Colleagues,

Many of us are aware of the multiple reports that discuss the current and projected cybersecurity workforce and skills gap.

Are you aware of everything our Chapter offers? We offer a wide variety of events and opportunities to help you throughout your career. Our Training Committee organizes and hosts two Security+ Exam Prep Review Seminars each year, as well as a CISSP Exam Prep Review Seminar. More than a dozen volunteer instructors teach the Security+ and CISSP material each year, helping the students ensure their readiness for the certification exam, and enhancing their own knowledge of the material in the process. Our Training Committee also organizes approximately seven Mini-Seminars each year, providing career broadening opportunities for attendees, and providing a convenient – and FREE – way to earn continuing education credits. Information on our training events is posted on the Chapter website, the Chapter newsletter, and is sent out in emails.

We also host two conferences annually, a one-day conference in the spring, and a two-day conference in the fall. The Cyber Focus Day is held in the late March timeframe, and the Cyber Security Training and Technology Forum is held in the late August timeframe. These conferences are free to members, providing an opportunity to earn up to 21 continuing education credits if you attend both conferences.

Our Mentorship Committee offers dedicated mentors who have a passion to give back to our members and help them grow through all stages of their careers. If you’re interested in being a mentor or a mentee, please contact our Mentorship Committee Chair, Melissa Absher, via the link on our Chapter website, under Key Personnel. To help women throughout their cybersecurity careers, and to encourage other women to consider a cybersecurity career, we started a

(Continued on page 4)

The ISSA Colorado Springs Newsletter incorporates open source news articles in compliance with USC Title 17, Section 107, Paragraph a (slightly truncated to avoid copyright infringement) as a training method to educate readers on security matters.

The views expressed in articles obtained from public sources within this newsletter do not necessarily reflect those of ISSA, this Chapter or its leadership.
Special Report: HP Enterprise let Russia scrutinize cyber defense system used by Pentagon

By Joel Schectman, Dustin Volz, Jack Stubbs, Reuters, October 2, 2017

Hewlett Packard Enterprise allowed a Russian defense agency to review the inner workings of cyber defense software used by the Pentagon to guard its computer networks, according to Russian regulatory records and interviews with people with direct knowledge of the issue.

The HPE system, called ArcSight, serves as a cybersecurity nerve center for much of the U.S. military, alerting analysts when it detects that computer systems may have come under attack. ArcSight is also widely used in the private sector.

The Russian review of ArcSight’s source code, the closely guarded internal instructions of the software, was part of HPE’s effort to win the certification required to sell the product to Russia’s public sector, according to the regulatory records seen by Reuters and confirmed by a company spokeswoman.

Six former U.S. intelligence officials, as well as former ArcSight employees and independent security experts, said the source code review could help Moscow discover weaknesses in the software, potentially helping attackers to blind the U.S. military to a cyber attack.

“It’s a huge security vulnerability,” said Greg Martin, a former security architect for ArcSight. “You are definitely giving inner access and potential exploits to an adversary.”

Despite the potential risks to the Pentagon, no one Reuters spoke with was aware of any hacks or cyber espionage that were made possible by the review process.

The ArcSight review took place last year, at a time when Washington was accusing Moscow of an increasing number of cyber attacks against American companies, U.S. politicians and government agencies, including the Pentagon. Russia has repeatedly denied the allegations.

The case highlights a growing tension for U.S. technology companies that must weigh their role as protectors of U.S. cybersecurity while continuing to pursue business with Washington’s adversaries such as Russia and China, say security experts.

The review was conducted by Echelon, a company with close ties to the Russian military, on behalf of Russia’s Federal Service for Technical and Export Control (FSTEC), a defense agency tasked with countering cyber espionage.

Echelon president and majority owner Alexey Markov said in an email to Reuters that he is required to report any vulnerabilities his team discovers to the Russian government.

But he said he does so only after alerting the software developer of the problem and getting its permission to disclose the vulnerability. Echelon did not provide details about HPE’s source code review, citing a non-disclosure agreement with the company.

FSTEC confirmed Markov’s account, saying in a statement that Russian testing laboratories immediately inform foreign developers if they discover vulnerabilities, before submitting a report to a government “database of information security threats.”

One reason Russia requests the reviews before allowing sales to government agencies and state-run companies is to ensure that U.S. intelligence services have not placed spy tools in the software.

HPE said no “backdoor vulnerabilities” were discovered in the Russian review. It declined to provide further details.

HPE said it allows Russian government-accredited testing companies to review source code in order to win the Russian defense certifications it needs to sell products to Russia’s public sector.

An HPE spokeswoman said source code reviews are conducted by the Russian testing company at an HPE research and development center outside of Russia, where the software maker closely supervises the process. No code is allowed to leave the premises, and HPE has allowed such reviews in Russia for years, she said.

Those measures ensure “our source code and products are in no way compromised,” she said.

First, I would like to welcome our 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.

Overall it’s been a quiet month on the membership front. We’re at ~514 members as of the end of October. Elections will be upcoming soon. We still seem to have a lot of members who are not receiving emails from the Chapter. Please take a couple of minutes to review your profile on your ISSA International account. Please ensure all your information is current and up to date, especially your contact information. It is critical that we have valid email addresses for everyone as that is our primary method of communicating with members. We have recently been getting a lot of bounces, particularly from military email addresses ending in .mil. A lot of military firewalls have been updated recently to filter email, particularly from *.org addresses. Also, when people change companies, they frequently forget to update their ISSA profile. If you haven’t been receiving chapter emails, this could be the reason so please consider updating your email address to a personal email rather than your work or military address. Just a thought as we don’t want anyone to miss the opportunity to vote for chapter officers in the upcoming elections.

Thanks,
David Reed
Membership Committee Chairman
dreed54321@comcast.net

<table>
<thead>
<tr>
<th>New Members</th>
</tr>
</thead>
<tbody>
<tr>
<td>Josiah Robberson</td>
</tr>
<tr>
<td>Daniel Flores</td>
</tr>
<tr>
<td>Katherine Martin</td>
</tr>
<tr>
<td>Ardis Hinton</td>
</tr>
<tr>
<td>Elizabeth Stern</td>
</tr>
<tr>
<td>David R. Parsons</td>
</tr>
</tbody>
</table>

ISSA Chapter of the Year 2017
Attention all members!!!

Do you know someone who contributed to the chapter or other community event related to the information or cybersecurity disciplines? If so, please take a moment to recognize that person and notify the Awards & Recognition Committee so we can honor their contributions at the 2017 Holiday Luncheon scheduled in December. There is nothing formal you need to submit, just a short paragraph explaining who the person is and what you believe they should be recognized for. The deadline for submission is November 16th, 2017.

Please email Shawn Murray, Chair of the Awards & Recognition Committee at: shawn.murray@issa.org.

Colleen

Attention all members!!!

Do you know someone who contributed to the chapter or other community event related to the information or cybersecurity disciplines? If so, please take a moment to recognize that person and notify the Awards & Recognition Committee so we can honor their contributions at the 2017 Holiday Luncheon scheduled in December. There is nothing formal you need to submit, just a short paragraph explaining who the person is and what you believe they should be recognized for. The deadline for submission is November 16th, 2017.

Please email Shawn Murray, Chair of the Awards & Recognition Committee at: shawn.murray@issa.org.

Colleen

special interest group to focus on women in security. If you’re interested in joining this group, or learning more about it, please contact June Shores at: pro-outreach@issa-cos.org. Did you know we reach out to many local organizations (e.g. ISC2, AFA, AFCEA, etc.) and receive email messages and calendar items from those organizations? If you’re interested in learning more about this, contact our Director of Professional Outreach at: pro-outreach@issa-cos.org.

We have many more committees to help our Chapter manage – and excel – in numerous initiatives. We have a newly established Hospitality Committee to help members feel welcome, to help them know and understand what our Chapter offers, and to help them know who to talk to if they’re interested in any Chapter initiative. We also have a newly established IT Committee to help with staging, maintaining, and administering technology requirements in support of Chapter operations and scheduled events. Our Recognition Committee manages the Chapter’s awards and recognition programs, ensuring members are recognized at our annual awards and recognition ceremony. This includes recognition for significant volunteer work, as well as submitting for Senior Member, Fellow, and Distinguished Fellow status.

Our Transformation Committee identifies new/better ways of conducting Chapter business, helping the Board, and the Chapter, present a more professional image throughout all Chapter initiatives, products, and services. Our Sponsorship and Events Committee (really need additional help here) communicates with companies interested in sponsoring Chapter events, and also works with sponsors and volunteers to ensure Chapter events are organized and any issues/concerns are addressed. Our Newsletter Committee (currently one deep) collects interesting cybersecurity articles, solicits info from Board and Chapter members, and publishes an amazing monthly Chapter newsletter. And our Ethics Committee helps ensure we present and maintain the highest ethical standards at all times.

All of these committees provide a valuable service to our members, and the Chapter as a whole, and their work is critical to the success of our Chapter. Volunteering to help with any of these committees, even for just a short period of time, is a great way to get some experience that can be leveraged in your job and perhaps even on your resume. If you’re interested in learning more about any of these committees, or joining one, please email the committee chair via our Chapter website link, under Key Personnel, or just email the Board at: cos-board@issa-cos.org. Whatever you’re interested in, or whatever your question is, we’ll connect you to the right person.

Thank you all for your continued engagement and support of the 2017 Chapter of the Year!!!
Free Splunk Training for Former Service Members

As part of the $100 million Splunk Pledge (https://workplus.splunk.com/veterans), we have committed to supporting the effort to train the workforce of tomorrow by equipping veterans and former service members with the Splunk skills they need for today’s jobs — all at no cost to them.

New Network Security Standards Will Protect Internet’s Routing

By Staff, NIST, October 3, 2017

As technology improves and merges malware with artificial intelligence, timeless methods such as covering ones mouth may become more important than ever when discussing sensitive information to prevent leaks.

Electronic messages traveling across the internet are under constant threat from data thieves, but new security standards created with the technical guidance of the National Institute of Standards and Technology (NIST) will reduce the risk of messages being intercepted or stolen. These standards address a security weakness that has been a part of the internet since its earliest days (link is external).

The set of standards, known as Secure Inter-Domain Routing (SIDR), have been published by the Internet Engineering Task Force (IETF) and represent the first comprehensive effort to defend the internet's routing system from attack. The effort has been led by a collaboration between NIST and the Department of Homeland Security (DHS) Science and Technology Directorate, working closely with the internet industry. The new specifications provide the first standardized approach for global defense against sophisticated attacks on the internet’s routing system.

The overall strategy creates a defense mechanism for the Border Gateway Protocol (BGP), the system that routers—the devices that direct information toward its destination—use to determine the path data takes as it travels across the collection of networks that comprise the internet. BGP forms the technical glue holding the internet together, but historically, its lack of security mechanisms makes it an easy target for hacking.

"BGP is a global scale system, where routing data for hundreds of thousands of destinations is exchanged between tens of thousands of networks. The informal trust mechanisms we’ve relied on in the past can’t be scaled up to protect a system of that size," said Doug Montgomery, a NIST computer scientist and manager of the NIST project. "BGP as currently deployed has no built-in security mechanisms, so it is common to see examples of 'route hijacks' and 'path detours' by malicious parties meant to capture, eavesdrop upon or deny legitimate internet data exchanges."

BGP was created in the late 1980s to allow routers to exchange information and calculate the best path among millions of possibilities for data to travel across the internet. BGP enables the modern commercial internet, but it evolved at a time when security was not a significant concern, and internet operators have been coping with security problems as a result.

Known BGP attacks since 2008 have resulted in stolen financial payments and network disruption, but so far, these have been relatively small-scale. In many ways, Montgomery said, we are simply lucky that there haven't been more focused and malicious attacks that take advantage of BGP's vulnerabilities.

"The fact that they haven't been dramatically exploited yet shouldn't make you feel better," he said. "Think of how much of our critical infrastructure relies on internet technology—transportation, communication, financial systems, etcetera. Someday, someone will have the motivation."

Read the rest here:
ISSA Fellow Program – A Message from the Recorder

2018 Fellows Cycle Now Open

The Colorado Springs ISSA Chapter has over 500 current members. Many of you have been members for several years and may qualify for the ISSA fellow program. The Fellow Program recognizes sustained membership and contributions to the profession. If you think you or another ISSA associate may qualify in the fellow program, please contact Shawn P. Murray at 5871charlois@gmail.com or at 719-362-0666 to coordinate the process. Shawn is the chair of the chapter awards committee and will help you through the steps. Below are some additional details on the ISSA Fellow Program. Qualification information is also presented below:

No more than 1% of members may hold Distinguished Fellow status at any given time. Fellow status will be limited to a maximum of 2% of the membership.

Nominations and applications are accepted on an annual cycle. The current cycle opened September 1, 2017 and applications will be accepted until March 23, 2018 at 5:00pm Eastern Time. Following the application period, there will be a ten week review period followed by the notification and presentation process. Fellows and Distinguished Fellows will be recognized at the 2018 ISSA International Conference.

Familiarize yourself with the Fellow Program, and the submission guidelines. If you have questions, contact Shawn or The ISSA Fellow Manager or call 866 349 5818 (US toll free) extension 4082.

To Become a Senior Member

Any member can achieve Senior Member status. This is the first step in the Fellow Program. What are the criteria?

Senior Member Qualifications

• 5 years of ISSA membership
• 10 years relevant professional experience

All Senior Member applications require an endorsement from their home chapter to qualify.

Click here to access the Senior Member application.
Click here for the Senior Member endorsement form.

To Become a Fellow or Distinguished Fellow

Have you led an information security team or project for five or more years? Do you have at least eight years of ISSA membership and served for three years in a leadership role (as a chapter officer or Board member or in an International role)? You may be eligible to become an ISSA Fellow or Distinguished Fellow. Please contact Shawn and become familiar with the Fellow Program Guidelines and use the current forms to ensure you comply with all requirements.

Fellow Qualifications

• 8 years of association membership.
• 3 years of volunteer leadership in the association.

(Continued on page 7)
• 5 years of significant performance in the profession such as substantial job responsibilities in leading a team or project, performing research with some measure of success or faculty developing and teaching courses.

All Fellow applications require a nomination to qualify.

Click here to access the Fellow application.  
Click here to nominate a Fellow.  
Click here to submit a Fellow letter of recommendation.

**Distinguished Fellow Qualifications**

• 12 years association membership.  
• 5 years of sustained volunteer leadership in the association.  
• 10 years of documented exceptional service to the security community and a significant contribution to security posture or capability.

All Distinguished Fellow applications require a nomination to qualify.

Click here to access the Distinguished Fellow application.  
Click here to nominate a Distinguished Fellow.  
Click here to submit a Distinguished Fellow letter of recommendation.

Please help us identify candidates that we can recognize in our chapter! Please contact:

Shawn P. Murray  
Chapter Recorder  
Awards & Recognition Committee Chair  
5871charlois@gmail.com  
719-362-0666
My name is Dawn Wellein, and I am running for re-election as a Member at Large in our amazing Chapter! My current day job is a cyber analyst on a military satellite program at SMDC/ARSTRAT. Over the past 2 years, I served as one of the four Members at Large we have in this Chapter and learned a great deal about our Chapter as well as ISSA International. I enjoyed meeting many of you at Chapter meetings and events as well as listening to your opinions and suggestions. I would like to continue my service to our Chapter, and would appreciate your vote to make that happen as a Member at Large for another 2-year term! Thank you.

More election information will be coming in the December Newsletter.

2nd Annual Rocky Mountain Technology Summit

Join us and receive complimentary registration (a $249 value) to the 2nd Annual Rocky Mountain Technology Summit coming to the Crowne Plaza Convention Center, in Denver on November 15th, 2017 from 7am-4pm.

Register HERE with the promo code issa to secure your spot and waive the $249 registration fee.

The theme for 2017 is "Expanding the Frontiers of IT and Security."

Conference Highlights:
- Four (4) concurrent educational sessions
- Peer networking
- 6 CPE credits
- Exhibit hall with 50+ vendors
- Complimentary breakfast, lunch and cocktail reception
- Raffle prizes including a TRIP FOR 2 to a destination of your choice!

Conference Sessions include: (Agenda in development)
- Opening Keynote: TBD
- Threat Lifecycle Management
- Stress-Free Backup Storage
- The Future of Communication. Communication technology Accelerating Better Business Outcomes
- Securing Your Data Supply Chain
- Preparing For Cloudy Weather in Business
- Simplifying BC/DR with Quorum onQ
- The Data Center Revolution: IT approaches the Speed of Light
- Weaponization of IoT and DDoS
- IT Infrastructure: Simplicity=Savings
- Seamless Recovery - Even from Ransomware
- Audience and Panel Discussions: Tying it All Together, Today's Takeaways
- Technology Demo
Digital Danger Zone

October 9-11, 2017 – San Diego, California

With bargain airline prices, the Colorado Springs ISSA chapter was well represented at the 2017 ISSA International conference. In summary, International put on a world-class event! The conference included first-rate speakers, a handful of select hi-tech product vendors, light but appetizing eats, an awesome venue, and a crowd pleasing social event... on board the USS Midway. To see more close-up and personal photos, paste this link in your browser: goo.gl/xymYpP

Colorado Springs all smiles after receiving the Chapter of the Year award.

From L to R: Glenn York, June Shores, Scott Frisch (VP), Anna Johnston, Frank Gearhart, Tiffany McCullough (guest of Frank), Shawn Murray, and Kurt Danis.
By Scott Simkin, SecurityWeek, October 23, 2017

As an industry, we’ve evolved to address the challenges that today’s cyberthreat landscape presents, with both tactics and technology. We’ve not yet surmounted the challenges, but there are innovative minds in garages and boardrooms across the country trying to do just that. In the meantime, there are fundamentals that have stood the test of time and can help prevent successful cyber breaches from occurring despite the pace at which the landscape shifts.

To help ensure a solid foundation of protection from cyberattacks, I offer you The Ten Cybersecurity Commandments – the most important and fundamental practices to help ensure successful cyberattacks are avoided, business productivity is left undisrupted, and customers continue to place their trust in your brand.

1. **Ensure that systems, applications and users are patched.** The importance of applying the latest security patches cannot be overstated. Attackers will always attempt the easiest route to break into an organization, which is often an unpatched system. As for employees, make sure ongoing user training is implemented, and ensure that strong password policies are in place, along with multi-factor authentication requirements.

2. **Share preventions natively.** The best chance of preventing cyberattacks and defeating adversaries is when effective security controls on the network, endpoint and cloud operate together as parts of a single platform. This means security teams won’t have to manage and orchestrate separate policies, enforcement, visibility and threat intelligence. Each element can gain leverage from the other so that what’s discovered on the endpoint, for instance, can automatically be prevented on the network and in the cloud, without manual intervention.

3. **Implement a consistent security model, regardless of user location or device type.** When there is consistency of prevention across all locations, attackers lack the ability to gain an initial foothold in a less protected area and pivot to other parts of the organization. Whether it is a remote user or system, the core data center or perimeter, a cloud-based service or a SaaS-based application, you must ensure there are no gaps in security posture. Consider extending the perimeter to remote users and networks in the same way that you would if they were on the core network.

4. **Practice the principle of least privilege.** Segmentation is a requirement, and micro-segmentation is fast becoming one. No one or no one thing needs to talk to everything. There should be no default trust for any entity, regardless of what it is or where it is. By establishing Zero Trust boundaries that compartmentalize different segments of the network, organizations can protect data from unauthorized apps or users, reduce the exposure of vulnerable systems, and prevent the lateral movement of malware throughout the network.

5. **Embrace advanced endpoint methodologies.** Ensure that endpoint protection can share threat intelligence seamlessly across the network and endpoint, and prevent known and unknown malware on the endpoint itself. Endpoint technology should be able to identify and prevent exploits without any prior knowledge; otherwise, it can’t effectively protect your organization.

6. **Make safe application enablement a requirement.** Security teams must be able to determine the exact identity of applications traversing the network, irrespective of port, protocol, evasive tactic or encryption (TLS/SSL or SSH), and apply safe application enablement policies based on business needs.

7. **Gain leverage from threat intelligence.** Controls and preventions are only as good as their visibility into known and unknown threats, and their ability to instrument security infrastructure that blocks what’s discovered. If your security technology is constantly learning, whether through discreet observables like new malware samples or machine learning, it should have a wide enough data set to know what is good, and what is bad, and tie all of that back across network, endpoint and cloud to implement new prevention measures.

Read the rest here: http://www.securityweek.com/ten-cybersecurity-commandments
By AFP, Help Net Security, October 3, 2017

US officials are studying ways to end the use of social security numbers for identification following a series of data breaches compromising the data for millions of Americans, a Trump administration official said Tuesday.

Rob Joyce, the White House cybersecurity coordinator, told a forum at the Washington Post that officials were studying ways to use "modern cryptographic identifiers" to replace social security numbers.

Joyce's comments come after news that some 145 million Americans may have had personal information leaked, including the important social security numbers, in a breach at Equifax, one of three big US firms which collect data for credit applications.

"I feel very strongly that the social security number has outlived its usefulness," Joyce said.

"It's a flawed system."

For years, social security numbers have been used by Americans to open bank accounts or establish their identity when applying for credit. But stolen social security numbers can be used by criminals to open bogus accounts or for other types of identity theft.

"If you think about it, every time we use the social security number we put it at risk," Joyce said.

"That is the identifier that connects you to all sort of credit and digital and information online."

He said the administration has asked officials from several agencies to come up with ideas for "a better system" which may involve cryptography.

This may involved "a public and private key" including "something that could be revoked if it has been compromised," Joyce added.

The official spoke as US lawmakers opened hearings on the Equifax breach, believed to be one of the worst because of the sensitivity of data leaked.

Read the rest here: http://www.securityweek.com/us-reviewing-better-tech-identifiers-after-hacks-trump-aide

---

**Training News**

Want to gain knowledge on something new? Want to brush up, get a refresher, on something you may already know? Want to earn a few continuing education units (e.g. CPE/CEUs)? Join us at our next ISSA Colorado Springs mini-seminar! Join the discussion and share your knowledge, thoughts, and perspectives.

Our topics include:

- Sherwood Applied Business Security Architecture (SABSA) Certification (the real McCoy), presented by Kurt Danis
- Insider Threat, presented by Debi Caldwell

Details:

- Date: Saturday, 11 November 2017
- Location: College America, 2020 N. Academy Blvd., Colorado Springs, CO 80909
- Time: 9am to noon
- Cost: FREE to ISSA members, guests, and non-ISSA members

Registration:


This is a great training opportunity for those wanting to broaden their knowledge or need CPE/CEUs to maintain their existing certifications. It’s also a great opportunity to share your knowledge and experience with other members of our Chapter, and gain experience as a speaker, by volunteering to be one of our presenters.

If you have any questions, contact our Training Committee leads at: Training@ISSA-COS.org.
Apple gave Uber's app 'unprecedented' access to sensitive Apple features that can record iPhone screens

By Kif Leswing, Business Insider, October 5, 2017

Uber's iPhone app has a secret back door to powerful Apple features, allowing the ride-hailing service to potentially record a user's screen and access other personal information without their knowledge.

This access to special iPhone functions — which are so powerful that Apple almost always keeps them off-limits to outside companies — is not disclosed in any consumer-facing information included with Uber's app.

Although there is no evidence that Uber used its access to take advantage of the iPhone features, the revelation that the app has access to privileged Apple code raises important questions for a company already under investigation for other controversial business practices.

Uber told Business Insider the code was not being used and was essentially a vestige of an earlier version of its Apple Watch app.

However, it has set off alarm bells among experts.

"Granting such a sensitive entitlement to a third party is unprecedented, as far as I can tell — no other app developers have been able to convince Apple to grant them entitlements they've needed to let their apps utilize certain privileged system functionality," Will Strafach, a security researcher who discovered the situation, told Business Insider.

Nearly every iPhone app uses what is called an "entitlement" — basically, a way for software to enable features like the camera or Apple Pay on iPhones and iPads. Most of these can be easily found and turned on by outside app developers.

But there are certain entitlements used only by Apple, giving the company's software tight integration with the iPhone. These bits have names that start with "com.apple.private," and they are considered so sensitive that any third-party app found using them is rejected from the App Store.

After digging around in the code of Uber's app, Strafach discovered it used an entitlement called "com.apple.private.allow-explicit-graphics-priority."

"It is very odd to see Uber as the only app (I checked tens of thousands of other apps using my company's internal data set derived from the App Store) besides Apple's own apps granted access to this sensitive entitlement," Strafach said in an email. Another person said that out of the top 200 free apps, no other used private Apple entitlements.

Uber says Apple gave it permission to use the private entitlement and that it used it for an earlier version of its Apple Watch app to render maps on the iPhone. The entitlement is not currently being used, Uber says.

"Apple gave us this permission because early versions of Apple Watch were unable to adequately handle the level of map rendering in the Uber app," an Uber representative, Melanie Ensign, told Business Insider. "Subsequent updates to Apple Watch and our app removed this dependency, and we're working with Apple to remove the API completely."

Lots of other iOS developers would like special access to private Apple entitlements for both legitimate and illegitimate.

Read the rest here: http://www.businessinsider.com/uber-iphone-app-secret-access-sensitive-apple-features-2017-10

Update Your Profile!
Don’t forget to periodically logon to www.issa.org and update your personal information.
Russian Hackers Stole NSA Tools From Contractor Who Used Kaspersky Software

By Ken Dilanian, NBC News, October 5, 2017

Russian government hackers stole highly sensitive U.S. spying tools after a contractor brought classified material home and put it on a computer that used Kaspersky antivirus software, a former senior intelligence official briefed on the matter told NBC News.

The details were first reported Thursday by The Wall Street Journal.

The contractor, whose name has not been made public, worked for the National Security Agency, which specializes in hacking computers and eavesdropping on communications.

The Journal said the stolen material included secret details about how the NSA penetrates foreign computer networks, the computer code it uses for such spying and how it defends networks inside the U.S.

The report also said it was unclear whether the contractor had lost his job or is facing prosecution. He is not believed to have wittingly cooperated with a foreign government.

The man took his work home in violation of NSA rules, and Russian hackers were able to identify the material and access his machine because he was using Kaspersky software, the former official said.

The case explains why the U.S. government has cracked down on Kaspersky in recent months, banning its use by government agencies, he added.

Kaspersky is an anti-virus company owned by Eugene Kaspersky, who has long been accused by U.S. officials of having ties with Russian intelligence officials. But until recently, the company's products were widely for sale in the U.S. and used by some federal agencies.

The loss of secrets is "extremely damaging," the former official said, because it offers Russia great insights into how the NSA steals data. It will make the NSA's job harder.

"Not only is the work of the NSA and CIA increasingly visible, there is a certain aggression implied by this," he said. "It's a 'game-on' moment."

Kaspersky, he said, should be treated as a hostile actor.

Kaspersky said in a statement to NBC News that it could neither confirm nor deny the incident.

"Kaspersky Lab has not been provided any evidence substantiating the company's involvement in the alleged incident," the statement said. "It is unfortunate that news coverage of unproven claims continues to perpetuate accusations about the company. As a private company, Kaspersky Lab does not have inappropriate ties to any government, including Russia, and the only conclusion seems to be that Kaspersky Lab is caught in the middle of a geopolitical fight."

Another NSA contractor, Harold Martin, has been charged with taking home classified material without permission. He had pleaded not guilty, and he is not the person implicated in this case, the former official said.

A third contractor, Edward Snowden, famously removed reams of classified information NSA facilities and leaked it to the news media. But Snowden for the most part did not reveal spying tools, so the current case could in some ways prove more damaging.

Sen. Ben Sasse, R-Neb., a member of the Armed Services Committee, said the NSA "needs to get its head out of the sand and solve its contractor problem. Russia is a clear adversary in cyberspace and we can't afford these self-inflicted injuries."

An NSA spokesman declined to comment. An agency official who asked not to be named said the NSA is committed to improving its internal security.

Read the rest here:
and
Stop Trying to Fix the User

By Bruce Schneier, IEEE Security and Privacy, Undated

Every few years, a researcher replicates a security study by littering USB sticks around an organization’s grounds and waiting to see how many people pick them up and plug them in, causing the autorun function to install innocuous malware on their computers. These studies are great for making security professionals feel superior. The researchers get to demonstrate their security expertise and use the results as “teachable moments” for others. “If only everyone was more security aware and had more security training,” they say, “the Internet would be a much safer place.”

Enough of that. The problem isn’t the users: it’s that we’ve designed our computer systems’ security so badly that we demand the user do all of these counterintuitive things. Why can’t users choose easy-to-remember passwords? Why can’t they click on links in emails with wild abandon? Why can’t they plug a USB stick into a computer without facing a myriad of viruses? Why are we trying to fix the user instead of solving the underlying security problem?

Traditionally, we’ve thought about security and usability as a tradeoff: a more secure system is less functional and more annoying, and a more capable, flexible, and powerful system is less secure. This “either/or” thinking results in systems that are neither usable nor secure.

Our industry is littered with examples. First: security warnings. Despite researchers’ good intentions, these warnings just inure people to them. I’ve read dozens of studies about how to get people to pay attention to security warnings. We can tweak their wording, highlight them in red, and jiggle them on the screen, but nothing works because users know the warnings are invariably meaningless. They don’t see “the certificate has expired; are you sure you want to go to this webpage?” They see “I’m an annoying message preventing you from reading a webpage. Click here to get rid of me.”

Next: passwords. It makes no sense to force users to generate passwords for websites they only log in to once or twice a year. Users realize this: they store those passwords in their browsers, or they never even bother trying to remember them, using the “I forgot my password” link as a way to bypass the system completely-effectively falling back on the security of their email account.

And finally: phishing links. Users are free to click around the Web until they encounter a link to a phishing website. Then everyone wants to know how to train the user not to click on suspicious links. But you can’t train users not to click on links when you’ve spent the past two decades teaching them that links are there to be clicked.

We must stop trying to fix the user to achieve security. We’ll never get there, and research toward those goals just obscures the real problems. Usable security doesn’t mean “getting people to do what we want.” It means creating security that works, given (or despite) what people do. It means security solutions that deliver on users’ security goals without—as the 19th-century Dutch cryptographer Auguste Kerckhoffs aptly put it—“stress of mind, or knowledge of a long series of rules.”

Read the rest here:
http://ieeexplore.ieee.org/document/7676198/authors

Cautionary Tale: Job Search

By “A Reader”

In my current job search, I received a call from someone who identified herself as a recruiter. She described a SWEET senior cybersecurity position that required a clearance and not far from the house, making for a nice, short commute.

After the typical recruiter screening questions, she said that she needed my SSN and DPOB to pass to her security officer in order to confirm my clearance.

Always skeptical, I told her that I didn’t give that information out to recruiters, but if she gave me her company’s DSS CAGE Code, I could give the security officer a call and pass this information directly to them. She seemed confused by the terms DSS and CAGE Code as well as not having her security officer’s name or number.

After telling her to give me a call as soon as she gets that information, I hung up and dialed the number that popped up on my phone. Yep! The number was not in service and a web search did not turn up the company. So, I just wanted to let others know that they need to keep their guards up while job hunting and sometimes, the too-good-to-be-true job opening is just that, too good to be true.
Ensuring the Cybersecurity of Manufacturing Systems

By Timothy Zimmerman, NIST, October 6, 2017

Cybersecurity, at this point in the technological age, has become a household word. Every week, almost like clockwork, it seems there is a story on the news about a newly discovered hack or data breach often made possible by poor cybersecurity practices. Many of these incidents are focused around stolen data, which resides in our IT, or information technology, infrastructure. However, the breaches that interest me are those that affect the systems and devices that monitor and manipulate much of the world around us and have real-world health and safety consequences if they are compromised. These extremely important systems and devices are known as operational technologies, or OT.

Typically hidden in plain sight, OT controls many of the processes we rely on every day, including traffic signals, power distribution, hydroelectric dams, water treatment, building HVAC, oil and gas distribution, nuclear power plants, and many varieties of manufacturing. Again, the most important characteristic of OT is their ability to reach out from the digital world and manipulate the physical world where we humans reside. It’s not difficult to imagine some of the disasters that could occur if these critical OT processes were to be compromised because of poor cybersecurity practices.

So, how do these systems manipulate the physical world? At the most basic level, they’re not much different from my coffee maker, whose proper function I rely on for my proper function every morning.

Inside the coffee maker there is a tiny computer, a series of valves and heating elements that work together to create, in my opinion, the most delicious and invigorating elixir the world has ever known. If the computer failed to manage the coffee-making process, the consequences can vary from simple disappointment, e.g., no coffee because the water was never heated, to catastrophic, e.g., the heating element stayed on all day, caught fire and burned down my house. The same is true for more elaborate OT systems, like manufacturing machines and robots, which can include thousands of sensors and actuators.

So, what’s the problem with securing these devices? Well, not so long ago, OT systems were built using proprietary hardware and software and their operational details were not well known. Today, however, OT leverages many of the same technologies that were originally created for IT, e.g., networking, the internet, operating systems, user management, USB ports and web servers. Because of this shared technology, it’s easy to assume that any type of cybersecurity technology could be implemented to protect OT, but this is not the case.

For example, cybersecurity devices that filter unauthorized network traffic on an IT network could cripple an OT network simply by preventing important data from reaching its destination, and, in some cases, can cause failures just by delaying data. Software used to scan a network for vulnerabilities may send unfamiliar messages to OT devices and can cause them to fail, which is especially bad if the device is actively controlling a process. Even something as simple as antivirus software can have a detrimental impact on the performance of these critical systems and may be impossible to implement altogether.

This is where our research begins. In our laboratory testbed, we install, integrate and test these cybersecurity technologies on emulated manufacturing systems. We have all the parts and pieces to reproduce manufacturing systems in the lab, including identical industrial controllers, network hardware, human-machine interfaces and even robots. The main difference between our testbed OT and the real manufacturing processes are the additional measurement devices we use to evaluate their operational characteristics.

Standards and guidelines detailing best practices for protecting IT and OT have already been produced by industry, trade groups and government agencies. However, one thing they are missing is guidance that describes how to balance those protections with potential negative impacts they may have on performance. To fill this gap, my group is working to produce guidelines, test methods, metrics and tools based on measurement science and standards to give industry the confidence it needs to effectively apply cybersecurity protections on their systems without negatively affecting their performance, safety or reliability. Our work has already resulted in a manufacturing profile for the Cybersecurity Framework, which outlines a risk-based approach to help manufacturers implement, manage and improve their cybersecurity posture using industry standards and best practices. And to put the manufacturing profile to the test, we will be using it to protect our robotic and process control testbed under many different configurations and scenarios while measuring the performance impacts to the system.

Read the rest here:
Finding a good candidate, or possibly any candidate, to fill one of the thousands of open cybersecurity positions available is one of the greatest challenges facing security executives today.

So with that in mind, SC asked some of the top names in the industry what traits they look for in a job applicant.

1. **Continuous Learner**

Shamla Naidoo, Chief Information Security Officer, IBM

The cybersecurity landscape is evolving continuously and rapidly, and therefore the most important quality I look for in a security hire is someone who can do the same – someone with natural curiosity that will lead to continual learning. The security workforce needs people who will be a part of inventing the solutions that will keep us safe not only today but in the future. For me, it’s about hiring someone who has intellectual depth but is willing to learn from others, without ego – not just experience to perform the role. I look for demonstrable willingness to learn new things and think outside of the box, with specific examples of where they’ve done this successfully in the past.

2. **Persistence**

Reg Harnish, CEO of GreyCastle Security

“The most important quality I look for when hiring new talent is persistence. Are they determined? Do they have the gumption to do the job right? In the cybersecurity world, the problems people face are not only ever-changing, but also very difficult to start with, so persistence is key. Additionally, a certain level of persistence requires confidence, which is a must in this industry, as security consultants have to deal with the full gamut of employees, from CEOs and board-level executives to end users. There’s no time to second guess yourself.”

3. **Curious and Perceptive**

Renee Walrath, Founder of Walrath Recruiting

“To work in cybersecurity, curiosity is an absolutely essential trait. Anyone who gets comfortable in fighting off threats in the same fashion, will quickly be outdated, and subject to breaches. To be successful you have to be curious, and seek out new weaknesses before they become weaknesses. A cybersecurity professional needs to be a continuous learner to stay one step ahead of external threats. Proactively learning and updating systems is the only way to stay ahead.”

Perceptive: “A good cybersecurity professional needs to see problems from both sides. They have to be in the mindset of the company, thinking of what they want to protect. They also have to look through the lens of an external threat, and perceive any weaknesses or places to attack. Having both perspectives will make it easier to build a strategy to defend against an external threats.”

4. **Cerebral, Instinctive and Emotional**

Chris Drake, CEO Armor

The dynamic nature of cyber security dictates that a person will need to wear a variety of hats and excel in diverse areas to be successful. While tangible skills like these are critical, there are several intangible characteristics that can serve as the foundation for rising above the crowd, including:

Cerebral – intelligence, process and reason

Instinctive – innate desire, awareness, quick thinking

Emotional – heart, passion, sense of duty, pride, morality, justice

It doesn't stop there, however. Working in cyber security is different from other sectors of IT. There is a tremendous amount of collaboration across various disciplines, which requires qualities that might not be as significant in other IT roles. This includes attributes such as creativity, confidence, focus, reliability and humility. Interestingly, we’ve found that those with musical talent have an innate ability to synchronize these skills and emerge as a solid security expert.

Read the rest here: https://www.scmagazine.com/top-10-most-desired-traits-for-cybersecurity-job-candidates/article/689345/?email_hash=55969B59507ACF1E1E61F3F49338E185&spMailingID=18220123&spUserID=MzY5Njg0MDc2NTU0S0&spJobID=1120220895&spReportId=MTEyMDIyMDg5NQS2
ISSA Nametags

Do you want an ISSA nametag for your very own to wear to meetings, conferences, and events? You can now order/pick up yours directly from:

*Blue Ribbon Trophies & Awards*

245 E Taylor St (behind Johnny’s Navajo Hogan on North Nevada)

Colorado Springs

(719) 260-9911

Although their hours are officially Monday through Friday until 5:30 pm, they are occasionally in the shop on Saturdays. This is a small business so cash/check would be appreciated. Email wbusovsky@aol.com to order.

CISSP Study Guide Discount

Ashley Edwards, Senior Account Manager, Wiley
aedwards@wiley.com


50% off for ISSA chapters

Promo code CSP50

Items of Interest

**GET A JOB!**

Colorado Springs ISSA chapter member Melody Wilson maintains a “Jobs” page at Cyberjoblist.com. There is no charge. The jobs are set to remain listed for 30 days. Job listing originators re-post them again for another 30 days. It is designed for Colorado Springs, but once in awhile a job is listed outside the area.

You can also sign-up on the Cyberjoblist.com site for Job Alerts to be notified when a new job listing is posted!
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...

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: doncreamert@email.com

Ensure that “Newsletter” is in the subject line.

Looking forward to seeing you in print!

The Improbable Origins of PowerPoint

By David C. Brock, IEEE Spectrum, October 31, 2017

Walking into the hall to deliver the speech was a “daunting experience,” the speaker later recalled, but “we had projectors and all sorts of technology to help us make the case.” The technology in question was PowerPoint, the presentation software produced by Microsoft. The speaker was Colin Powell, then the U.S. Secretary of State.

Read the rest here: https://spectrum.ieee.org/tech-history/cyberspace/the-improbable-origins-of-powerpoint