Colleagues,

Have you been thinking about getting a certification? Whether you’re new to the cybersecurity field, a senior cybersecurity professional, or somewhere in between, there are many reasons to consider becoming certified or obtaining additional certifications. The challenge, perhaps, is deciding which certification to get. There are many certifications to consider, from several certifying agencies. If you’re wondering what certification to get, here’s a short synopsis of some certifications you may want to consider, and the websites where you can get additional information. This is just a partial list of certifications available from some of the more common certifying agencies, so be sure to look at the websites for additional information on these, or other certifications.

CompTIA – info copied from: https://certification.comptia.org/certifications

A+ is the starting point for a career in IT. The performance-based exams certify foundational IT skills across a variety of devices and operating systems.

Network+ certifies the essential skills needed to confidently design, configure, manage and troubleshoot any wired and wireless devices.

Security+ provides a global benchmark for best practices in IT network and operational security, one of the fastest-growing fields in IT.

Cybersecurity Analyst (CSA+) is an international, vendor-neutral cybersecurity certification that applies behavioral analytics to improve the overall state of IT security. CSA+ validates critical knowledge and skills that are required to prevent, detect and combat cybersecurity threats.

CompTIA Advanced Security Practitioner (CASP) meets the growing demand for advanced IT security in the enterprise. Recommended for IT professionals with at least 5 years of experience, CASP certifies critical thinking and judgment across a broad spectrum of security disciplines and requires candidates to implement clear solutions in complex environments.

ISACA – info copied from: http://www.isaca.org/CERTIFICATION/Pages/default.aspx

The views expressed in articles obtained from public sources within this newsletter do not necessarily reflect those of ISSA, this Chapter or its leadership.
Cops use murdered woman's Fitbit to charge her husband

By Amanda Watts, CNN, April 26, 2017

The Wikileaks ’Vault7’ release from earlier this month reignited the reality of state-sponsored espionage, and what our governments know about us.

The attack, as Richard Dabate described it to police, was horrific.

A masked intruder barged into his Connecticut home, he said, tied up and tortured him and -- when his wife came home -- shot and killed her.

His story, however, would not hold up with investigators. And when cops ultimately charged him with murdering his wife, they relied on evidence gathered from an unlikely source:

The Fitbit his wife was wearing.

It was December 23, 2015. Dabate told detectives he put his two kids on the bus that morning, waved goodbye to his wife, Connie, and left for work.

Soon afterward, the wife headed for a fitness class at the local YMCA, with a Fitbit on her waistband.

In his version of the incident, as outlined in a warrant obtained by CNN affiliate WTIC, Dabate said he went back home when he realized he'd forgotten his laptop.

That was between 8:45 a.m. and 9 a.m., he told detectives.

He heard a noise, he said, and went upstairs to investigate.

That's where he spotted an intruder, he said: a 6'2" man with a stocky build wearing a "camouflaged suit with a mask."

Right then, Dabate said he heard his wife return home and yelled for her to run.

After a brief struggle, the intruder shot and killed the wife, Dabate said.

At that point, he told detectives the intruder half tied him to a chair and began burning him with a torch.

The two tussled, he said. And at one point, Dabate said he turned the torch on the intruder.

The man “dropped the torch, put his hands to his face, and ran out,” he said.

Dabate said he crawled upstairs with the chair still attached to his wrist, pushed the panic button on his alarm and called 911.

It was 10:11 a.m.

Police scoured the area but couldn't find a suspect.

K-9s were brought in to locate any evidence that someone fled the property; the only thing they picked up tracked directly to Dabate, police said.

Investigator said they also found no evidence of forced entry and nothing in the house was taken.

They obtained search warrants for Connie Dabate’s Fitbit, both of their cell phones, computers and house alarm logs.

Synchronizing those logs, here’s what detectives say they found, according to the warrant:

- At 9:01 a.m. Richard Dabate logged into Outlook from an IP address assigned to the internet at the house.
- At 9:04 a.m., Dabate sent his supervisor an e-mail saying an alarm had gone off at his house and he's got to go back and check on it.
- Connie's Fitbit registered movement at 9:23 a.m., the same time the garage door opened into the kitchen.
- Connie Dabate was active on Facebook between 9:40 and 9:46 a.m., posting videos to her page with her iPhone. She was utilizing the IP address at their house.
- While she was at home, her Fitbit recorded a distance of 1,217 feet between 9:18 a.m. and 10:05 a.m. when movement stops.

If Richard Dabate’s claims were correct, detectives say the total distance it would take the victim to walk from her vehicle to the basement, where she died, would be no more than 125 feet.

Read the rest here:

We are holding steady on our membership—~481 members as of the end of March. Overall, we are maintaining our membership with renewals and new memberships—both general and students/Freemiums. Kudos to everyone who referred a student or general member. Keep those renewals and new members coming in! Remember that for each referral you make, you are entered into the ISSA International quarterly drawing for various prizes.

We are holding steady on our membership—~485 members as of the end of April. Overall, we are maintaining our membership with renewals and new memberships—both general and students/Freemiums. Kudos to everyone who referred a student or general member. Keep those renewals and new members coming in! Remember that for each referral you make, you are entered into the ISSA International quarterly drawing for various prizes.

There appears to be some confusion about the Freemium program. It is now an official ISSA program instead of the pilot program we've been working with for the last couple of years. It is no longer showing as a member type when you try to join. Now we issue a code to potential student members that they input on the payment page that cancels out the student membership fees. Eligibility rules governing the program remain the same: Full time students, not fully employed in Cybersecurity, etc. If you are referring a student, please have them contact me and I can confirm their eligibility for Freemium (or not). If they are eligible, I will provide a chapter unique payment code for them to use in the payment block when they join as a “Student” member so they can join for free. Students who don’t meet the Freemium criteria can still enroll as “Student” members, too. However, they will have to pay the current student membership rate of $55. If you know of students who might be eligible have them contact me.

I would also like to take this opportunity to strongly recommend that members consider applying for the ISSA Fellows program if you meet the requirements. This includes Senior Members, Fellows, and Distinguished Fellows. The requirements can be found on the ISSA website at http://www.issa.org/?page=FellowProgram. Recognition of this type is not only personally rewarding but it can also be a good item to have on your resume. Also, it helps improve the recognition of the Chapter within the greater ISSA community. While it does take a little effort to put your package together there are plenty of people who have done it who can provide examples, reviews and other assistance. Once your package is submitted, it’s relatively painless after that. Your dues stay the same, you aren’t required to run for any offices, you still get free lunch (or dinner) and you still get all the other benefits of regular membership. So, please, at least think about it and feel free to contact me if you want to discuss it.

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.

David Reed
Membership Committee Chairman
dreed54321@comcast.net
The uniquely management-focused Certified Information Security Manager (CISM) certification promotes international security practices and recognizes the individual who manages, designs, and oversees and assesses an enterprise’s information security.

The Certified Information Security Auditor (CISA) designation is a globally recognized certification for IS audit control, assurance and security professionals. Being CISA-certified showcases your audit experience, skills and knowledge, and demonstrates you are capable to assess vulnerabilities, report on compliance and institute controls within the enterprise.

Certified in the Governance of Enterprise IT (CGEIT) recognizes a wide range of professionals for their knowledge and application of enterprise IT governance principles and practices. As a CGEIT certified professional, you demonstrate that you are capable of bringing IT governance into an organization—that you grasp the complex subject holistically, and therefore, enhance value to the enterprise.

Certified in Risk and Information Systems Control (CRISC) is the only certification that prepares and enables IT professionals for the unique challenges of IT and enterprise risk management, and positions them to become strategic partners to the enterprise.

(ISC)² – info copied from: https://www.isc2.org/credentials/default.aspx

The Systems Security Certified Practitioner (SSCP) certification is the ideal credential for those with proven technical skills and practical security knowledge in hands-on operational IT roles. The SSCP indicates a practitioner’s technical ability to tackle the operational demands and responsibilities of security practitioners, including authentication, security testing, intrusion detection/prevention, incident response and recovery, attacks and countermeasures, cryptography, malicious code countermeasures, and more.

The Certified Authorization Professional (CAP) certification is an objective measure of the knowledge, skills and abilities required for personnel involved in the process of authorizing and maintaining information systems. Specifically, this credential applies to those responsible for formalizing processes used to assess risk and establish security requirements and documentation.

The Certified Cyber Forensics Professional (CCFP) credential indicates expertise in forensics techniques and procedures, standards of practice, and legal and ethical principles to assure accurate, complete, and reliable digital evidence admissible in a court of law. It also indicates the ability to apply forensics to other information security disciplines, such as e-discovery, malware analysis, or incident response. In other words, the CCFP is an objective measure of excellence valued by courts and employers alike.

The Certified Cloud Security Professional (CCSP) credential denotes professionals with deep-seated knowledge and competency derived from hands-on experience with cyber, information, software and cloud computing infrastructure security. CCSPs help you achieve the highest standard for cloud security expertise and enable your organization to benefit from the power of cloud computing while keeping sensitive data secure.

The vendor-neutral Certified Information Systems Security Professional (CISSP) certification is the ideal credential for those with proven deep technical and managerial competence, skills, experience, and credibility to design, engineer, implement, and manage their overall information security program to protect organizations from growing sophisticated attacks.

EC-Council – info copied from: https://www.eccouncil.org/programs/

A Certified Ethical Hacker is a skilled professional who understands and knows how to look for weaknesses and vulnerabilities in target systems and uses the same knowledge and tools as a malicious hacker, but in a lawful and legitimate manner to assess the security posture of a target system(s).

EC-Council’s Computer Hacking Forensic Investigator (CHFI) certifies individuals in the specific security discipline of computer forensics from a vendor-neutral perspective. The CHFI certification will fortify the application knowledge of law enforcement personnel, system administrators, security officers, defense and military personnel, legal professionals, bankers, security professionals, and anyone who is concerned about the integrity of the network infrastructure.

The Certified Chief Information Security Officer (CCISO) program is the first of its kind training and certification program aimed at producing top-level information security executives. The CCISO does not focus solely on technical knowledge but on the application of information security management principles from an executive management point of view.

Our Chapter offers Security+ and CISSP Exam Prep Review Seminars and we’ve formed study groups for other certifications. If there’s interest, we may be able to form a new study group to help review certification material to ensure you’re prepared for the exam. Training for certifications can also be obtained from commercial companies in the local area.

Reach out to a Board member, our Training Committee, or our Mentoring Committee if you have any questions or would like to talk to someone about pursuing a certification.
UCCS Cyber Security Club: 2016/17 Year in Review

Young professionals achieve success while preparing for a future in Cybersecurity.

By Ernest M. Campos, Collegiate Mentor and ISSA-COS Volunteer, April 21, 2017

The University of Colorado, Colorado Springs (UCCS) is well known for hosting a highly-regarded Cybersecurity academic program. Graduates from this program are often scouted by recruiters two, sometimes three, years prior to graduation. Internship opportunities abound from several well-known high tech companies and often lead to immediate full-time job opportunities following graduation.

In addition to UCCS’s formal academic programs, there exists an extra-curricular organization focused solely on competing within Cybersecurity Capture the Flag (CTF) events held throughout the academic year. Competing under the team name “PeakChaos,” the UCCS Cybersecurity Club was developed with a strong objective: “Prepare, Compete, Perform”. The practical preparation necessary to compete in CTF events comes from a devotion that extends far beyond the classroom. Meeting weekly, the group self-educates its members on many of the hardcore skills not commonly taught within academic classrooms.

Board Members

The board members for the 2016/17 academic year included the following officers: Wayne Havey, JJ Cramer, Spencer Powell, Adam Barker, and Sawyer Peterson. Collectively, these individuals share the load of organizing sessions for club members to train and perfect their skills, submit registrations for CTF events, participate in the competitive events, and handle the socialization and promotion of the organization. This year, club participation exceeded 50 uniquely skilled members. Additionally, the offices maintained communication with over 360 of its past members – an impressive alumni total considering the otherwise “under-the-radar” organization has only been in existence since 2012. It wasn’t until the 2016 academic year that UCCS officially recognized the group as a university sponsored extra-curricular club.

Competitive Landscape

During the 2016/17 academic year, PeakChaos participated in 10 CTF events. Two of the more challenging events this season were “The Boston Key Party” and “iCTF”; both very difficult competitions featuring highly competitive teams. Competitors are geographically located throughout the United States and include teams such as: “ppp” (Plaid Parliament of Pwning) and "Shellphish." Both ppp and Shellphish are well known throughout the CTF community and participate in many of the same competitions PeakChaos competes. Other highly rated competitors include teams that represent Carnegie Mellon University and the University of California, Santa Barbara. Among all these notable teams, PeakChaos stands out as a team to be taken seriously, a team gaining in its competitive rankings, and a team with a broad and deep level of technical competence.

Competitive Results

During the 2016/17 season, PeakChaos placed very well within several respectable competitions. Their most prominent placements included:

• 1st place: Colorado Springs local CTF, sponsored by Deloitte.Consulting (www.deloitte.com)
• 12th percentile (60/492): CTF(x).

(Continued on page 10)
Suspect OKs Amazon to hand over Echo recordings in murder case

By Elliott C. McLaughlin, CNN, April 26, 2017

Amazon, go ahead and hand over the recordings in that murder case.

A high-profile attorney has taken over as lead counsel for an Arkansas man accused of killing his friend, a former police officer, after a night of drinking and football. A prosecutor had sought recordings from the defendant's Amazon Echo smart speaker as evidence in the case, a request the online retailer had rebuffed.

According to a court document, lawyer Kathleen Zellner ended the legal tug of war Friday when she filed a motion saying her client, James Bates, would voluntarily hand over the recordings. Amazon provided the data to prosecutors later that day, the document says.

Zellner, who rose to fame as the attorney for Steve Avery in Netflix's "Making a Murderer," could not immediately be reached for comment at her Downers Grove, Illinois, office Tuesday.

She confirmed in a tweet, which was also posted to her law firm's website, that the defense had agreed to hand over the recordings.

"My client James Bates is innocent," the tweet said.

Amazon had pushed back against Benton County, Arkansas, Prosecuting Attorney Nathan Smith's demand for information from the smart speaker, setting up a legal battle pitting investigators' quest for technology evidence against American privacy rights.

"Given the important First Amendment and privacy implications at stake, the warrant should be quashed unless the Court finds that the State has met its heightened burden for compelled production of such materials," Amazon's lawyers wrote in a February memo seeking to quash Smith's request for a search warrant.

In a statement sent to CNN last year, the company said, "Amazon objects to overbroad or otherwise inappropriate demands as a matter of course."

Smith has said he hopes the voice-activated Echo -- which answers users' questions, plays music, reads news and connects to other smart devices -- will provide information on how a man came to be found dead in 31-year-old Bates' hot tub.

Kimberly Weber, who previously was lead defense counsel in Bates' case, told CNN in December there was nothing useful on the device and applauded Amazon for protecting her client's privacy.

Bates, who was arrested last year on suspicion of first-degree murder, is free on a $350,000 bond.

A discovery hearing in the case was scheduled for Wednesday, but it's unclear if the hearing is still necessary now that Bates has acquiesced to the prosecutor's request for the recordings.

As technology has become more integral to daily life, authorities have increasingly sought evidence from mobile phones, laptops, social media, even the "Warcraft" video game. Attempting to mine a smart speaker for information may be a first though.

Joel Reidenberg, the founding academic director for Fordham University's Center on Law and Information Policy, told CNN it's the first such case he's seen, but he isn't surprised that smart speakers are already the subject of a court battle.

While some might argue that voice technologies such as Echo, Siri or Google Home, which assist users with queries and tasks, come with a different expectation of privacy than, say, social media postings or Internet searches, Reidenberg said he feels such an attitude is naive.

According to Amazon, Echo works by constantly listening for the "wake word" -- "Alexa" or "Amazon," by default -- and then records your voice and transfers it to a processor for analysis so that it can fulfill requests or answer questions. The recordings are streamed and stored remotely, and can be reviewed or deleted over time, Amazon says.

"How is that any different from you sitting at your keyboard typing?" Reidenberg asked.

The Amazon Echo became a subject of the November 2015 murder case because someone present on the night of the death recalled hearing music streaming through the device, prosecutors say.

Bates had invited two friends -- one of them former Georgia police officer Victor Collins, 47 -- over to his Bentonville home, where they watched college football, drank beer and shot vodka, according to the search warrant affidavit filed in Benton County Circuit Court. The men decided to get into Bates' hot tub, and Bates said he went to bed around 1 a.m. When he awoke in the morning, Collins was floating face-down in the hot tub, the affidavit says.

Weber previously told CNN that Collins was Bates' friend, and his death was a tragic accident, possibly stemming from his drinking. Collins' blood-alcohol content at the time of death was .32, four times the legal limit to drive in Arkansas, she said.

Read the rest here:
Malware Hunts And Kills Poorly Secured Internet Of Things Devices Before They Can Be Integrated Into Botnets

By Karl Bode, TechDirt, April 24, 2017

Researchers say they've discovered a new wave of malware with one purpose: to disable poorly secured routers and internet of things devices before they can be compromised and integrated into botnets. We've often noted how internet-of-broken-things devices ("smart" doorbells, fridges, video cameras, etc.) have such flimsy security that they're often hacked and integrated into botnets in just a matter of seconds after being connected to the internet. These devices are then quickly integrated into botnets that have been responsible for some of the worst DDoS attacks we've ever seen (including last October's attack on DYN).

And most security researchers firmly believe we haven't seen anything yet.

Enter PDoS (permanent denial of service) attack bots, which scan the internet for routers with default, unchanged passwords, or "smart" doorbells, dolls or other devices with paper-mache grade security. From there, PDoS attack bots issue a series of commands that wipe device media, corrupt all storage, and disconnect the device from the internet. Last month, researchers from security firm Radware set up an intentionally poorly-secured honeypot that they say saw roughly 2,250 PDoS attempts during just a four-day span.

The lion's share of these attacks came from two botnets dubbed BrickerBot.1 and BrickerBot.2 -- with nodes busily bricking poorly-secured devices around the world. Initially researchers say they thought that somebody crafted malware specifically to tackle the IoT threat. But given the broad targeting of the botnets (including server-attached storage devices), they also think it's possible that the goal may just be good, old, vanilla mayhem:

"When I discovered the first BrickerBot, I thought it was a drastic attempt to stop the IoT Botnet DDoS threat," Radware researcher Pascal Geenens told Ars. "I thought this was a competitor hacker who wanted to take out his competition and get access to the list of IP [addresses] of bots that were in the competitor's botnet. But upon discovery of the second BrickerBot this theory changed, as the second one is targeting any Linux-based system—not only embedded, BusyBox-based Linux with flash storage. What motivates people to randomly destroy things? Anger, maybe? A troll, maybe?"

As it stands, BrickerBot.2 can only access machines that feature default administrative passwords and have the telnet protocol enabled, limiting the overall potential impact. Regardless, the end result still isn't pleasant for those on the receiving end of a BrickerBot.2 attack:

"...In addition to corrupting the storage device, BrickerBot.2 wipes all stored files, removes the default Internet gateway, disables TCP timestamps, and limits the maximum number of kernel threads to just one. That all but ensures that most damaged devices won't be restored without a major undertaking. Radware has more details about the attacks here."

It's still entirely possible the goal here is to actually help the internet by killing poorly-secured hardware before they can be conscripted into the shitshow that is the internet of things. After all, BrickerBot.2 appears to be an evolution of the Linux.Wifatch malware, which first appeared in October 2015. It seems more than likely that additional malware strains taking cues from the Mirai malware will inevitably appear in the wild, the goal potentially being not necessarily mayhem -- but preventing the massive, crippling DDoS attacks most security experts feel are inevitable in the next year or two.

The problem (aside from this being illegal and destructive) is that the type of person that's likely to go out and purchase a poorly-secured "gee whiz" IOT device or router without considering security -- is the same type of person that's not going to understand why that device just stopped working for no coherent reason. As a result, they're likely to rush out and buy another, poorly-secured device, bringing the incompetence full circle with a zero net gain. As such, Security expert Victor Gevers is urging malware authors like this to consider a more constructive path toward the same end goal:

Read the rest here:
By Joshua Goldfarb, Security Week, April 12, 2017

In the incident response world, we used to draw a clear line between the capabilities of attackers affiliated with nation-states and those not affiliated with any nation-state. Nation-state attackers always seemed to be the most well equipped and the most sophisticated attackers. Then, over the last few years, that line began to blur.

The sophistication of attackers with criminal or financial, rather than nation-state motives began to increase significantly. We now find ourselves in a completely different threat landscape. As the 2017 M-Trends report notes, “Today, the line between the level of sophistication of certain financial attackers and advanced state sponsored attackers is not just blurred – it no longer exists.”

Of course, there is no shortage of pundits running around talking about pandas, tigers, and bears (oh my!). But as someone who has spent most of his career as a defender, criminal attack groups have captured my attention for quite some time now. Am I saying that we no longer need to worry about nation-state attackers? No, of course not. Rather, what I am saying is that most organizations should probably be paying far more attention to criminal attack groups than they currently do.

Let’s take a look at a few of the reasons why:

A Numbers Game

While nation-state sponsored attacks often grab headlines, they are not something most security teams spend a majority of their time on. Of course, when a nation-state attack hits, it can be quite ugly and can consume the entirety of a security team for an extended period of time. But day-to-day, there is plenty of other activity to keep a security team busy.

There are many reasons why this is the case, but part of it is a simple numbers game. While the capabilities and resources of various nation-states vary widely, the number of attack groups is relatively finite in number. There aren’t millions of countries in the world, but around 200 (give or take). Each of these countries can have anywhere from 0 to N state-sponsored attack groups (where N can be a fairly large number for a small number of nation-states).

On the other hand, when we expand our criteria to look at attack groups organized around criminal or financial motives, there are literally tens of thousands of such groups, or perhaps even more. It is difficult to pinpoint the exact number, and of course, the sophistication of these groups will vary widely. But fundamentally, what we have here is a numbers game. With so many attack groups, the chance that one or more of them is interested in some data or information that you are entrusted with safeguarding is fairly high.

Flexibility and Spontaneity

For those of you who have worked in large organizations for any amount of time, you understand that large organizations cannot move as quickly and nimbly as smaller organizations. Smaller, less formal, more loosely organized attack groups can form flexibly and spontaneously around specific objectives and missions. These attack groups can recruit talent and adopt tools, techniques, and procedures as necessary for their day-to-day work without prolonged and protracted bureaucratic processes. For us on the defensive side, that often means a significant number of adversaries that are both more sophisticated and more agile than we are.

All About the Information

As you are likely aware, the motives of each attack group vary widely. As a result of this, so does the data or information they target. As we expand the list of attack groups, not surprisingly, the array of targeted information expands as well. And of course, this has the ultimate effect of greatly expanding the list of potential victim organizations. Not surprisingly, this is essentially what we’ve seen happen over the last few years. Targeted attacks are no longer the exclusive “privilege” of governments, militaries, defense contractors, and other traditional targets.

Read the rest here:
Quantum Computers May Have Higher ‘Speed Limits’ Than Thought

By Staff, NIST, March 24, 2017

How fast will a quantum computer be able to calculate? While fully functional versions of these long-sought technological marvels have yet to be built, one theorist at the National Institute of Standards and Technology (NIST) has shown that, if they can be realized, there may be fewer limits to their speed than previously put forth.

The findings—described as a “thought experiment” by NIST’s Stephen Jordan—are about a different aspect of quantum computing speed than another group of NIST researchers explored about two years ago. While the previous findings were concerned with how fast information can travel between two switches in a computer’s processor, Jordan’s new paper deals with how quickly those switches can flip from one state to another.

The rate of flipping is equivalent to the “clock speed” of conventional processors. To make computations, the processor sends out mathematical instructions known as logic operations that change the configurations of the switches. Present day CPUs have clock speeds measured in gigahertz, which means that they are capable of performing a few billion elementary logic operations per second.

Because they harness the power of quantum mechanics to make their calculations, quantum computers will necessarily have vastly different architectures than today’s machines. Their switches, called quantum bits or “qubits,” will be able to represent more than just a 1 or 0, as conventional processors do; they will be able to represent multiple values simultaneously, giving them powers conventional computers do not possess.

Jordan’s paper disputes longstanding conclusions about what quantum states imply about clock speed. According to quantum mechanics, the rate at which a quantum state can change—and therefore the rate at which a qubit can flip—is limited by how much energy it has. While Jordan believes these findings to be valid, several subsequent papers over the years have argued that they also imply a limit to how fast a quantum computer can calculate in general.

“At first glance this seems quite plausible,” Jordan said. “If you’re performing more logic operations, it makes sense that your switches would need to go through more changes. In both conventional and quantum computing designs, each time a logic operation occurs”—making its switches flip—“the computer hops to a new state.”

Using the mathematics of quantum systems, Jordan shows is that it is possible to engineer a quantum computer that does not have this limitation. In fact, with the right design, he said, the computer “could perform an arbitrarily large number of logic operations while only hopping through a constant number of distinct states.”

Counterintuitively, in such a quantum computer, the number of logic operations carried out per second could be vastly larger than the rate at which any qubit can be flipped. This would allow quantum computers that embrace this design to break previously suggested speed limits.

What advantages might this faster clock speed grant? One of the primary applications envisioned for quantum computers is the simulation of other physical systems. The theoretical speed limit on clock speed was thought to place an upper bound on the difficulty of this task. Any physical system, the argument went, could be thought of as a sort of computer—one with a clock speed limited by the system’s energy. The number of clock cycles needed to simulate the system on a quantum computer should be comparable to the number of clock cycles the original system carried out.

However, these newly discovered loopholes to the computational speed limit are a “double-edged sword.” If energy does not limit the speed of a quantum computer, then quantum computers could simulate physical systems of greater complexity than previously thought. But energy doesn’t limit the computational complexity of naturally occurring systems either, and this could make them harder to simulate on quantum computers.

Jordan said his findings do not imply that there are no limits to how fast a quantum computer could conceivably calculate, but that these limits derive from other aspects of physics than merely the availability of energy.

“For example, if you take into account geometrical constraints, like how densely you can pack information, and a limit to how fast you can transmit information (namely, the speed of light), then I think you can make more solid arguments,” he said. “That will tell you where the real limits to computational speed lie.”

The article may be found here: https://www.nist.gov/news-events/news/2017/03/quantum-computers-may-have-higher-speed-limits-thought
24th percentile (228/948): The BostonKeyParty.

Still to come this season (at the time of this writing) are the "Secure Set CTF," hosted by Secure Set, LLC (www.secureset.com) based in Denver, CO with a recent expansion into Colorado Springs; and, an invitation to compete in the "Space Apps Challenge," hosted by NASA.

Competitive Skills – Real-world Applications

In addition to participating in CTFs, many members of the group have also participated in advanced research projects that utilize their cyber-hacking skills. An example of one such project was a proposal for performing penetration testing against modern vehicular technology. In this project, participants challenged the security integrity of Plug-In and WI-FI connectivity. The objective was to apply forced infiltration to identify weaknesses in the vehicle’s computer modules that would enable hackers to penetrate, intrude, manipulate, and gain control of various features and capabilities.

The practical skills honed by members of PeakChaos have resulted in the group becoming a targeted resource pool for recruiting ambitious, young professionals. Notable companies such as the Harris Corporation (www.harris.com) have pursued members for positions within their Cybersecurity and Software Engineering departments. Other companies such as Raytheon (www.raytheon.com) have also established a history of offering internship and employment opportunities prior to graduation.

Among the strongest marketable skills members obtain and practice include:

- An intricate understanding of how computers operate from the low (machine) level to the high (logical) level
- An overall understanding of computer security including: binary security (e.g. buffer overflows) and web security (e.g. SQL injection)
- An ability to apply security techniques into one’s own written code; a vastly important skill that remains an under-taught skill set within academic institutions.

The Future of PeakChaos

With a growing interest among industry organizations to host, promote, and sponsor CTFs, an increasing number of new competitions are popping up each year. As they do, PeakChaos plans to expand its annual membership thus, amplifying both the number of events and the number of members participating in events each year.

As the Cybersecurity community within Colorado Springs continues to grow, UCCS has been working aggressively to ensure it maintains a relevant and influential place within that growing community. Government organizations have also found value in collaborating with academic institutions to leverage knowledge, technology, and shared funding for the purpose of achieving a common goal – technological growth at an exponential pace. Based on the contributions and communal efforts of industry, academia, and Government; smaller, well-focused groups with big-dreams and even bigger hearts stand to achieve their goals.

Among these groups: PeakChaos, the UCCS Cybersecurity Club who is on the up-slope of demonstrating itself as a serious CTF competitor and as a conduit for linking its members with the Cybersecurity community at large.

About the Author

Ernest M. Campos has served as the collegiate mentor for the UCCS Cybersecurity Club for the 2015/16 and 2016/17 academic years. He is employed with the Harris Corporation as the Deputy Director of Cybersecurity for the SENSOR contract. Ernest volunteers with the ISSA-COS chapter as Chairperson for the Transformation Committee and as a professional mentor for the chapter’s Mentoring Program.

If you are interested in exploring opportunities to serve as a collegiate mentor, professional mentor, or as a chapter volunteer, please contact ISSA-COS via the chapter website. Opportunities to volunteer currently exist and the chapter will provide training and guidance to support your involvement.
I love watching reality shows about paramedics. It is thrilling to see the EMTs rush to a scene and take immediate action to save the life of some unfortunate victim. They are often forced to guess the trauma or ailment of the patient and hope that the treatment they administer is the correct one.

In cybersecurity, we often work the same way, and that is not necessarily a good thing. We are often required to make snap decisions about which files are safe and which are potentially toxic, and we are constantly rushing and responding to alerts about something bad that has already happened. As defenders, it feels as though we never have the time to take a measured, thoughtful approach.

Wouldn’t it be great if we could spend more time acting like the doctors and surgeons who work away from emergency rooms and ICUs? Doctors are afforded adequate time to assess the situation and run tests so that they can fully understand the details of the problem, and plan their response before administering treatment.

The need to decide and act in real time is one of the biggest problems for our security systems. A network gateway device has only milliseconds to decide if an observed file is safe or not and many protocols, including HTTP, cannot tolerate significant delays. As a result, we are forced to use fast but unreliable indicators to decide which files to ignore, and which to block. Like the EMT, we are up against the clock and working without enough information. Inevitably, we will allow infected files through, and wind up blocking files that are clean. False positives create a usability problem, and false negatives let malware penetrate our networks.

In emergency medicine, doctors often order tests where the results will not be known until treatment has been underway for some time. If the doctor’s diagnosis of the condition is wrong, the situation could go from bad to worse. For example, if a patient is treated for a drug overdose, and they are actually suffering from a stroke, there could be a lot of damage to the patient’s brain before they realize the error and change course on the therapy.

Similarly, many security architectures provide a second level of screening where files that originally passed the quick scan are examined more carefully. This can involve static analysis, detonation, and other approaches which are much more reliable but can take up to a couple of minutes to complete. By the time the tests indicate that a file should have been blocked it has had plenty of time to infect the endpoint. The defenders are forced to respond and recover to clean up the infection before it causes damage or spreads.

Email security is a great example of the advantages of being able to take your time. Over the last few years, email gateways have gotten really good at scanning for malware attachments. Why? Because email is a store and forward protocol. The gateway can take as much time as it needs to analyze any file. Most users will hardly notice their mail arriving in their inbox a minute or two late.

Does that mean organizations are not getting attacked through email anymore? Not at all. Just as bacteria evolved to resist antibiotics, attackers have evolved to avoid email scanners. Rather than sending malware in attachments, criminals now send links which will deliver the files through the web, pushing the defensive team back in the position of trying to make decisions in real time.

The next move is to shift web scanning from real time to at leisure. The first opportunity for this is at the email gateway itself. The scanner could check the suspicious URL to see if it delivers a file and it could then scan that file before delivering the email. Unfortunately, that strategy is easy for the attacker to counter. The attacker can make the website complex by using active content and multiple links. The scanner will find it difficult to know what will happen when the URL is opened by the user. Even worse, it is not difficult for a website to recognize a scanner and show it a different, and clean, version of the page. As a result, the malware filled version of the file will be delivered only when a human clicks that link in the email.

Read the rest here:
The Colorado Springs ISSA Chapter has over 400 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.

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 December 2, 2016 and applications will be accepted until July 10, 2017, 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 2016 ISSA International Conference. Submissions received after August 1, 2016 will be considered in the following cycle.

Familiarize yourself with the Fellow Program, and the submission guidelines (http://c.ymcdn.com/sites/www.issa.org/resource/resmgr/Fellow_Program/Fellow_Policies_Revised_June.pdf). If you have questions, contact Shawn or The ISSA Fellow Manager (fellow@issa.org) 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?

- 5 years of ISSA membership and 10 years relevant professional experience
- All Senior Member applications require an endorsement from their home chapter to qualify.

For your convenience, please feel free to use this Senior Member Application Check-list to confirm eligibility and completion of application.

To access the Senior Member application go to: https://www.issa.org/?Senior_member_App

For the Senior Member endorsement form go to: https://www.issa.org/?Senior_Mem_Endorse

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.

- 8 years of association membership, 3 years of volunteer leadership in the association and 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...
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.

- All Fellow applications require a nomination to qualify
  
  To access the Fellow application go to:
  https://www.issa.org/?Fellow_App

  To nominate a Fellow go to:
  https://www.issa.org/?Fellow_Nom

  To submit a Fellow letter of recommendation go to:
  https://www.issa.org/?Fellow_Recommend

- 12 years association membership, 5 years of sustained volunteer leadership in the association, and 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.
  
  To access the Distinguished Fellow application go to:
  https://www.issa.org/?Distinguished_Fellow

  To nominate a Distinguished Fellow go to:
  https://www.issa.org/?D_Fellow_Nom

  To submit a Distinguished Fellow letter of recommendation go to:
  https://www.issa.org/?Fellow_Recommend

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

Shawn P. Murray, Chapter Recorder
5871charlois@gmail.com, 719-362-0666
How Spy Agency Hackers Pose As – Anybody

By Levi Maxey, The Cypher Brief, April 18, 2017

A false flag operation – pretending to be someone else while conducting spycraft or warfare – is an age-old tactic. With the advent of cyber espionage and digital warfare, those maneuvering in the virtual domain can use false flags.

In the Digital Age, determining the origins of cyber attacks is already difficult, but cyber actors can further muddy attribution by diverting blame for attacks to others. Ultimately, are such devious methods effective in leading investigators astray, even to the point of mistaken retaliation? The answer is, it’s complicated.

By definition, false flag operations that succeed in framing others will not appear to observers as a false flag at all, and blame will likely fall on those who are framed. On the other hand, investigators may see through attempts at a false flag, but they may not know whether the perpetrator’s intention was to deceive everyone or a select few. In some cases, the attacker may have wanted simply to cloud the issue so that the victim can’t make a strong case for a forceful response.

The term false flag originated in naval warfare. It referred to ships that hoisted the flags of other nations to shift blame or confuse an enemy. Sometimes ship crews even donned uniforms with emblems from a third nation. Tim Maurer, the co-director of the Cyber Policy Initiative at the Carnegie Endowment for International Peace, cites the example of the British navy ship Baralong, which flew the American flag before the U.S. entered World War I, and fired on a German U-boat.

False flag operations in cyberspace – like those in the physical world – are difficult to identify with confidence. Unless investigators have intelligence to confirm that a false flag operation occurred, most examples are based on conjecture.

One incident generally accepted as a false flag operation took place in April 2015, when hackers targeted TV5Monde, corrupting and destroying internet-connected hardware that controlled the French news channel’s operations, knocking its broadcast offline. A supposedly ISIS-affiliated group calling itself the Cyber Caliphate lodged a claim of responsibility, but forensic investigators and French intelligence quickly focused their suspicions on another group called APT28, purportedly connected to Russian military intelligence.

The TV5Monde false flag play was relatively simple. All it took was a fake online persona and a misleading statement of culpability. Other modes of false flag operations can be more technically deceptive.

In a white paper published last October, researchers from Kaspersky Lab, a Moscow-based cybersecurity firm, explored a 2015 espionage campaign targeting the Peruvian military and other government agencies. The attackers, nicknamed TigerMilk, used a stolen digital certificate that had showed up in the Stuxnet worm, a piece of weaponized code that famously sabotaged Iranian nuclear installations. The Equation Group, thought to be a hacking unit of the National Security Agency, originally employed the purloined certificate to gain surreptitious access to the Microsoft Windows systems. However, Microsoft had since revoked the certificate, suggesting that the actors who deployed it were not sophisticated and therefore couldn’t possibly be the NSA – one of the most capable cyber operators in the world. By using the certificate, despite no apparent tactical value, the hackers were seemingly attempting to direct investigators to conclude, erroneously, that the U.S. was culpable.

Maurer says false flag attackers can mislead forensic investigators by creating a scenario that suggests that “malicious activity originates from whomever the attacker is trying to frame.” Another red herring, he says, is “to use malware that’s been tied to another malicious actor as part of the offensive cyber operation.”

To lay a false trail, he says, “sophisticated actors could use hackers skilled in other languages and keyboards or operate only during certain times that correspond with whatever time zone the actor who’s to be blamed operates in.” Hackers bent on framing somebody else could hijack the known attack infrastructure of that entity to leave a trail of false clues for forensic investigators.

Misdirection through language imitation is a tactic recently attempted by the Lazarus group, which is thought to be an arm of the North Korean regime, has been held responsible for the December 2014 attack on Sony Pictures and is suspected of various attacks around the world targeting the global SWIFT banking system. Pyongyang’s hackers did a bad job of writing fake Russian comments into their malware. Native Russian speakers quickly noticed these anomalies, causing experts to believe the imbroglio was a sloppy attempt by the North Koreans to finger the notorious Russian-speaking hacking community – both criminal and government.

Read the rest here: https://www.thecipherbrief.com/article/tech/how-spy-agency-hackers- proported-attackers-1092
What home products are most susceptible to cyber burglars?

By Ryan Francis, CSO Online, April 5, 2017

No matter how intelligent they claim to be, many smart home gadgets are vulnerable to hackers. Nowadays even the lock on your front door is susceptible to a cyberattack. No longer do you only have to worry about someone simply picking the lock, now a burglar could go through cyberspace to unlatch the door.

Just like the lock on your front door to keep out burglars, you should protect your high-tech devices from cyber threats. Start by choosing different passwords for your internet router and each of your smart devices. It is also important to use multi-factor authentication as an added protection to prevent a hacker who guesses your password from breaking into your home. You should regularly install manufacturer updates to make sure you are running the most current security system in your home.

Ovum's "Smart Home Devices Forecast: 2016–21" found that the largest smart home markets will be China and the US, because of high availability of devices and greater consumer interest in smart home services and products. Device sales will grow to more than 1.4 billion units by 2021, up from 224 million in 2016, driven particularly by sales of security devices, such as cameras, door locks, and sensors, and by utilities devices, such as connected light bulbs and smart thermostats. Ovum predicts that each smart home household will use on average 8.7 devices, bringing the total smart home active installed base to 4 billion devices.

In the matter of the Dyn situation, it was those Internet of Things devices that created the voluminous distributed denial of service attack. A DVR was used to attack Dyn’s network. To reduce the impact of such attacks, officials at InsuranceQuotes have noted some of the more popular smart home gadgets in your home that could be vulnerable.

The smart hub: This is the virtual key to your home. It serves as the central monitoring station that all of your smart home devices connect to, and alerts emergency responders when something is wrong. By hacking into the Hub, cyber criminals can gain entry to your home. Smart Hubs can fall victim to jammers that block the signal between your various smart gadgets and the Hub. So make sure they come with anti-jamming software that detects these intrusions.

Smart surveillance cameras: These cameras monitor your home for burglars, but they can also give cyber criminals a peek inside. This could help burglars figure out when you are away from home, and where you hide your most valuable possessions. Protect your home by choosing a difficult password and setting up multi-factor authentication, so they won’t have eyes inside your home.

Smart locks: These locks are designed to secure your home from burglars, but some are prone to hacking. Secure your home by changing your password often and setting up multi-factor authentication, so intruders can’t walk right in the front door. Also, make sure you have an old fashioned, hard key as a backup, in case of total failure.

Smart garage doors: These garage doors conveniently open when you’re heading home from the grocery store, or a long day at work. But they have also proven to be vulnerable to hackers, who can gain access to your home through the garage. Protect your garage by choosing a difficult password and always have a manual way to access the area.

Smart thermostats: These thermostats make it easy to adjust the temperature in your home without getting out of bed. But they are also vulnerable to hackers, who can make your life miserable by cranking up the heat in the summer, or running the air conditioning in the winter. Protect yourself from pranksters by encrypting your password and setting up multi-factor authentication.

Smart lights: These lights come in handy when you’re at work and realize you left the kitchen lights on. But if they fall into the wrong hands, a hacker could keep you up all night — not to mention, raise your electricity bill — by flicking the lights on and off. Or, they could cut the lights before a break-in. Stay in control of your lights by changing your password frequently and setting up multi-factor authentication.

Read the rest here: http://www.csoonline.com/article/3186808/security/what-home-products-are-most-susceptible-to-cyber-burglars.html

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!
NSA, DOE say China's supercomputing advances put U.S. at risk

By Patrick Thibodeau, Computerworld, March 15, 2017

Advanced computing experts at the National Security Agency and the Department of Energy are warning that China is "extremely likely" to take leadership in supercomputing as early as 2020, unless the U.S. acts quickly to increase spending.

China's supercomputing advances are not only putting national security at risk, but also U.S. leadership in high-tech manufacturing. If China succeeds, it may "undermine profitable parts of the U.S. economy," according to a report titled U.S. Leadership in High Performance Computing by HPC technical experts at the NSA, the DOE, the National Science Foundation and other agencies.

"To maintain U.S. leadership in HPC," the report says, "a surge" of U.S. "investment and action is needed to address HPC priorities."

Concern about China's technical advances have been raised before by U.S. scientists and industry groups, but never in such striking terms -- or by representatives of a spy agency.

The report stems from a workshop held in September that was attended by 60 people, many scientists, 40 of whom work in government, with the balance representing industry and academia. The report, which summarizes that meeting, was just posted online.

The threat from China is so acute that "absent aggressive action by the U.S. -- the U.S. will lose leadership and not control its own future in HPC," the report states.

Indeed, the report says that "assuming status quo conditions, the meeting participants believe that a change in HPC leadership was extremely likely, with only minor disagreement on the timescale; many suggested that China would be leading the U.S. as early as 2020."

China supercomputing systems have been leading the Top 500 list, the global ranking of supercomputers, for several years. But that's not a measure of supercomputing leadership alone.

One workshop attendee, Paul Messina, a computer scientist and distinguished fellow at Argonne National Labs and the head of its Exascale Computing Project, sketched out the HPC leadership criteria: It means leadership in producing and using systems, as well as "first mover advantage." It also means staying in the lead at all times. The U.S. needs to control its HPC destiny and "can't depend on other countries to sell us what we need," he said in an email.

Something to keep in mind is that this report was written at a time when many assumed that supercomputing funding was not under threat. The report calls for more spending while the Trump administration, along with the Republican-controlled Congress, is planning major cuts in the federal budget.

"National security requires the best computing available, and loss of leadership in HPC will severely compromise our national security," the report says. "Loss of leadership in HPC could significantly reduce the U.S. nuclear deterrence and the sophistication of our future weapons systems."

Among those at the meeting was Barry Bolding, a senior vice president and chief strategy officer at supercomputer company Cray. "I will say from Cray's view, [the report] accurately reflects the discussion of the workshop and mostly accurately reflects some of our primary concerns regarding HPC competitiveness."

Steve Conway, an HPC analyst and research vice president at Hyperion Research, said the meeting "and report are important for alerting the U.S. HPC community, especially government officials, to the dangers of taking U.S. HPC leadership for granted when other nations, particularly China, are intent on seizing global leadership of the market for supercomputers."

The report makes three overarching observations about China's Sunway TaihuLight system, which at 93 petaflops, is ranked first on the Top500 list of supercomputers.

The TaihuLight supercomputer is "homegrown," and includes processors that were designed and fabricated in China. The Chinese chip design "includes architectural innovations," and was designed using "a true co-design approach" where the applications are tuned to take advantage of the chip design, the report said.

The machine "is not a stunt," the report notes, meaning China didn't develop this system for bragging rights. The machine "is being used for cutting edge research," and three of the six finalists for the Gordon Bell Prize, the top research award in HPC, were the result of Chinese efforts.

The report offers something particularly insightful about China's motivations.

"Meeting participants, especially those from industry, noted that it can be easy for Americans to draw the wrong conclusions about what HPC investments by China mean -- without considering China's motivations," the report states.

Read the rest here:

Link to the report:
March Cyber Focus Day

ISSA Photos are courtesy of our Chapter Photographer Warren Pearce.
The Information Systems Security Association (ISSA)® is a not-for-profit, international organization of information security professionals and practitioners. It provides educational forums, publications, and peer interaction opportunities that enhance the knowledge, skill, and professional growth of its members.

The primary goal of the ISSA is to promote management practices that will ensure the confidentiality, integrity, and availability of information resources. The ISSA facilitates interaction and education to create a more successful environment for global information systems security and for the professionals involved. Members include practitioners at all levels of the security field in a broad range of industries such as communications, education, healthcare, manufacturing, financial, and government.

Article for the Newsletter?
If you would like to submit an article...

Do you have something that the Colorado Springs ISSA community should know about? Tell us about it!
We are always looking for articles that may be of interest to the broader Colorado Springs security community.
Send your article ideas to Don Creamer at:
doncreamer@outlook.com
Ensure that “Newsletter” is in the subject line.
Looking forward to seeing you in print!

Even the World’s Largest Internet Companies Get Phished, Just Like Your Grandma
By Libby Watson, Gizmodo, April 28, 2017

If you’ve ever been duped by a phishing scam, you can feel a little less stupid about it today, because you’ve been joined in that sad club by Google and Facebook.

Phishing attacks, where scammers pose as a trusted company or person via email and trick people into—for example—clicking a link, signing into a fake website, or even handing over their bank details, are a huge problem. And it works surprisingly often, particularly on older people (and senior members of Hillary Clinton’s campaign staff). But it seems even the world’s largest internet companies—organizations that have shaped the internet itself—are not immune from such attacks.

Read the rest here:
http://gizmodo.com/even-the-worlds-largest-internet-companies-get-phished-1794741454