducting a membership drive that not only brought us a lot of new members but through it we saw a large uptick in the number of students and female members, establishing a partnership with UCCS which includes mentoring some of their students, and now planning our first-ever networking event. These changes were made to bring about a renewed energy to our chapter but we can’t stop and rest on our laurels. We always need to be thinking long-term,
Sign Up at irs.gov
Before Crooks Do It For You

By Brian Krebs, Krebs on Security, March 15, 2015

If you’re an American and haven’t yet created an account at irs.gov, you may want to take care of that before tax fraudsters create an account in your name and steal your personal and tax data in the process.

Recently, KrebsOnSecurity heard from Michael Kasper, a 35-year-old reader who tried to obtain a copy of his most recent tax transcript with the Internal Revenue Service (IRS). Kasper said he sought the transcript after trying to file his taxes through the desktop version of TurboTax, and being informed by TurboTax that the IRS had rejected the request because his return had already been filed.

Kasper said he phoned the IRS’s identity theft hotline (800-908-4490) and was told a direct deposit was being made that very same day for his tax refund — a request made with his Social Security number and address but to be deposited into a bank account that he didn’t recognize.

“Since I was alerting them that this transaction was fraudulent, their privacy rules prevented them from telling me any more information, such as the routing number and account number of that deposit,” Kasper said. “They basically admitted this was to protect the privacy of the criminal, not because they were going to investigate right away. In fact, they were very clear that the matter would not be investigated further until a fraud affidavit and accompanying documentation were processed by mail.”

In the following weeks, Kasper contacted the IRS, who told him they had no new information on his case. When he tried to get a transcript of the fraudulent return using the “Get Transcript” function on IRS.gov, he learned that someone had already registered through the IRS’s site using his Social Security number and an unknown email address.

“If I called the IRS to fix this, and spent another hour on hold, they explained they could not tell me what the email address was due to privacy regulations,” Kasper recalled. “They also said they could not change the email address, all they could do was ban access to eServices for my account, which they did. It was something at least.”

Undeterred, Kasper researched further and discovered that he could still obtain a copy of the fraudulent return by filling out the IRS Form 4506 and paying a $50 processing fee. Several days later, the IRS mailed Kasper a photocopy of the fraudulent return filed in his name — complete with the bank routing and account number that received the $8,936 phony refund filed in his name.

“That’s right, $50 just for the right to see my own return,” Kasper said. “And once again the right hand does not know what the left hand is doing, because it cost me just $50 to get them to ignore their own privacy rules. The most interesting thing about this strange rule is that the IRS also refuses to look at the account data itself until it is fully investigated. Banks are required by law to report suspicious refund deposits, but the IRS does not even bother to contact banks to let them know a refund deposit was reported fraudulent; at least in the case of individual taxpayers who call, confirm their identity and report it, just like I did.”

Kasper said the transcript indicates the fraudsters filed his refund request using the IRS web site’s own free e-file website for those with incomes over $60,000. It also showed the routing number for First National Bank of Pennsylvania and the checking account number of the individual who got the deposit plus the date that they filed: January 31, 2015.

The transcript suggests that the fraudsters who claimed his refund had done so by copying all of the data from his previous year’s W2, and by increasing the previous year’s amounts slightly. Kasper said he can’t prove it, but he believes the scammers obtained that W2 data directly from the IRS itself, after creating an account at the IRS portal in his name (but using a different email address) and requesting his transcript.

Read the rest here:
http://krebsonsecurity.com/2015/03/sign-up-atsirs-gov-before-crooks-do-it-for-you/
Membership Update

We sponsored the Cyber Focus day at UCCS in March and had a great turnout. Unfortunately I had to miss it as I was on business travel. Even so, we were able to add several new members based on everyone else’s efforts. In all, we’ve added 13 new members in March which brings us very close to the 400 goal. Please keep up the renewals and the recruiting efforts and we’ll get there.

This month we are sponsoring an ISSA professional networking evening rather than having our normal monthly meetings. It will be 21 April from 6-8 pm in the First Command Banquet Hall at Sky Sox Stadium. If you’re not familiar with the Sky Sox, their stadium is located near Barnes and Tutt. We are limiting participation to 125 members so register as soon as possible at Event Brite: https://www.eventbrite.com/e/colorado-springs-issa-professional-networking-tickets-16353761541. Also, if your plans change after registering please cancel your reservation so another member can sign up.

We are still awaiting a response from ISSA International on some changes that will allow us to expand our student outreach and sponsorships. Hopefully, we’ll have that in place very soon.

Tim Hoffman, Melissa Absher and I had a brainstorming session in March to discuss the student mentorship program. Lots of good ideas on how we can leverage what we’re already doing with ISSA International’s mentorship program to expand and improve what we’ve started with our student mentorship program. More information will be coming out as those efforts get fleshed out. If you’re interested in either being a mentor or being mentored contact either Melissa 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

New Members
March
- Thomas Hornstrom
- David Regal
- Beverly Selby
- Barbara Nelson
- Sherri Payne
- Roberta Anderson
- Colby Fierro
- Peter Iles
- Michael Clark
- Juan Rodriguez
- Trisha Shanahan
- Jim Henderson
- Lawrence Williamson

A Note From Our President

which for an organization such as ours is about 6 months. Your chapter board is always thinking…how we can make the next conference different from the last, how can we better meet our members’ needs, what can we do so members really look forward to coming to meetings and events, etc.

The bottom-line is we like the momentum the chapter has but we want to provide opportunities for you to continue to grow professionally so we really need to hear from you concerning your professional needs and where the chapter can help you. Find a board member and let us know. Thanks much!

Cheers!

Pat
Please let me echo the information that Pat has put out about the conference and how great our members are. I especially thank Paul Hagood for carrying boxes from my car, Pam Miller for taking care of sign in and Russ Weeks for taking care of the vendors and speakers. These people and all of the other volunteers made the conference a successful one.

Updated calendar events:

- April 21 is the networking event at Sky Sox.
- May 13 is a regular lunch meeting.
- June 10 is a regular lunch meeting
- July 8 is a regular lunch meeting
- Aug 19 and 20 is the CSTTF.

Cindy
Training Team Update

CISSP

The new, Official (ISC)2 Guide to the CISSP CBK book, 4th edition, is out and it is significantly different than previous editions. The CISSP Common Body of Knowledge (CBK) has been reorganized into the following eight domains:

- Security and Risk Management
- Asset Security
- Security Engineering
- Communication and Network Security
- Identity and Access Management
- Security Assessment and Testing
- Security Operations
- Software Development Security

Additionally, according to Mr. Tipton’s Foreword in the book, 40 percent of the content is new. The Training Team will be revising and updating our CISSP Exam Prep Review Seminar material to correspond to the new CISSP CBK. If you are a CISSP and would like to help with developing slides and/or teaching one of the new CISSP domains, or if you have questions, please contact Colleen Murphy at: crmurphy.cs@hotmail.com.

Security+

The first Security+ Exam Prep Review Seminar for 2015 is scheduled for 11 April at Colorado Technical University (CTU) and it’s already sold out. The next Security+ seminar is scheduled for 11 July, so stay tuned to this newsletter for information and updates as we get closer to July.

Looking for a volunteer opportunity? Looking for a way to share your knowledge/expertise? Looking for a way to earn CompTIA CEUs? We need additional Security+ certified members to teach one or more of the Security+ 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 criteria. Security+ instructors must be Security+ certified, but no other certification is required. Additionally, you must hold the certification for one year prior to teaching the material to minimize the possibility of inadvertently disclosing any exam questions. If you are Security+ certified and would like to volunteer to teach one of the Security+ domains, or if you have questions, please contact Colleen Murphy at: crmurphy.cs@hotmail.com.

Study Groups

Organized study groups are in progress for the CISSP concentration, Information Systems Security Architecture Professional (ISSAP), and for the Certified Authorization Professional (CAP) certification. Also, a few members have expressed interest in participating in a study group for the Certified Information Systems Manager (CISM) certification but we still need someone to organize and facilitate this study group. If you hold the CISM certification, please consider volunteering your time and knowledge by organizing and guiding a CISM study group. Additional study groups can be organized for other certifications if there are enough members interested and if someone is willing to take on the role of organizing the group and scheduling the meetings.

Contact Colleen Murphy (crmurphy.cs@hotmail.com) if you’re interested in organizing a study group, want to participate in a study group, or if you have questions.

We have a lot planned for this year, so stay tuned for updates.
By Adam Segal, Real Clear Defense, March 5, 2015

They don’t prepare you for this in college or admit it in job interviews. The harsh reality is that if you are middle-aged, write computer code for a living, and earn a six-figure salary, you’re headed for the unemployment lines. Your market value declines as you age and it becomes harder and harder to get a job.

The Director of National Intelligence released his annual threat assessment last week, and cyberattacks top the list. There were at least three headlines in Clapper’s written and oral statements. First, while a “cyber armageddon”—a destructive attack that debilitates wide swathes of U.S. infrastructure—might be possible, it is very unlikely. Instead, the risk is from an “ongoing series of low-to-moderate level cyber attacks,” which will “impose cumulative costs on U.S. economic competitiveness and national security.”

Second, China may get most of the press coverage, but Russia is a serious challenge. In fact, Clapper admitted that the “Russian cyber threat is more severe than we’ve previously assessed.” Third, Clapper accused Iran of hacking the Sands Casino and warned that the next wave of attacks could change or manipulate information, impairing decision making by government officials, corporate executives, or investors.

As several other U.S. government officials have done over the last several months, Clapper also claimed that attribution has become easier. Hackers can no longer assume that their attacks will be undetected and they can no longer expect that when attacks are unmasked, their identities will remain anonymous. With enough time and resources, attacks can be attributed. This, however, has not created deterrence. Breaking into networks remains easy, the gains of the attacks high, and the relatively long delays between attack and attribution create a permissive environment.

This seems to be especially true in the case of China. Clapper notes that Chinese cyber espionage continues despite “detailed” private cybersecurity reports attributing attack on U.S. companies and government agencies, “scathing” public denouncements, and “stern” U.S. government demarches. Clapper does suggest one way of limiting attacks. Because Chinese hackers use relatively simple tools and techniques, improving defenses would force them to develop more sophisticated, expensive, and time-consuming methods. The costs of economic espionage would go up.

Coincidentally, I was at a conference last week in Washington focused on this exact question: how do you raise the cost to Chinese hackers? There was a great deal of skepticism that the United States would be able to get China to accept a norm against the cyber-enabled theft of intellectual property, trade secrets, or business strategies. Other states do not believe the United States actually adheres to the norm, and many friends of the United States actively engage in cyber-enabled economic espionage. One participant, for example, noted an uptick in attacks on U.S. companies coming from South Korea.

There was also little sense that big technology companies would be interested in pursuing trade or other sanctions against the Chinese firms that are thought to be benefiting from the theft. Smaller firms might have the stomach for a fight, but the larger firms, with sizable investments in the market, are already overexposed to retaliation from the Chinese government. Things are already bad, with foreign technology being removed from government procurement lists and a draft counterterrorism law that would require firms to hand over encryption keys and install backdoors, and they fear that it will only get worse.

Instead of raising the costs by engaging in active defense where small groups of U.S. hackers with highly detailed intelligence disrupt attacks in China before they hit U.S. networks, the one idea that generated any enthusiasm was to lower the value of the information Chinese hackers stole through deception. Here the model is the Farewell Dossier. In 1981, French intelligence obtained the services of Col. Vladimir I. Vetrov, “Farewell,” who photographed and supplied 4,000 documents on KGB efforts to obtain scientific and technical secrets. President Mitterrand offered the information to President Reagan, and the CIA discovered that the Soviets had already stolen radar, computer, machine tool, and semiconductor technology. In an effort to conduct its own version of economic warfare on Moscow and poison the collection efforts, the CIA fed fake information to Soviet agents that would later fail. (Fans of The Americans will recognize this plot line. Elizabeth and Phillip send stolen plans of propellers that cause a submarine to sink.)

Read the rest here:
http://www.realcleardefense.com/articles/2015/03/05/one-way_to_counter_chinese_hacking_poison_the_well___107700.html
Why Venture Capitalists Love Security Firms Right Now

By Mario Trujillo, The Hill, March 15, 2015

Google Executive Chairman Eric Schmidt expressed confidence Wednesday that technology companies would win the debate about encryption over the government.

As companies increase encryption on users’ devices in response to revelations about government surveillance programs, the FBI and others have argued the technology could stifle law enforcement.

"We don't know how to build a trap door in these systems, which is only available to the good guys," Schmidt said Wednesday at the American Enterprise Institute. "If we put a trap door in our system, first we would have to disclose it, because people would find out anyway, and second, some evil person, in addition to the good guys would figure out a way to get in it. And I think the whole trust of this model is really really broken."

The FBI has pushed back on the moves, saying investigations could be stalled and more suspects could walk free if the encryption becomes the norm.

"We've taken a very tough line in the industry over this issue, and I think we will win this one, at least in America, because the encryption technology is broadly understood [and] the current encryption technology is largely unbreakable," he said.

Schmidt said he is sympathetic to the argument that the government needs to see what is going on. But he said he is not sympathetic to the idea that governments can do it without a court order. Schmidt said Google receives thousands of national security requests for information, which he said is manageable.

"So my answer to the government and the US government, is it's called a front door," he said.

Read the rest here:

By Mike Orcutt, MIT Technology Review, March 17, 2015

Venture capitalists poured a record $2.3 billion into cybersecurity companies in 2014, a year marked by frequent reports of hacks on high-profile companies.

Yearly investment in cybersecurity startups been on the rise for several years now, and is up 156 percent since 2011, according to CB Insights. The trend will likely continue, as 75 percent of CIOs surveyed by Piper Jaffray said they would increase spending on security in 2015.

Though the technologies offered by the startups probably won’t swing the balance away from the attackers, they could help businesses adapt to the strong likelihood of getting hacked, says Lucas Nelson, who focuses on security as a principal investor at Gotham Ventures. New technologies reaching the market could help victims of break-ins by reducing the amount of time it takes to detect hackers and reverse the damage they cause, he says.

A new class of opportunities has also emerged because so much business has been moved to the cloud during the past five years. “There hasn’t been a commensurate level of spending in cloud security,” says Nelson.

Read the rest here:
Biometric security could do away with passwords


With hackers and cyber thieves running rampant online, efforts to create stronger online identity protection are leading major tech firms to invest in biometric security methods. Analysts predict that 15 percent of mobile devices will be accessed with biometrics in 2015, and the number will grow to 50 percent by 2020.

With hackers and cyber thieves running rampant online, efforts to create stronger online identity protection are leading major tech firms to invest in biometric security methods.

As Business Insider reports, firms are incorporating biometrics — the recognition of a user through fingerprint, iris, voice, or facial scans — to stay ahead in a competitive industry.

“I would love to kill the password dead as a primary security method because it’s terrible,” said White House cybersecurity coordinator Michael Daniel to a security tech forum last year.

Daniel’s statement foreshadowed larger industry moves, first and foremost with Apple’s successful introduction of Touch ID in its latest lines of iPhones. This move on the part of such a large company has led to a growing conversation about biometrics, and has spurred others to follow.

Samsung has now introduced its own fingerprint scanner, and Qualcomm recently unveiled its 3D fingerprint technology, which is now being built into the chips of many of its devices.

In tens of millions of cases, passwords have been stolen in breaches of major retailers, including companies such as Target, Home Depot, and JP Morgan Chase. It is one of the principal elements of identity theft.

“Biometrics are likely to be a major part of any new identity verification effort,” said Ramesh Kesanupalli, the vice president of Fast Identity Online Alliance (FIDO). “If you don’t eliminate dependency on the password you’re not solving the problem, you are only treating the symptom.” FIDO includes 170 members including manufacturers of hardware and software.

Many industry experts also share that outlook.

“Moving the world away from passwords is an enormous task, and FIDO will succeed where others have failed,” said Microsoft program manager Dustin Ingalis.

International Data Corp predicts that 15 percent of mobile devices will be accessed with biometrics in 2015, and the number will grow to 50 percent by 2020.

Some worry, though, that instead of fixing security problems, biometrics will only create a new universe of risks.

“If you have a credit card that gets compromise you can get a new credit card, but what do you do if your iris or your fingerprints get compromised?” said Sascha Meinrath, head of the New America Foundation’s X-Lab, which studies new technologies. “This presents an entire new realm of security problems,” he said.

Meinrath said that there have already been successful efforts to fake people’s fingerprints, and that the security that biometrics could provide could also be compromised.

At the least, biometrics will serve as an important weapon in the fight against cyber terrorism, especially at a time when major companies have suffered large losses from data theft.

Read the rest here:
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 Fishing – 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
Cybergeddon: Why the Internet could be the next “failed state”

By Sean Gallagher, Ars Technica  March 2, 2015

In the New York City of the late 1970s, things looked bad. The city government was bankrupt, urban blight was rampant, and crime was high. But people still went to the city every day because that was where everything was happening. And despite the foreboding feelings hanging over New York at the time, the vast majority of those people had at most minor brushes with crime.

Today, we all dabble in some place that looks a lot like 1970s New York City—the Internet. (For those needing a more recent simile, think the Baltimore of The Wire). Low-level crime remains rampant, while increasingly sophisticated crime syndicates go after big scores. There is a cacophony of hateful speech, vice of every kind, and policemen of various sorts trying to keep a lid on all of it—or at least, trying to keep the chaos away from most law-abiding citizens. But people still use the Internet every day, though the ones who consider themselves “street smart” do so with varying levels of defenses installed. Things sort of work.

Just like 1970s New York, however, there’s a pervasive feeling that everything could go completely to hell with the slightest push—into a place to be escaped from with the aid of a digital Snake Plissken. In other words, the Internet might soon look less like 1970s New York and more like 1990s Mogadishu: warring factions destroying the most fundamental of services, "security zones" reducing or eliminating free movement, and security costs making it prohibitive for anyone but the most well-funded operations to do business without becoming a "soft target" for political or economic gain.

That day is not yet nigh, but logic suggests the status quo can't continue forever. The recent rash of major breaches of corporate networks, including the theft of personal information from the health insurer Anthem and the theft of as much as a billion dollars from over 100 banks are symptoms of a much larger trend of cybercrime and espionage. And while the issue has been once again raised to national importance by the White House, it could be argued that governments have done more to exacerbate the problem than address it. Fears of digital warfare and crime are shifting budget priorities, funding the rapid expansion of the security industry and being used as a reason for proposals for new laws and policy that could reshape the Internet.

“If we think our kids and grandkids are going to have as awesome and free an Internet as the one we have, we really have to look at why we think that,” Jason Healey, director of the Cyber Statecraft Initiative at the Atlantic Council of the United States, told Ars.

The soothsayer

The alternative futures for the Internet are not pretty. In presentations at multiple security conferences, Healey has suggested that the Internet could “start to look like Somalia”—a failed state where security is impossible, going about daily life is hazardous, and armed camps openly wage war over the network.

Healey's analysis has been reinforced by events over the past two years: record data breaches, zero-day vulnerabilities released that affected a preponderance of Internet services, and visibility into the vast state surveillance of the Internet. The Internet has been “weaponized,” not just by the NSA and its foreign counterparts but by other states and Internet crime organizations. A thriving market for vulnerabilities attracts the bright and ambitious to work on discovering "zero days" for profit.

While a total breakdown of the Internet is unlikely, Healey and others believe that it's nearly as unlikely that today's status quo can be sustained. Other possible scenarios wouldn't bring networked life to its knees, but they all would make the Internet a very different "place" than it is today.

Five years ago, Healey was on a team advising the Department of Defense about the structure of its future IT workforce. To do that, the team needed to understand what the networked world would look like in the next decade. Healey was researching the issue, and he started to look at scenarios where “maybe the future is going to look very different from the past,” he said. “Attackers have had an advantage for 35 years—what if that relationship is going to shift?”

The potential answers Healey found were presented in a 2010 paper. He further refined them in a 2011 article in the Georgetown Journal of International Affairs called "The Five Futures of Cyber Conflict and Cooperation." The most optimistic and least likely of Healey’s scenarios was a "cyber paradise," he told Ars. "Defense is way better than offense—you’d have to be really amazing, like the NSA or KGB, to get anything done as an attacker." But as he looked at trends, he realized that maybe the classic relationship above wouldn’t be shifting. “It’s way more likely that it’s going to go in the other direction—that offense is going to have a significantly larger advantage than it does now.”

Read the rest here:
Costly shift to new credit cards won't fix security issues

By Nandita Bose, Reuters, March 3, 2015

A multi-staged, targeted campaign is striking the international energy sector in order to spy on companies and steal sensitive information.

New technology about to be deployed by credit card companies will require U.S. consumers to carry a new kind of card and retailers across the nation to upgrade payment terminals. But despite a price tag of $8.65 billion, the shift will address only a narrow range of security issues.

Credit card companies have set an October deadline for the switch to chip-enabled cards, which come with embedded computer chips that make them far more difficult to clone. Counterfeit cards, however, account for only about 37 percent of credit card fraud, and the new technology will be nearly as vulnerable to other kinds of hacking and cyber attacks as current swipe-card systems, security experts say.

Moreover, U.S. banks and card companies will not issue personal identification numbers (PINs) with the new credit cards, an additional security measure that would render stolen or lost cards virtually useless when making in-person purchases at a retail outlet. Instead, they will stick with the present system of requiring signatures.

Anre Williams, president of global merchants services at American Express, cited cost and complexity as reasons for not issuing PIN numbers, which would require a much larger investment by card issuers. "It is the PIN management system that takes the effort," Williams said, in part because of the additional customer support it requires.

Chip technology has been widely used in Europe for nearly two decades, but banks there typically require PINs. Even so, the technology leaves data unprotected at three key points, security experts say: When it enters a payment terminal, when it is transmitted through a processor, and when it is stored in a retailer’s information systems. It also does not protect online transactions.

"The simplest way to circumvent chip-and-PIN is to use a stolen card number to make an online purchase," said Paul Kleinschnitz, a senior vice-president for cyber security solutions at card processor First Data Corp.

Analysts predict that credit card fraud at brick-and-mortar retailers will fall after the introduction of chip-enabled cards, but that online fraud will rise, as has happened in other countries using the technology. Research and consulting firm Aite Group estimates U.S. online card fraud will more than double to $6.6 billion from $3.3 billion between 2015 and 2018.

Retailers and security experts say it would make more sense for the United States to jump instead to a more secure system, such as point-to-point encryption. This technology is superior to chip-and-PIN, which first was deployed about 20 years ago, because it scrambles data to make it unreadable from the moment a transaction starts.

But the newer technology would cost as much as twice what the chip card transition will cost, and does not have the older technology’s long track record.

Moreover, some security experts say that mobile payment services such as Apple Pay, a service from Apple that stores data on the cloud, have the potential in coming years to secure payments without the need to swipe or tap a card at all.

**Liability for Breaches**

The dispute over the effectiveness of dueling payment security systems offers insight into a broader battle over who bears liability for breaches: retailers or the financial firms that extend the credit.

Currently, card issuers are generally liable for fraudulent charges. After the October deadline, if a retailer is not using a terminal that can read the new cards and a security breach occurs involving a chip card, the retailer will be liable, though consumers will still deal with their banks in the event of a fraudulent charge. If the retailer is chip-and-PIN enabled, the card issuer will be liable.

The liability issue has engendered anger on the part of some retailers, but it has also provided an incentive for compliance with the new standards.

"When banks and card companies are only concerned about shifting the liability to the retailer, you have to comply first," Brooks Brothers Chief Executive Officer Claudio Del Vecchio said. "And then think of solutions that will fix your problems."

The clothing retailer expects to meet the October deadline, but Del Vecchio declined to give details on the cost involved.

Read the rest here:
http://www.reuters.com/article/2015/03/03/us-usa-cybersecurity-retail-insight-idUSKBN0LZ0GC20150303
FAA should address weaknesses in air traffic control systems: GAO

The Federal Aviation Administration (FAA) has taken steps to protect its air traffic control systems from cyber-based and other threats, but significant security control weaknesses remain, threatening the agency’s ability to ensure the safe and uninterrupted operation of the national airspace system (NAS), the GAO says in a new report. The GAO report says that FAA also did not fully implement its agency-wide information security program.

By Homeland Security News Wire, March 9, 2015

One of the most shocking parts of the recently discovered spying network Equation Group is its mysterious module designed to reprogram or reflash a computer hard drive’s firmware with malicious code. The Kaspersky researchers who uncovered this said its ability to subvert hard drive firmware—the guts of any computer—“surpasses anything else” they had ever seen.

The Federal Aviation Administration (FAA) has taken steps to protect its air traffic control systems from cyber-based and other threats, but significant security control weaknesses remain, threatening the agency’s ability to ensure the safe and uninterrupted operation of the national airspace system (NAS), the GAO says in a new report.

These weaknesses include weaknesses in controls intended to prevent, limit, and detect unauthorized access to computer resources, such as controls for protecting system boundaries, identifying and authenticating users, authorizing users to access systems, encrypting sensitive data, and auditing and monitoring activity on FAA’s systems. Additionally, shortcomings in boundary protection controls between less-secure systems and the operational national airspace system (NAS) environment increase the risk from these weaknesses.

The GAO report says that FAA also did not fully implement its agency-wide information security program. As required by the Federal Information Security Management Act of 2002, federal agencies should implement a security program that provides a framework for implementing controls at the agency. FAA’s implementation of its security program, however, was incomplete. For example, it did not always sufficiently test security controls to determine that they were operating as intended; resolve identified security weaknesses in a timely fashion; or complete or adequately test plans for restoring system operations in the event of a disruption or disaster.

Additionally, the group responsible for incident detection and response for NAS systems did not have sufficient access to security logs or network sensors on the operational network, limiting FAA’s ability to detect and respond to security incidents affecting its mission-critical systems.

The weaknesses in FAA’s security controls and implementation of its security program existed, in part, because FAA had not fully established an integrated, organization-wide approach to managing information security risk that is aligned with its mission. National Institute of Standards and Technology guidance calls for agencies to establish and implement a security governance structure, an executive-level risk management function, and a risk management strategy in order to manage risk to their systems and information.

FAA has established a Cyber Security Steering Committee to provide an agency-wide risk management function. However, it has not fully established the governance structure and practices to ensure that its information security decisions are aligned with its mission. For example, it has not (1) clearly established roles and responsibilities for information security for the NAS, or (2) updated its information security strategic plan to reflect significant changes in the NAS environment, such as increased reliance on computer networks.

The GAO says that until FAA effectively implements security controls, establishes stronger agency-wide information security risk management processes, fully implements its NAS information security program, and ensures that remedial actions are addressed in a timely manner, the weaknesses GAO identified are likely to continue, placing the safe and uninterrupted operation of the nation’s air traffic control system at increased and unnecessary risk.

The GAO notes that in support of FAA mission, FAA relies on the NAS — one of the U.S. critical infrastructures — which comprises air traffic control systems, procedures, facilities, aircraft, and people who operate and maintain them. Given the critical role of the NAS and the increasing connectivity of FAA’s systems, it is essential that the agency implement effective information security controls to protect its air traffic control systems from internal and external threats.

Read the rest here: http://www.homelandsecuritynewswire.com/dr20150309-faa-should-address-weaknesses-in-air-traffic-control-systems-gao
Reconnaissance malware wave strikes energy sector

Symantec says a new Trojan-based campaign, focused on the Middle East, is targeting the energy industry and its trade secrets.

By Charlie Osborne for Zero Day, March 31, 2015

A multi-staged, targeted campaign is striking the international energy sector in order to spy on companies and steal sensitive information.

Between January and February this year, security researchers from Symantec observed the targeted attack campaign focus on "energy companies around the world, with a focus on the Middle East." According to the team, the new campaign uses an information stealer dubbed Trojan.Laziok.

Laziok acts as a reconnaissance tool which allows cyberattackers to infiltrate computer systems and steal data concerning computer systems themselves -- so hackers can choose whether to continue the assault or not -- with the overall aim of finding and stealing trade secrets.

The security firm discovered that the majority of targets are linked to the petroleum, gas and helium industries. The UAE, Pakistan, Saudi Arabia and Kuwait are most often targeted, but businesses in the US and UK have also experienced attacks.

Symantec says the initial attack vector stems from the moneytrans[.]eu domain, which acts as an SMTP server. Emails sent from this domain contain a malicious file containing an exploit for the Microsoft Windows Common Controls ActiveX Control Remote Code Execution Vulnerability (CVE-2012-0158). Once a victim clicks on the email and opens the attachment -- usually in the guise of an Excel file -- Laziok is dropped.

When the Trojan has found its way into a computer system, the malicious code hides itself in the %SystemDrive%\Documents and Settings\All Users\Application Data\System\Oracle directory before renaming itself with well-known and seemingly legitimate names, such as search.exe and chrome.exe. The Trojan then begins to gather system data including computer names, installed software, RAM size, CPU details and antivirus software installation.

This information is then sent to the cyberattackers for processing. Additional malware payloads may then be sent back to the compromised system, which can damage networks or focus on data theft.

Read the rest here: http://www.zdnet.com/article/reconnaissance-malware-wave-strikes-energy-sector/
What You Need To Know About Nation-State Hacked Hard Drives

The nation-state Equation Group compromise of most popular hard drives won't be a widespread threat, but future disk security -- and forensic integrity -- remain unclear.

By Sean Gallagher, Ars Technica  March 2, 2015

The recent discovery that a nation-state hacking group had fashioned its own tools to reprogram more than a dozen major vendors' hard drives such that it could harbor malware and store stolen information in them undetected has cast a shadow over the security and reliability of these disk drives.

Most security experts weren't shocked that a nation-state was messing with hard drive firmware--hard drive attacks had been demonstrated by researchers over the past year, and it was only a matter of time before an in-the-wild attack was found. Even so, the so-called Equation Group's ability to wrest control of such a broad array of drive products was eye-opening, given the level of skill, time and financial resources such a feat required.

"The more telling part of the Kaspersky Lab report was that the hard drive malware supported a large number of hard drive vendors. That is a lot of work to set up and test and maintain," says HD Moore, chief research officer with Rapid7.

Kaspersky Lab last month announced that it had discovered a leading-edge nation-state group, which it dubbed the Equation Group, that among other things had built malware modules that can reprogram hard drive brands, ensuring that the malware remains undetected by antivirus software and that even if a hard drive is reformatted or the operating system is reinstalled, the malware can't be eradicated. The attackers could also swap one drive sector with a malware-infected one, and use the drive to store stolen information, for example.

Vitaly Kamluk, director of the EEMA Research center at Kaspersky Lab, contends that it would take a skilled programmer months or years to successfully pull off this type of hack. "This is what makes this whole group gods among APT actors. We haven't seen anything close to this" before, Kamluk says. "You would have to get internal documents from the vendor," for instance.

So now that most major hard drive brands apparently have been compromised by the Equation Group-- which has not been officially identified by Kaspersky Lab but most experts say is most likely the NSA--what next?

Big-name hard drive vendors for the most part have remained mum or vague about the Equation Group findings. Neither Hitachi nor Toshiba responded to press inquiries about the firmware hack. Meanwhile, a Seagate spokesperson told Dark Reading that the company "has no specific knowledge of any allegations regarding third-parties accessing our drives."

"Seagate is absolutely committed to ensuring the highest levels of security of the data belonging to our users. For over seven years Seagate has been shipping drives offering industry-leading levels of self encryption, while putting in place secure measures to prevent tampering or reverse engineering of its firmware and other technologies," he said.

Hard drive vendors indeed could enhance the security of their drives to thwart such attacks in the future. Many of the newest ARM processors come with secure boot mode support as well as digital signatures of both the boot loader and OS kernel, Rapid7's Moore says. "Securing the ARM chips on the drive controllers isn't impossible and there are ways to make rogue firmware installation harder," he says. "Granted, there is likely a way to bypass those just like all other 'secure' boot modes and it would make flashing and diagnostics more complicated, but they could certainly improve the security, all the same."

A secure boot basically includes cryptographic checks in each stage of the boot process, which would prevent malware from running during that process.

Still, the majority of organizations won't need to worry about their hard drives getting hacked this way, security experts say. While the Equation Group hard drive hack is alarming and sophisticated, it's not likely to become a widespread threat vector, but instead used in very limited and targeted attacks. "One of the reasons you're not going to see these kinds of attacks widespread is because they are very hardware-specific," Moore says. "That effort is too high for most [attackers] intent on causing harm. Most nation-states wouldn't want to go through that much effort," either, he says.

Read the rest here:
The Pentagon is looking to hire 3,000 infosec pros

By HelpNet Security, March 10, 2015

A multi-staged, targeted campaign is striking the international energy sector in order to spy on companies and steal sensitive information.

The US Department of Defense has gotten permission and is aiming to hire 3,000 infosec professionals to work at the US Cyber Command by the end of this year, and is set to make the majority of the members of its Cyber Mission Force (CMF) achieve at least initial operational capability by the end of the 2016 Fiscal Year.

According to Aliya Sternstein, salaries start at $42,399 and can eventually rise to over triple that amount ($132,122).

The good news for potential employees is that the DoD doesn’t have to evaluate the applicants by traditional competitive criteria - to gain employment with the CMF, the applicants will have to demonstrate unique cybersecurity skills and knowledge.

The US Cyber Command was instituted in 2010, and was tasked with protecting the Department of Defense’s information networks and critical infrastructure, as well as to carry out cyber attacks against adversaries.

"USCYBERCOM confronted serious challenges from the outset. DoD networks had been planned and initially constructed decades earlier in an environment in which redundancy, resiliency, and defensibility were not always primary design characteristics," Admiral Mike Rogers, the Head of the Cyber Command, shared with the members of the US House committee on Armed Service's Subcommittee on Emerging Threats and Capabilities.

"Operators in USCYBERCOM, not surprisingly, could not even see all of our networks, let alone monitor all the traffic coming into and out of them from the Internet. Our people were and are professionals, so that issue was rapidly engaged, but nonetheless the sheer volume of work involved in starting a new, subunified command was substantial."

"The bad news was that USCYBERCOM was built from the ground up by cutting manning to the bone, initially sacrificing vital support functions and institutional infrastructure to build mission capabilities as fast as possible," he noted, and announced that things are slowly changing.

The Cyber Mission Force is currently half-staffed, but are working on filling out their rosters and qualifying their personnel.

Admiral Rogers is aware that this won’t be easy. "We are already hard pressed to find qualified personnel to man our CMF rosters, to get them cleared, and to get them trained and supported across all 133 teams," he noted, and mentioned that the final number of personnel should be around 6,200.

He is also aware that luring cybersecurity pros from the civil sector will be hard, and that certain monetary and other incentives will have to be put on the table in order to do it. Also, that this situation is only going to get worse as the US economy continues to get better.

Read the rest here:
http://www.net-security.org/secworld.php?id=18061

Cyber-Risk May Take a Bite Out of Apple Watch

By Tara Seals, Info Security, March, 2015

Apple has unveiled the Apple Watch—a smart wearable that will function as a Mac-on-the-wrist. It has tech-heads excited, but security researchers warn that consumers should be careful of the potential cyber-risks that the gadget’s on-board connectivity represents.

“Our goal has always been to make powerful technology more accessible,” Apple says of the watch. “More relevant. And ultimately, more personal. Apple Watch represents a new chapter in the relationship people have with technology. It’s the most personal product we’ve ever made, because it’s the first one designed to be worn.”

And therein lies the first problem, according to some.

“I don’t feel the need to walk around with a beacon on my wrist that wouldn’t even last long enough if I was caught in an avalanche,” said Brett Fernicola, chief information security officer at STEALTHbits Technologies, in an email. “I’ll pass on the smartwatch craze and stick to a traditional watch that does one thing well, tell time without ever having to come off my wrist or put my personal information in danger.”

The danger comes from the fact that the watch will come equipped with Wi-Fi and Bluetooth, which is of course a boon for its role in the internet of things (IoT). Imagine that it can automatically upload GPS-based running route information to a maps app on an iPad, for a topographical representation of one’s marathon training, progress, say. Or, a smart fridge can send a reminder to the watch when the wearer enters a grocery store, noting that the milk is past its expiration date. It can happen. And probably will.

Read the rest here:
How hard is it to permanently delete data?

By Mark Pomerleau, GCN, March 31, 2015

The list of software known to use the same HTTPS-breaking technology recently found preinstalled on Lenovo laptops has risen dramatically with the discovery of at least 12 new titles, including one that's categorized as a malicious trojan by a major antivirus provider.

The controversy surrounding former Secretary of State Hillary Clinton's email has brought data destruction to the forefront of the national conversation. Clinton used a server housed at her New York residence for her personal and official emails and online communications while she was at Foggy Bottom. Lawmakers investigating the 2012 death of an ambassador in Libya have been concerned that official government emails from Clinton that might assist in the investigation were deleted despite assurances from Clinton that she turned over all emails pertaining to government work to the State Department.

Now reports say Clinton "wiped the server," deleting all emails. But how easy is it to permanently wipe data from servers or storage media? According to experts who were interviewed recently by the Washington Post, the congressional committee charged with investigating the U.S. ambassador's death in Benghazi might still be able to obtain Clinton's deleted emails — in the event they can access the server.

Provided Clinton simply hit the delete button on her emails, they probably still exist. Files are not permanently deleted when a user hits the delete button. "Instead, the pointer the computer uses to find the file is removed, and the computer treats the space on your hard drive as reusable," explained the Post. "Though, depending on the amount of activity one performs on a device, data that is randomly stored could replace deleted items as it needs the space. Typically, additional steps must be taken in order to permanently delete items from a server.

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
</table>

If experienced experts were able to access Clinton's server with the intention of retrieving emails, they might create a "physical forensic image," which "creates an identical, bit-by-bit, zero-by-zero copy of the original hard drive," the Post reported. This step is used to view the emails as they would appear in a read-only format preventing alterations. Following the physical forensic image, experts might attempt to locate and extract databases that house emails and then conduct a forensic analysis of unallocated spaces within those databases.

However, an equally skilled technician tasked with permanently deleting data from servers could make it very difficult for investigators to retrieve emails or discern if items were even deleted. On the other hand, the Post suggested, any IT pro working with government data would have created some type of back-up to hard drives, the Internet or magnetic tape.

In spite of data retention regulations, agencies need a way to reliably destroy government data and the media housing it. When agencies discard old equipment, for example, they have a variety of data destruction tools they can use. These include:

- Read the rest here:
  http://gcn.com/articles/2015/03/31/deleted-emails.aspx?
Sophisticated Cyber Crime Methods are Changing the Definition of Hacking

By Lauren Ingram, Penn State, March 2, 2015

More than 100 banks in 30 countries have joined the ranks of Anthem Blue Cross Blue Shield and Sony Pictures. As targets of unprecedented, and likely some of the most costly, cyber attacks in history, the financial institutions, insurance company and film studio are reeling after record-setting amounts of data, money, internal emails and more were stolen by hacker groups, which in some instances are believed to have been sanctioned by nation-states. Just last year, thieves behind the Target and Home Depot breaches made off with customer credit card numbers and cost the corporations millions of dollars.

But most data breaches don’t make headline news, and sometimes companies don’t know they’ve been hacked until it’s too late. In 2014 alone, there were more than 740 breaches in the financial, business, health care, education and government sectors, according to the Identity Theft Resource Center. That figure is expected to climb in 2015.

Penn State’s own intrusion detection and prevention system operated by Security Operations and Services, the University’s cybersecurity team, identifies and blocks approximately 157,000 hostile systems from accessing 200,000 computers on the University network on any given day. And within the next year, areas across Penn State will participate in a security assessment to gather data to use as a benchmark for future planning. For a vast institution like Penn State, what one area does in the realm of its own network security processes can have profound implications on the rest of the University.

“This is the world we live in now,” said Matthew Snyder, chief information security officer for the Penn State Milton S. Hershey Medical Center. “If you would have told me a couple of years ago that a data breach could cost $1 billion, I would have thought you were crazy. Now, it’s not too far fetched — these guys don’t play by the rules.”

Laws and regulations that the majority of the world adheres to mean very little to a growing faction of cyber criminals, commonly referred to as advanced persistent threat (APT) actors. Since emerging in the early 2000s, APT actors use sophisticated tools and tactics to gain access to and steal digital information they can use or sell at a later date. With economic and political motivations, these groups are characterized by their ability to patiently infiltrate computer networks and remain undetected for up to two years on average before being caught or revealing themselves — by then, the data breach has already happened.

The world is dealing with a level of sophistication among APT actors that over time has also become highly coordinated, according to Kevin Morooney, vice provost for Information Technology at Penn State.

There’s a spectrum of hundreds of known APT actors that are going after everything from intellectual property and health data to credit card and social security numbers — a far cry from the earliest days of the Internet when hacking was almost like a kind of playful vandalism. Eventually, hacking became more sophisticated and economically focused, but was still primarily unorganized.

“Today, these threat organizations are well-funded and run like large companies with business plans, many employees and headquarters,” Morooney said. “That kind of threat flies in the face of how universities have generally chosen to design their network architectures and accompanying services: open, fast and available.”

Institutions of higher education rely on sharing knowledge and information to promote collaboration and educational achievement. But, they also have an imperative to protect the troves of intellectual property and personally identifiable information in their care.

Safeguarding this data has always been a serious job, but it’s getting even more complicated since the majority of breaches are the result of malicious or criminal activity (and not employee error or system glitches), according to a 2014 Cost of Data Breach Study by the Ponemon Institute.

Read the rest here:
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? Can you interview one of the "movers and shakers"? 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!

John Deere Thinks People Will Pirate Music With In-Car Computers

By Adam Clark Estes, Gizmodo, April 3, 2015

Did you know that it’s illegal to tinker with the code in your in-car computer? Thanks to the nuances of the Digital Millennium Copyright Act (DMCA), you’re not even supposed to inspect the inner workings of your vehicle’s circuitry. This is absurd, which is why the Electronic Frontier Foundation (EFF) is fighting for a better policy.

The EFF is currently entrenched in a legal battle to challenge DMCA overreach. In a new blog post—colorfully titled “Automakers Say You Don’t Really Own Your Car”—the digital rights advocates share some of the absurdity that many vehicle manufacturers are slinging to justify the DMCA’s applications to in-car computers. This is the best:


Published at no cost to ISSA Colorado Springs by Sumerduck Publishing™, Woodland Park, Colorado