ACADEMIC SECURITY AND COUNTER EXPLOITATION PROGRAM

https://asce.tamus.edu

THE OPEN SOURCE MEDIA SUMMARY

January 11, 2023

RESEARCH GETS A BOOST IN FINAL 2023 SPENDING AGREEMENT

Science News Staff | Science | December 20, 2022

Congress unveiled a belated $1.7 trillion spending bill on 20 December that keeps the U.S. government running for the next 9 months. Lawmakers did the best they could for basic research. But their desire to increase the defense budget kept them from delivering a major promised boost for the National Science Foundation (NSF) and held several other civilian agencies to small increases. The 4155-page legislation, called an omnibus spending bill, is expected to be approved and signed into law by the end of the week, before an agreement expires that allows agencies to keep doing business at current spending levels. Here are some research-related highlights in the massive bill, the result of months of negotiations between members of the House of Representatives and the Senate. NIH's budget will grow in 2023 by $2.5 billion, or 5.6%, to $47.5 billion. President Joe Biden's administration had requested an increase of only $274 million. Each of NIH's 27 institutes and centers would receive a boost of at least 3.8%. The National Cancer Institute will receive $150 million more to shore up sagging grant success rates. Research on Alzheimer's disease will receive a $226 million boost, to $3.7 billion. Other areas tagged for increases include health disparities, HIV/AIDs research, and opioids research.

Read the full article here.

THE BIDEN NATIONAL CYBER STRATEGY IS UNLIKE ANY BEFORE IT

Tim Starks and Aaron Schaffer | The Washington Post | January 6, 2023

The Biden administration is nearing publication of a national cybersecurity blueprint that for the first time embraces a major role for regulation. The strategy, which is a sea change from past blueprints, will arrive in the aftermath of a series of major cyberattacks — such as the 2021 Colonial Pipeline ransomware attack, which sparked a fuel panic on the East Coast — that prompted the administration to rethink voluntary measures. In response, the Biden administration has issued or is in the process of issuing a number of cybersecurity regulations using preexisting executive branch powers, such as requirements for key pipeline operators to develop detailed plans for responding to cybersecurity incidents. Congress, too, passed legislation requiring critical infrastructure owners and operators to disclose to the federal government within 72 hours when they suffer a major cyberattack. The forthcoming strategy, led by National Cyber Director Chris Inglis's office in the White House, builds on that approach, according to senior administration officials who spoke on the condition of anonymity because the document is not yet public. President Biden is expected to sign the document, which is moving through the final stages of interagency approval involving more than 20 departments and agencies, in the coming weeks.

Read the full article here.

PENTAGON PLANS TO FORMALLY PROPOSE CHANGES TO CMMC PROGRAM AHEAD OF OFFICIAL LAUNCH

Sara Friedman | Inside Cybersecurity | January 10, 2023

Full implementation of the Pentagon’s CMMC program for defense contractors will likely shift to 2024 based on revised estimates from the Defense Department in the fall 2022 unified agenda, which indicates two proposed rules are expected for release in the coming months. The Pentagon is implementing major changes to its Cybersecurity Maturity Model Certification program coming out of a 2021 internal review and had planned to seek an interim final designation to change defense acquisition regulations.

Read the full article here.

CHINESE RESEARCHERS CLAIM THEY CRACKED ENCRYPTION WITH QUANTUM COMPUTERS

Jason Nelson | Yahoo Finance | January 5, 2023

While the world continues to reel from how far artificial intelligence has come with projects like ChatGPT, Chinese researchers recently claimed that they have been able to crack encryption using quantum computing—something scientists have assumed was years away from happening. A group of Chinese researchers published a "scientific paper" last month that said they used quantum computers to break a standard RSA algorithm that many industries—including banking, mobile phones, and data storage—use for their encryption measures. According to the Financial Times, the Chinese researchers said they had used their algorithm to factor a number with 48 bits on a quantum computer with ten qubits (quantum bits) and that they had not yet tried to scale it up to work on a much bigger system. While the claim has raised some concern about the state of the art in security, many experts consider the breakthrough to be impossible—at least for now. "A colleague of ours calls it the biggest hoax he has seen in about 25 years," Global Quantum Intelligence CEO & Co-Founder Andre Konig told Decrypt in an interview. "The paper itself doesn't announce anything really new." Konig calls the paper's claims hype-driven and a spin on existing methodologies and approaches, lacking a proof of concept that would demonstrate the successful breaking of current encryption standards.

Read the full article here.

PAPERS AND PATENTS ARE BECOMING LESS DISRUPTIVE OVER TIME

Michael Park, Erin Leahey, and Russell J. Funk | Nature | January 4, 2023

Theories of scientific and technological change view discovery and invention as endogenous processes, wherein previous accumulated knowledge enables future progress by allowing researchers to, in Newton’s words, ‘stand on the shoulders of giants’. Recent decades have witnessed exponential growth in the volume of new scientific and technological knowledge, thereby creating conditions that should be ripe for major advances. Yet contrary to this view, studies suggest that progress is slowing in several major fields. Here, we analyse these claims at scale across six decades, using data on 45 million papers and 3.9 million patents from six large-scale datasets, together with a new quantitative metric—the CD index12—that characterizes how papers and patents change networks of citations in science and technology. We find that papers and patents are increasingly less likely to break with the past in ways that push science and technology in new directions. This pattern holds universally across fields and is robust across multiple different citation- and text-based metrics. Subsequently, we link this decline in disruptiveness to a narrowing in the use of previous knowledge, allowing us to reconcile the patterns we observe with the ‘shoulders of giants’ view. We find that the observed declines are unlikely to be driven by changes in the quality of published science, citation practices or field-specific factors.

Read the full article here.

EXCLUSIVE: RUSSIAN HACKERS TARGETED U.S. NUCLEAR SCIENTISTS

James Pearson and Christopher Bing | Reuters | January 6, 2023

A Russian hacking team known as Cold River targeted three nuclear research laboratories in the United States this past summer, according to internet records reviewed by Reuters and five cyber security experts. Between August and September, as President Vladimir Putin indicated Russia would be willing to use nuclear weapons to defend its territory, Cold River targeted the Brookhaven (BNL), Argonne (ANL) and Lawrence Livermore National Laboratories (LLNL), according to internet records that showed the hackers creating fake login pages for each institution and emailing nuclear scientists in a bid to make them reveal their passwords. Reuters was unable to determine why the labs were targeted or if any attempted intrusion was successful. A BNL spokesperson declined to comment. LLNL did not respond to a request for comment. An ANL spokesperson referred questions to the U.S. Department of Energy, which declined to comment. Cold River has escalated its hacking campaign against Kyiv's allies since the invasion of Ukraine, according to cybersecurity researchers and western government officials.

Read the full article here.

BIDEN SIGNS BILL TO PUNISH IP THEFT

Grace Dille | MeriTalk | January 6, 2023

President Biden on Jan. 5 signed into law the Protecting American Intellectual Property Act that aims to prevent China-based corporations – and other foreign companies – from stealing U.S. intellectual property. Sens. Chris Van Hollen, D-Md., and Ben Sasse, R-Neb., introduced the legislation, which will mandate economic penalties on firms and individuals involved in stealing American intellectual property. “In China and other countries across the globe, foreign corporations are working – often in coordination with authoritarian regimes – to steal our cutting edge technologies to gain unfair advantages at America’s expense,” Sen. Van Hollen said in a Jan. 5 press release. “This also results in the off-shoring of American jobs and causes harm to our economy and our national security.” “We must act to deter these predatory practices by imposing high costs. That’s why I worked with Senator Sasse to write bipartisan legislation that creates clear consequences for the theft of U.S. intellectual property.

Read the full article here.

LAWMAKERS ARE TRYING TO BAN TIKTOK. THAT WON'T BE EASY -- IT'S PART OF OUR CULTURE NOW

Faith Karimi | CNN | January 7, 2023

Gabby Beckford's plan to visit the British Virgin Islands started with a flurry of searches on what to wear, eat and do in between exploring the islands' pristine beaches and sapphire waters. But instead of using Google or other search engines, she turned to TikTok. "On TikTok, I can search what restaurants to go to, I can see what people ate and their reaction to the food," says Beckford, 27, who's visiting the British territory in the Caribbean this week. "I can see what they're wearing, what the weather's like." Beckford, a travel content creator who splits her time between Seattle and Washington, DC, says TikTok has become a lifeline for her and many other users. She says the short-form video platform is much more than cat videos and posts by "influencers." To her it's a one-stop shop for a wide range of content, from mental health advice to product reviews, all presented in bite-sized clips that don't require plowing through blocks of text. "It's visual," she says. "I can tell who posted the content, and whether it's done with me in mind." Beckford's devotion to TikTok illustrates why US lawmakers and others, who view the platform as a security threat because of its parent company's roots in China, will have a challenge trying to scrub it from Americans' digital lives.

Read the full article here.

CHINA’S RETURN INCENTIVE SCHEME LURES YOUNG SCIENTISTS – SUPERSTARS NOT SO MUCH

Holly Chik | South China Morning Post | January 6, 2023

A long-term Chinese incentive programme was successful at enticing high-calibre, overseas-trained scientists to return home, but was less accomplished at luring back top researchers, according to a new study. It was one of the findings by a team of researchers from Shanghai Jiao Tong University, Tsinghua University and the University of Hong Kong, who evaluated the impact and policy implications of the “generously funded” Young Thousand Talents (YTT) programme. The scheme was established in 2010 to recruit and nurture early-career expatriate scientists who return to China after receiving PhDs abroad. Scientists aged 40 and under were induced by YTT to return home if they were offered better funding and larger research teams to support their work, according to the study. “While ‘the best are yet to come’, China’s YTT programme was attractive to young expatriates who had the capability but not the funding to run their own labs for independent research,” the researchers said in an article published Friday in the peer-reviewed journal Science. But the best scientists were less likely to return, they found.

Read the full article here.

IN HYBRID WORKPLACES, INFECTED USBS MOVE FROM HOME TO OFFICE

Billy Hurley | IT Brew | December 1, 2022

This holiday season: Don’t be fooled by a decorative gift box, especially if it contains an Amazon voucher, a thank-you note, and a USB drive. In early 2022, the FBI warned that a basket from “FIN7” cybercriminals containing “BadUSB” ransomware hidden in the storage key was being delivered to US businesses. And that terrible present—as the name suggests, a bad USB—seems to be on the rise. While threat actors still send malicious storage drives, hoping that curious employees can’t resist seeing what’s on there, hybrid work has led to infected devices moving from home to office. “Maybe they share USB keys between their personal laptop, their family PC, their work machine, and printer…So, the infection is actually happening outside of the organization, but directly affecting the organization’s endpoint when they use that USB again.

Read the full article here.

ARE META AND TWITTER USHERING IN A NEW AGE OF INSIDER THREATS?

Ian McShane | Dark Reading | January 3, 2023

Most of the attention paid to cybersecurity by practitioners and the general public alike is to threats that are external, such as attackers and scammers acting individually or as part of a larger organization. But a pair of stories this month alleging insider abuse at Meta and Twitter have served as harsh reminders that sometimes the call is coming from inside the house. Reportedly, employees at both companies have recently used internal workarounds or private channels to sell access to platforms and verification, in some instances for bribes, creating a precarious and unmoderated black market for people who have already been denied re-entry to the platforms by official mechanisms. Twitter employees, Elon Musk appeared to imply in a tweet shortly after taking over as CEO of the company, may have sold verification status to users off the books for as much as $15,000. The Wall Street Journal, meanwhile, reported that more than two dozen employees and third-party contractors at Meta abused an internal account recovery tool to restore accounts for people who otherwise had no recourse to recover an account.

Read the full article here.

A BREACH AT LASTPASS HAS PASSWORD LESSONS FOR ALL OF US

Brian Neeley | Business News | January 5, 2023

While many of us unplugged from the internet over the holidays to spend time with loved ones, LastPass, the maker of a popular security program for managing digital passwords, delivered a most unwanted gift. It recently published details about a security breach in which cybercriminals obtained copies of customers' password vaults, potentially exposing millions of people's online information. From a hacker's point of view, this is equivalent to hitting the jackpot. When you use a password manager like LastPass or 1Password, it stores a list containing all the usernames and passwords for the sites and apps you use, including banking, healthcare, email and social networking accounts Huh. It keeps track of that list, called a vault, in its own online cloud so you can easily access your passwords from any device. LastPass said the hackers stole a copy of the list of usernames and passwords for each customer from the company's servers. This breach was one of the worst things that could happen to a security product designed to take care of your passwords.

Read the full article here.

GUIDANCE FOR USPAB AUTHORIZATION REQUESTS (REVISION 1.0)

Directorate of Defense Trade Controls | Guidance for USPAB Authorization Requests | December 7, 2022

In order to assist industry, DDTC is providing more comprehensive guidance for submissions of requests to authorize exports of defense services by U.S. Persons Abroad. Exporters may also wish to consult the FAQs on "Defense Services and U.S. Persons Abroad" that are published on the DDTC website. A U.S. Person Abroad (USPAB) is an individual U.S. person (as defined in ITAR § 120.62) who resides overseas, works for a foreign employer, and provides defense services as defined in ITAR § 120.32(a)(1) and/or (3) to their employer or other foreign parties. All USPABs require DDTC authorization prior to furnishing defense services to any foreign person. The USPAB is the applicant of a USPAB authorization request because the USPAB is the U.S. person furnishing defense services to a foreign person. The USPAB's employer is the foreign end-user as the recipient of the defense services. Wherever the word applicant is used throughout this guidance, it refers to the USPAB. A USPAB license authorizes a USPAB to furnish defense services to his or her foreign employer.

Read the full article here.

THE TEXAS A&M UNIVERSITY SYSTEM

The Academic Security and Counter Exploitation Program is coordinated by The Texas A&M University System Research Security Office as a service to the academic community.
https://rso.tamus.edu

ASCE
ACADEMIC SECURITY AND COUNTER EXPLOITATION PROGRAM