Colorado Springs Chapter ISSA Information Systems Security Association
WWW.ISSA-COS.ORG

ISSA-COS NEWSLETTER

VOLUME 8 NUMBER 3 MARCH 2019

Colorado Springs, Colorado

Spring is Coming

ISSA-COS Members,

Welcome to March…shamrocks, corn beef & cabbage, and lots of college basketball! But the best part of all…the **2019 Cyber Focus Day** conference co-hosted by ISSA-COS and the Federal Business Council (FBC)! The theme for this year's conference is "**Cybersecurity for all Industries**" and to support that theme, we are opening the doors to all industries within Colorado Springs. The venue is set, the agenda is set, the registration website is set, and most of the guest speakers are also set. There are still plenty of sponsor opportunities so, if you or someone you know is interested, let us know and we will get you registered. Sponsorship even comes with a booth to advertise your company or organization. For your convenience, an updated agenda is included elsewhere in this month's newsletter.

This month, we are also heavily promoting the expansion of our Special Interest Groups (SIGs). These groups will launch during the Cyber Focus Day conference and will include a focus on the following Affinity and Industry groups:

Affinity Groups

- Women in Security
- Mentoring in Security
- Young Professionals in Security
- Executives in Security

Industry Groups

- Healthcare in Security
- Finance in Security
- Retail in Security
- DoD in Security

Participants at the CFD conference will have an opportunity to participate in one Affinity group and one Industry group. When you attend a group, be sure to add your name to the SIG member list so you can receive emails regarding future events for the groups you join.

Also being promoted this month is the ***2019 Best of ISSA-COS*** article submission. Members are encouraged to practice their research and writing skills and submit a personally written article from one of the following 18 Cybersecurity-

(Continued on page 5)

A Note From Our President

By Mr. Ernest Campos

Ong's Hat: The Early Internet Conspiracy Game That Got Too Real

By Jed Oelbaul, Gizmodo, February 21, 2019

On a sunny morning in early 2000, Joseph Matheny woke up to find conspiracy theorists camped out on his lawn again. He was making coffee when he noticed a face peering in a ground-floor window of the small, three-story building he rented in Santa Cruz. Past the peeper, there were three other men in their early 20s loitering awkwardly. Matheny sighed and stepped outside. He already knew what they wanted. They wanted to know the truth about Ong's Hat. They wanted the secret to interdimensional travel.

They were not looking for trouble, just information, and he was able to get them to leave with some cryptic comments and a quick lecture on personal boundaries. But Matheny, a mobile game developer who said he spent the 1990s working for some of tech's biggest names had been on edge since about a year earlier, when he had to march an unruly intruder off the property at gunpoint, after an attempted break-in. According to Matheny, he and his girlfriend at the time had been receiving threatening phone calls and emails. Someone was anonymously contacting his employers claiming Matheny was dangerous, a liability. After more than a decade of secrets, the chickens were coming home to roost. The Ong's Hat experiment had grown out of his control.

"But even as the Ashram made great strides with its unorthodox work, danger was brewing."

Ong's Hat is one of the internet's earliest conspiracy theories, but before that, it was a place, a ruin almost 3,000 miles away from Santa Cruz, deep in the woods of New Jersey's Pine Barrens. Rumors swirled for years that something profound had once happened there, a confluence of mad science and the paranormal that had warped reality itself, opening a door into strange, unfathomable worlds.

Covering more than 1 million acres of largely unspoiled primordial forest, the Pine Barrens feel impossibly dense and vast, a wild and lonely place where sandy trails wind past mysterious lichen and rare flora, like the gnarly pygmy pitch pine. Once home to shipbuilding, coal mining, and bog iron trades, the area's industries declined over a century ago, and the Pinelands are now dotted with the remains of abandoned towns and rotting factories.

Often referred to as a ghost town, it's not clear how much of a town Ong's Hat ever was. Local lore tacks the unusual name to Jacob Ong, a 17th-century settler who, legend has it, angrily threw his hat into a tree after a lover's quarrel. Some Ong-family descendants say the name was once "Ong's Hut," and it was only ever one or two buildings. Henry Charlton Beck, who depicted historical Ong's Hat as a rowdy, boozy outpost in his 1936 book, *Forgotten Towns of Southern New Jersey*, later recanted his descriptions, saying he'd fallen for "elaborate traps" set by locals to mislead him about the town's past. Whatever it once was, Ong's Hat has since been completely swallowed by the forest, though the name stubbornly pops up on maps and lives on in the nearby Ong's Hat Road.

None of that is why there was a crew of nosy young men on Matheny's lawn that day in 2000, or why Ong's Hat has become a site of pilgrimage for fans of the supernatural. There's another legend and it goes, briefly, like this: According to a pamphlet that began popping up in late '80s—"Ong's Hat: Gateway to the Dimensions, a Full-Color Brochure for the Institute of Chaos Studies and Moorish Science Ashram"—Ong's Hat was once home to secret experiments led by the Dobbs Twins, a pair of Princeton scientists who'd been forced to build a secret lab out in the Pine Barrens after their work in "Chaos Studies" got them booted from the academy. Nearby, a mystic scholar and carpet salesman named Wali Fard had established the ragtag Moorish Science Ashram, and over time the scientists and spiritual seekers met and began to merge their pursuits, blending meditation, physics, alchemy, and metaphysical disciplines like remote viewing in never-before-seen ways

Read the rest here:

https://gizmodo.com/ongs-hat-the-early-internet-conspiracy-game-that-got-t-1832229488

Membership Update

I just spent a day in Denver at the Data Connectors Cybersecurity Conference. I was pleasantly surprised that our Colorado Springs ISSA Chapter's activities are very well recognized by the Denver cybersecurity community for both the types and quality of our events. I was particularly surprised by the recognition of non-ISSA members. It really is all about our great volunteers who put in so much effort to make our events successful.

New Members January & February
Lowell Mann Jr.
Adam Price
Nathaniel Button
Terrance Daniels
Mathew Stiles
Stephen Parish
Marc Sanchez
Brian Jones
Harlan Shoop
Sean Zebrowski
Jorden Smith
Stephen Treanor
Joshua Haddock
Mark Morris
Samuel Johnson
Brenda Stephens

Welcome to 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.

Watch for all the upcoming activities. Our new President, Ernest Campos, is implementing lots of new opportunities for the chapter. Please watch the Newsletter, communications and eVites to ensure you stay aware of what's going on in the chapter. As always, if you have any membership questions don't hesitate to contact me.

Our membership remains at ~473 members as of the end of February. Kudos to all the members who've referred 70% of our new members so far this year. As you're going about your daily activities, please continue to take the time to engage your colleagues, ask if they're ISSA members, and if not take a couple of minutes to convince them of the value of becoming a member of our chapter. Word of mouth is our primary method of advertising. If you don't take the time to tell people of our organization, folks won't know all the advantages we bring to their professional life. Renewals are also critical to maintaining our membership. If you are considering not renewing, please talk to me or one of the other board members to help us understand what we can do better to support our membership and retain you as an active chapter member.

Thanks,

David Reed

Membership Committee Chairman

membership@issa-cos.org

New Chapter By-Laws have been posted on the ISSA-COS website and may be found here:

https://issa-cos.org/wp-content/uploads/2018/12/Colorado-Springs-ISSA-ByLaws-FINAL-Dec-2018.pdf

OFFICIAL INVITATION

RATED TOP 50 INFOSEC CONFERENCE WORLDWIDE

CYBER SECURITY SUMMIT
DENVER 2019

TUESDAY, APRIL 2 | 7:45AM - 6:00PM | HILTON DENVER CITY CENTER

Denver, CO ISSA

EXCLUSIVE INVITE

COMPLIMENTARY ADMISSION
WITH PROMO CODE:
ISSA19BOARD

Standard Admission is $350, Now Free With Code.
This Pass is for C-Suite / Sr. Level Executives and Directors / Managers only and includes a Catered Breakfast, Lunch & Cocktail Reception.

SALES/MARKETING PROFESSIONALS AND STUDENTS / PROFESSORS NOT PERMITTED.

REGISTER NOW AT CYBERSUMMITUSA.COM

THOUGHT LEADERS: LEARN FROM EXPERTS & ADVISORS (PARTIAL LIST)

Ike Barnes
Asst. to Special Agent in Charge, Electronic Crimes Task Force
US Secret Service, Denver

Ryan Spelman
Senior Director
Center for Internet Security

Aaron Janssen
Sr. Sales Engineer
Malwarebytes

Gavin Matthews
Product Manager
Automox

Tory Smith
Special Agent
The FBI

TECH SHOWCASE: EVALUATE THE LATEST SOLUTIONS FROM (PARTIAL LIST)

ARCTIC WOLF · ARMOR · AUTOMOX · Bitdefender · CISCO · CODE42 · DARKTRACE · DELL · ERICOM

ExtraHop · LOGPOINT · Malwarebytes · ORACLE · Pulse Secure · SailPoint · SECURONIX · TEVORA

INSIGHT: INTERACTIVE PANELS & DISCUSSIONS

- Morning Security Briefing with the U.S. Secret Service
- Darktrace Presentation: Autonomous Cyber Defense: AI and the Immune System Approach
- Insider Threat: What the CISO and Every IT Security Management Team Must Face & Govern 24/7
- ExtraHop Presentation: Next Generation SOC
- Afternoon Security Briefing with the FBI
- Cloud INsecurity: Common Pitfalls that Organizations Make when Moving to the Cloud and How to Avoid Them
- Incident Response: What to do Before, During and After a Breach

CONTACT MHUTTON@CYBERSUMMITUSA.COM FOR SPEAKER / EXHIBITOR OPPORTUNITIES.

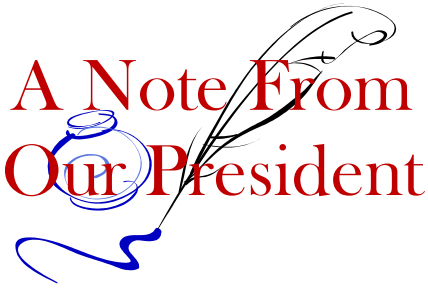
6 CPE CREDITS Executives in full day attendance will receive 6 CPE credits following the Summit.

(Continued from page 1)

related fields. Not an expert writer? No problem. The Best of ISSA-COS is for all talents and the chapter will take the time to review your work before it is published in September for the Peak Cyber conference. Deadline for submissions is August 16, 2019 but, don't delay. Get your articles in early!

Cybersecurity-related Fields

- Network and Infrastructure Security
- Web Security
- Endpoint Security
- Application Security
- Managed Security Service Providers
- Data Security
- Mobile Security
- Risk and Compliance
- Identity and Access Management
- Security Operations and Incident Response
- Threat Intelligence
- Internet of Things (IoT)
- Messaging Security
- Digital Rights Management
- Security Consulting
- Blockchain
- Fraud and Transaction Security
- Cloud Security



Next, let's take some time to recognize our new sponsors. ISSA-COS recently secured a new **Platinum Sponsor – Murray Security Services (MSS)**. MSS is not only providing financial support to our chapter, they are also donating numerous training scholarships for both the CFD and Peak Cyber conferences. These scholarships are redeemable for industry certification training provided by MSS. The scholarships will be distributed during the conferences and are also transferrable! For more information about MSS, follow the link to the MSS website via our own website (www.issa-cos.org).

Next, we are recognizing a new category of sponsor – an Aero Sponsor. Aero Sponsors are individuals, companies, and organizations who provide financial donations to our chapter to help offset the annual membership fees for members in need. Last month, ISSA-COS secured our first **Aero Sponsor – CT Cubed**. CT Cubed donated financial support for two members of our chapter. The support will be discretely awarded to the recipients and CT Cubed will continue to be recognized or their generosity throughout the 2019 calendar year. For more information about CT Cubed, follow the link to the CT Cubed website via our own website (www.issa-cos.org).

Last of all, I'd like to recognize a special member of our chapter who was recently nominated for a very prestigious community award. **Ms. Amy Coffman** has been nominated to receive the Athena Award presented by our local Colorado Springs Chamber and Economic Development Counsel. The Athena Award celebrates outstanding businesswomen who inspire others through their business accomplishments, mentorship of others and community service. Amy fulfills all these attributes and is a strong supporter and member of our own ISSA-COS chapter. The winner of Athena Award will be announced during a luncheon held on April 4th at the Antlers Hotel. For more information and to register to attend, search for "2019 Athena Award Colorado Springs". Please consider attending this event to help support Amy and to congratulate her for being recognized.

In closing, the Board of Directors hopes you will attend the CFD on March 28th. We look forward to seeing you, meeting, you, and talking with you. Encourage your friends and colleagues to attend the conference and to consider joining our chapter. The year is still young and there are lots of events on our calendar for the rest of the year.

Respectfully,

Ernest Campos

Meet the Board Member

As members of the Colorado Springs Chapter of the ISSA you get to enjoy a great number of benefits such as Monthly Meetings, Mini Seminars, Conferences and networking with peers. As a not-for-profit organization these things can only be accomplished thanks to the volunteers who make them happen. In this new monthly feature, a member of the Board will be highlighted so you can get to know just a few of the hard working people who make the Chapter successful.

Since this is a new feature, I decided to introduce myself first so you know who is writing the article and give other Board members a "heads-up" I will be asking them for information in up coming editions of the newsletter. My name is Mike Crandall and I have the honor of being the Vice President of the Chapter as selected by our President Ernest Campos. I have been a member of ISSA since 2005 always in the Colorado Springs Chapter. I decided to join the Board to promote Cyber Security and support those in our community who are in this field. Having been a member for so long I felt it was not only my turn to take on the role but I was now in a place where I had the time to dedicate for that purpose.

I have been working in the Information Security arena for well over 20 years now. Starting in the early 90's when I was in the right place at the right time and fortunate enough to be on the team that was developing the DoD's first ever Defense in Depth network security concept called "Barrier Reef". Developed by five young Airmen in a basement we provided the building blocks of how the DoD implemented network security using De-Militarized Zones (DMZs), Firewalls, Proxies and network monitoring tools. Later, I was on the team that developed and implemented the first ever Network Operations and Security (NOSC) for the Air Force at Ramstein AB, Germany. Our concept was adopted and implemented at Langley and eventually across the Air Force at every Major Command.

My career took me to Schriever AFB, Colorado where I worked in Wing Information Assurance and responsible for the Air Force Satellite Control Network and associated networks that connected/utilized it. Retiring in 2010 I moved on to the civilian sector working for a large Government contractor until I started my own company Digital Beachhead in 2015.

As Vice President of the Chapter it is my goal to help bring our knowledge to the small business community who needs it. Over 70% of small businesses that are breached go out of business within one year. With the knowledge in our Chapter I hope we can provide the education and tools to help combat this in our community. I would like to expand our membership, find create ways to gain sponsorships to fund our programs and utilize our resources to not only benefit our members but our community. I look forward to the year ahead and am open to any/all members reaching out to me with ideas, suggestions and ways to improve our chapter. I can be reached at vp@issa-cos.org

Next month we will get to know our new President, Ernest Campos!

Mike Crandall

ISSA-COS Vice-President

Platinum Sponsor—Murray Security Services

Cyber Focus Day – Thursday, March 28, 2019
Location: UCCS, Berger Hall – FREE PARKING!

Times	Duration	Agenda	Sponsor/Speaker
0700 – 0800	60m	**Exhibit Hall Setup**	n/a
0800 – 0900	60m	**Attendee Arrival** Sign-in for Pre-registrants Registration for Walk-ins Initiate Meal Service (Continental Breakfast)	n/a
0900 – 0910	10m	**Call to Order** Attendees are Seated Meal Service Continues	**Ernest Campos**, ISSA-COS President
0910 – 0920	10m	**Opening Announcements** Recognition of Honorees Abbreviated Chapter Business Schedule of Events	**Ernest Campos**, ISSA-COS President
0920 – 0925	5m	**Introduction of Opening Keynote Speaker**	**Ernest Campos**, ISSA-COS President
0925 – 1010	45m	**Opening Keynote Speaker – Presentation (with Q&A)**	Sponsor: TBD Speaker: TBD
1010 – 1020	10m	**Break**	n/a
1020 – 1105	45m	**Training Speaker #1 – Presentation (with Q&A)**	Sponsor: **Global Knowledge** Speaker: **Bob Withers**
1105 – 1150	45m	**Training Speaker #2 – Presentation (with Q&A)**	Sponsor: TBD Speaker: TBD
1150 – 1200	10m	**Pre-lunch Announcements** Preview of afternoon sessions Instructions for dining options Return time	**Mike Crandall**, ISSA-COS Vice-President
1200 – 1300	60m	**Lunch Break**	n/a
1300 – 1345	45m	**SIGs – AFFINITY Style Groups** *(Attendees pick one)*	n/a
		Women in Security (WIS) – **W***[omen]***IS**	WIS Leader: **June Shores** Guest Speaker: **Lisa Gilbert**
		Young Professional in Security (YIS) – **Y***[oung Profession-als]***IS**	YIS Leader: **Jeremiah Walker** Guest Speaker: TBD
		Mentoring in Security (MIS) – **M***[entoring]***IS**	MIS Leader: **Carissa Nichols** Guest Speaker: TBD
		Executives in Security (EIS) – **E***[xecutives]***IS**	EIS Leader: TBD Guest Speaker: **Dr. Shawn Murray**
1345 – 1400	15m	**Break**	n/a
1400 – 1445	45m	**SIGs – INDUSTRY Style Groups** *(Attendees pick one)*	n/a
		Finance in Security (FIG) – **F***[inance]***IS**	FIS Leader: **Mark Maluscka** Guest Speaker: TBD
		Healthcare in Security (HIS) – **H***[ealthcare]***IS**	HIS Leader: **Dennis Schorn** Guest Speaker: TBD
		Retail in Security (RIS) – **R***[etail]***IS**	RIS Leader: TBD Guest Speaker: **Mr. Jack Callaghan**
		DoD in Security (DoDIS) – **D***[oD]***IS**	DoDIS Leader: **Steven Mulig** Guest Speaker: **Dr. Andy Heo**
1445 – 1500	15m	**Break**	n/a
1500 – 1545	45m	**Closing Keynote Speaker – Presentation (with Q&A)**	Sponsor: TBD Speaker: TBD
1545 – 1600	15m	**Closing Remarks** Final Recognition of Honorees Abbreviated Chapter Business Call to Close	**Ernest Campos**, ISSA-COS President

Once hailed as unhackable, blockchains are now getting hacked

By Mike Orcutt, Technology Review, February 19, 2019

Early last month, the security team at Coinbase noticed something strange going on in Ethereum Classic, one of the cryptocurrencies people can buy and sell using Coinbase's popular exchange platform. Its blockchain, the history of all its transactions, was under attack.

An attacker had somehow gained control of more than half of the network's computing power and was using it to rewrite the transaction history. That made it possible to spend the same cryptocurrency more than once—known as "double spends." The attacker was spotted pulling this off to the tune of $1.1 million. Coinbase claims that no currency was actually stolen from any of its accounts. But a second popular exchange, Gate.io, has admitted it wasn't so lucky, losing around $200,000 to the attacker (who, strangely, returned half of it days later).

Just a year ago, this nightmare scenario was mostly theoretical. But the so-called 51% attack against Ethereum Classic was just the latest in a series of recent attacks on blockchains that have heightened the stakes for the nascent industry.

In total, hackers have stolen nearly $2 billion worth of cryptocurrency since the beginning of 2017, mostly from exchanges, and that's just what has been revealed publicly. These are not just opportunistic lone attackers, either. Sophisticated cybercrime organizations are now doing it too: analytics firm Chainalysis recently said that just two groups, both of which are apparently still active, may have stolen a combined $1 billion from exchanges.

We shouldn't be surprised. Blockchains are particularly attractive to thieves because fraudulent transactions can't be reversed as they often can be in the traditional financial system. Besides that, we've long known that just as blockchains have unique security features, they have unique vulnerabilities. Marketing slogans and headlines that called the technology "unhackable" were dead wrong.

That's been understood, at least in theory, since Bitcoin emerged a decade ago. But in the past year, amidst a Cambrian explosion of new cryptocurrency projects, we've started to see what this means in practice—and what these inherent weaknesses could mean for the future of blockchains and digital assets.

How do you hack a blockchain?

Before we go any further, let's get a few terms straight.

A **blockchain** is a cryptographic database maintained by a network of computers, each of which stores a copy of the most up-to-date version. A blockchain **protocol** is a set of rules that dictate how the computers in the network, called **nodes**, should verify new transactions and add them to the database. The protocol employs cryptography, game theory, and economics to create incentives for the nodes to work toward securing the network instead of attacking it for personal gain. If set up correctly, this system can make it extremely difficult and expensive to add false transactions but relatively easy to verify valid ones.

That's what's made the technology so appealing to many industries, beginning with finance. Soon-to-launch services from big-name institutions like Fidelity Investments and Intercontinental Exchange, the owner of the New York Stock Exchange, will start to enmesh blockchains in the existing financial system. Even central banks are now looking into using them for new digital forms of national currency.

But the more complex a blockchain system is, the more ways there are to make mistakes while setting it up. Earlier this month, the company in charge of Zcash—a cryptocurrency that uses extremely complicated math to let users transact in private—revealed that it had secretly fixed a "subtle cryptographic flaw" accidentally baked into the protocol. An attacker could have exploited it to make unlimited counterfeit Zcash. Fortunately, no one seems to have actually done that.

The protocol isn't the only thing that has to be secure. To trade cryptocurrency on your own, or run a node, you have to run a software **client**, which can also contain vulnerabilities. In September, developers of Bitcoin's main client, called Bitcoin Core, had to scramble to fix a bug (also in secret) that could have let attackers mint more bitcoins than the system is supposed to allow.

Read the rest here:

https://www.technologyreview.com/s/612974/once-hailed-as-unhackable-blockchains-are-now-getting-hacked/

If you want a vision of the future, imagine not a boot stamping on a face, but keystroke logging on govt contractors' PCs

By Thomas Claburn, The Register, February 13, 2019

The potential for cyberwarfare between the United States and Russia is openly discussed, and – if not actually defined – is well understood. The British attitude is clear and defined, and the threat of retaliation – not necessarily cyber retaliation – is explicit.

Anyone working on a substantial contract with the US state of New Jersey could soon be required to install software that captures the screen and tracks keystrokes – to verify all hours billed are legit.

That's if proposed legislation – coincidentally shaped by a maker of work verification software – is approved.

What's more: New Jersey is not alone. These rules are being mulled in nearly two dozen states across America.

A draft law that just cleared the New Jersey State Assembly, NJ A3989, requires any contractor working on a New Jersey contract worth more than $100,000 "to use software to verify that all hours billed for work under the contract for services performed on a computer are eligible charges."

The text of the bill comes courtesy of TransparentBusiness, a New York-based firm that provides work tracking software. "TransparentBusiness gives state managers real-time information about the work performed for the state by programmers, architects, engineers, and other professionals, but does not intrude on their privacy," the company explains on its website.

And similar bills, many echoing the TransparentBusiness template, are being considered in at least 21 other states.

The mandated software – which is not vendor-specific – must provide the applicable state agency with real-time access to collected data. It must gather data automatically – by taking screenshots and capturing keystroke and mouse event frequency – and make the information available on demand to management and government.

It must provide automated real-time cost status for each task, along with a professional bio – not private or confidential info – of those doing the work. And it must provide the relevant agency with a feedback mechanism.

The system should "ensure appropriate privacy and confidentiality of any data for individuals." There's no specific security requirement.

The bill as presently written requires contractors to retain said data for seven years after payment from the state, and forbids them from passing along the cost of the verification software to the state. Its stated purpose is to prevent fraud.

A similarly worded bill was introduced last year in the Rhode Island State Legislature. It's currently being held in committee for further study.

Procurement

"We have indeed been evangelizing the benefits of transparency in government procurement," said TransparentBusiness CEO Alex Konanykhin in an email to *The Register*. "I have no doubt that transparent verification of billable hours will soon become the new standard of public and corporate procurement. (Blind management is so last century!)"

In addition to his role as boss of TransparentBusiness, Konanykhin is the chair of the board of KGMi Group, a holding company for a variety of other firms. Among these is Yandiki, another firm with an interest in worker data analysis.

"We support NJ A3989 as it can save New Jersey tens of millions of dollars at zero cost," Konanykhin said.

Politics in America

In addition to New Jersey and Rhode Island, similar bills have been introduced in Illinois, Minnesota, Missouri, and many other states. Konanykhin says he hopes to have like-minded bills introduced in every state. His firm has hired a lobbyist to push for a work verification law in Virginia.

Read the rest here:

https://www.theregister.co.uk/2019/02/13/work_verification_accountability_bills/

Training News

The Colorado Springs Chapter of ISSA is hosting a three day Security+ Exam Preparation Seminar

Those who have been studying and are close to sitting for the exam will gain the most out of this exam review seminar. This seminar will be covering the CompTIA SY0-501 exam criteria.

Already Security+ certified? Attending this review seminar will earn you 18 Continuing Education Units (CEU). You are welcome to attend just one day or all three days.

First priority seats will be to paying students not yet Security+ certified.

SY0-501 Domains Covered Include:

- Threats, Attacks and Vulnerabilities
- Technologies and Tools
- Architecture and Design
- Identity and Access Management
- Risk Management
- Cryptography and PKI

Location: Colorado Technical University (CTU), Room 113

4435 N. Chestnut St., Colorado Springs, CO 80907

Date: Saturday, April 6,13,& 20, 2019

Time: Both days: Check in between 8:15 AM – 8:40 AM

Class starts at 8:45 AM and runs to approximately 4:30 PM (*1/2 hour lunch.)* Lunch will be ½ an hour or 45 minutes. End time can vary, but no later than 5:00 PM.

*If extra instruction time is needed, lunch may be less than an hour and/or end time could run past 4:30 PM, no later than 5:00 PM.

Cost: $50.00 (includes all three days and refreshments)

Hope to see you there,

Please let us know if you have any questions.

Thank you very much,

Jeff Tomkiewicz, Deputy VP of Training

Susan Ross, Past Deputy VP of Training

Update Your Profile!

Don't forget to periodically logon to *www.issa.org* and update your personal information.

SPECIAL INTEREST GROUPS (SIGS)

Special Interest Groups (SIGs) are groups comprised of Cybersecurity professionals who gather together to share information and experiences common to their respective groups. ISSA-COS presents SIGs in two major categories: Affinity Groups and Industry Groups. On a quarterly basis, ISSA-COS brings together both groups to participate in formally structured events. During these gatherings, participants have an opportunity to first attend one of four (4) Affinity Groups then, one of four (4) Industry Groups. CPEs/CPUs are awarded for attend these events.

In-between formal gatherings, the SIG Leaders for each individual SIG are encouraged to coordinate informal gatherings. ISSA-COS encourages SIG leaders to consider hosting informal gatherings at social venues such as sporting events, restaurants, bars, or breweries. Informal gatherings may also include participating in a community improvement project, a group walk or hike, or a picnic/BBQ.

Affinity Groups

Affinity Groups are designed for community professionals with like-minded interests in the field of Cybersecurity. Affinity Groups gather to share security related experiences, impart knowledge and education, and help one another solve common problems and issues. The Affinity Groups currently promoted by ISSA-COS include:

Women in Security – **W***[omen]***IS**

Young Professional in Security – **Y***[oung Professionals]***IS**

Mentoring in Security – **M***[entoring]***IS**

Executives in Security – **E***[xecutives]***IS**

Industry Groups

Industry Groups are designed for community professionals who work within similar industries and have a common interest in Cybersecurity. Industry Groups gather together to discuss security related topics and share solutions to problems affecting their perspective industries. They also exchange Cybersecurity related tips, information, and education specific to their industries. The Industry Groups currently promoted by ISSA-COS include:

Finance in Security – **F***[inance]***IS**

Healthcare in Security – **H***[ealthcare]***IS**

Retail in Security – **R***[etail]***IS**

DoD in Security – **D***[oD]***IS**

ISSA-COS invites you to join us at our next SIG gathering or any one of our many other events.

For additional information, contact: info@issa-cos.org or visit **www.issa-cos.org**.

Google Fined €50 Million Over GDPR Violations

By Staff, SANS NewsBites, January 21, 2019

French data regulator CNIL has fined Google 50 million (US$ 57 million) for violations of the General Data Protection Regulation(GDPR). CNIL says that Google failed to make its data collection policies easily accessible and that it did not obtain sufficient, specific, consent for ad personalization across its services.

The ruling against Google focuses on making it hard for users to understand what data is being collected and sold, as well as the basic opt-out, if you can figure out how philosophy that causes users to automatically give away their data when enrolling in a service and is prohibited by GDPR. Users and not just regulators are giving real pushback against abuse of their privacy. While the GDPR fine represents less than 3 hours of Google revenue, Googles updated Code of Conduct commits the company to being measured against the highest possible standards of ethical business conduct. They came up short here and should change their conduct. [Honan] While the 50 million fine is the item grabbing the headlines, the key issue here is the finding by CNIL of the unlawfulness of Googles approach to gathering peoples personal data. This will have bigger implications for Google, and many other organizations, in how they ensure they legally gather and use peoples personal data in line with the GDPR.

This and future GDPR decisions could lead to two things. First, changes to privacy policies and settings from providers such as Google and Facebook to demystify their use of this data and second, a chance find out if the expert advice we followed to meet GDPR is accurate.

The Googles and Facebooks of the world will be fine, and they can afford to take on EU regulators. Its the blue team defenders I'm worried about, having to justify their every move to keep their own networks safe, having nothing to do with a business model that sells data about their users to third parties. Based on the denials and delays of legitimate security work due to privacy shops citing GDPR, either GDPR authors failed to make it clear that security logs for protecting the enterprise are good for privacy (breach = zero privacy after all), and/or the privacy community isn't getting that message. Cybersecurity folks cannot protect their networks and fix GDPR and the privacy community's (mis)understanding of GDPR.

Aero Sponsor
CT Cubed

The problem of certifications that don't measure practical skills

By Ken Clark, Certification Magazine, February 19, 2018

The confidence of being certified is wonderfully comforting! Certification is knowledge for the hiree, and proof for the hirer. Certification provides reasonable assurance that a prospective employee can talk the technical talk, and also walk the technical walk (so to speak).

Any certified worker wants to be capable of performing the role for which they've been hired, and that worker's employer most definitely wants the newcomer to be able to perform the role for which they've been hired. I once had an experience that sheds some light on this common circumstance.

Years ago, I was employed by a large organization, specifically in the capacity of what my employer referred to as an "enabler." My role was to function as an on-site, front-line, in-person, technical support presence for multiple diverse departments. I responded to numerous trouble tickets related to personal computer hardware, operating systems, application software, and printing-related issues.

My job was to resolve any issue related to desktop computing, and to know whether an issue would be best served if escalated to a network infrastructure, server, or telecommunications team. Regardless of whether I escalated a trouble ticket, or personally saw it through from inception to resolution, it was my responsibility to follow each ticket through to resolution.

My role was to "enable" each employee I worked with to effectively utilize computers, as well as computer-related technology, to better fulfill their roles within their respective departments. If the people I worked with didn't know what they were doing any better after meeting with me than before, then I hadn't done my job.

On a particular Monday morning, I was informed that an intern would be starting midweek. I was asked to shadow and train this individual — let's call him Mark — for a week or two until he knew the ropes and could make his way around and function solo. The appointed morning arrived, and I was able to greet and welcome Mark to his new role, and his first day on the job.

Mark was a pleasure. He was able to fluidly converse on a variety of both work-related and extracurricular topics. He was certainly conversant as we reviewed the assortment of trouble tickets that had been assigned that day and were awaiting our response.

This made perfect sense to me, as Mark had a fistful of up-to-date and applicable industry certifications, including CompTIA's A+ and one of Microsoft's various MCSE (Microsoft Certified Systems Engineer) credentials. He was able to read through each ticket and provide a solid theoretical response to what he felt was the root cause of each reported issue.

After a couple of hours spent reviewing tickets and verbally orienting Mark on the organization — including details about each department in the company — we set out to respond to our first trouble ticket of the day.

Something peculiar occurred, however, upon arrival at the desktop computer for which the issue had been reported. The formerly conversant Mark, who had verbally rehearsed multiple scenarios and probable outcomes to the problem we faced, sat befuddled at the computer keyboard.

After a moment or two, he turned to me and kindly asked how to commence troubleshooting. The confident technician I'd met that morning had suddenly come face-to-face with his own lack of practical hands-on experience. It's one thing to read about fixing computer problems, and another thing to actually fix them.

My interest was piqued. Before me was sudden and unanticipated proof that a fully certified individual might well be able to talk a good talk, while not necessarily being able to walk a solidly confident walk. Mark didn't possess the IT wherewithal to perform the role for which he had been hired.

Admittedly, after a week with me looking over his shoulder, Mark was fully functional within every department. The question, however, remained in my mind: "Why hadn't Mark's certifications given him the practical hands-on know-how he needed to hit the ground running on day one?"

Fast-forward a few years to my current support job with TestOut Corporation. Within my first year of employment, and through many inbound customer communications (primarily originating at institutions of higher education), I learned that my experience with Mark was not uncommon.

Read the rest here:

http://certmag.com/problem-certifications-dont-measure-practical-skills/

Better security achieved with randomly generating biological encryption keys

By Staff, Penn State College of Engineering, December 19, 2018

Data breaches, hacked systems and hostage malware are frequently topics of evening newscasts — including stories of department store, hospital, government and bank data leaking into unsavory hands — but now a team of engineers has an encryption key approach that is unclonable and not reverse-engineerable, protecting information even as computers become faster and nimbler.

"Currently, encryption is done with mathematical algorithms that are called one-way functions," said Saptarshi Das, assistant professor of engineering science and mechanics, Penn State. "These are easy to create in one direction, but very difficult to do in the opposite direction."

An example of this is multiplying two prime numbers. Assuming the original numbers are very large, reverse engineering from the result becomes very time and computer-resource heavy.

"However, now that computers are becoming more powerful and quantum computing is on the horizon, using encryption that relies on its effectiveness because it is monumentally time consuming to decrypt won't fly anymore," said Das.

Only truly random encryption keys are unclonable and not capable of being reverse-engineered because there is no pattern or formula in the process. Even so-called random number generators are really pseudo-random number generators.

"We need to go back to nature and identify real random things," said Das. "Because there is no mathematical basis for many biological processes, no computer can unravel them."

The researchers, who also included Akhil Dodda, graduate student in engineering science and mechanics; Akshay Wali, graduate student in electrical engineering; and Yang Wu, postdoctoral fellow in engineering science and mechanics, looked at human T cells. They photographed a random, 2-dimensional array of T cells in solution and then digitized the image by creating pixels on the image and making the T cell pixels "ones" and the empty spaces "zeros."

"When we started there were a few papers out using nanomaterials," said Dodda. "However, they weather (nanomaterials) out of the material and are stationary."

Living cells, regardless of the type, can be kept around for a long time and because they move constantly, can be photographed repeatedly to create new encryption keys.

"We need a lot of keys because the population of the world is 7 billion," said Das. "Each person will generate a megabyte of data every second by 2020."

Besides encryption keys for personal computers, the keys are also needed for medical, financial and business data, and much more. If something is hacked or malfunctions, this method would also allow rapid replacement of the encryption key.

"It is very difficult to reverse-engineer these systems," said Dodda. "Not being able to reverse-engineer these keys is an area of strength."

The researchers are currently using 2,000 T cells per encryption key. The team reports in a recent issue of Advanced Theory and Simulation that even if someone knows the key generation mechanism, including cell type, cell density, key generation rate and key sampling instance, it is impossible for anyone to breach the system. It is simply not possible from that information to bust the encryption.

"We need something secure, and biological species-encrypted security systems will keep our data safe and secure everywhere and anytime," said Wali.

Read the rest here:

https://www.esm.psu.edu/news/2018-fall/das-biological-encryption.aspx

How far should organizations be able to go to defend against cyberattacks?

By Scott Shackelford , Homeland Security News Wire, February 15, 2019

Organizations can and should be encouraged to take passive defense measures, like gathering intelligence on potential attackers and reporting intrusions. But in my view they should be discouraged – if not prevented – from acting aggressively, because of the risk of destabilizing corporate and international relations. If the quest for cyber peace degenerates into a tit-for-tat battle of digital vigilantism, global insecurity will be greater, not less.

The deluge of cyberattacks sweeping across the world has governments and companies thinking about new ways to protect their digital systems, and the corporate and state secrets stored within. For a long time, cybersecurity experts have erected firewalls to keep out unwanted traffic and set up decoy targets on their networks to distract hackers who do get in. They have also scoured the internet for hints about what cybercriminals might be up to next to better protect themselves and their clients.

Now, though, many leaders and officials are starting to think about stepping up their defensive activities, by taking more active measures. An extreme option within this field of active defense is sometimes called “hacking back” into an adversary’s systems to get clues about what they’re doing, shut down the attack or even delete data or otherwise damage an attacker’s computers.

I have been researching the benefits and drawbacks of various active defense options with Danuvasin Charoen of the Thai National Institute of Development Administration and Kalea Miao, an undergraduate Cox scholar at the Indiana University Kelley School of Business. We have found a surprising number and variety of firms – and countries – exploring various ways to be more proactive in their cybersecurity practices, often with little fanfare.

Getting active

On the surface, it might seem like the proverb is right: “The best defense is a good offense.” The damage from cyberattacks can be enormous: In May 2017, a single incident, the WannaCry cyber attack, affected hundreds of thousands of systems around the world and caused more than US$4 billion in lost productivity and data recovery costs. One month later, another attack, called NotPetya, cost global shipping giant Maersk $300 million and reduced the company to relying on the Facebook-owned WhatsApp messaging system for official corporate communications.

Faced with this scale of loss, some companies want to step up their defenses. Firms with sophisticated technology systems know what’s needed to protect their customers, networks and valuable trade secrets. They also likely have employees with the skills to track down hackers and penetrate the attackers’ own systems. But the ethics and implications of justifying a cyberattack as defensive get very complicated very quickly.

It’s often unclear, for example, exactly who is behind an attack – uncertainty that can last for days, months or even years. So who should the hack-back target? What if a privately owned U.S. company believed that it was under attack from a firm owned by the Chinese government? If it hacked back, would that be an act of war between the countries? What should happen to repair corporate and international relations if the company was wrong and its attacker was somewhere else? Companies shouldn’t be empowered to start global cyber conflicts that could have dire consequences, but online and offline.

Of course, it’s also important to think about what might happen if other countries allow their companies to hack back against U.S.government or corporate efforts. More U.S. firms could fall victim to cyberattacks as a result, and might find little legal recourse.

Engaging with the law

At the moment, hacking back is illegal, in the U.S. and in many nations around the world. In the U.S., the Computer Fraud and Abuse Act makes it a crime to access another computer without authorization. Every member of the G-7, including the U.S., as well as Thailand and Australia, has banned hacking back. In 2018, more than 50 countries – but not the U.S.– signed an agreement that private firms based in their nations are not allowed to hack back.

However, supporters of active defensive tactics are pushing their message hard. The Republican Party’s 2016 presidential platform promised to ensure “users have a self-defense right to deal with hackers as they see fit.” In March 2018, the Georgia state legislature passed a bill to permit “active defense measures that are designed to prevent or detect unauthorized computer access.” Two months later, then-Gov. Nathan Deal vetoed it, at the urging of technology firms concerned about its “national security implications and other potential ramifications.”

Read the rest here

http://www.homelandsecuritynewswire.com/dr20190215-how-far-should-organizations-be-able-to-go-to-defend-against-cyberattacks

ISSA Photos are courtesy of our Chapter Photographer

Warren Pearce


PEPSI


ISSA

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

Information Systems Security Association
Developing and Connecting Cybersecurity Leaders Globally
Colorado Springs Chapter

WWW.ISSA-COS.ORG

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?

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

Send your article ideas to the Newsletter at:

newsletter@issa-cos.org

Chapter Officers:

President*: Ernest Campos
Vice President*: Michael Crandall
Executive Vice President*: Scott Frisch
Treasurer: Mark Maluschka
- Deputy Treasurer: **Vacant**

Recorder/Historian: Russ Weeks
- Deputy: Mike Daetwyler

Dir. of Professional Outreach: Katie Martin
- Deputy: **Vacant**

Director of Communications : Anna Johnston
- Deputy: Christine Mack

Director of Certifications: Derrick Lopez
- Deputy: Luke Walcher

Vice President of Membership: David Reed
- Deputy: Melissa Absher

Vice President of Training: Mark Heinrich
- Deputy: Jeff Tomkiewicz

Member at Large: James Asimah
Member at Large: Bill Blake
Member at Large: Jim Blake
Member at Large: **Vacant**

Committee Chairs:

Training: Mark Heinrich
Hospitality: Stephen Parish
Ethics: Timothy Westland
Recognition: Jorden Smith
Media : Don Creamer
IT Committee: Patrick Sheehan
Speaker's Bureau: William (Jay) Carson

Executive Assistant: Andrea Heinz

** Executive Board Members*

Significant Interest Group Leads:

Chair: **Vacant**
Women in Security : June Shore
Young Prof. in Security: Jeremiah Walker
Mentoring in Security: Carissa Nichols
Executives in Security: **Vacant**
Finance in Security: Mark Maluschka
Healthcare in Security: **Vacant**
Retail in Security: **Vacant**
DoD in Security: **Vacant**

Past Senior Leadership

President Emeritus: Dr. George J. Proeller
President Emeritus: Mark Spencer
Past President: Pat Laverty
Past President: Frank Gearhart
Past President: Cindy Thornburg
Past President: Colleen Murphy

By Rhett Jones, Gizmodo, February 21, 2019

What if I told you Facebook allowed advertisers to target users who were interested in Nazis?

On Thursday, the Los Angeles Times reported that Facebook's target advertising system has been identifying users who are interested in Nazis and its related culture in order to provide paying advertisers with an opportunity to reach them directly. Some of the terms suggested to advertisers to narrow down their targeted audience included "Joseph Goebbels," "Josef Mengele," "Heinrich Himmler," and "National Socialist black metal." When the LA Times ran tests to promote a white nationalist punk band, "detailed targeting" suggestions became extremely specific. From the report:

Read the rest here:

https://gizmodo.com/of-course-1832798696

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