Colleagues,

The 7th Annual Cybersecurity Training & Technology Forum (CSTTF) was a huge success! Thank you to everyone! Events like this require support from a lot of people, and I’m pleased to say we had some exceptional volunteers help in many different areas. Your help is greatly appreciated!

We also held a “Women in Security” networking/social event in the evening on 30 Aug, after the first day of the CSTTF. This was an initial/kick-off meeting to discuss the possibility of forming a group to focus and encourage women to pursue cybersecurity or cybersecurity-related fields. We’re off to a great start, with numerous women signed up to participate. If you’d like to be added to this group, or think you might like to join it, please let me know. Our next meeting is tentatively planned for late October. Watch for more info on it as we determine date/location/time of the meeting.

It’s time to look forward now, to our upcoming events. Our next Chapter Membership meetings are on 13 (dinner) and 14 (lunch) September, at Catalyst Campus. And on 16 September we’ll have our next Mini-Seminar at CollegeAmerica from 9am to noon. Remember, you can get three hours of continuing education by attending one of these Mini-Seminars, as well as network with your peers. Watch for details on these events on our website and via emails.

We’re also planning a Networking Event, to be held at the Warehouse Restaurant, on 5 October. We’ll get more details out on it as soon as possible, but please mark your calendars now for this networking/social event. Watch for more info about this event on our website and via emails.

Thank you all for your continued engagement and support – of the 2017 Chapter of the Year!!!

Colleen
LAST CHRISTMAS, NATHAN Seidle's wife gave him a second-hand safe she'd found on Craigslist. It was, at first glance, a strange gift. The couple already owned the same model, a $120 SentrySafe combination fire safe they'd bought from Home Depot. But this one, his wife explained, had a particular feature: The original owner had locked it and forgotten the combination. Her challenge to Seidle: Open it.

Seidle isn't much of a safecracker. But as the founder of the Niwot, Colorado-based company SparkFun, a DIY and open-source hardware supplier, he's a pretty experienced builder of homemade gadgets, tools, and robots. So over the next four months, he and his SparkFun colleagues set about building a bot that could crack the safe for them. The result: A fully automated device, built from off-the-shelf and 3-D printed components, that can open his model of SentrySafe in a maximum of 73 minutes, or half that time on average, with no human interaction. In fact, in the demonstration Seidle gave WIRED in the video above, the process took just 15 minutes.

In the process of building his safecracking robot, which he will demonstrate live at the Defcon cybersecurity conference next week, Seidle discovered a series of real vulnerabilities in the relatively cheap, but popular, SentrySafe he tested. But the larger lesson of his work goes beyond his particular safe's security flaws. It points instead to a new reality for vendors of physical security equipment: If automated tools can crack your locks or safes, the increasing affordability of those tools makes you more vulnerable than ever. "You're going to have an army of geeks like myself poking and prodding and trying to do things like this," says Seidle. "The nature of the toolset is getting cheaper, so more nerds are getting brave with their puzzling."

To build their safecracking robot, Seidle and his SparkFun accomplishments Rob Reynolds and Joel Bartlett used about $200 in parts. Those include a $20 Arduino board, a $40 motor, an aluminum frame, 3-D printed components including a coupler that attaches to the safe's dial, some magnets to hold it onto the safe's face, and sensors that can check if the bot has successfully turned the safe's handle, and when it passes the "zero" when turning the dial.

In the most basic sense, the resulting safecracker works by "bruteforcing" the SentrySafe—trying every possible combination. Like your high school locker's combination lock, the safe has three internal rotors that each have to be set to a certain position—by dialing a series of three numbers—to open it. Since each of those rotors has 100 positions, corresponding to as many numbers on the safe's dial, trying all one million combinations (100 x 100 x 100) at the speed of about ten seconds per guess would take nearly four months.

So Seidle started looking for shortcuts. First he found that, like many safes, his SentrySafe had some tolerance for error. If the combination includes a 12, for instance, 11 or 13 would work, too. That simple convenience measure meant his bot could try every third number instead of every single number, immediately paring down the total test time to just over four days. Seidle also realized that the bot didn't actually need to return the dial to its original position before trying every combination. By making attempts in a certain careful order, it could keep two of the three rotors in place, while trying new numbers on just the last, vastly cutting the time to try new combinations to a maximum of four seconds per try. That reduced the maximum bruteforcing time to about one day and 16 hours, or under a day on average.

But Seidle found one more clever trick, this time taking advantage of a design quirk in the safe intended to prevent traditional safecracking. Because the safe has a rod that slips into slots in the three rotors when they're aligned to the combination's numbers, a human safecracker can apply light pressure to the safe's handle, turn its dial, and listen or feel for the moment when that rod slips into those slots. To block that technique, the third rotor of Seidle's SentrySafe is indented with twelve notches that catch the rod if someone turns the dial while pulling the handle.

Read the rest here: http://www.realcleardefense.com/articles/2017/07/31/pentagon_would_ban_contractors_that_dont_protect_data_111923.html
Wow! We just closed out another successful conference at the end of August with over 500 registered attendees. There were interesting presentations, great opportunities to network with peers and vendors and a “Recognizing Women in Cyber” event in the evening. Thanks to all the folks who volunteered to help with planning, coordination, and execution.

Email reminders: Please take a couple of minutes to review your profile on your ISSA International account. Please ensure all your information is current and up to date, especially your contact information. It is critical that we have valid email addresses for everyone as that is our primary method of communicating with members. We have recently been getting a lot of bounces, particularly from military email addresses ending in .mil. A lot of military firewalls have been updated recently to filter email, particularly from *.org addresses. Also, when people change companies, they frequently forget to update their ISSA profile. If you haven’t been receiving chapter emails, this could be the reason so please consider updating your email address to a personal email rather than your work or military address. Just a thought. Thanks,

We’re at ~528 members as of the end of August.

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
dreland54321@comcast.net

<table>
<thead>
<tr>
<th>New Members August</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vickie Gibbs</td>
</tr>
<tr>
<td>Mike Allen</td>
</tr>
<tr>
<td>Jon Cohenour</td>
</tr>
<tr>
<td>Randy Harris</td>
</tr>
<tr>
<td>Brenda Hollingsworth</td>
</tr>
<tr>
<td>Elaine Maresca</td>
</tr>
<tr>
<td>Jeff Bivens</td>
</tr>
<tr>
<td>Ramesh Adhikari</td>
</tr>
<tr>
<td>Jackson Chaser</td>
</tr>
<tr>
<td>Nicholas Mazour</td>
</tr>
<tr>
<td>Chelsey Leffler</td>
</tr>
<tr>
<td>Leo Hergenroeder</td>
</tr>
<tr>
<td>Dan Katz</td>
</tr>
<tr>
<td>Hector Cardenas</td>
</tr>
<tr>
<td>Patrick Parnell</td>
</tr>
<tr>
<td>Fred Sayler</td>
</tr>
<tr>
<td>David Sorkness</td>
</tr>
<tr>
<td>Steve Swigart</td>
</tr>
<tr>
<td>Becky Manka</td>
</tr>
<tr>
<td>Cory Smith</td>
</tr>
<tr>
<td>Marquel Waites</td>
</tr>
<tr>
<td>Lynnae Batts</td>
</tr>
</tbody>
</table>
With a Gentle Touch, NIST Scientists Push Us Closer to Flash Memory Successor

By Staff, NIST, August 8, 2017

Sometimes a light touch is best: When you’re telling a joke or hammering a tiny finishing nail into a wall, a gentle delivery often succeeds most effectively. Research at the National Institute of Standards and Technology (NIST) suggests it also may be true in the microscopic world of computer memory, where a team of scientists may have found that subtlety solves some of the issues with a novel memory switch.

This technology, resistive random access memory (RRAM), could form the basis of a better kind of nonvolatile computer memory, where data is retained even when the power is off. Nonvolatile memory is already familiar as the basis for flash memory in thumb drives, but flash technology has essentially reached its size and performance limits. For several years, the industry has been hunting for a replacement.

RRAM could surpass flash in many key respects: It is potentially faster and less energy-intensive. It also could pack far more memory into a given space—its switches are so small that a terabyte could be packed into a space the size of a postage stamp. But RRAM has yet to be broadly commercialized because of technical hurdles that need addressing.

One hurdle is its variability. A practical memory switch needs two distinct states, representing either a one or a zero, and component designers need a predictable way to make the switch flip. Conventional memory switches flip reliably when they receive a pulse of electricity, but we’re not there yet with RRAM switches, which are still flighty.

“You can tell them to flip and they won’t,” said NIST guest researcher David Nminibapiel. “The amount needed to flip one this time may not be enough the next time around, but if you use too much energy and overshoot it, you can make the variability problem even worse. And even if you flip it successfully, the two memory states can overlap, making it unclear whether the switch has a one or a zero stored.”

This randomness cuts into the technology’s advantages, but in two recent papers, the research team has found a potential solution. The key lies in controlling the energy delivered to the switch by using multiple, short pulses instead of one long pulse.

Typically, chip designers have used relatively strong pulses of about a nanosecond in duration. The NIST team, however, decided to try a lighter touch—using less energetic pulses of 100 picoseconds, about a tenth as long. They found that sending a few of these gentler signals was useful for exploring the behavior of RRAM switches as well as for flipping them.

“Shorter pulses reduce the variability,” Nminibapiel said. “The issue still exists, but if you tap the switch a few times with a lighter ‘hammer,’ you can move it gradually, while simultaneously giving you a way to check it each time to see if it flipped successfully.”

Because the lighter touch does not push the switch significantly from its two target states, the overlapping issue can be significantly reduced, meaning one and zero can be clearly distinguished. Nminibapiel added that the use of shorter pulses also proved instrumental to uncovering the next serious challenge for RRAM switches—their instability.

“We achieved high endurance, good stability and uniformity comparable to using longer pulse widths,” he said. “Instability affects our ability to maintain the memory state, though. Eliminating this instability is a problem for another day, but at least we’ve clarified the problem for the next round of research.”

Read the rest here:

CSIAC - an excellent professional development resource for DoD cybersecurity professionals

By Kurt Danis, ISSA-COS, 24 August 2017

As stated on their website, the “Cyber Security and Information Systems Information Analysis Center (CSIAC) is a Department of Defense (DoD) Information Analysis Center (IAC). CSIAC is sponsored by the Defense Technical Information Center (DTIC)”. You will notice online journals, webinars, digests, and webinars are available. A special section called, “Cybersecurity” contains more items of interest. The home site is www.csiac.org

(Continued on page 5)
The tech behind the DARPA Grand Challenge winner will now be used by the Pentagon

By Chris Bing, CyberScoop, August 11, 2017

After witnessing the raw power of a machine that can fix its own software security flaws at DEF CON 24 more than one year ago, the Pentagon has officially purchased the revolutionary technology from a small, Pittsburgh-based firm.

The makers of a supercomputer designed to automatically detect, patch and exploit existing software vulnerabilities were recently awarded a seven-figure contract from the Department of Defense to apply the cutting-edge technology to military systems, including U.S. Navy ships and aircraft.

The Pentagon’s startup-centric office, named the Defense Innovation Unit Experimental (DIUx), is currently overseeing the venture.

The two-year contract is part of a program dubbed “Voltron,” which will offer the technology to a variety of different defense agencies in an effort to find coding flaws in both operating systems and custom programs used by the U.S. military.

Voltron represents a multi-contract effort — which includes but is not limited to the aforementioned deal — with the mission of leveraging breakthrough artificial intelligence in order to discover issues in military software. While this type of intensive security research would typically require a team of specialized experts, Voltron will allow for faster results without a dedicated workforce, U.S. officials familiar with the program told CyberScoop.

David Brumley, CEO of ForAllSecure, the company behind the innovative technology, said the DOD is largely interested in the supercomputer, dubbed Mayhem, for the “self-healing” capabilities it posses. The technology is “extremely scalable,” as it functions on LinuxX86, a popular operating system in the U.S. government. It will soon also work on Microsoft Windows.

The advantage Mayhem presents, Brumley told CyberScoop in a phone interview, lies in its ability to create, test and apply patches in real time onto unique systems that are critically important and cannot crash.

“The Defense Department understands the value of autonomy and they have for a long time,” Brumley said. “Last year, when they saw the GCG, I think that was really the first time they saw autonomy in cyber … the reception since then has been incredible.”

Although the capability has the potential to be used for offensive hacking purposes, the contract as it’s currently written only outlines specific defensive use cases, including realtime and continuous penetration testing and custom patching. A “patch” can be described as a specialty software update that is used to cover holes or flaws in software, which could be leveraged by a hacker.

The Pentagon’s contract with ForAllSecure was awarded two weeks ago. CyberScoop is the first to report on the details of this business deal.

Mayhem was originally created to compete in and eventually win an international hacking competition organized by the Defense Advanced Research Projects Agency (DARPA) in 2016. Held at DEF CON 24, this high-profile tournament, known as the Cyber Grand Challenge (CGC), opened the door for Pittsburgh-based ForAllSecure to showcase their machine: a system capable of automatically healing a friendly system while simultaneously scanning and attacking vulnerabilities in adversary systems.

Brumley said that a handful of foreign military organizations had reached out to his company since the competition in order to acquire or otherwise partner with ForAllSecure to leverage Mayhem. He declined these advances, but is already currently supplying the technology to a cohort of prominent, U.S.-based private sector technology firms.

Read the rest here:

(Continued from page 4)

For example, the webinar, “eMASS, the True Story” is an excellent brief on the eMASS process with several characterizations about the tool. You’ll find the briefer quite down to earth and well-informed with the tool – Enterprise Mission Assurance Support Service (eMASS), as well as Risk Management Framework. This is not DISA or the system developer touting the features of the tool, but rather an end-user walking through the RMF package development process on the tool. Enjoy!

Reference: https://www.csiac.org/podcast/emass-the-true-story/
A project called Hack the Air Force is paying “white hat” hackers over $130,000 for finding weak points in its websites, the service announced this morning. It’s the Defense Department’s third “bug bounty” — a high-profile initiative of Obama’s last Defense Secretary, Ashton Carter, that’s survived under Trump.

Hack the Pentagon found 138 unique, validated vulnerabilities last spring, Hack The Army found 118 late fall, and now Hack the Air Force found 207. Those numbers are unnervingly high, but the whole point is to get friendly hackers to find the weak points before hostile hackers can exploit them.

It’s a strictly regulated exercise, not the Wild West. All three iterations were run by crowdsourcing company HackerOne, which vets the participating hackers and runs a background check on them before they get their money. Some 272 “vetted hackers” participated in Hack the Air Force.

Many high-scoring participants were under 20, with the biggest bounties going to a 17-year-old. Most participants were US civilians, but two were active-duty troops and – a first for the program – 33 were foreign citizens. Before you panic that the Russians are coming, all 33 come from the “Five Eyes” countries with which the US shares its most sensitive intelligence: United Kingdom, Canada, Australia and New Zealand.

Still, listening to any outsiders, let alone foreigners and teenagers, is a dramatic culture shift for the Defense Department. In fact, old policies actively discouraged the public from reporting vulnerabilities and ordered independent security experts not to probe Pentagon systems.

Leading the charge has been Chris Lynch of the Defense Digital Service, another Ash Carter creation that brings in Silicon Valley gurus in sneakers and hoodies for short tours shaking up the suit-and-uniform culture of the Pentagon. The technophilic Carter spent a lot of time and effort on outreach to the commercial tech sector, including multiple trips with reporters in tow, and founded three offices called DIUX (Defense Innovation Unit Experimental) in Palo Alto, Austin, and Boston. Secretary Jim Mattis hasn’t matched this enthusiasm — it’s harder to imagine who could equal Carter here — and it’s an open question whether these initiatives will survive.

The bug bounty program probably has a better chance than other Carter initiatives, in part because Carter’s equally technophilic deputy, Robert Work, stayed on under Mattis for months until Patrick Shanahan could be confirmed.

“Work carrying over smoothed things,” said James Lewis, cybersecurity expert at the Center for Strategic & International Studies. Plus, he told me, “the programs seem to be effective, so I wouldn’t be surprised to see people keep it.

It’s also helpful that cash incentives for crowdsourcing are already routine in the commercial sector. The Pentagon is simply borrowing a proven private sector technique here, something the Trump Administration generally approves.

Read the rest here: http://breakingdefense.com/2017/08/hack-us-please-air-force-pays-130k-in-bug-bounties-under-obama-program/
Best practices for passwords updated after original author regrets his advice

By Nock Statt, The Verge, August 7, 2017

A vast majority of the trusted tips and tricks we employ when crafting a custom password actually make us more vulnerable to hackers, according to the expert who popularized the tips back in 2003. In an interview with The Wall Street Journal, former National Institute of Standards and Technology manager Bill Burr admitted that a document he authored on crafting strong passwords was misguided. “Much of what I did I now regret,” says Burr, who is 72 years old and now retired.

The problem wasn’t that Burr was advising people to make passwords that are inherently easy to crack, but that his advice steered everyday computer users toward lazy mistakes and easy-to-predict practices. Burr’s eight-page password document, titled “NIST Special Publication 800-63. Appendix A,” advised people to use irregular capitalization, special characters, and at least one numeral. That might result in a password like “P@ssW0rd123!” While that may make it seem secure on the surface (neglecting of course that “password” is a bad password), the issue is that most people tend to use the same exact techniques when crafting these digital combo locks. That results in strings of characters and numbers that hackers could easily predict and algorithms that specifically target those weaknesses.

Even worse, Burr suggested people should change passwords regularly, at least every 90 days. This advice, which was then adopted by academic institutions, government bodies, and large corporations, pushed users to make easy-to-crack passwords. Most people can probably point to a password they’ve created that was deemed strong simply because it had a special character like the “!” or “?” symbol and a numeric string like “123.” And when prompted to change a password, who hasn’t altered it only slightly to avoid the hassle of coming up with an all-new code?

A popular xkcd comic from cartoonist Randall Munroe, published back in August 2011, poked a hole in this common logic by pointing out how the password “Tr0ub4dor&3” could be cracked in about three days with standard techniques, due to its predictable capitalization, numeric substitutions, and special character use. The password “correct horse battery staple,” written as a single phrase, would take 550 years. (Security experts have confirmed Munroe’s math, according to the WSJ.) “Through 20 years of effort, we have correctly trained everyone to use passwords that are hard for humans to remember, but easy for computers to guess,” Munroe wrote at the bottom.

In other words, the passwords you should be using are obscure, almost unexplainable phrases full of human randomness that make them easy to commit to memory and yet almost impossible for an automated system to make sense of. Of course, for those who use password managers like LastPass, you can generate cryptographically secure passwords on the fly. But it’s still important to have a hard-to-crack master password.

“In the end, it was probably too complicated for a lot of folks to understand very well, and the truth is, it was barking up the wrong tree,” Burr admits of his advice. The new NIST standards that were published in June, authored by technical advisor Paul Grassi, did away with much of Burr’s advice.

Read the rest here:
NIST Releases Cybersecurity Definitions for the Workforce

By Dawn Kawamoto, Dark Reading, August 7, 2017

In an effort to bring consistency when describing the tasks, duties, roles, and titles of cybersecurity professionals, the National Institute of Standards and Technology released the finalized draft version of its framework.

Employers and recruiters may have an easier time describing the type of infosec professionals they are seeking to hire or advance in their careers now that the government’s National Institute of Standards and Technology (NIST) has released the finalized draft version of its cybersecurity lexicon framework.

NIST’s National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework aims to provide organizations with a common vocabulary when describing the role, area of specialty, category of work, and the knowledge, skills, and abilities (KSA) of cybersecurity professionals.

“The NICE Cybersecurity Workforce Framework improves communication, about how to identify, recruit, develop, and retain cyber security talent," according to the NIST report. "It is a resource from which organizations or sectors can develop additional publications, or tools that meet their needs to define or provide guidance on different aspects of workforce development, planning, training, and education.”

Employers, recruiters, and guidance counselors, for example, may use the framework as a resource when writing cybersecurity job descriptions, or use it to define with greater clarity the types of IT security professionals in the workforce, according to the NIST report.

As for cybersecurity professionals, the IT security vocabulary framework may aid in giving job seekers and employers a common language and understanding when various skills and abilities are listed in job openings, NIST states.

In the education and training fields, the framework may provide guideposts in developing curriculum or training certificate programs, because industry players will have a common understanding of the skills and tasks that will be needed in a job.

The creation of the framework relied on more than 20 government departments and agencies, the private sector, and academia to create a broad understanding of the cybersecurity market. The committee has created two earlier versions of the framework before this final version was approved, according to the report.

The definitions that emerged addressed the broader categories of work roles, which include a detailed list of cybersecurity work role groupings and the tasks that they perform. Specialty areas, meanwhile, include functions or concentrated work done in the cybersecurity industry, the report states. KSAs represent the required tasks needed to get the job done, as well as relevant education and training.

Read the rest here:
The topic of ethical hacking was on everyone’s mind at Def Con, the hacker convention last week in Las Vegas. It’s the security community’s annual gathering, where thousands of hackers gathered to show their latest exploits, discuss new security research and swap cyberwar stories. Many of the hackers I spoke to were gravely concerned about Russia’s wide-ranging interference in last year’s election. They wanted to know: How can we stop attacks like these in the future?

The problem, they told me, is that the government doesn’t make it easy for well-meaning hackers to pitch in on defense. Laws like the Computer Fraud and Abuse Act make poking around inside many government systems, even for innocent research purposes, a criminal offense. More than 209,000 cybersecurity jobs in the United States currently sit unfilled, according to a 2015 analysis of labor data by Peninsula Press, and the former head of the National Security Agency said last year that the agency’s cybersecurity experts “are increasingly leaving in large numbers” for jobs in the private sector.

Partly, that’s because private sector jobs tend to pay more. But it’s also because the government can be an inhospitable place for a hacker. Talented hackers can be disqualified for government jobs by strict background checks, and dissuaded by hiring processes that favor candidates with more formal credentials. At Def Con, I heard stories about hackers who had interviewed for government security jobs only to be turned away because they’d smoked pot as a teenager, or violated copyright law by jail-smoking video for Rick Astley’s “Never Gonna Give You Up.”

These rules may keep a few bad apples away from critical government systems, but they also prevent many talented hackers from contributing. At Def Con, I spoke with Sean Kanuck, a former C.I.A. intelligence analyst who served as the federal government’s national intelligence officer for cybersurveillance from 2011 to 2016. He said that hackers could be enormously valuable, if they were properly enlisted in the fight against attacks.

“Those people may be all hackers, and they may occasionally break the law, but they all still want the banking system to work,” Mr. Kanuck said. “All of them, if they end up in a hospital room, they want the infusion pump working. There’s common ground. And the knowledge here is incredible.”

The private sector has already discovered the benefits of hackers. Most major tech companies — including Facebook, Apple and Microsoft — offer “bug bounty” programs, in which they offer financial rewards to hackers who find holes in their security measures. These companies know that paying hackers up front for their expertise is significantly cheaper than cleaning up after a breach, and they understand that the risk of a hacker going rogue inside their systems is outweighed by the benefits of having well-trained experts catch bugs and vulnerabilities before the bad guys do.

Government agencies are beginning to experiment with a similar approach. The Defense Department offered the first-ever federal bug bounty program last year, called Hack the Pentagon. The agency allowed more than 1,400 hackers to take aim at its public-facing websites without fear of punishment, and the effort resulted in 138 legitimate vulnerabilities being reported. A similar program involving the Department of Homeland Security has been proposed in the Senate.

The most talked-about session at this year’s Def Con was when hackers were let loose on a series of computerized voting machines. These machines had been used in recent American elections, and most ran on comically outdated software. Hackers eventually broke into every machine and were able to manipulate the software to register fake ballots and change vote totals. (One enterprising hacker even rigged a voting machine to play the music video for Rick Astley’s “Never Gonna Give You Up.”)

There is, of course, the problem of outdated software. But some of the world’s best security researchers have also been prohibited from poking and prodding at these machines by a thicket of copyright and anti-tampering laws. (The reason Def Con was able to test them at all is a 2015 exemption to the Digital Millennium Copyright Act that gave researchers a temporary pass to experiment on voting machines.) Now that white-hat hackers have found flaws in these machines, they can pass that knowledge on to the manufacturers and election officials, who can secure the machines ahead of the next election cycle.

Read the rest here:
Popular weather app AccuWeather has been caught sending geolocation data to a third-party data monetization firm, even when the user has switched off location sharing.

AccuWeather is one of the most popular weather apps in Apple's app store, with a near perfect four-star rating and millions of downloads to its name. But what the app doesn't say is that it sends sensitive data to a firm designed to monetize user locations without users' explicit permission.

Security researcher Will Strafach intercepted the traffic from an iPhone running the latest version of AccuWeather and its servers and found that even when the app didn't have permission to access the device's precise location, the app would send the Wi-Fi router name and its unique MAC address to the servers of data monetization firm Reveal Mobile every few hours. That data can be correlated with public data to reveal an approximate location of a user's device.

We independently verified the findings, and were able to geolocate an AccuWeather-running iPhone in our New York office within just a few meters, using nothing more than the Wi-Fi router's MAC address and public data.

When the location is enabled, it sends the down-to-the-meter precise coordinates of the user, including speed and altitude, back to the data firm.

That's where Reveal Mobile comes in. The data firm isn't an advertiser per se but helps provide data for advertisers. Reveal says it "turns the location data coming out of those apps into meaningful audience data," and "we listen for [latitude and longitude] data and when a device "bumps" into a Bluetooth beacon," according to a brochure on its website.

For its part, Reveal Mobile executives said on a call last week with ZDNet that though company does collect Wi-Fi data and MAC address information, it "does not use it" for location data.

"Everything is anonymized," said Brian Handley, the company's chief executive. "We're not ever tracking an individual device," but described a situation where his company can point advertising to customers inside a Starbucks location, for example.

According to one AccuWeather executive, Reveal Mobile's technology "has not been in our application long enough to be usable yet."

"In the future, AccuWeather plans to use data through Reveal Mobile for audience segmentation and analysis, to build a greater audience understanding and create more contextually relevant and helpful experiences for users and for advertisers," said David Mitchell, AccuWeather's executive vice president of emerging platforms, on the call.

But while AccuWeather's privacy says that the company and its partners may use geolocation tracking technologies, its privacy policy doesn't specifically state that this data will be used for advertising, Strafach told ZDNet.

"Essentially I see a few problems," he said. "AccuWeather get GPS access under an entirely innocent premise -- no users expect the location data to be used this way," he said.

Several people have tweeted at Strafach in recent days to say they have deleted the app, based on his findings.

"When GPS access is not allowed, the app sends the [Wi-Fi network name] and possibly uses their Bluetooth beacon technology. This seems especially problematic as their website plainly states that use of Wi-Fi information is for geolocation, and that seems a bit over the line for situations where the user pretty clearly does not wish to share their location," he said.

In a blog post detailing his findings, Strafach said that similar opt-out geolocation tracking behaviors have in the past caught the eye of the enforcement arm of the Federal Trade Commission.

A 2016 case saw the FTC bring action against one offending app after it "deceived consumers by presenting them with an option to not share their information, even though it was shared automatically rendering the option meaningless."

Read the rest here:

Two-Factor Authentication Is A Mess

By Russell Brandom, The Verge, July 10, 2017

For years, two-factor authentication has been the most important advice in personal cybersecurity — one that consumer tech companies were surprisingly slow to recognize. The movement seemed to coalesce in 2012, after journalist Mat Honan saw hackers compromise his Twitter, Amazon, and iCloud accounts, an incident he later detailed in Wired. At the time, few companies offered easy forms of two-factor, leaving limited options for users worried about a Honan-style hack. The result was a massive public campaign that demanded companies to adopt the feature, presenting two-factor as a simple, effective way to block account takeovers.

Five years later, the advice is starting to wear thin. Nearly all major web services now provide some form of two-factor authentication, but they vary greatly in how well they protect accounts. Dedicated hackers have little problem bypassing through the weaker implementations, either by intercepting codes or exploiting account-recovery systems. We talk about two-factor like aspirin — a uniform, all-purpose fix that’s straightforward to apply — but the reality is far more complex. The general framework still offers meaningful protection, but it’s time to be honest about its limits. In 2017, just having two-factor is no longer enough.

For much of the last five years, the center of the campaign for two-factor has been twofactorauth.org, a site run by Carl Rosengren that’s dedicated to naming and shaming any product that doesn’t offer two-factor. At a glance, it can tell you which sites offer more than just a password login, and offers you an easy way to tweet at companies that don’t. Today, the site sends out hundreds of thousands of shaming tweets a day.

The campaign seems to have worked; nearly every company now offers some form of two-factor. Netflix is the biggest holdout — “I feel like I should buy a cake or something when that happens,” Rosengren says. Late adopters like Amazon and BitBucket have caved to demands, and every single VPN or cryptocurrency product listed by the site offers two-factor. The only email services without it are obscure players like Migadu and Mail.com. There are still a few problem sectors like airlines and banks, but most services have gotten the message: consumers want two-factor. If you don’t offer it, they’ll find a service that does.

But victory has been messier than anyone expected. There are dozens of different varieties of two-factor now, expanding far beyond the site’s ability to catalog them. Some send verification codes over SMS text, while others use email or more hardened verification apps like Duo and Google Auth. For $18, you can get a special USB drive to serve as your second factor. The only email services without it are obscure players like Migadu and Mail.com. There are still a few problem sectors like airlines and banks, but most services have gotten the message: consumers want two-factor. If you don’t offer it, they’ll find a service that does.

“Today, the site sends out hundreds of thousands of shaming tweets a day. The campaign seems to have worked; nearly every company now offers some form of two-factor. Netflix is the biggest holdout — “I feel like I should buy a cake or something when that happens,” Rosengren says. Late adopters like Amazon and BitBucket have caved to demands, and every single VPN or cryptocurrency product listed by the site offers two-factor. The only email services without it are obscure players like Migadu and Mail.com. There are still a few problem sectors like airlines and banks, but most services have gotten the message: consumers want two-factor. If you don’t offer it, they’ll find a service that does.

But victory has been messier than anyone expected. There are dozens of different varieties of two-factor now, expanding far beyond the site’s ability to catalog them. Some send verification codes over SMS text, while others use email or more hardened verification apps like Duo and Google Auth. For $18, you can get a special USB drive to serve as your second factor. The only email services without it are obscure players like Migadu and Mail.com. There are still a few problem sectors like airlines and banks, but most services have gotten the message: consumers want two-factor. If you don’t offer it, they’ll find a service that does.

But victory has been messier than anyone expected. There are dozens of different varieties of two-factor now, expanding far beyond the site’s ability to catalog them. Some send verification codes over SMS text, while others use email or more hardened verification apps like Duo and Google Auth. For $18, you can get a special USB drive to serve as your second factor. The only email services without it are obscure players like Migadu and Mail.com. There are still a few problem sectors like airlines and banks, but most services have gotten the message: consumers want two-factor. If you don’t offer it, they’ll find a service that does.

But victory has been messier than anyone expected. There are dozens of different varieties of two-factor now, expanding far beyond the site’s ability to catalog them. Some send verification codes over SMS text, while others use email or more hardened verification apps like Duo and Google Auth. For $18, you can get a special USB drive to serve as your second factor. The only email services without it are obscure players like Migadu and Mail.com. There are still a few problem sectors like airlines and banks, but most services have gotten the message: consumers want two-factor. If you don’t offer it, they’ll find a service that does.

But victory has been messier than anyone expected. There are dozens of different varieties of two-factor now, expanding far beyond the site’s ability to catalog them. Some send verification codes over SMS text, while others use email or more hardened verification apps like Duo and Google Auth. For $18, you can get a special USB drive to serve as your second factor. The only email services without it are obscure players like Migadu and Mail.com. There are still a few problem sectors like airlines and banks, but most services have gotten the message: consumers want two-factor. If you don’t offer it, they’ll find a service that does.

But victory has been messier than anyone expected. There are dozens of different varieties of two-factor now, expanding far beyond the site’s ability to catalog them. Some send verification codes over SMS text, while others use email or more hardened verification apps like Duo and Google Auth. For $18, you can get a special USB drive to serve as your second factor. The only email services without it are obscure players like Migadu and Mail.com. There are still a few problem sectors like airlines and banks, but most services have gotten the message: consumers want two-factor. If you don’t offer it, they’ll find a service that does.
Information Security Spending to Reach $93 Billion in 2018: Gartner

By Jevin Townsend, Security Week, August 16, 2017

Gartner has predicted that worldwide information security spending will reach $86.4 billion in 2017; a seven percent growth over the year. Spending is expected to increase to $93 billion in 2018.

The fastest growing sector is security services; especially in IT outsourcing, consulting and implementation services. The only area where growth is likely to slow down is hardware support services, which are becoming less necessary with the continuing adoption of virtual appliances, public cloud and Security as a Service (SaaS) solutions.

Much of the growth is thus expected to come from upgrading the IT infrastructure to a perceived more secure posture than by simply buying additional security products.

"Improving security is not just about spending on new technologies," said Sid Deshpande, principal research analyst at Gartner. "As seen in the recent spate of global security incidents, doing the basics right has never been more important. Organizations can improve their security posture significantly just by addressing basic security and risk related hygiene elements like threat centric vulnerability management, centralized log management, internal network segmentation, backups and systemhardening," he said.

Faster growth is likely to come from the security testing market, particularly in relation to application security testing as part of DevOps. This is no surprise to RJ Gazarek, Product Manager at Thycotic. "Thycotic research on DevOps security practices," he told SecurityWeek, "has shown that more than 60% of DevOps organizations are not managing credentials in scripts in any way. This is a major security problem that needs to be addressed immediately, especially as more breaches are making the news, and people realize that the way into an organization is to find the department with the weakest security practice and get to work infiltrating."

Neither the growth nor the areas of growth surprise Nathan Wenzler, chief security strategist at AsTech. "If we watch how the trend of attacks has gone over the past several years, we see more and more criminals moving away from targeting servers and workstations, and toward applications and people," he explained.

"As an industry, we've gotten better and better about protecting devices; but now the focus has to turn to other assets, and thus, the increase in spending Gartner is forecasting in DevOps and services. Essentially, wherever the criminals go, corporate spending is soon to follow," Wenzler said.

There is, however, one area in which Gartner sees actual product growth: data leak prevention (DLP). The belief is that fears over the far-reaching and severe implications of the EU General Data Protection Regulation is spurring, and will continue to spur, DLP purchasing through 2018.

GDPR will come into force in May 2018. From that date onward, any company anywhere in the world that handles the personal information of European citizens could be liable for a fine of up to 4% of global turnover if they do not adequately protect that data. "The EU General Data Protection Regulation (GDPR) has created renewed interest, and will drive 65 percent of data loss prevention buying decisions today through 2018," says Gartner.

Where companies already have some form of DLP already in place, Gartner believes that interest is now focused on enhancing the DLP control: "specifically, integrated DLP such as data classification, data masking and data discovery." These will all be required for GDPR compliance, both in protecting the data and being able to retrieve it for removal if required by the user concerned.

Just this week, Amazon Web Services launched a new machine learning security service that helps its customers discover, classify and protect sensitive data.

However, some security experts believe that Gartner is being too conservative in its spending growth estimates. "Gartner has taken a very conservative evaluation on information security spending that it will grow by only 7%," Joseph Carson, chief security scientist at Thycotic, told SecurityWeek. I believe that the actual number will be much higher given that many aggressive regulations will come into enforcement in 2018, including the EU General Data Protection Regulation (GDPR).

Read the rest here:
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.

Items of Interest

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

You can also sign-up on the Cyberjoblist.com site for Job Alerts to be notified when a new job listing is posted!
100% of government IT workers said employees are biggest threat to cybersecurity

By Alison DeNisco, Tech Republic, August 23, 2017

The government sector lags behind others in implementing modern cybersecurity defenses, according to a new report from security firm Netwrix. This failure to update has led to an increase in breaches: 72% of government entities worldwide had their security compromised in 2016, the report found. And only 14% of government organizations consider themselves to be well-protected against cyber threats.

Government agencies are targeted by hackers due to the sensitive information they store, including citizens’ data (such as addresses, driver’s license numbers, Social Security numbers, financial data, and healthcare records). They also house information critical to local or national security. Other hackers are interested in gaining access to important infrastructure to damage control systems or disrupt public services, the report noted.

However, the main threat is less nefarious than you may expect: Employees. A whopping 100% of IT specialists working for government agencies worldwide said they see employees as the biggest threat to security. In 2016, human error caused security incidents in 57% of government entities, and system downtime for 14% of them. Additionally, 43% of government IT professionals said they investigated security incidents that involved insider misuse.

"All government entities surveyed consider their own employees to pose the biggest threat," wrote Ryan Brooks, product evangelist at Netwrix, in a blog post about the findings. "It is interesting how the loudest headlines (state-sponsored attacks carried out by hackers, for example) don't always correspond with the respondents’ perceptions and priorities."

Still, the majority of government organizations have not implemented security governance or risk management within their IT infrastructures, the report found. And 75% of respondents said there were no dedicated security personnel in their agencies, leaving compliance and security to be shouldered by IT operations teams alone. As a result, junior and middle IT staff reported a lack of time (57%) and lack of budget (54%) as the main factors preventing them from taking a stronger security approach. The growing complexity of IT infrastructure (43%) and data assets (43%) were also factors.

Read the rest here:

U.S. Military vows to tweak and fling malware back at creators

By Robert Abel, SC Magazine, August 15, 2017

U.S. military hackers are taking a cliché move right from classic war movies and applying it to real life modern cyberwarfare by tossing malware "grenades" back at the enemy.

While they won’t be throwing actual bombs in this context, military officials are throwing enemy malware right back on its creator after recently announcing they are tired of just taking hits from outside players, according to The Register.

U.S. Defense Intelligence Agency officials vowed to take action Monday at the US Department of Defense Intelligence Information Systems (DoDIIS) conference in Missouri.

"Once we’ve isolated malware, I want to reengineer it and prep to use it against the same adversary who sought to use against us," Lieutenant General Vincent Stewart told attendees. "We must disrupt to exist."

Read the rest here:
A group of advisors to the White House have warned President Donald Trump and his administration of the risk of a cyber attack against critical infrastructure in the United States that could be comparable to the events of September 11, 2001.

The warning came from the National Infrastructure Advisory Council (NIAC), a group commissioned by the National Security Council (NSC) to review more the federal government’s capability to secure infrastructure against targeted cyber attacks.

In a report published by the NIAC, it called for “direction and leadership to dramatically reduce cyber risks,” and warned a failure to take action would leave could result in catastrophic outcomes.

“The challenges the NIAC identified are well-known and reflected in study after study,” the NIAC wrote. “There is a narrow and fleeting window of opportunity before a watershed, 9/11-level cyber-attack to organize effectively and take bold action. We call on the Administration to use this moment of foresight to take bold, decisive actions.”

While the warning from the advisory group was deadly serious, the NIAC presented several recommendations that could help prevent such a disaster from occurring.

On the top of the to-do list provided by the council was establishing separate and secure networks for critical infrastructure, including building “dark fiber” networks for traffic from critical control systems, as well as backup communications protocols for emergencies.

Such a change would place a gap between the open, public internet and the private communications infrastructure built to allow devices vital to the function of critical infrastructure to communicate.

Historically, that is how such systems were built, but as the infrastructure for telecommunications companies changed to meet the demands of the public, it forced utilities companies and other facilities to transfer vital data over the standard wireless protocol used by all data, leaving it potentially vulnerable to interception or attack.

Also on the list of suggestions from NIAC was improved information sharing that would allow for quick declassification and improved threat intelligence sharing. The report also called for improved scanning tools and assessment practices and an exchange program between public and private organizations to strengthen skill sets of IT professionals.

To make all of this happen, the NIAC called for the creation of “limited time, outcome-based market incentives” to encourage the owners of critical infrastructure—especially in the private sector—to invest in the necessary technology.

While it called for incentivizing the technological advances, the NIAC also made clear such motivations shouldn’t be required. The report found both the government and private sector have “tremendous” resources to invest in cyber defense but have failed to organize, harness or focus them properly.

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.

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: doncream@outlook.com

Ensure that “Newsletter” is in the subject line.

Looking forward to seeing you in print!

Are Facebook Messenger and Other Apps Listening to You Through Your Phone?

By Rain Noe, Core 77, August 1, 2017

A Core77 staffer recently recounted how she had been talking about a particular product with a friend. Not Googling it, just discussing it verbally. In subsequent days she noticed ads popping up on her feed for that particular product. Coincidence?

Read the rest here:

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