Annual Cyber Security Training and Technology Forum (CSTTF)

Colleagues,

CSTTF conference is on 24 and 25 August at the Double Tree Hilton Hotel on Lake Avenue. If you have not registered for this event, I ask that you go look at the agenda. Also talked to co-workers and friends about signing up for the event. Would like to see the attendance at 500 plus this year. To sign up for the event go to https://www.fbcinc.com/e/CSTTF/.

As with any conference that the chapter sponsors we will need volunteers. We will need a couple of people to be at the sign in desk, people to sit at the ISSA table and finally people to help introduce the speakers. The more people that we have to help the less time each one of us will have to do. If you are interested in helping please email me at thornbuc@aol.com.

I will be setting up the schedule and letting everyone know where and when. I know we have a lot of people in the chapter that wants to help and this is a small way to do that.

Cindy

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

The views expressed in articles obtained from public sources within this newsletter do not necessarily reflect those of ISSA, this Chapter or its leadership.
By Joseph Cox, Motherboard, June 26, 2016

Because users are protected by a veil of technological anonymity, the dark web is often portrayed as a space beyond the reach of law enforcement, where criminals can run amok without fear of prosecution.

That couldn’t be more wrong.

In fact, police all over the world have deployed a wide array of different techniques to identify and ultimately convict dark web drug dealers, weapon buyers, child pornographers, and more in the past several years. If anything, law enforcement agencies have become more accustomed to working in this space, and are likely to develop even more ways to bust technologically savvy criminals.

Just like in analog investigations, going undercover on the dark web can be a highly effective tactic. For six months, investigators posed as a weapons seller. Naturally, anyone wanting to purchase guns had to provide a postal address, making it fairly trivial for the police to then link real identities to potential customers. In all, law enforcement busted over a dozen people. Similar operations have been carried out against those trying to buy poisons.

Undercover agents have also penetrated wider dark web organisations. On the original Silk Road, authorities took over the account of a staff member. The impostor gained so much trust that they were quickly invited straight into the site’s replacement, launched in late 2014. From the very start of the second Silk Road, investigators already had a man on the inside, able to contact directly with the marketplace’s owners, and feed information to other agents. In Australia, Queensland Police’s Task Force Argos assumed the role of a notorious child abuse site administrator for months, leading to the arrest of pedophiles all over the world.

In a way, law enforcement have taken advantage of the protections offered by Tor to blend in with everyone else—on the dark web, you never really know who is on the other end of a conversation.

One way to circumvent Tor is to attack the endpoint; that is, the computers of users themselves. That’s what the FBI did on a massive dark web child pornography site called Playpen: the agency deployed malware so that when a user clicked on a child pornography related forum their real IP address was sent to investigators, revealing their likely location. (The FBI seized Playpen after the administrator had misconfigured the site, exposing its IP address to the normal internet).

Hacking could quite possibly be the most effective way of identifying people on the dark web, at least judging by the number of computers unmasked. As part of the operation, the FBI harvested over 1000 US based IP addresses, and Europol generated 3,229 of its own cases. Those leads won’t all necessarily lead to convictions, but over 135 people have been charged in the US so far, and new cases keep on rolling in. The FBI has used this mass-hacking approach several times, and could very well have hit innocent users of a privacy focused email service.

At least one foreign law enforcement agency has hacked dark web suspects too. In December 2014, the unnamed agency sent a child pornography site moderator a link to a video, which was configured to route their traffic outside of the Tor network.

Another hack didn’t attack endpoints, but abused a vulnerability in Tor itself, allowing researchers from Carnegie Mellon University’s Software Engineering Institute (SEI) to learn the IP addresses of dark web marketplaces as well as users. Even though this attack wasn’t carried out by the FBI itself, the feds just subpoenaed SEI for the identifying information. SEI’s research was carried out back in the first half of 2014, but likely related convictions are still coming through: a man recently pleaded guilty to running a dark web marketplace after the FBI fed UK police with a slew of IP addresses.

Read the rest here:
Membership Update

We are continuing to increase our membership—up to 426 members as of the end of June. We are successfully increasing our membership with renewals and new memberships—both general and students. 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 will continue to push our Freemium student program. We currently have 29 Freemium students as well as several other student members. We will be trying to track participation metrics to support our case for making the Freemium program a permanent program within ISSA. I would personally appreciate hearing from our Freemium students periodically regarding what activities they have participated in as well as their perspective on those activities. Were they relevant and useful? Any ideas to improve our activities would also be welcome. Your inputs will be critical to our ability to “sell” the Freemium program to the ISSA International board so please take a couple of minutes and provide some feedback to us. The easiest way would be a quick email to me at dreed54321@comcast.net.

I would also 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

<table>
<thead>
<tr>
<th>New Members</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Rey Garate</td>
<td></td>
</tr>
<tr>
<td>Erik Henrickson</td>
<td></td>
</tr>
<tr>
<td>Theresa Johnson-Akse</td>
<td></td>
</tr>
<tr>
<td>David Guthrie</td>
<td></td>
</tr>
<tr>
<td>Abdullah Abumouzah</td>
<td></td>
</tr>
<tr>
<td>Matthew Bradley</td>
<td></td>
</tr>
<tr>
<td>Sidney Bernard</td>
<td></td>
</tr>
<tr>
<td>Qwincy Houston</td>
<td></td>
</tr>
</tbody>
</table>

Update Your Profile!

Don’t forget to periodically logon to www.issa.org and update your personal information.
The Big Hack
The day cars drove themselves into walls and the hospitals froze


On December 4, 2017, at a little before nine in the morning, an executive at Goldman Sachs was swiping through the day’s market report in the backseat of a hired SUV heading south on the West Side Highway when his car suddenly swerved to the left, throwing him against the window and pinning a sedan and its driver against the concrete median. A taxi ran into the SUV’s rear fender and spun into the next lane, forcing a school-bus driver to slam on his brakes. Within minutes, nothing was moving from the Intrepid to the Whitney. When the Goldman exec came to, his driver swore that the crash hadn’t been his fault: The car had done it.

Moments later, on the George Washington Bridge, an SUV veered in front of an 18-wheeler, causing it to jackknife across all four lanes and block traffic heading into the city. The crashes were not a coincidence. Within minutes, there were pileups on 51st Street, the southbound BQE, as far north as the Merritt Parkway, and inside the Midtown Tunnel. By nine, Canal Street was paralyzed, as was the corner of 23rd and Broadway, and every tentacle of what used to be called the Triborough Bridge. At the center of each accident was an SUV of the same make and model, but as the calls came in to the city’s 911 centers in the Bronx and Brooklyn, the operators simply chalked them up to Monday-morning road rage. No one had yet realized that New York City had just been hit by a cyberattack — or that, with the city’s water system, mass transportation, banks, emergency services, and pretty much everything else now wired together in the name of technological progress, the worst was yet to come.

A third-year resident in the emergency room at Columbia University Medical Center in Washington Heights walked through the hospital as a television was airing images from the accident on the George Washington Bridge: that meant several crash victims would soon be heading her way. When she got to her computer, she tried logging into the network to check on the patients who were already there, but she was greeted with an error message that read WE’RE NOT LOOKING FOR BITCOIN THIS TIME.

Columbia, like major institutions across the country, had spent the past few years fighting so-called ransomware attacks, in which hackers locked a hospital or city hall or police department out of its own network until a ransom was paid. Hospital security teams had gotten wise to the problem, but every network’s defenses had the same vulnerability: the people who used it. For weeks, a group of hackers had been sending LinkedIn messages to employees at Columbia pretending to be recruiters from Mount Sinai. When an employee opened an attachment featuring the recruiting pitch — as ten of them did — and enabled the macros as prompted onscreen — four of them did — they unknowingly unleashed malware onto their computer and gave the hackers a beachhead. After months of lurking, the hackers blocked Columbia’s doctors and nurses from accessing their network, including patient files. Doctors couldn’t access prescription records telling them which patients were scheduled to take which drugs when and resorted to improvised paper-record keeping, which many of the younger doctors had never done before. In nearly every corridor, they were consulting with one another in a panic, asking how much of their own expertise was really stored in the cloud and had just disappeared.

The crowd in the waiting room swelled and grew more tense as nurses ran by patients, unable to give updates on when they might be seen. Various procedures were taking longer than they should have — one man was kept on a powerful antibiotic for several hours, with serious side effects, before a delayed lab result came back reporting that he should go off the medication — and the staff was having trouble keeping track of patients. A little before noon, a man walked into the hospital looking for his wife, whom he had dropped off early that morning for a simple surgical procedure. A few minutes later, the nurse told him that it appeared his wife had been discharged.

Most New Yorkers were proceeding with their day unaware. But the city’s head of cybersecurity had begun to connect the dots: Six hospitals had already informed him that their systems had been shut down, and the city had sent out warnings to all the others. One Police Plaza had just reported that it, too, was locked out of the programs it used to dispatch officers and emergency personnel, which made responding to the traffic accidents around the city that much harder.

After a few phone calls to friends in the private sector, the cybersecurity chief got more nervous. At the beginning of 2017, one friend told him, she had been called to investigate a mysterious occurrence at a water-treatment plant: The valves that controlled the amount of chlorine released into the water had been opening and closing with unexplained irregularity. An alarm had gone off, so none of the tainted water had reached consumers, and the company’s CEO brushed off the consultant’s request to make the news public so others could prepare for similar attacks.

Read the rest here:
http://nymag.com/daily/intelligencer/2016/06/the-hack-that-could-take-down-nyc.html
Crafty plan to give FBI warrantless access to browser histories axed

By Iain Thomson, The Register, June 11, 2016

A sly attempt to grant the FBI warrantless access to people's browser histories in the US has been shot down by politicians.

Unfortunately, the Electronic Communications Privacy Act (ECPA) Amendments Act of 2015, which would have brought in some privacy safeguards for Americans, was cut down in the crossfire.

The ECPA Amendments Act is very simple: it amends the 1986 Electronic Communications Privacy Act, which gives cops and agents warrantless access to any email that has been read or is more than 180 days old.

That 30-year-old act made sense back in the day of 20MB hard drives and when we stored own emails on our own computers: if we deleted something to save space or to simply destroy it, it was gone. But in today's cloudy world, where we have no real control over our information, it has proven a privacy nightmare. (By the way, the ECPA was used against Microsoft by the Feds in New York in 2014 to demand emails from a data center in Ireland.)

The ECPA Amendments Act of 2015 would have eliminated the 180-day rule, and ensures investigators get a warrant for the contents of emails.

In a stunning display of bipartisanship, the House of Representatives voted unanimously for their version of the updated law, the Email Privacy Act, in April, and the President gave it his full backing. The ECPA Amendments Act was expected to therefore breeze through the Senate, and into the law books, but now it's been put on hold by its sponsors.

The reason for the halt is the amendment tacked on by Senator John Cornyn (R-TX) on Tuesday that would allow the FBI to obtain someone's internet browsing history and the metadata of all their internet use without a warrant. If Cornyn's amendment was passed, the Feds would simply have to issue a National Security Letter (NSL) to get the information.

Organizing an NSL is a lot easier than getting a warrant, and the FBI posts thousands every year with very little judicial oversight. In the past, the Feds claimed the letters granted them access to citizens' internet history, but this was ruled unlawful in 2008.

The bill's sponsors, Senators Patrick Leahy (D-VT) and Mike Lee (R-UT), told a session of the Senate Committee on the Judiciary that Cornyn's amendment had wrecked years of careful bipartisan negotiations and would seriously harm US citizens' privacy. As such, they weren't prepared to let the bill go forward.

"The Cornyn National Security Letters amendment is something that I cannot in good conscience have attached to this bill," said Lee. "We want to make sure that when we get this passed, it enhances rather than diminishes our interests protected by the Fourth Amendment."

Responding to Senator Cornyn's claims that his amendment allows g-men to get their hands on "just metadata" cut no ice with people who understand how revealing this information can be. Lee also accused Cornyn of sharp practice by waiting until the last few days before a vote could be scheduled to introduce his controversial amendment, which would not be accepted by the House.

His cosponsor, Senator Leahy, was equally cutting, accusing Cornyn of introducing a "poison pill" amendment to the legislation at the last minute that wouldn't pass in the Senate or the House of Representatives. He accused Cornyn of trying to "tank" the bill.

"I worry about getting into what has been a slippery slope in the past with these National Security Letters," Leahy said. "We all know the real scandal in the FBI – even under good leadership – when National Security Letters were used by low-ranking members of the FBI for what appeared to be vendettas, sometimes destroying people's businesses."

That law enforcement promised that they would be used wisely wasn't reassuring, he said, because similar assurances had been given in the past. J Edgar Hoover had used his powers to make the FBI into an instrument of control and that could not be allowed to happen again, he opined.

But Senator Cornyn was unfazed by the furor and said he would carry on pushing for his amendment, saying it was critical in the fight against terrorism. He said getting access to this metadata was the "number-one legislative priority" of the FBI's director, James Comey, and that the House of Representatives would support it "whether they liked it or not."

Read the rest here:
http://www.theregister.co.uk/2016/06/11/poison_pill_amendment_email_privacy/
Russian ISPs will need to store content and metadata, open backdoors

By Glyn Moody, ArsTechnica, June 28, 2016

Russia's lower house of parliament, the State Duma, has approved a series of new online surveillance measures as part of a wide-ranging anti-terrorism law. In a tweet, Edward Snowden, currently living in Russia, wrote: "Russia's new Big Brother law is an unworkable, unjustifiable violation of rights that should never be signed."

As well as being able to demand access to encrypted services, the authorities will require Russia's telecom companies to store not just metadata, but the actual content of messages too, for a period of six months. Metadata alone must then be held for a total of three years, according to a summary of the new law on the Meduza site. Authorities will be able to access the stored content and metadata information on demand.

Snowden pointed out the difficulties of implementing the new law: "'Store 6 months of content' is not just dangerous, it's impractical. What is that, ~100PB of storage for even a tiny 50Gbps ISP?" He added: "This bill will take money and liberty from every Russian without improving safety."

Three of Russia's largest telecom companies agreed. According to The Washington Times, the three companies—MTS, Megafon and Vimpelcom—"have each publicly rejected the proposal and said it would require infrastructure that would cost more to build and maintain than the companies could ever make. Yandex, a Russian search engine, said legislation would cause an "excessive limitation of the rights of the companies and users."

The Telegraph quotes Andrei Soldatov, an expert on the Russian security services, as saying that it would be "technically impossible to implement the eavesdropping measures." However, he suggested the Russian authorities were well aware of that: "The real objective doesn't seem to be surveillance, but to intimidate companies into cooperating with the authorities ahead of parliamentary elections in September."

Another measure aims to rein in social media. Meduza's summary explains: "Publishing online incitements to terrorism, or even expressing approval of terrorism on the Internet, will be regarded legally as publishing such comments in the mass media, subjecting individuals to the same strict penalties now imposed on media outlets." The maximum sentence for this is seven years of imprisonment.

Russia already has thoroughgoing surveillance operations in place, including SORM. The European Court of Human Rights ruled that the system of secret interception of mobile telephone communications in Russia violated the European Convention on Human Rights.

The new law has been drafted and promoted by the right-wing politician Irina Anatolyevna Yarovaya. Wikipedia says of her: "She gained fame as the author and co-author of multiple controversial, very unpopular and very low-quality laws, including the toughening of responsibility for violation of the rules of holding rallies, tightening immigration, criminal libel, and registration requirements for 'foreign agents' for non-profit organisations with foreign funding."

Two of the harshest measures proposed in the original draft of the new law—the ability to revoke convicted criminals' Russian citizenship and their right to travel abroad—were dropped at the last moment.

TRAINING POLICY: Specialized Cyber Personnel with Specialized Credentials

By Kurt Danis, ISSA-COS, July 1, 2016

This article briefly describes some of the emerging DoD cybersecurity qualification policies and follow-on initiatives.

Professional development standards are stepping up. Military, civilian, and defense contract personnel fulfilling specialty cyber roles are facing more stringent cybersecurity job requirements that include more advanced levels of experience, degrees, and certifications. “Core” cyber professionals in the DoD must meet higher cyber IT and cybersecurity management qualification requirements. Furthermore, to maintain these standards, military personnel systems are being updated and used “…to identify and track personnel, positions, and [certification] status…” metrics.

For example, while the Army Training and Certification Tracking System (ATCTS) has been around for many years, the latest update reflects alignment with the new DoD Directive 8140.01, DoD Cyberspace Workforce Framework (DCWF) initiative. Army personnel assigned to cybersecurity positions are required to report their credentials in ATCTS. Army cybersecurity requirements are more specific and rigorous. “The DCWF is based on the integration of the National Initiative for Cybersecurity Education (NICE) workforce framework and the Joint Cyberspace Training and Certification Standards (JCT&CS), both of which reflect foundational contributions from the National Security Agency, to provide a lexicon of work roles by area of specialty, each with a baseline set of required knowledge, skills, and abilities (KSA) as well as functions.”

Air Force Manual (AFMAN) 33-285 with Change 1 effective 26 May 2016, defines special experience identifies (SE) codes essentially represent specific military or civilian cyber positions; each one mandating a required DoD Approved Baseline Certification (i.e. the certifications published by DISA and referenced by the current DoD 8570 Manual).

Likewise, the Secretary of the Navy Manual (SECNAV M-5239.2), dated 27 June 2016, using a similar term defines specialty area (SA) codes, and mandates “Civilian, military, and contracted support personnel assigned to perform cyberspace specialty area tasks must meet qualification standards....” Similar to the paygrade alignment for advanced cybersecurity positions in the Air Force, the general construct for proficiency levels in the Navy is outlined here:

A. Entry/Apprentice – Basic understanding of computer systems and related cybersecurity software and hardware components.
   1. 1-3 years’ experience (recommended)
   2. Enlisted E-1 through E-4
   3. Officer O-1 through O-2
   4. Civilian Grades 5, 7, and 9

B. Intermediate/Journeyman – Working knowledge and application of [information system (IS)] and security operational characteristics for a variety of computer platforms, networks, software applications, and OSs.
   1. 4-6 years’ experience (recommended)
   2. Enlisted E-5 through E-6
   3. Officer O-3 through O-4
   4. Civilian Grades 9, 11, 12

C. Expert – Advanced application and mastery of IS, plans, and functions, and is responsible for the management of complex projects, and initiatives with large scope.
   1. 7+ years’ experience (recommended)
   2. Enlisted E-7 through E-9
   3. Officer O-5 through O-6/W-1 through W-5
   4. Civilian Grades 13 and above

Finally, where many defense contractor personnel are highly experienced and certified, the impact may not be so great. Nevertheless, the expectation for specialized credentials will generally be the same. The difference lies in the burden for training time, training cost, and travel – which typically rest on the contractor or the contractor’s employer unless provisioned by the contract.

In conclusion, cyber professions who progress professionally will continue to discover great opportunities.
It’s Way Too Easy to Hack the Hospital

By Monte Reel and Jordan Robertson, Bloomberg, November, 2015

In the fall of 2013, Billy Rios flew from his home in California to Rochester, Minn., for an assignment at the Mayo Clinic, the largest integrated nonprofit medical group practice in the world. Rios is a “white hat” hacker, which means customers hire him to break into their own computers. His roster of clients has included the Pentagon, major defense contractors, Microsoft, Google, and some others he can’t talk about.

He’s tinkered with weapons systems, with aircraft components, and even with the electrical grid, hacking into the largest public utility district in Washington state to show officials how they might improve public safety. The Mayo Clinic job, in comparison, seemed pretty tame. He assumed he was going on a routine bug hunt, a week of solo work in clean and quiet rooms.

But when he showed up, he was surprised to find himself in a conference room full of familiar faces. The Mayo Clinic had assembled an all-star team of about a dozen computer jocks, investigators from some of the biggest cybersecurity firms in the country, as well as the kind of hackers who draw crowds at conferences such as Black Hat and Def Con. The researchers split into teams, and hospital officials presented them with about 40 different medical devices. Do your worst, the researchers were instructed. Hack whatever you can.

Like the printers, copiers, and office telephones used across all industries, many medical devices today are networked, running standard operating systems and living on the Internet just as laptops and smartphones do. Like the rest of the Internet of Things—devices that range from cars to garden sprinklers—they communicate with servers, and many can be controlled remotely. As quickly became apparent to Rios and the others, hospital servers, and many can be controlled remotely. As quickly from cars to garden sprinklers, and even with the electrical grid, hacking into the largest public utility district in Washington state to show officials how they might improve public safety. The Mayo Clinic job, in comparison, seemed pretty tame. He assumed he was going on a routine bug hunt, a week of solo work in clean and quiet rooms.

But when he showed up, he was surprised to find himself in a conference room full of familiar faces. The Mayo Clinic had assembled an all-star team of about a dozen computer jocks, investigators from some of the biggest cybersecurity firms in the country, as well as the kind of hackers who draw crowds at conferences such as Black Hat and Def Con. The researchers split into teams, and hospital officials presented them with about 40 different medical devices. Do your worst, the researchers were instructed. Hack whatever you can.

Like the printers, copiers, and office telephones used across all industries, many medical devices today are networked, running standard operating systems and living on the Internet just as laptops and smartphones do. Like the rest of the Internet of Things—devices that range from cars to garden sprinklers—they communicate with servers, and many can be controlled remotely. As quickly became apparent to Rios and the others, hospital administrators have a lot of reasons to fear hackers. For a full week, the group spent their days looking for backdoors into magnetic resonance imaging scanners, ultrasound equipment, ventilators, electroconvulsive therapy machines, and dozens of other contraptions. The teams gathered each evening inside the hospital to trade casualty reports.

“Every day, it was like every device on the menu got crushed,” Rios says. “It was all bad. Really, really bad.” The teams didn’t have time to dive deeply into the vulnerabilities they found, partly because they found so many—defenseless operating systems, generic passwords that couldn’t be changed, and so on.

The Mayo Clinic emerged from those sessions with a fresh set of security requirements for its medical device suppliers, requiring that each device be tested to meet standards before purchasing contracts were signed. Rios applauded the clinic, but he knew that only a few hospitals in the world had the resources and influence to pull that off, and he walked away from the job with an unshakable conviction: Sooner or later, hospitals would be hacked, and patients would be hurt. He’d gotten privileged glimpses into all sorts of sensitive industries, but hospitals seemed at least a decade behind the standard security curve.

“Someone is going to take it to the next level. They always do,” says Rios. “The second someone tries to do this, they’ll be able to do it. The only barrier is the goodwill of a stranger.”

Rios lives on a quiet street in Half Moon Bay, a town about 25 miles south of San Francisco, pressed against a rugged curl of coastline where scary, 50-foot waves attract the state’s gutsiest surfers. He’s 37, a former U.S. Marine and veteran of the war in Iraq. In the Marines, Rios worked in a signal intelligence unit and afterward took a position at the Defense Information Systems Agency. He practices jiu-jitsu, wanders the beach in board shorts, and shares his house with his wife, a 6-year-old daughter, and a 4-year-old son. His small home office is crowded with computers, a soldering station, and a slew of medical devices.

Shortly after flying home from the Mayo gig, Rios ordered his first device—a Hospira Symbiq infusion pump. He wasn’t targeting that particular manufacturer or model to investigate; he simply happened to find one posted on EBay for about $100. It was an odd feeling, putting it in his online shopping cart. Was buying one of these without some sort of license even legal? he wondered. Is it OK to crack this open?

Infusion pumps can be found in almost every hospital room, usually affixed to a metal stand next to the patient’s bed, automatically delivering intravenous drips, injectable drugs, or other fluids into a patient’s bloodstream. Hospira, a company that was bought by Pfizer this year, is a leading manufacturer of the devices, with several different models on the market. On the company’s website, an article explains that “smart pumps” are designed to improve patient safety by automating intravenous drug delivery, which it says accounts for 56 percent of all medication errors.

Read the rest here:
Proprietary Algorithms Are Being Used To Enhance Criminal Sentences And Preventing Defendants From Challenging Them

By Tim Cushing, TechDirt, June 24, 2016

When law enforcement agencies want to know what people are up to, they no longer have to send officers out to walk a beat. It can all be done in-house, using as many data points as can be collected without a warrant. Multiple companies offer “pre-crime” databases for determining criminal activity “hot spots,” which allow officers to make foregone conclusions based on what someone might do, rather than what they’ve actually done.

Not that it’s doing much good. For all the time, money, and effort being put into it, the databases seem to be of little utility.

Many law enforcement agencies use software to predict potential crime hot spots, and the police in Kansas City, Mo., and other places have used data to identify potential criminals and to try to intervene.

[...]

In Chicago, where there has been a sharp rise in violent crime this year, the police have used an algorithm to compile a list of people most likely to shoot or be shot. Over Memorial Day weekend, when 64 people were shot in Chicago, the police said 50 of the victims were on that list.

So much for "intervention." Having a list of people who have a higher risk of being shot doesn’t mean much when all it’s used for is confirming the database’s hunches. However, these same databases are being put to use in a much more functional way: determining sentence lengths for the criminals who have been arrested.

When Eric L. Loomis was sentenced for eluding the police in La Crosse, Wis., the judge told him he presented a "high risk" to the community and handed down a six-year prison term.

The judge said he had arrived at his sentencing decision in part because of Mr. Loomis’s rating on the Compas assessment, a secret algorithm used in the Wisconsin justice system to calculate the likelihood that someone will commit another crime.

We’re locking up more people for more years based on criminal activity they’ll no longer have the option of possibly performing. This is nothing new. Sentencing enhancement is based on a lot of factors, not all of them confined to proprietary databases. But what is new are the algorithms used to determine these sentence enhancements, most of which belong to private companies who are completely uninterested in sharing this crucial part of the equation with the public.

In Mr. Loomis’ case, the software determined he would be likely to engage in further criminal activity in the future. A so-called "Compas score" -- provided by Northpointe Inc. -- resulted in a six-year sentence for eluding an officer and operating a vehicle without the owner's consent. His lawyer is challenging this sentence enhancement and going after Northpointe, which refuses to release any information about how the Compas score is compiled.

What Northpointe has released are statements that confirm the code is proprietary and that the Compas score is "backed by research" -- although it is similarly unwilling to release this research.

The problem here isn't so much the use of algorithms to determine sentence lengths. After all, state and federal guidelines for sentence lengths are used all of the time during sentencing, which includes factors such as the likelihood of future criminal activity. But these guidelines can be viewed by the public and are much more easily challenged in court.

The use of private contractors to provide input on sentencing renders the process opaque. Defendants can't adequately challenge sentence enhancements without knowing the details of the "score" being presented by prosecutors to judges. The algorithms' inner workings should either be made available to defendants upon request, or the "score" should be determined solely by government agencies, where the data and determining factors can be inspected by the public.

We're now in the unfortunate situation where companies are telling judges how long someone should be locked up -- using data which itself might be highly questionable. The feeling seems to be that if enough data is gathered, good things will happen. But as we can see from Chicago's implementation of this technology, the only thing it's done so far is add confirmation bias toetags to the ever-increasing number of bodies in the city's morgues.

Read the rest here: https://www.techdirt.com/articles/20160623/06112634789/proprietary-algorithms-are-being-used-to-enhance-criminal-sentences-preventing-defendants-challenging-them.shtml
Strategy for growing cybersecurity professionals. The National Security Agency (NSA), the Department of Homeland Security (DHS), and the existing Centers of Academic Excellence (CAEs) in Information Assurance coordinated together to develop more active cybersecurity Knowledge Units (KUs) in lieu of the Committee of National Security System (CNSS) courseware standards (4011, 4012, 4013, 4014, 4015, and 4016). As a result, academic institutions nation-wide can be designated as Centers of Academic Excellence in Cyber Defense (CAE-CD). The academic requirement for CAE-CDs in education is based solely on the respective sets of KUs posted here: https://www.iad.gov/NIETP/CAERequirements.cfm

How does the CAE-CD construct relate to the NICE framework? The short answer is, it doesn’t. The National Initiative for Cybersecurity Education (NICE) Workforce Framework 2.0 was developed with the purpose of promoting the nation’s cybersecurity workforce. On the other hand, the CAE-CD was developed with the purpose of promoting cybersecurity education and establishing a specific academic standard. (i.e. This standard leads to more cybersecurity professionals for national security systems.) A comparative relationship between the two was mapped out here: https://www.iad.gov/NIETP/documents/Requirements/NSA_DHS_CAER_KU_Mapping_to_NICE_FW_2.0.pdf

Today, there are 209 Centers of Academic Excellence (CAEs). Institutions in Colorado that have been awarded with the CAE-CD designation include:

- Colorado School of Mines
- Colorado State University-Pueblo
- Colorado Technical University
- United States Air Force Academy
- University of Colorado, Colorado Springs
- University of Denver

Three CAE Programs. “NSA and DHS jointly sponsor the national CAE-CD education programs, Two-Year Education (CAE-2Y) programs, and Research (CAE-R) programs. The goal of these programs is to reduce vulnerability in our national information infrastructure by promoting higher education and research in CD and producing a growing number of professionals with CD expertise in various disciplines. Students attending CAE-CDE and CAE-R schools are eligible to apply for scholarships and grants through the Department of Defense Information Assurance Scholarship Program and the Federal Cyber Service Scholarship for Service Program. Designation as a Center does not carry a commitment for funding from NSA or DHS.

CAE-CD institutions receive formal recognition from the U.S. Government as well as opportunities for prestige and publicity for their role in securing our Nation’s information systems.”

1Formerly, the Committee of National Security System (CNSS) courseware standards (4011, 4012, 4013, 4014, 4015, and 4016) established the requirements for any academic institution to certify professionals for national security systems. However, it became extremely difficult to update the CNSS standards, as it required approval from 21 government department and agencies. At the same time, NSA has been faced with a charter to grow cybersecurity professionals according to CNSS Directive No. 500, Information Assurance (IA) Education, Training, and Awareness, August 2006.

2The goal of these programs is to reduce vulnerability in our national information infrastructure by promoting higher education and research in IA/CD and producing a growing number of professionals with IA/CD expertise in various disciplines….. Students attending CAE IA/CD-E and CAE IA/CD-R schools are eligible to apply for scholarships and grants through the DoD Information Assurance Scholarship Program and the Federal Cyber Service Scholarship for Service Program. Designation as a Center does not carry a commitment for funding from NSA or DHS. CAE IA/CD institutions receive formal recognition from the U.S. Government as well as opportunities for prestige and publicity for their role in securing our Nation’s information systems.”

3Retrieved on 13 Jun 2016 from https://www.iad.gov/NIETP/aboutCAE.cfm

4Retrieved on 15 June 2016 from https://www.iad.gov/NIETP/reports/cae_designated_institutions.cfm
By Kurt Danis, ISSA-COS, June 24, 2016

Here’s a bird’s eye view of one event you might like to be “in the know” about…

Four years ago, it was called the North Alabama Cyber Security Summit. Then the event was called the Southeastern Cyber Security Summit. And now, with over 1500 attendees, the National Cyber Summit (NCS) has become an exceptionally large and economical event. Yes, it’s still FREE. To make this possible, NCS was a joint effort by the local ISSA chapter, Auburn University, Cyber Huntsville (a non-profit organization), Southeastern Cyber Security Foundation, and the University of Alabama in Huntsville. This year’s event included more senior officials, a greater presence by the financial industry, several US government agency representatives, and strong sponsor support by commercial IT vendors and some defense contractors. Most of the cyber speakers articulated and addressed policy issues, disciplined approaches to cybersecurity, challenges they faced in their field, ongoing developments, new technology, and operational approaches for cybersecurity. During the Summit, the NSA and DHS recognized numerous colleges and universities that were designated as Centers of Academic Excellence (CAEs).

What’s online? Good question! While some briefs were sensitive, those that were not sensitive were recorded on video and/or the slides were posted here:
http://www.nationalcybersummit.com/2016/06/11/post-summit-information/

OPM updates cyber hack page to promote greater outreach

By Carten Cordell, Federal Times, June 28, 2016

The Office of Personnel Management recently updated a webpage devoted to providing the public with information about its efforts to address last summer’s cyber breach.

Acting OPM Director Beth Cobert announced a series of updates related to the agency’s initiatives in the wake of the breach that exposed the personal information of 21.5 million people.

“We want to take a moment to update you on our continued response, including what services we have provided to those impacted by these intrusions, what OPM and its interagency partners are doing to enhance cybersecurity, and the steps all federal employees can take to practice good cyber hygiene,” Cobert said in a letter to federal employees.

The new Frequently Asked Questions page provides users with sections explaining what occurred during the hack, what information was taken, who was impacted as a result and ongoing efforts by OPM to both improve its cybersecurity and offer protections to those affected.

The agency noted on its FAQ page that because background investigation information was exposed in the hack, additional people may have been impacted beyond the 21.5 million identified.

But OPM said in these cases that the Social Security numbers of the individuals were not exposed, so the credit and identity protections won’t be extended. The agency also didn’t specify how many were impacted.

Read the rest here:
By Scott Maucione, WFED, June 23, 2016

The Obama administration is still struggling on how it would respond to a cyber attack on U.S. water systems, financial structure or electrical grid.

Defense Department Acting Assistant Secretary for Homeland Defense and Global Security Thomas Atkin was unable to provide specifics to the House Armed Services Committee this week on when exactly DoD would get involved if there was a cyber attack to critical U.S. infrastructure.

"When DOD gets involved is an attack of significant consequence, we have the responsibility to defend against an attack of significant consequence," Atkin said during the June 22 hearing.

"How do you define significant consequence?" Rep. Tulsi Gabbard (D-Hawaii) asked Atkin.

Atkin responded loss of life, physical damage, economic impact or foreign policy are all factors.

But Gabbard pushed harder.

"As you define loss of life, if there was an attack on an electrical grid, caused a major power outage, hospitals no longer able to care for people and loss of life in that respect. Would that fall under that definition?" Gabbard said.

Atkin was unwilling to hypothesize on scenarios, but said different factors would have to be evaluated for an attack to be considered one of significant consequence. Atkin added DoD would assist the Department of Homeland Security, which has jurisdiction over attacks on the homeland, if asked.

The interaction comes as Congress is considering elevating U.S. Cyber Command to a full combatant command.

The exchange between Gabbard and Atkin highlights a larger debate that has been brewing between Congress and the White House.

Congress has repeatedly asked the administration for a cyber deterrence policy, which would outline how the United States would respond to a cyber attack.

Congress pushed the White House for a cyber deterrence strategy to warn enemies there are repercussions for cyber attacks on the United States.

"Suppose there is an attack like the one on [the Office of Personnel Management]. Do you respond by counterattacking? Do you respond by trying to enact other measures? What do we do in case of a cyber attack?" Senate Armed Services Committee Chairman John McCain (R-Arizona) said last September.

The White House issued a policy in December that outlined some areas where the United States might retaliate after a cyber attack.

But, after Wednesday's hearing, it's clear all of the kinks have not been worked out.

McCain called the December cyber strategy "thin" and "wholly-lacking any new information about the administration's plan to integrate ends, ways, and means to meaningfully deter attacks in cyber space. It mostly reiterates steps taken and pronouncements made over the past few years, all of which we know have failed to deter our adversaries or decrease the vulnerability of our nation in cyber space."

House Armed Services Chairman Mac Thornberry was concerned by Atkin's testimony on Wednesday as well.

"My concern is we know where it's coming from. Country XYZ that has tremendous cyber capability is preparing to do something and the question is whether we wait and let them do it or try to at least take defensive action to manage the consequence of it," Thornberry said.

Read the rest here:
Ethical hacking at the DoD draws interest from HHS

By Carten Cordell, Federal Times, June 23, 2016

It's a well-documented fact that an organization may be under attack and not even know it, with malware spreading undetected across the network for days, weeks or even years.

The Department of Defense's recent "Hack the Pentagon" bounty program was such a hit that the Department of Health and Human Services is starting to take a look at it.

The Department of Defense's recent "Hack the Pentagon" bounty program was such a hit that the Department of Health and Human Services is starting to take a look at it.

HHS officials mentioned the DoD's recently completed pilot program-which paid bounties to hackers who were able to discover cyber vulnerabilities at the agency, also known as ethical hacking-as a possible way to address cybersecurity issues in health care.

Speaking at the Collaboration of Health IT Policy and Standards Committees meeting on June 23, Lucia Savage, chief privacy officer at HHS's Office of the National Coordinator for Health Information Technology, said that the practice could show promise at HHS if it was scaled up to meet health care needs.

Savage said that ethical hacking was a hot topic at a recent Federal Drug Administration workshop focusing on medical device security as a way to test the cybersecurity-worthiness of the items in question.

"This is a struggle for devices as well," she said. "You can't hack something in the field, because what if the hacker disrupts the operation of the device. Similarly, health data and EHRs, we may not want to have the hacker accessing your live data because that might cause other problems relative to your obligation to keep that data confidential.

"Given that space and given the need to improve cybersecurity, is there something that ONC can do to improve that rate at which ethical hacking occurs in health care?"

Savage said her office was working on plans to see how the practice could be effectively applied to the health care and medical devices sector, in collaboration with the FDA, but the advantages could be promising.

"I think that this is a technique that has been found highly valuable in the rest of industry," she said. "One of the things we are thinking about is how to get this to take root as a security hygiene process within the health care system."

The committees-which are composed of health care stakeholders who offer policy and standards recommendations to the National Coordinator for Health IT-queried Savage on what plans ONC might have for ethically hacking devices, especially related to Internet of Things capabilities.

But because ONC focuses on health IT and FDA regulates medical devices, Savage said her office was looking at ways ethical hacking could work, in partnership, rather than directly hacking devices.

"I just want to be super clear, our focus is on security hacking for the devices," Savage said. "We don't have any authority on the safety or efficacy of devices or health IT. I will say that the work we are doing, we're doing it in concert, sort of thinking through how to solve the problem."

Dr. Dale Nordenberg, CEO of Novasano Health and Science and a Health IT standards committee member, said that hacking medical devices could prove difficult because every medical device is hackable, leaving weaknesses and solutions to be worked out with a litany of detail.

"The issue is that once a vulnerability is identified, the industry is highly resistant to exposing to the public that specific vulnerability because the manufacturer has to get engaged," he said.

Read the rest here:
Windows zero-day exploit offered for sale on underground market

By Zeljka Zorz, HelpNetSecurity, June 1, 2016

Someone is selling an exploit for a Windows zero-day on an underground market for Russian-speaking cyber criminals, and the current price is set at $90,000.

Trustwave researchers have discovered the advertisement in early May and believe it to be genuine, although they point out that it’s impossible to know for sure unless one buys the exploit and tries it out.

“Zero days have long been sold in the shadows. In this business you usually need to ‘know people who know people’ in order to buy or sell this kind of commodity. This type of business transaction is conducted in a private manner, meaning either direct contact between a potential buyer and the seller or possibly mediated by a middle man,” they added, and noted that this particular offer is definitely an anomaly.

“It goes to show that zero days are coming out of the shadows and are fast becoming a commodity for the masses, a worrying trend indeed,” they added.

The exploit in question is for a Local Privilege Escalation (LPE) vulnerability in Windows and, the seller claims, it works on all versions of the OS, including Windows 10 and Windows Server versions, and all OS architectures.

“It seems the seller has put in the effort to present himself/herself as a trustworthy seller with a valid offering. One of the main indicators for this is the fact that the seller insists on conducting the deal using the forum’s admin as the escrow,” they noted.

The seller also provided two video demonstrations of the exploit in action on Windows 10, which show a successful elevation of the CMD EXE process to the SYSTEM account (highest level of privilege on the OS), and the exploit bypassing Microsoft’s Enhanced Mitigation Experience Toolkit (EMET).

The seller promises that the exploit will be sold to one single buyer, and offers to provide source code of the exploit, a demo of it, free of charge updates to address any Windows version that the exploit might not work on, vulnerability details, and a consultation on integrating the exploit.

While a Remote Code Execution (RCE) exploit would likely be more pricy, this one is also a great way to compromise Windows systems.

As Trustwave researchers noted, it could be used to perform sandbox escapes, install rootkits, modify system properties that allow persistence on the system, install additional malicious software, etc.

They notified Microsoft of the offering, and hopefully the limited vulnerability information provided by the seller will be enough to point them in the right direction and allow them to discover and patch the flaw themselves.

Read the rest here:
https://www.helpnetsecurity.com/2016/06/01/windows-zero-day-exploit-offered-for-sale-on-underground-market

Computer crash wipes out a decade of US Air Force data

By Ry Crist, CNet, June 14, 2016

A corrupted database in the US Air Force’s inspector general and legislative liaison divisions has reportedly put more than 100,000 internal investigation records in jeopardy.

The database, called the Automated Case Tracking System, was run by defense firm Lockheed Martin. It was corrupted last month and the firm spent two weeks trying to recover data before notifying the Air Force on June 6, according to Defense One.

The database held information about current investigations as well as all records related to IG complaints, appeals and Freedom of Information Act requests, according to The Hill.

"The database crashed and there is no data," Air Force spokeswoman Ann Stefanek told The Hill "At this time we don't have any evidence of malicious intent."

Air Force officials are now turning to cybersecurity professionals at the Pentagon for help with the matter.

Read the rest here:
Cyber-Jihad: Is a Digital Doomsday on the Horizon?

By Stormi O'Donnell, Secureworld, June 23, 2016

“This new malicious actor is consumed with the religious extremism of the crusades and armed with a full arsenal of technological weaponry that can bring an attack directly to the doorstep of every organization, man, woman and child in the United States and Europe. Cyber-Jihad has quickly arrived on the scene and will only continue to grow and hyper-evolve,” a report from the Institute for Critical Infrastructure Technology reads.

Welcome to the new reality, where a digital doomsday caused by terrorists is not just a scare tactic, but a serious threat. Just a few short years ago, terrorist groups for the most part were not capable of carrying out a devastating cyber attack. However, the emergence of the Dark Web, along with new recruiting techniques, has opened the door to cyber warfare with implications never before seen.

Perhaps the most technologically advanced of the terrorist groups is the Islamic State. ISIS recruits foreign members online through social media platforms, which has opened the door to technologically savvy members who are easy to train.

“Vindictive upstarts and script kiddies are able to rapidly hone their skills under the tutelage and assistance of hackers operating ISIS’s Cyber Help Desk and big targets become easy prey with step by step, point and click cyber attacks in this ideologically driven crusade,” the report reads.

The recruitment and training is only half of the problem. The Dark Web is a place where you can purchase any type of cyber attack from anywhere in the world, and the terrorist group does not appear to be cash-strapped. In January, reports surfaced that ISIS was offering upwards of $10,000 to Indian hackers in exchange for stolen government information.

“There are various underground communities online where hackers interact regularly. Our investigation reveals that for the past six months, lucrative offers for stealing government data came pouring in and hackers were offered a huge sum. Such amount has never been offered to any Indian hacker before. We found that the offers were being made to spread ISIS reach in the country,” Kislay Choudhary, cybercrime expert, told the Daily Mail India in January.

A massive cyber attack on a major city could leave people without electricity, clean water, or worse.

“Cyber-terrorist groups can use layered attacks to devastating effects. For instance, a group could hire a hacker to cause chaos in a city by disrupting its traffic system or water flow or it could conduct a physical attack to inflict losses and incite panic. After emergency services were burdened with casualties and the injured, the terrorists could launch DDoS and ransomware attacks against hospital and emergency response services. The extremists could use malware to steal confidential information from the infected systems while law enforcement attempted to respond to the attacks. Next, attacks against the SCADA and ICS systems supporting the local electric grid could further plunge the target city into turmoil,” The ICT report lays out the possible consequences.

Read the rest here:
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.

Anonymous Member Fights ISIS With Porn

By Angela Chen, Gizmodo, June 14, 2016

Everyone wants to fight ISIS. One member of Anonymous is doing it by hacking into their Twitter accounts and making them tweet porn.

WauchulaGhost, who for some strange reason did not want to give his real name, told the Washington Post that ISIS “doesn’t like porn” and doesn’t like women in general. (He’s definitely right about the latter, given the reports of mass rape and keeping of sex slaves.)

The logic goes that therefore hacking accounts with porn helps to run them off the social network. “We just started using [pornbots] to poke fun at them and diminish their presence online,” he adds.

Read the rest here:

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