Happy Holidays!

Colleagues,

The end of the year is rapidly approaching, which means its election time. Several Board of Director positions are up for election this year, so watch for the ballot and cast your vote as soon as possible. Learn more about who’s running by reading information on the candidates in this newsletter.

Our December “Annual Awards” luncheon is on Thursday, 7 December, at the Marriott Hotel (5580 Tech Center Dr). Registrations are in progress, so be sure to sign up quickly. This luncheon is a closed event, for members only, and not visible or searchable on Eventbrite.

Deadline to RSVP is 7 pm Sunday, December 3.

Registration and meal choice information was distributed to chapter members via email on November 18th. If you did not receive this email (or don’t have it anymore), and want to register to attend, please contact Elizabeth at communications@issa-cos.org.

As we come to the end of 2017, I want to thank you all for your continued engagement and support of the 2017 Chapter of the Year!!!

Hope to see you at the Luncheon.

Happy Holidays!

Colleen

A Note From Our President

By Ms. Colleen Murphy

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.
Amazon Key Flaw Could Let Rogue Deliverymen Disable Your Camera

By Andy Greenberg, Wired, November 16, 2017

When Amazon launched its Amazon Key service last month, it also offered a remedy for anyone—realistically, most people—who might be creeped out that the service gives random strangers unfettered access to your home. That security antidote? An internet-enabled camera called Cloud Cam, designed to sit opposite your door and reassuringly record every Amazon Key delivery.

But now security researchers have demonstrated that with a simple program run from any computer in Wi-Fi range, that camera can be not only disabled but frozen. A viewer watching its live or recorded stream sees only a closed door, even as their actual door is opened and someone slips inside. That attack would potentially enable rogue delivery people to stealthily steal from Amazon customers, or otherwise invade their inner sanctum.

And while the threat of a camera-hacking courier seems an unlikely way for your house to be burgled, the researchers argue it potentially strips away a key safeguard in Amazon’s security system. When WIRED brought the research to Amazon’s attention, the company responded that it plans to send out an automatic software update to address the issue later this week.

“The camera is very much something Amazon is relying on in pitching the security of this as a safe solution,” says Ben Caudill, the founder of the Seattle-based security firm Rhino Security Labs, whose researchers discovered and demonstrated the Amazon Key attack. “Disabling that camera on command is a pretty powerful capability when you’re talking about environments where you’re relying heavily on that being a critical safety mechanism.”

The Rhino Labs proof-of-concept attack on Amazon Key is relatively simple. In their demonstration, shown in the video above, a delivery person unlocks the door with their Amazon Key app, opens the door, drops off a package, and then closes the door behind them. Normally, they’d then lock the door with their app. In this attack, they instead run a program on their laptop—or, Rhino’s researchers suggest, on a simple handheld device anyone could build using a Raspberry Pi minicomputer and an antenna—that sends a series of “deauthorization” commands to the home’s Cloud Cam.

That so-called deauth technique isn’t exactly a software bug in Cloud Cam. It’s an issue for practically all Wi-Fi devices, one that allows anyone to spoof a command from a Wi-Fi router that temporarily kicks a device off the network. In this case, Rhino’s script sends the command again and again, to keep the camera offline as long as the script is running. Most disturbingly, Amazon’s camera doesn’t respond to that attack by going dark or alerting the user that the camera is offline. Instead, it continues to show any live viewer—or anyone watching back a recording—the last frame the camera saw when it was connected.

That means the deauth command sent by the delivery-person-turned-hacker standing just outside your door can freeze the camera on the image of a closed door, while he then waltzes in a second time and closes the door behind them. Once inside, the intruder can simply move beyond the view of the Cloud Cam, stop sending the deauth command to allow the camera to reconnect, and hit the lock button on their app. Neither the lock’s logs nor the video record would appear amiss to the Amazon Key user, even as a stranger runs amok inside their house.

“As a partially trusted Amazon delivery person, you can compromise the security of anyone’s house you have temporary access to without any logs or entries that would be unusual or suspicious,” Caudill says.

“We currently notify customers if the camera is offline for an extended period,” Amazon said in a statement. “Later this week we will deploy an update to more quickly provide notifications if the camera goes offline during delivery.”

Read the rest here: https://www.wired.com/story/amazon-key-flaw-let-deliverymen-disable-your-camera/
Overall it’s been another quiet month on the membership front. We’re at ~500 members as of the end of November. Elections have started and will be completed in early December in time to announce the new board members at the ISSA-COS Annual Recognition Lunch on December 7th. If you haven’t signed up for that please do so as soon as possible. As you may have noticed our membership numbers have dropped over the last several months. This was not unexpected due to the large influx of Freemium Student members we added during the pilot program. Now that the Free Student membership has been formalized, we anticipated a drop in numbers.

The chapter will be migrating to a new email provider soon. I don’t want to steal the new IT Committee’s thunder so I’ll let them discuss the changes in detail. From a membership communication standpoint, it will be critical that we have current, accessible email addresses for all our members. Please take a couple of minutes to review your profile on your ISSA International account. Ensure all your information is current and up to date, especially your contact information. Confirm 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. 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.

Finally, 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.

Thanks,

David Reed
Membership Committee Chairman
dreed54321@comcast.net
Should the United Nations to take a stronger role on Internet governance?

*Should the Internet be monitored by an international agency?*

Chapter Review by Kurt Danis, ISSA-COS, November 15, 2017

Chapter 9 from a book titled: *Strategy -- Context and Adaptation from Archidamus to Airpower*, 2016, multiple authors

In Chapter 9, "Four Dimensions to the Digital Debate" by Air Force Col. Richard Bailey (now retired), the author writes about different social tensions. One of the social tensions Bailey writes about is "Liberty and Order". With a historical backdrop he writes, "In 1958, President Dwight Eisenhower secured funding for a new research wing for the Pentagon, and the Advanced Research Project Agency (ARPA) was born. Originally, the agency's mission was to advance the understanding of nuclear and ballistic-missile technology, but it was a side project of an engineer named Licklider that made ARPA famous. His vision of sharing computer power in an open forum led to partnering with university research centers and planted the seeds for the modern Internet. But these early developers were much more hopeful about what sharing information could bring than fearful of any harm that could from a misuse of the technology. In fact, most cyberspace historians posit that the early pioneers were so enamored with the idea of a rapidly evolving marketplace of ideas (the liberty of thought and the freedom to share those thoughts) that they paid very little attention to the propensity for nefarious activity."

Fast forward to our time frame in the context of cybercrime and debates about cyberwar, the author goes on to say, China and Russia have vocalized recommendations through the United Nations to take a stronger role in Internet governance. Yet, this is contrary to freedom-loving Western democracies --- "...many nations will eschew [deliberately avoid using] strong central control over cyberspace, even at the risk of a higher level of vulnerability."

CONCLUSION: Some opponents cite Posse Comitatus to arrest notions of an over-reaching federal government. For this reason, there still is no federated government policy endorsed by stakeholders such as the FCC, Dept of Commerce, Dept of Energy, DoD, DHS, NSA, the banking industry, or the critical infrastructure owners of our nation. The author (Bailey), concludes his "Liberty and Order" piece by saying no matter how the governance piece turns out, it will likely be result in some type of screening or monitoring in cyberspace.

Update Your Profile!

Don’t forget to periodically logon to [www.issa.org](http://www.issa.org) and update your personal information.
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.

Mentorship Committee Update

Thank you to all who have participated in the Mentorship Program this past year! The next meeting will be the Mentors meeting in January 2018.

Mission Statement

Provide curious mentees at any stage of their information security career lifecycle with access to mentors who share their knowledge and experience in ensuring the confidentiality, integrity, and availability of information resources throughout a variety of industries.

Overview

The ISSA-COS Mentorship Program is designed to be mentee driven. Mentees determine the number of mentors they meet with depending on their questions, needs, and availability. The goal is to provide mentees with quality mentoring opportunities in a professional and problem solving environment. There will be group meetings twice a year (April & October) for all mentors and mentees to meet, greet, and discuss information security. Individual meetings between mentees and mentors will be scheduled throughout the year determined by the mentee and mentor. Mentees and mentors are expected to prepare for individual meetings by writing down questions and discussion topics prior to the meeting. e-Mentoring is also an option for those who need remote options. Mentors will meet as a group twice a year (January & June) to collaborate and share resources. Small group meetings to discuss specific topics and field trips to companies and organizations will be scheduled ad hoc.

Why Mentor?

Give back to the security community by sharing your knowledge and experience, provide career insight to mentees, grow your network.

Why be a Mentee?

Gain access to knowledge and experience in different security areas and industries.

Enrollment Process

- Be an ISSA Member
- Complete the Mentorship Enrollment Form
- Submit form with your resume to a Mentorship Committee Chair
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 Anna Johnston, and I am running for Communications Director. I am a transplant to Colorado having spent close to 20 years in the MD/VA/DC area working for NSA spending most of my time in the Information Assurance Directorate. I currently am a government contractor continuing to support the mission. Shortly after joining ISSA-COS, I volunteered to be the Deputy of Communication supporting the incumbent and also volunteered to assist in the Transformation Committee tasked to transform our IT and communication processes and mechanisms. With my involvement in these areas supporting ISSA-COS, I believe I have the experience necessary to bring new ideas, procedures, and processes to how we communicate within and outside of our growing organization. Specifically, I am looking at how we can leverage new technologies to convey to you upcoming calendar events and seek ways to stream-line the current communication processes that are in place today. Thank you.

Hello, I’m Mark Maluschka, and I am running for ISSA – COS Treasurer for several reasons. First, I would like to give back to the chapter. I also want to continue the good work of previous treasurers while also looking for opportunities to add more value to the chapter. I am a relatively new member of ISSA – COS having joined in April 2016, but since joining have attended numerous offerings by ISSA – COS, have participated in the ISSA – COS mentoring program, and am currently an active member of the Transformation Committee. I work for Wells Fargo as an Operational Risk Consultant in the Technology Risk Management group. The group evaluates at all risks to technology, security, process, availability, etc., and makes recommendations for improvement. I have previously worked as an accountant / financial analyst responsible for monthly financial statements for privately held healthcare management companies. In this position I managed the team which produced the monthly compensation (checks) for over a thousand health care providers. I have a Bachelors of Arts in Economics, a MBA and information security certifications. I will keep the chapter’s best interest at the forefront and would appreciate the opportunity to serve. Thank you.

My name is Dave Reed, and I am running for re-election as your Vice President of Membership. My goals for the next two years are twofold: 1. Solidify our last two years’ significant membership growth—stabilize the membership and continue to grow. 2. Maintain the Chapter’s focus on our chapter members’ needs and providing useful opportunities for professional growth.

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.

DoD boosting use of secret tablets

By Amber Corrin, C4ISRNet, November 7, 2017

The Defense Information Systems Agency is expanding a pilot program introduced earlier this year, offering wider availability of classified tablets across the Department of Defense.

What started initially as 25 tablet devices fielded to senior military leadership now will be made available beginning in February, according to Jacob Marcellus, DISA mobility portfolio manager.

“That pilot was so successful … I’m getting probably about 25 emails a week asking for these devices,” Marcellus said Nov. 6 at the annual DISA Forecast to Industry, held in Washington.

The classified tablet pilot, known as DoD Mobility Classified Capability-Secret, or DMCC-S, is part of the broader Commercial Solutions for Classified program run by the National Security Agency. It’s also just part of DISA plans for expanding commercial mobility across DoD. DISA oversees a significant slice of mobility management for the military, running DoD’s largest mobility management program with more than 100,000 users, Marcellus said.

Read the rest here:
ISC² certification progression for last 10 years

By Kurt Danis, Dep. Director of Certifications, ISSA-COS, November 28, 2017

The following numbers represent the top 10 active certifications world-wide offered by the International Information Systems Security Certification Consortium, Inc. (ISC)² as of October 16, 2017.

- 120,149 CISSP® Certified Information Systems Security Professional
- 3,736 SSCP® Systems Security Certified Practitioner
- 2,443 CAP® Certified Authorization Professional
- 2,427 CCSP® Certified Cloud Security Professional
- 2,082 CSSLP® Certified Secure Software Lifecycle Professional
- 1,939 ISSAP® Information Systems Security Architecture Professional
- 1,170 ISSMP® Information Systems Security Management Professional
- 1,116 ISSEP® Information Systems Security Engineering Professional
- 1,008 HCISPP® HealthCare Information Security and Privacy Practitioner
- 143 CCFP-US® Certified Cyber Forensics Professional (US)

For (ISC)², certs must earn their keep; or, deactivation is possible. In fact, the CCFP-US, first introduced in 2013 (p. 6, InfoSecurity Professional, Issue Number 22, 2013), will become an “inactive credential” on August 21, 2020. Growth rate was about 1% after 2 years. The credential will remain a recognized (ISC)² certification until that date.

On a positive note, the CCSP also introduced in 2013 continues to grow rapidly. In November 2015, the CCSP multiplied over 21 times to a total 2,427 (as shown above). The CCSP was built on existing certifications; namely, the CISSP and Cloud Security Alliance’s Certificate of Cloud Security Knowledge (CCSK). Chances are good the CCSP will surpass the CAP and SSCP in coming years.

Let’s talk about the “Gold Standard”. As of last month, the US is off the chart with 78,341 CISSPs. Secondly, there should be no surprise the English speaking world is led prominently by the US, the UK, and Canada for CISSPs. And thirdly, CISSP people come from 166 countries. Some of the top countries outside the US are shown in the red progression bar chart.

With respect for our profession, CISSP metrics demonstrate there is a remarkable growth of cybersecurity professionals in nearly every country.

Current ISC2 certification metrics retrieved on 28 Nov 2017 from: https://goo.gl/FepCS4
Top Ten—Differences Between RMF and CSF

By P. Devon Schall, CISSP, RDRP, Risk Management Framework Today...and Tomorrow, October 2017

I was reading an article recently about Cybersecurity Framework (CSF) and the continued confusion with Risk Management Framework (RMF). In the research, the consensus was the majority of government IT professionals don’t fully understand CSF or RMF and find it easy to confuse the two. As a follow up to my previous CSF article, I hope the top 10 list below can continue to clear up the differences in the frameworks.

10. RMF automated tools do not support CSF. Numerous tools have been developed (such as DoD eMASS) to streamline RMF process workflow. There are no known plans for any of these tools to provide CSF support.

9. RMF is much more prescriptive than CSF. RMF’s audience is the entire federal government and CSF was initially developed for critical infrastructure. CSF has also been recommended for use in organizations regardless of size, degree of cybersecurity risk, or cybersecurity sophistication including industry. Bottom line: RMF has a very prescriptive process including formal Authorization to Operate (ATO) whereas CSF is still in initial stages of implementation with recommended voluntary usage.

8. RMF is much more extensively documented than CSF. The document outlining CSF titled “The Framework for Improving Critical Infrastructure” is 41 pages. “The Guide for Applying the Risk Management Framework to Federal Information Systems” is 102 pages and is supported by numerous NIST Special Publications (SPs). It is very easy to start reading RMF documentation and get “stuck in the weeds”. One of my favorite aspects of CSF is approachable documentation.

7. CSF is aimed at private industry. The National Institute of Standards and Technology (NIST) encourages CSF use in private industry, particularly those supporting “critical infrastructure” (e.g., transportation, public utilities). A great example can be seen in the Intel Corp. case study “An Intel Use case for the Cybersecurity Framework in Action”. RMF is aimed primarily at government and is only rarely used in the private sector.

6. The steps in the RMF and CSF process are different. The RMF process has six steps. These steps are: Categorize, Select, Implement, Assess, Authorize, and Monitor. The CSF process has seven-steps. CSF steps are: Prioritize and Scope, Orient, Create a Current Profile, Conduct a Risk Assessment, Create a Target Profile, Determine, Analyze, and Prioritize Gaps, and Implement Action Plan.

5. RMF controls can be used with CSF, but CSF does not have its own set of security controls. CSF maps to a variety of functions titled: Identify, Protect, Detect, Respond, and Recovery. Each of these functions ties to categories that can be satisfied via a variety of controls families such as COBIT 5, NIST SP 800-53, and ISO/IEC 27001.

4. CSF does not have Authorizing Officials (AOs) or an Authority to Operate (ATO). RMF involves ATOs with determined authorization periods requiring approval by an Authorizing Official (AO). In contrast, CSF is a voluntary framework intended to strengthen cybersecurity posture. CSF does not have an AO function or finite ATO’s.

3. RMF generally requires the participation of a variety of government entities. For example, Joe Contractor cannot go through the complete RMF process alone. The involvement of government officials is required in achieving an ATO. CSF can be implemented without government assistance.

2. NIST has recommended that CSF be used to strengthen RMF. Elements of CSF can be used to make RMF more robust. Personally, I don’t know who has the time to make RMF more complicated than it is, but with unlimited time to implement cybersecurity frameworks anything is possible.

1. CSF is not intended to replace RMF. CSF is NOT a “rip and replace” of RMF. The sweat and tears we have gone through in learning RMF are not in vain. NIST has suggested we may see some CSF language in new releases of NIST SPs, but overall the goals of the two frameworks are very different.

Source: October, 2017 Volume 7, Issue 4, Risk Management Framework Today... and Tomorrow. RMF Today... and Tomorrow was republished by permission, and is a publication of BAI Information Security, Fairlawn, Virginia. Phone: 1-800-RMF-1903, Email: rmf@rmf.org
More than two years after historic breach, OPM continues to struggle with cybersecurity

By Chris Bing, CyberScoop, November 6, 2017

The Office of Personnel Management continues to struggle with cybersecurity more than two years after the agency first publicly acknowledged they were breached due to poor security practices, according to a newly released Office of the Inspector General report.

The report, which focuses on the state of systems during fiscal year 2017, concludes that while OPM has “made improvements in its Security Assessment and Authorization (Authorization) program,” inspectors were nonetheless able to find a “significant deficiency in OPM’s information security management structure.”

This translated to a poor overall cybersecurity score, as defined by the National Institute of Standards and Technology, of two out of five for OPM. The score from the OIG is supposed to define the “maturity” level of an organization in relation to the security of information systems.

This lackluster rating is due in large part to inaction by the agency regarding prior security recommendations referenced in other audits.

“OPM is not making substantial progress in implementing our FISMA recommendations from prior audits,” the report reads. “While resource limitations certainly impact the effectiveness of OPM’s cybersecurity program, the staff currently in place is not fulfilling its responsibilities that are outlined in OPM policies and required by FISMA.”

A piece of legislation known as the Federal Information Security Modernization Act, or FISMA, which was enacted into law during the Obama administration in 2014, requires inspector general offices to conduct annual information security assessments within multiple federal agencies.

The OIG-OPM report disclosed Monday is a result of FISMA being implemented.

Although OPM has reportedly made improvements in several recognized issue areas, including for example with the agencies’ increased ability to quickly remEDIATE cyberattacks due to a more competent incident response process, it “continues to struggle” in other domains. The OIG took note — repeatedly — of what they precisely described as a longstanding lack of “contingency planning” and a failure to enforce continuous monitoring program policies.

OPM failed to test contingency plans that it had devised — like those used in emergency situations, data breaches and unpredictable system failures — across a number of different divisions; representing a continuation of past problems, the report identified.

According to the OIG, the lack of such testing could one day be catastrophic.

Read the rest here:
Cybersecurity pros targeted in latest attack by Group 74

By Doug Olenik, SC Magazine, October 23, 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.

The threat actor known as Group 74 has initiated a new campaign that uses a malicious Visual Basic for Applications (VBA) macro embedded in a document advertising the Cyber Conflict U.S. Conference (CYCON) to target people interested in cybersecurity issues.

The VBA injects and then executes a new variant of the reconnaissance malware Seduploader, which Group 74 is known to use, Cisco Talos reported. Group 74 is part of the same organization that also goes by aka Tsar Team, Sophacy, APT28 and Fancy Bear. The lure is an attached two-page Word document with the filename Conference_on_Cyber_Conflict that for added effect also contains the logo of the organizer and sponsor.

Making this a particularly powerful piece of seduction is that CYCON is a legitimate conference being held Nov. 7-8, 2017 at the Ronald Reagan Building in Washington D.C. that is assembled by the U.S. Military Academy and the NATO Cooperative Cyber Defence Centre of Excellence. The document's content is nothing more than text cut and pasted from the conference’s website.

Cisco Talos noted the document was created on October 4 and a spike in activity happened three days later.

“Analysis of this campaign shows us once more that attackers are creative and use the news to compromise the targets. This campaign has most likely been created to allow the targeting of people linked to or interested by cybersecurity, so probably the people who are more sensitive to cybersecurity threats,” Cisco Talos wrote.

In the past Group 74 used Seduploader to drop privilege escalation malware, but this attack only contains the persistence mechanism contained in two files, netwf.bat which executes the payload netwf.dll.

Once installed Sedupload can capture screenshots, act as a data/configuration exfiltration device, execute code and download files.

Read the rest here:

How to Change Your MAC Address in Windows 10 (and Why You Might Want To)

By Andre Da Costa, GroovyPost, November 8, 2017

As we’ve explained in our article on how to find your MAC address, a MAC address serves as a permanent, physical identifier for any device that connects to a network. That includes your phone, your router, your computer, your printer, your Apple TV, anything that connects to your internet. If your computer has an Ethernet port and a WiFi adapter, you have two MAC addresses: one for Ethernet and one for wireless.

MAC addresses are useful for identifying devices on a network. For home users, you might use MAC filtering to restrict access to your WiFi network. The reason that a MAC address works better for these administrative tasks is that, unlike IP addresses, the MAC address doesn’t change.

Or at least it’s not supposed to.

The MAC address is “burned-in” to the physical device at the factory. But it’s fairly simple to change your MAC address by “spoofing” it as another MAC address.

Why would you want to do this?

MAC spoofing can be used maliciously to circumvent network controls, but it’s really only effective for blacklists—that is, if someone specifically blocked your device from the network. For whitelists, you’d have to know the MAC address of a specific device you’re trying to spoof.

Changing your MAC address has legitimate uses as well. You can use it to test your own MAC filtering settings. Or you can use it to assign specific rules to a set of devices within a certain MAC address range.

At any rate, the fact that you’ve read this far means you probably have a vested interest in changing your MAC address. So, without further ado, here’s how to do it.

Edit Your Network Adapters MAC Address to Bypass Network Restrictions in Windows 10

Press Windows key + X on your keyboard then click Device Manager. Expand Network adapters, right-click your Ethernet or Wireless adapter then click Properties.

Select the Advanced tab. Within the Property box, scroll down then select Locally Administered Address then select the Value radio box; there you will see your adapters MAC address. To edit the address, click in the value box then clear its contents then enter a new address. A Mac address consists of six pairs of hexadecimal digits. Enter a new set without the hyphens, click OK then restart your computer.

Read the rest here for additional details left out of the above:
Massive US military social media spying archive left wide open in AWS S3 buckets

By Iain Thomson, The Register, November 17, 2017

Three misconfigured AWS S3 buckets have been discovered wide open on the public internet containing "dozens of terabytes" of social media posts and similar pages – all scraped from around the world by the US military to identify and profile persons of interest.

The archives were found by UpGuard’s veteran security-breach hunter Chris Vickery during a routine scan of open Amazon-hosted data silos, and the trio weren't exactly hidden. The buckets were named centcom-backup, centcom-archive, and pacom-archive.

CENTCOM is the common abbreviation for the US Central Command, which controls the army, navy, air force, marines and special ops in the Middle East, north Africa and central Asia. PACOM is the name for US Pacific Command, covering the rest of southern Asia, China and Australasia.

Vickery told The Register today he stumbled upon them by accident while running a scan for the word "COM" in publicly accessible S3 buckets. After refining his search, the CENTCOM archive popped up, and at first he thought it was related to Chinese multinational Tencent, but quickly realized it was a US military archive of astounding size.

"For the research I downloaded 400GB of samples but there were many terabytes of data up there," he said. "It's mainly compressed text files that can expand out by a factor of ten so there's dozens and dozens of terabytes out there and that's a conservative estimate."

Just one of the buckets contained 1.8 billion social media posts automatically fetched over the past eight years up to today. It mainly contains postings made in central Asia, however Vickery noted that some of the material is taken from comments made by American citizens.

The databases also reveal some interesting clues as to what this information is being used for. Documents make reference to the fact that the archive was collected as part of the US government's Outpost program, which is a social media monitoring and influencing campaign designed to target overseas youths and steer them away from terrorism.

Vickery found the Outpost development configuration files in the archive, as well as Apache Lucene indexes of keywords designed to be used with the open-source search engine Elasticsearch. Another file refers to Coral, which may well be a reference to the US military's Coral Reef data-mining program.

"Coral Reef is a way to analyze a major data source to provide the analyst the ability to mine significant amounts of data and provide suggestive associations between individuals to build out that social network," Mark Kitz, technical director for the Army Distributed Common Ground System – Army, told the Armed Forces Communications and Electronics Association magazine Signal back in 2012.

"Previously, we would mine through those intelligence reports or whatever data would be available, and that would be very manual-intensive."

Before you start scrabbling for your tinfoil hats, the army hasn’t made a secret of Coral Reef, even broadcasting the awards the software has won. And social media monitoring isn’t anything new, either.

However, it is disturbing quite how easily this material was to find, how poorly configured it was, and that the archives weren’t even given innocuous names. If America's enemies – or to be honest, anyone at all – are looking for intelligence, these buckets were a free source of information to mine.

After years of security cockups like this in the public and private sectors, Amazon has tried to help its customers avoid configuring their S3 buckets as publicly accessible stores, by adding full folder encryption, yellow warning lights when buckets aren't locked down, and tighter access controls.

"This was found before these new Amazon controls were added," Vickery said. "So we have yet to see how effective that yellow button will be."

Read the rest here:
https://www.theregister.co.uk/2017/11/17/us_military_spying_archive_exposed/
Curing The Security Sickness in Medical Devices

By Jalal Bouhdada, Security Week, November 22, 2017

Just as the rapid development of the Internet of Things (IoT) has transformed traditional industries and service sectors, it is also having a great impact in the world of healthcare. It’s easy to argue, in fact, that no area is being transformed by digital technologies as rapidly or with as many benefits for society as new medical technologies.

But the understandable desire to press ahead and unlock those benefits has led to a lack of scrutiny on the subject of digital security in devices for treatment and monitoring, and a spate of high profile problems in the area has begun to concern many. In the US, the Food and Drug Agency (FDA) has issued formal warnings about cybersecurity vulnerabilities in four separate products in the last 18 months. It has also hosted an array of consultations and workshops focussing on the cybersecurity of medical devices. The most recent product notice from the FDA, regarding an exploitable flaw in connected cardiac pacemakers, seems to be finally wakening the industry up to the threats that connected technologies bring.

Fortunately, there are solutions which can allow healthcare innovation to continue unimpeded, and plenty of lessons that can be learned from experiences in other areas. The rulebook for minimizing the risk of unauthorised access, and limiting potential damage in the event of a device being compromised, is broadly the same as protecting other connected and operational technologies: better collaboration, lifecycle management, network monitoring and a “secure by design” ethos to new products.

What we don’t have is time: securing medical devices is a life and death issue, and most in the field fear that a new major attack is imminent. Vendors, practitioners and security experts must all work closely together to combat the well-funded actors who pose a threat.

Connected healthcare

The benefits of connected medical devices are unquestionable, with much progress being made in terms of treatments and cures. For example, we’ve already seen low cost blood sugar monitoring implants that can synchronize with a smartphone to help diabetics manage their condition. Networked X-ray and ultrasound machines that can deliver instant images to a practitioner’s desktop are also speeding up diagnosis and treatments in emergency rooms from Seattle to Singapore.

The problem is as medical devices have become increasingly connected, they have also become exposed to an array of potential security flaws. This connectivity and the benefits it has bestowed upon us, such as remote monitoring and data gathering and analysis, has brought with it new risks.

The most obvious is that of a direct attack on a medical device over the internet, but even restricting access to a hospital’s network, for example, doesn’t guarantee safety. When devices are connected to hospital networks they also become potentially vulnerable to indirect attacks.

When the WannaCry ransomware shut down large sections of the UK National Health Service’s IT systems earlier this year, it was aiming to disrupt services in order to achieve ransom payments on behalf of its creators. While not directly targeting medical devices, this does highlight the possibility that a future attack on hospital IT systems could use compromised desktops to infect the connected medical devices being relied upon to keep us alive.

The reverse scenario, in which a poorly secured medical device acts as a gateway to IT infrastructure and patient records, is no less troubling.

The diagnosis

Healthcare providers should be well aware of these dangers as security experts have been warning of them for many years. At the very least, medical device manufacturers need to be conscious of the legislative work around the world that is aimed at enforcing better protection of networks and systems. Close reading of new data privacy and breach disclosure laws will help encourage good practice, and in the US the FDA has strict requirements around public safety and is acutely aware of the issues, as demonstrated by the recent pacemaker recall.

To help meet these compliance obligations and secure the safety of patients, the security industry and medical device manufacturers must develop closer relationships, ensuring that new devices are manufactured with best-practice defences baked in.

The ability to identify and react to new and emerging threats in a timely manner is tough, but not insurmountable through proper collaboration. There are many lessons that have been learned from other sectors and industries that can be applied to the emerging threat landscape in healthcare.

For new devices, mitigating the risk to both the business of medical provision and the quality of patient care begins with a solid framework for managing devices and applications. This is achieved using a secure by design concept in which medical devices go through a Secure Systems Development Lifecycle (Secure SDLC) program.

Read the rest here: http://www.securityweek.com/curing-security-sickness-medical-devices
How the US decides which security flaws to keep secret

By Alfred Ng, C|Net, November 15, 2017

When the US government discovers a new security flaw, it faces an important question: Who should we tell about this?

The White House released its Vulnerabilities Equities Policy on Wednesday, detailing the process it follows to make that decision along with ten agencies, including the CIA, NSA and Homeland Security. It explains why some vulnerabilities are kept secret, while warnings are immediately issued for others.

These decisions are specifically regarding zero-day vulnerabilities, previously unknown security flaws that haven't yet been patched. Government agencies often find these vulnerabilities and sometimes turn them into their own hacking weapons. After the WannaCry ransomware spread thanks to a stolen NSA hacking tool, Microsoft's chief counsel criticized the government for keeping vulnerabilities a secret from companies that can patch them.

White House Cybersecurity Coordinator Rob Joyce said in a blog post Wednesday that it's critical to improve transparency of the process but he defended the government's decisions to keep certain vulnerabilities a secret.

"Although I don't believe withholding all vulnerabilities for operations is a responsible position, we see many nations choose it," Joyce said.

The process starts with finding the vulnerability and submitting it to the VEP's review board, which includes members of the following agencies:

- Department of Defense (including the NSA)
- CIA
- Department of Justice (Including the FBI)
- Department of State
- Department of Homeland Security
- Office of Director of National Intelligence
- Department of Treasury
- Department of Energy
- Department of Commerce
- Office of Management and Budget

The board then discusses four main points, starting with how much of a threat the newly discovered vulnerability is. It looks at how widespread the affected product is, how easy the vulnerability is to take advantage of, how much damage it could cause and how easily it could be fixed.

The second consideration is how the government could potentially use the vulnerability for its own purposes. The third and fourth talking points consider what risks the US would face with companies and other countries if it's revealed that the government knew about the vulnerability all along.

This review happens within five days. The process is sped up if there're already attacks going on using the vulnerability. After the discussions, the board reaches a consensus on whether or not to disclose the vulnerability to companies affected.

If the review board votes to disclose the vulnerability, it's responsible for informing affected companies within seven business days. If it chooses to keep the vulnerability a secret, it's reviewed annually by the board until the group changes it mind, or the zero-day becomes public knowledge.

Read the rest here:
Security efforts to bridge the talent gap mean little when workers don't want to stay in the industry.

By Kelly Sheridan, Dark Reading, November 7, 2017

We hear a lot about security's struggle to acquire talent but little about its inability to retain employees. The skill shortage is doomed to worsen if security can't improve tenure.

Earlier this year, Dr. Andrea Little Limbago, chief social scientist at Endgame, polled 300 security professionals to learn about their perspective on retention. Three-quarters had been in the industry for at least five years; 35% for over 11 years.

People normally describe the talent gap as a pipeline problem: the issue is getting people in the door. This is a "positive challenge" for the industry, she says. It has driven a strong focus on improving university security programs and introducing security into K-12 classes.

"It feels so much better to inspire kids to go into cybersecurity, but what's harder is looking at the industry itself and the all the parts that might need fixing," Limbago explains. All of these efforts are negated when industry norms force talented employees out the door.

**Burnout**

Survey results indicate burnout, industry culture, and ill-defined career paths are three key reasons people leave cybersecurity. Limbago says she was expecting the first two. Burnout is commonly mentioned at conferences and from friends in the industry, she notes.

Survey questions asked why respondents had left previous roles, and burnout and stress were common. When she followed up, Limbago learned businesses weren't taking them seriously, despite reports employees were working long hours and weekends without taking time off. More than 70% of respondents report working 41-60 hours each week; 10% work over 60.

"They felt their leadership, or their company, interpreted [burnout] as not being committed to their job, as opposed to taking it seriously as a problem," she explains. "It's something where organizations need to focus."

While stress was common, only one-third of respondents felt they were professionally challenged, followed by 28% who were somewhat challenged. Security can be stimulating but many tasks are redundant and don't leave time for critical thinking and technical skills.

"There's so much in processes that is so mundane to do hours and hours on end, day after day, especially things that could be automated by now," says Limbago. "You could see how that leads to burnout."

**Industry Culture**

The cultural aspect is a key challenge for both attracting and retaining talent. Nearly all (85% of) non-male respondents had experienced some level of discrimination at professional conferences, and more than half had experienced harassment at those events, Limbago found.

On a corporate environment level, the numbers are lower but still bleak. Nearly 60% of non-male respondents had experienced discrimination at their company, and 44% had experienced harassment within their company or a company events.

Limbago, who has experience working in academia and national security, which also has few women, says she didn't notice the gender dynamics as much as she has in security. While she reports a great community at her own company, she says oftentimes the conference environment can be "dispiriting."

"Little things here and there, you get used to overlooking and ignoring [them], but over the years it builds up a lot," she says. "Company culture becomes so much more important," she adds, and eventually internal corporate culture can affect conference culture as well.

**Ill-Defined Career Path**

Read the rest here:
https://www.darkreading.com/careers-and-people/burnout-culture-drive-security-talent-out-the-door/d/d-id/1330352?elq_mid=81388&elq_cid=22752161&mc=NL_DR_EDT_DR_daily_20171108&cid=NL_DR_EDT_DR_daily_20171108&elqTrackId=0a51442e4c444f89b7bc7ca7371bd222&elq=127ef1de96324ae4a639ed1e7721305d&elqaid=81388&elqat=1&elqCampaignId=28652
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 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
CISSP (ISC)2 Certified Information Systems Security Professional
50% off for ISSA chapters
Promo code CSP50

Items of Interest
ISSA Photos are courtesy of our Chapter Photographer Warren Pearce.

Additional photographs are available on the ISSA-COS.ORG website
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 cyber community.

Send your article ideas to Don Creamer at: doncreamer@outlook.com
Ensure that “Newsletter” is in the subject line.
Looking forward to seeing you in print!

Somebody wrote an email bot to waste scammers' time

By Mark Frauenfelder, BoingBoing, November 8, 2017

I love this. When you get a scam email, forward it to me@rescam.org and a bot will keep the scammer busy emailing back and forth with it, giving the scammer less time to rob gullible humans.

Introducing Re:scam – an artificially intelligent email bot made to reply to scam emails. Re:scam wastes scammers time with a never-ending series of questions and anecdotes so that scammers have less time to pursue real people.

Read the rest here:
https://boingboing.net/2017/11/08/somebody-wrote-an-email-bot-to.html