SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN

19 JUNE – 20 AUGUST 2021

TOPICAL REPORT

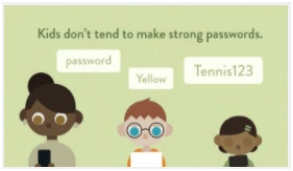
CYBERSECURITY

Gain insight and keep up-to-date with the latest publications carefully selected by the library from credible sources in academic publications, industry & market research and scientific & industry news.
If you have any sources to suggest for our report please let us know.

view past reports | subscribe to others | unsubscribe

news

CYBERSECURITY



NIST study on kids' passwords shows gap between knowledge of password best practices and behavior

"The problem isn't limited to just adults. Children may seem more technologically savvy because they've grown up in the digital space, but they still face the same cybersecurity threats. So, to shed light on what kids understand about passwords and their behavior in creating and using them, researchers at the National Institute of Standards and Technology (NIST) conducted a study that surveyed kids from third to 12th grade."
Source: EurekAlert!

Behind the scenes: A day in the life of a cybersecurity "threat hunter"

"Here's how one security operations analyst, an expert at incident reporting, began her career, collaborates with her colleagues and prioritizes incoming threats."
Source: Tech Republic

What is Pegasus? A cybersecurity expert explains how the spyware invades phones and what it does when it gets in

academic

CYBERSECURITY

Industrial Control System Testbed for Cybersecurity Research with Industrial Process Data

"Cybersecurity of industrial control systems (ICS) is an essential research area due to increasing critical asset-targeted cyberattacks and their potential severe consequences. Current intrusion detection systems (IDS) are primarily based on network traffic monitoring, which may be not sufficient for detecting comprehensive and carefully prepared cyberattacks... In this paper, a real-time ICS test bed, which includes a physical two-loop forced flow system, LabVIEW-based supervisory control and data acquisition (SCADA) system, and Kali Linux-incorporated cyber network that conducts attacks within the local area network (LAN), is deployed to generate relevant data. Three cyberattacks scenarios are carried out in this paper, including packets sniffing with man-in-the-middle (MITM) attack; denial-of-service (DoS) attack to SCADA slave with spoofed IP address; and change command with spoofed SCADA master by MITM attack."
Source: American Nuclear Society

Analysis of the Cybersecurity Weaknesses of DLT Ecosystem

reports

THREAT REPORTS

McAfee Labs Threats Reports June 2021

"Insights into malware, ransomware, and other cybersecurity threats from the McAfee threat research team."
Source: McAfee

A SANS 2021 Report: Top New Attacks and Threat Report

"In the SANS 2021 Top New Attacks and Threat Report, John Pescatore provides insight into the threats highlighted during the SANS panel discussion at the 2021 RSA Conference. This webcast will include practical advice from the paper, including insights from SANS instructors Ed Skoudis, Heather Mahalik, Johannes Ullrich, and Katie Nickels on the critical skills, processes and controls needed to protect their enterprises from these advanced attacks."
Source: SANS

List of data breaches and cyber attacks in July 2021 – 34 million records breached

"We found 86 security incidents in July 2021, which accounted for 33,727,641 breached records.
These figures are far lower than those that we've seen so far this year, bringing some much-needed good news in what was starting to look like

"End-to-end encryption is technology that scrambles messages on your phone and unscrambles them only on the recipients' phones, which means anyone who intercepts the messages in between can't read them. Dropbox, Facebook, Google, Microsoft, Twitter and Yahoo are among the companies whose apps and services use end-to-end encryption.
This kind of encryption is good for protecting your privacy, but governments don't like it because it makes it difficult for them to spy on people, whether tracking criminals and terrorists or, as some governments have been known to do, snooping on dissidents, protesters and journalists."
Source: The Conversation

New project uses empathy to teach students about cybersecurity and AI ethics

"While empathy is important in almost every aspect of daily life, it is not always a priority in the development of technology, especially technology using artificial intelligence (AI). iSchool researchers are working to address this gap by using empathy to teach high school students about cybersecurity and AI ethics issues. Led by Yang Wang, associate professor of information science at the University of Illinois Urbana-Champaign, the project, "Teaching High School Students about Cybersecurity and Artificial Intelligence Ethics via Empathy-Driven Hands-On Projects," has received a two-year, $297,575 National Science Foundation (NSF) Early-Concept Grant for Exploratory Research (EAGER). Yun Huang, assistant professor of information science, University of Illinois Urbana-Champaign; Pilyoung Kim, associate professor of psychology at the University of Denver; and Tom Yeh, associate professor of computer science at the University of Colorado Boulder, will serve as co-principal investigators."
Source: EurekAlert!

New cybersecurity technique keeps hackers guessing

"In collaboration with an international team of experts from Virginia Tech, the University of Queensland and Gwangju Institute of Science and Technology, researchers at the U.S. Army Combat Capabilities Development Command, known as DEVCOM, Army Research Laboratory devised a technique called DESOLATOR to help optimize a well-known cybersecurity strategy known as the moving target defense.
"The idea is that it's hard to hit a moving target," said Dr. Terrence Moore, Army mathematician. "If everything is static, the adversary can

"The article examines the cybersecurity status of DLT technology in the holistic context of dynamic management of cyber protection. The advent of the DLT technologies arrived together with the continuous expansion of the surface for cyber-attacks against information systems and communication networks. The analysis is targeted to unknown dangers against the DLT ecosystem."
Source: Springer Link

A Hybrid Recommender System for Cybersecurity Based on a Rating Approach

"The main function of a security analyst is to protect and make the best decisions for preserving the integrity of computer systems within an organization. To provide a quick response, the analyst usually depends on his good judgement, which should lead him to execute manual processes in a limited time. By dealing with too many anomalies, responses are only provided to those threats with the highest level of criticality. This research aims to propose a tool for helping analysts to filter out anomalies and latent risks. To meet this objective, a recommendation system based on collaborative filtering and knowledge was developed, generating ratings of the worst cases with the best available recommendations based on expert judgement. During tests, the system allowed an improvement in the response time from analysts to solve problems. It also eliminated subjectivity and reduced the number of manual processes."
Source: Springer Link

Practitioners' Views on Cybersecurity Control Adoption and Effectiveness

"Cybersecurity practitioners working in organisations implement risk controls aiming to improve the security of their systems. Determining prioritisation of the deployment of controls and understanding their likely impact on overall cybersecurity posture is challenging, yet without this understanding there is a risk of implementing inefficient or even harmful security practices. There is a critical need to comprehend the value of controls in reducing cyberrisk exposure in various organisational contexts, and the factors affecting their usage. Such information is important for research into cybersecurity risk and defences, for supporting cybersecurity decisions within organisations, and for external parties guiding cybersecurity practice such as standards bodies and cyber-insurance companies. Cybersecurity practitioners possess a wealth of field knowledge in this area, yet there has

a meteoric rise in cyber attacks and data breaches.
After seven months of 2021, we have recorded 815 security incidents in total, and 3,980,757,735 breached records."
Source: IT Governance UK

INDUSTRY

Global Network Firewall Market—Evolution Towards Hybrid Data Center Security and SASE

"Network firewalls are one of the oldest solution categories in the cybersecurity market. Much like firewalls that isolate parts of a building to prevent the spread of fire, network firewalls emerged to separate organizations' private networks from the public internet. Early firewalls enabled organizations to inspect incoming and outgoing traffic. Over time, firewalls evolved to include additional functionalities that allow organizations to examine traffic more deeply and provided organizations with more active security controls.
While network firewalls have been evolving in the past years, they did not emerge to secure environments that fully or partially rely on the cloud. The outbreak of the COVID-19 pandemic accelerated the transformation of the organizational perimeter. Since nearly all employees became remote and started using external applications, organizations faced a new challenge of securing decentralized and distributed environments. Because of that, a growing number of organizations will choose the newer generation of firewall solutions that are better suited for today's infrastructure. Secure Access Service Edge (SASE) will take the central stage in the network security market, with the firewall as a service (FWaaS) component gradually replacing legacy firewalls."
Source: Frost & Sullivan

Global BFSI Security Growth Opportunities

"This study examines opportunities for physical security (surveillance, command and control, communication equipment, and screening and detection), cybersecurity (firewalls, antivirus protection, active network detection solutions, and data analytics and storage), and converged security (access control and identity management, risk-averse security services, and managed services)

take their time looking at everything and choosing their targets. But if you shuffle the IP addresses fast enough, then the information assigned to the IP quickly becomes lost, and the adversary has to look for it again.""
Source: EurekAlert!

Creating a new strategy for today's software supply chain security

"The imminent arrival of guidelines of standards for vendors to test their codebase has organizations rushing to evaluate all software components in their supply chain -- if they haven't already begun. However, this is just the first step and more regulations will be rolled out through the year as more cyberattacks take place. For now, it's time for organizations to formulate a new supply chain security strategy for the cybersecurity challenges of today, and to lay the foundation for the future."
Source: Washington Technology

Information security: Developing practical policies and procedures

"Cybersecurity is one of the leading concerns among today's executives and risk management professionals. Yet despite its importance, organizations still lack pragmatic cybersecurity policies and procedures. Even in companies with relatively sophisticated information security functions, written policies and procedures often are designed primarily for compliance purposes instead of functioning as practical, useful tools that can help proactively manage risk."
Source: Security Magazine

CYBER ATTACK

Users Can Be Just As Dangerous As Hackers

"Among the problems stemming from our systemic failure with cybersecurity, which ranges from decades-old software-development practices to Chinese and Russian cyber-attacks, one problem gets far less attention than it should—the insider threat.

But the reality is that most organizations should be at least as worried about user management as they are about Bond villain-type hackers launching compromises from abroad.

Most organizations have deployed single sign-on and modern identity-management solutions. These generally allow easy on-boarding, been little academic work collecting and synthesising their views."
Source: University of Kent

Cybersecurity Policy and Strategy Management in FinTech

"The problem of cybersecurity is not limited to a particular department or section, but it is an enterprise-wide problem. It requires an interdisciplinary approach to address various cybersecurity issues arising from different sources in the organization. A comprehensive cybersecurity policy and strategy ensures healthy cybersecurity practices in the organization. This chapter provides an overwhelming introduction to the cybersecurity policies and strategies used to protect FinTech institutions from deadly cyberattacks. It prevents several cyberattacks by following fundamental cyber practices and educating users, employees, and people in the organization. These policies provide an extensive overview of a wide range of cyber practices, from selecting a password to predicting a cyberattack."
Source: Springer Link

CYBER ATTACKS

The Global Cyber Security Model: Counteracting Cyber Attacks through a Resilient Partnership Arrangement

"In this paper, insights are provided into how senior managers can establish a global cyber security model that raises cyber security awareness among staff in a partnership arrangement and ensures that cyber attacks are anticipated and dealt with in real time. We deployed a qualitative research strategy that involved a group interview involving cyber security and intelligence experts. The coding approach was used to identify the themes in the data and, in addition, a number of categories and subcategories were identified. The mind map approach was utilized to identify the thought processes of senior managers in relation to ensuring that the cyber security management process is effective. The global cyber security model can be used by senior managers to establish a framework for dealing with a range of cyber security attacks, as well as to upgrade the cyber security skill and knowledge base of individuals."

through 2030. It takes a closer look at market drivers and restraints, forecasts revenue for the decade, and lists the top competitors in each of the three market segments. It includes an industry threat and vulnerability analysis, presents selected results from a 2020 Frost & Sullivan information technology decision maker survey, and considers the new technologies that are available or being developed for each market segment."
Source: Frost & Sullivan

Cybersecurity Update

"In July 2020, we looked at Cybersecurity as the new frontier for investors. We said that the security of data and information must be paramount for all businesses and individuals. We claimed that there was still a lack of understanding of how easy it is to breach an unsecured environment. We made the case that cybersecurity will be amongst the fastest growing industries, expected to see high investments in online security and further M&A activity. Our thoughts were supported by a panel of experts from Akamai, Clango, Ibex Investors, and IHS Markit colleagues.

2020 was declared the worst year ever for cyberattacks by the US Department of Justice. That same department created a Ransomware Task Force in April 2021 as the number of attacks kept increasing and we can confidently say that 2021 is already worse than the previous year.

The European Commission announced plans to build a Joint Cyber Unit, run by a dedicated team of multinational experts that can be rapidly deployed to European countries in case of serious attacks, as the number of major incidents in Europe rose from 432 in 2019 to 756 in 2020."
Source: IHS Markit

user management, and off-boarding."
Source: The Hacker News

Why academic institutions are at risk of cyber attacks, and the library's role in cyber security and risk assessment

"Usually the risk of a cyberattack is not focused on one department but it exists across the whole organization. This means that every part of the organization has to have an awareness of security, says Brill. So for example, if you have a bookstore on campus that offers credit and debit card payments, it is important, that they follow payment card industry standards. Or if the campus has a healthcare facility, the university needs to make sure, that this data is stored securely, explains Brill. He points out that this is also true for libraries for whom information is at the center of their work. Libraries have to take the responsibility for securing their parts of the system, and be an active participant in the overall cybersecurity strategy.

According to Brill, when operationalizing cybersecurity, there is a deep intertwining between the elements. The library knows the information that it wants and it understands how that information should be appropriately distributed. The IT department will then, based on the library's instructions, make sure only people that are part of the university's network are given access to resources."
Source: Research Information

'Barely able to keep up': America's cyberwarriors are spread thin by attacks

"The cybersecurity industry is stretched thin. Ransomware attacks are now so prolific that some companies simply cannot help every newly hacked victim get back online. And a shortage of workers means no immediate help in sight."
Source: NBC News

Toyota, Nissan, others tie up to protect cars from cyberattack

"Ninety companies, including Toyota Motor and Nissan Motor, will form a consortium to protect connected cars from cyberattacks, Nikkei has learned.

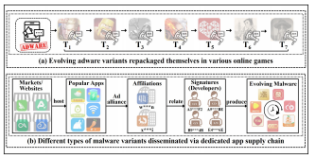
The companies will check their automotive software for security flaws and share information such as cyberattack trends to prevent hijacking and data theft. Companies are stepping up such efforts as self-driving cars come closer to reality.

Information technology companies such as Microsoft Japan, Trend Micro, NTT Communications and Sompo
Source: MDPI

A Framework for Modeling Cyber Attack Techniques from Security Vulnerability Descriptions

"Attack graphs are one of the main techniques used to automate the cybersecurity risk assessment process. In order to derive a relevant attack graph, up-to-date information on known cyber attack techniques should be represented as interaction rules. However, designing and creating new interaction rules is a time consuming task performed manually by security experts. We present a novel, end-to-end, automated framework for modeling new attack techniques from the textual description of security vulnerabilities. Given a description of a security vulnerability, the proposed framework first extracts the relevant attack entities required to model the attack, completes missing information on the vulnerability, and derives a new interaction rule that models the attack; this new rule is then integrated within the MulVal attack graph tool. The proposed framework implements a novel data science pipeline that includes a dedicated cybersecurity linguistic model trained on the NVD repository, a recurrent neural network model used for attack entity extraction, a logistic regression model used for completing the missing information, and a transition probability matrix for automatically generating new interaction rule."
Source: ACM Digital Library

MALWARE



Heterogeneous Temporal Graph Transformer: An Intelligent System for Evolving Android Malware Detection

"The explosive growth and increasing sophistication of Android malware call for new defensive techniques to protect mobile users against novel threats. To address this challenge, in this paper, we propose and develop an intelligent system named Dr.Droid to jointly model malware propagation and evolution for their detection at the first attempt. In Dr.Droid, we first exploit higher-level semantic and social relations within the ecosystem (e.g., app-market, app-developer, market-developer relations etc.) to characterize app propagation patterns; and then we present a structured heterogeneous graph to

Japan Insurance will join a group of carmakers, including Toyota and Nissan, and parts manufacturers such as Denso and Panasonic."
Source: Nikkei Asia

Why CISA's China Cyberattack Playbook Is Worthy of Your Attention

"At first glance, last week's advisory on state-sponsored China cyberattacks by the FBI and the Cybersecurity and Infrastructure Security Agency is nothing new. It outlines the tactics, techniques, and procedures they use. Plus, not every data center contains information that's of interest to the Chinese government.
But the report should be required reading for many, if not most, people that manage security on data center networks. That's because A) Companies that could potentially be impacted here go far beyond just those of direct strategic interest to China; B) The report includes a list of specific indicators of intrusion by if this particular set of attackers — which would help inform a response plan; and C) It includes both a set of recommended mitigation measures and contact information for the FBI and CISA offices working to address this threat who could be of assistance."
Source: Data Centre Knowledge

SOFTWARE

Keylime security software is deployed to IBM cloud

"Keylime, a cloud security software architecture, is being adopted into IBM's cloud fleet. Originally developed at MIT Lincoln Laboratory to allow system administrators to ensure the security of their cloud environment, Keylime is now a Cloud Native Computing Foundation sandbox technology with more than 30 open-source developers contributing to it from around the world. The software will enable IBM to remotely attest to the security of its thousands of cloud servers.
"It is exciting to see the hard work of the growing Keylime community coming to fruition," says Charles Munson, a researcher in the Secure Resilient Systems and Technology Group at Lincoln Laboratory who created Keylime with Nabil Schear, now at Netflix."
Source: MIT News

model the complex relations among different types of entities. To capture malware evolution, we further consider the temporal dependence and introduce a heterogeneous temporal graph to jointly model malware propagation and evolution by considering heterogeneous spatial dependencies with temporal dimensions."
Source: ACM Digital Library

Polymorphic and Metamorphic Malware

"CISOs must ensure that their cyber programs can detect and block the Advanced Evasion Techniques (AETs) of Metamorphic and Polymorphic Malware. This capability should exist at the endpoint, network and perimeter security stack and works best when data can be correlated across these three domains within the SIEM and generate targeted events (within a minimum number of false positives) that can be used by incident responders within the SOC and also by automated reactive response orchestration wherever possible. This chapter describes these types of advanced malware and their AETs, and discusses detection techniques."
Source: Springer Link

The Advanced Malware Prevention Playbook

"This chapter provides cyber risk assessment, detection, mitigation, and remediation practices for advanced malware including ransomware. The threat prevention and mitigation techniques include continuous patching, proactive hardening, secure backups, DNS sinkholing, kill-switch deployment, and reduction of the reliance on third party patching directly in production systems."
Source: Springer Link

ARTIFICIAL INTELLIGENCE

The future of Artificial Intelligence in Cybersecurity: A Comprehensive Survey

"AI in Cybersecurity Market scheme helps organizations in observance, detecting, reporting, and countering cyber threats to keep up information confidentiality. The increasing awareness among folks, advancements in info technology, up-gradation of intelligence and police work solutions, and increasing volume of knowledge gathered from numerous sources have demanded

MetricStream Raises Bar for Compliance, Cyber Security and Risk Management with Brazos Software Release

"MetricStream, the market leader in integrated risk management and governance, risk management, and compliance (GRC), today unveiled its latest software release, Brazos, which includes a myriad of innovations; highlighted by simplified regulatory compliance and real-time, integrated intelligence on regulatory changes, advanced IT and cyber risk quantification, and AI-powered recommendations for vendor risk management. The Brazos release sets a new standard by implementing artificial intelligence into multiple GRC products, as well as providing a simplified user experience and agility for faster time to value."
Source: PR Newswire

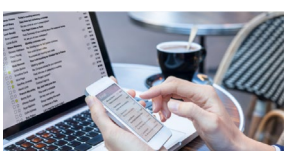
TECHNOLOGY

Is Your Mobile Provider Tracking Your Location? This New Technology Could Stop It.

"For the first time, researchers at the University of Southern California (USC) Viterbi School of Engineering and Princeton University have found a way to stop this privacy breach using existing cellular networks. The new system, presented at USENIX Security conference on Aug. 11, protects users' mobile privacy while providing normal mobile connectivity.

The new architecture, called "Pretty Good Phone Privacy" or PGPP, decouples phone connectivity from authentication and billing by anonymizing personal identifiers sent to cell towers. The software-based solution, described by the researchers as an "architecture change," does not alter cellular network hardware."
Source: USC School of Engineering

MALWARE



Mobile Malware: Threats and Solutions

"As users have increasingly moved from desktop operating systems to mobile devices as their primary form of computing, cyber attackers have taken notice and malware has followed. While the total volume of mobile malware is a fraction of that the utilization of reliable and improved cybersecurity solutions all told industries. The increase in the incidence and quality of cyber-attacks is driving AI-enabled cyber systems. Increasing incidents of huge cyber-attacks globally have created awareness among organizations for securing their information. The motive behind these cyber-criminals are political competition, competitors move for gain and harming the name of others, international information theft, and radical non-secular cluster interest. Most cyber-attacks are for gain. In this review we have presented some previous studies related to Cybersecurity which involves AI."
Source: EPrints

Towards a Machine Learning Based Situational Awareness Framework for Cybersecurity: An SDN Implementation

"The ever-increasing number of internet-connected devices, along with the continuous evolution of cyber-attacks, in terms of volume and ingenuity, has led to a widened cyber-threat landscape, rendering infrastructures prone to malicious attacks. Towards addressing systems' vulnerabilities and alleviating the impact of these threats, this paper presents a machine learning based situational awareness framework that detects existing and newly introduced network-enabled entities, utilizing the real-time awareness feature provided by the SDN paradigm, assesses them against known vulnerabilities, and assigns them to a connectivity-appropriate network slice. The assessed entities are continuously monitored by an ML-based IDS, which is trained with an enhanced dataset. Our endeavor aims to demonstrate that a neural network, trained with heterogeneous data stemming from the operational environment (common vulnerability enumeration IDs that correlate attacks with existing vulnerabilities), can achieve more accurate prediction rates than a conventional one, thus addressing some aspects of the situational awareness paradigm. The proposed framework was evaluated within a real-life environment and the results revealed an increase of more than 4% in the overall prediction accuracy."
Source: MDPI

Enhancing Cybersecurity via Artificial Intelligence: Risks, Rewards, and Frameworks

"Recent advances in artificial intelligence challenge classical models of productivity by increasing the scale, complexity, and range of tasks that can be meaningfully

created for desktops, it is nonetheless a growing security concern, as more and more high-value and sensitive tasks are performed on mobile devices."
Source: ESecurity Planet

Microsoft warning: This unusual malware attack has just added some new tricks

"Microsoft's Security Intelligence team is once again raising an alarm about the call center phishing and malware group behind what it calls BazaCall.
"We are tracking multiple active email campaigns that use BazarLoader to deliver a wide range of payloads. These campaigns appear disparate but share a common trait: their tactics attempt to challenge conventional email security solutions and best practices," Microsoft said in a tweet."
Source: ZD Net

Discord malware is a persistent and growing threat warns Sophos

"A few weeks back, leading cybersecurity company Sophos issued a warning that Discord is becoming an increasingly common target for hackers. The vicious few pushing out malware tend to target users of successful online services, and considering Discord's 140 million plus active users—with over 300 million registered to date—that makes the chat software a pretty juicy target.
Sophos notes the number of malware detections over the past couple of months has grown by almost 140 times what it was for the same period last year. And part of that problem comes down to how Discord files are stored in the cloud."
Source: PC Gamer

How To Protect Against Macro-Based Malware

"Macro-based malware in Microsoft Office products has been around since the '90s. However, since users have learned to combat it, it fell off the radar with hackers. N-Able, a technology partner for managed service providers, reported it's starting to see a resurgence of these attacks over the past few years — and they're not the only ones.
Cybercriminals are using social engineering to convince users to turn on macros to allow their malware to run (i.e. Locky). Typically, macro malware is transmitted through phishing emails containing malicious attachments."
Source: My Tech Decisions

Google can take two months to remove malware apps from app store

automated, including those associated with cybersecurity."
Source: IEEE Xplore

Cyber threat intelligence challenges: Leveraging blockchain intelligence with possible solution

"Technology of cyber threat intelligence (CTI) is a proof-based defense framework that proactively reacts by monitoring and exchanging security-related information of advanced cyber threats among different industries. The efficiency of CTI systems may be considerably impeded by developing and disseminating inappropriate protection policies. Although global attention is on the health and the economic challenges raised by COVID-19, this epidemic is certainly being exploited by cybercriminals across the globe. The attackers use the COVID-19 to embellish brands in a way that causes workers and consumers to make mistakes, spam, and ransomware attacks are at peak. In this article, we discuss many current and new cyber threat challenges and examine the latest case analysis. Finally, we have proposed a new system on Collaborative Cyber Threat Information Exchange (CCTI) underlining a wider group's capacity to help to recognize faults via an artificial intelligence computing essence focused on blockchain."
Source: Science Direct

Using a Collated Cybersecurity Dataset for Machine Learning and Artificial Intelligence

"Artificial Intelligence (AI) and Machine Learning (ML) algorithms can support the span of indicator-level, e.g. anomaly detection, to behavioral level cyber security modeling and inference. This contribution is based on a dataset named BRON which is amalgamated from public threat and vulnerability behavioral sources. We demonstrate how BRON can support prediction of related threat techniques and attack patterns. We also discuss other AI and ML uses of BRON to exploit its behavioral knowledge."
Source: Cornell University

GOVERNANCE

Shaping the ground for bilateral cybersecurity negotiations

"Apps that potentially contain malware remain on the Google Play Store for an average of 77 days after being detected, according to an analysis of software.
"The impression has been that app markets are doing a great job taking down malicious apps, so the problem is basically solved," says Gianluca Stringhini at Boston University. "It's not as much of a solved problem as is thought."
Source: New Scientist

RISK MANAGEMENT

Five Key Steps in Cybersecurity Risk Management

"For organizations, cybersecurity is a non-negotiable area of investment in order to protect their precious technical and financial data along with their IP content. Risks in cybersecurity can impact organizations at any point in time without warnings in advance. Such attacks and threats can be exceptionally difficult to handle once they are successfully executed by cyber criminals. Therefore, corporations must proactively manage cybersecurity risks to prevent cyber attacks. A specialized cybersecurity team in such organizations can create and regularly update a robust risk management plan. Here are the steps organizations can take while managing real-time cybersecurity risks."
Source: CXO Today

CLOUD SECURITY

5 Cybersecurity Tactics To Protect The Cloud

"Cybersecurity and risk management have moved on top of the boardroom agenda. According to a Gartner survey 61 percent of chief information officers (CIOs) are increasing their investment in cyber and information security. The global research and advisory firm predicts that the spending on information security and risk management technology and services will increase by 12.4 percent by the end of this year. Even more telling is that companies started adding cyber security experts directly to the board."
Source: Forbes

"Cyber issues are important for the bilateral relationship between China and the United States, but there are serious obstacles to reaching agreement on cybersecurity. Meaningful negotiation is not possible in the near term, given China's disinterest in compromise, except on its own terms, and the unfavorable U.S. position inherited by the Biden Administration. China is unlikely to make concessions and the U.S. is unlikely to accept at face value any concession China might offer to make. Progress is also hampered by the outdated concepts used in bilateral cybersecurity discussions, such as stability, escalation, or deterrence. These terms are inherited from the Cold War and no longer provide a useful conceptual framework or lexicon. The most pressing issues are cyber espionage and political interference using cyber means. The prospects for bilateral agreement on these topics are limited. Both the U.S. and China lack incentives to reach agreement."
Source: Springer Linnk

The relationship between online political participation and privacy protection: evidence from 10 Asian societies of different levels of cybersecurity

"Information disclosure during online political activities can place participants under the threat of personal data leakage and misuse, but privacy protection in the context of online political participation has rarely been studied. This study examined how online political participation is related to privacy protection behaviours. Using survey data of internet users from 10 Asian societies, our study suggests two important findings. First, online political participation was found to be positively related to privacy protection behaviours. Second, we examined whether such a positive association can be explained by two mediators: perceived privacy risk and internet efficacy, in countries of different cybersecurity capacity. Our data suggest that internet efficacy mediates the relationship between online political participation and privacy protection behaviours across countries with different levels of cybersecurity capacity, while perceived privacy risk only mediates the effects of online political participation on privacy protection behaviours in countries of low cybersecurity capacity."
Source: Taylor & Francis

SMART CITY

PHISHING

Phishing Attacks Often Target Small Businesses – Here's What to Watch for

"The most successful phishing attacks are those that combine technical expertise, e.g., the ability to spoof an email so it appears credible, with a little bit of online research such as identifying employees and their roles in the company. So, how can companies protect themselves against this type of attack?

The first thing is to understand that scammers can be extremely sophisticated and that any company may be vulnerable to this type of attack. Sometimes, it is hard to tell if an email is genuine. Second, appreciate that human factors are frequently exploited when it comes to phishing emails."

Source: Tripwire

This 'unique' phishing attack uses Morse code to hide its approach

"Microsoft has revealed the inner-workings of a phishing attack group's techniques that uses a 'jigsaw puzzle' technique plus unusual features like Morse code dashes and dots to hide its attacks.

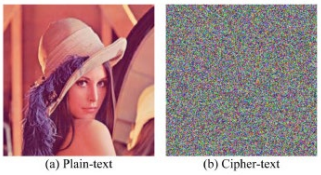
The group is using invoices in Excel HTML or web documents to distribute forms that capture credentials for later hacking efforts. The technique is notable because it bypasses traditional email filter systems.

"The HTML attachment is divided into several segments, including the JavaScript files used to steal passwords, which are then encoded using various mechanisms. These attackers moved from using plaintext HTML code to employing multiple encoding techniques, including old and unusual encryption methods like Morse code, to hide these attack segments," Microsoft Security Intelligence says."

Source: ZD Net

MEDICAL TECHNOLOGY

Cybersecurity by Design in Medical Devices



Quantum-Inspired Blockchain-Based Cybersecurity: Securing Smart Edge Utilities in IoT-Based Smart Cities

"Blockchain plays a vital task in cybersecurity. With the exerted efforts for realising large-scale quantum computers, most current cryptographic mechanisms may be hacked. Accordingly, we need a quantum tool utilised for designing blockchain frameworks to have the ability to be executed in the level of digital computers and resist the probable attacks from both digital and quantum computers. Quantum walks may be utilised as a quantum-inspired model for designing new cryptographic algorithms. In this paper, we present a new authentication and encryption protocol based on quantum-inspired quantum walks (QIQW). The proposed protocol is utilized to build a blockchain framework for secure data transmission among IoT devices."

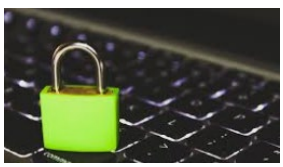
Source: Elsevier

Enhanced Cybersecurity in Smart Cities: Integration Methods of OPC UA and Suricata

"The increasing urbanisation and digitalisation taking place all around the world has increased the interest in Smart Cities (SCs). The main goal of any SC is to provide a high quality of life to its citizens by enhancing the quality of the public and private services. However, mass-adoption of the IoT technology and IT technology creates a series of security challenges that must be addressed. One of the most popular machine-to-machine communication protocols is OPC UA, and a widely accepted intrusion detection and prevention system is Suricata. The goal of this research is to find theoretical solutions upon which a successful integration can be achieved. The advantages and disadvantages are examined, and alternative methods are proposed."

Source: Springer Link

SECURE SOFTWARE DEVELOPMENT



"Medical devices and medical software are becoming increasingly connected to hospital networks, other medical devices or the Internet. As a result, manufacturers and developers are required to consider cybersecurity from the very early stages of development. This in turn necessitates comprehensive risk management along the entire lifecycle of a device."
Source: Medtech Intelligence

REMOTE WORKING

Why remote working leaves us vulnerable to cyber-attacks

"A cyber-crime group known as REvil took meticulous care when picking the timing for its most recent attack - US Independence Day, 4 July.
They knew many IT specialists and cyber-security experts would be on leave, enjoying a long weekend off work. Before long, more than 1,000 companies in the US, and at least 17 other countries, were under attack from hackers. Many firms were forced into a costly downtime period as a result.
Among those targeted during the incident was a well-known software provider, Kaseya."
Source: BBC

VIDEO CONFERENCING

How to pick a high-security video conferencing platform

"Tom Eagle, a senior director, analyst at Gartner, said that security for meeting software such as video conferencing has become a higher priority over the last year as organizations struggled with work-from-home and now hybrid work arrangements.
Eagle said the three pillars of security are cloud infrastructure and the network and application layers.
"All three should be considered by enterprise buyers in their evaluations of meeting solutions," he said.
Gartner has developed guidance for enterprise buyers to use when evaluating the security of conferencing and collaboration platforms."
Source: Tech Republic

Locating the Perpetrator: Industry Perspectives of Cellebrite Education and Roles of GIS Data in Cybersecurity and Digital Forensicsv

"Geographic Information Systems (GIS) data is incorporated into cybersecurity and digital forensics at many levels from the development of secure code, to the metadata stored by systems and employed during civil and criminal cases. This paper reports on the role of GIS Data in the development of both systems and the development of legal probable cause. Specifically, we report on how GIS data is incorporated into three advanced courses: Wireless Security, Secure Software Development, and Forensic Investigation of Wireless Network and Mobile Devices. GIS data needs to be accurate for many reasons including probable cause. We report on IRB-approved student surveys about their experience in the three courses. We find that overall students liked the courses and offered insights into future course improvements."
Source: Springer Link

REMOTE WORKING

Cybersecurity Awareness on Video Conferencing Service During Coronavirus Pandemic

"The entire world is looking for a solution that helps us to come out of the current pandemic situation caused by the novel coronavirus. It has not only caused lakhs of death but also the biggest economic shutdown. In this scenario, with the need for social distancing the world needs to have a certain strategy to sustain. Even though online e-commerce has hit new highs, now it is growing even faster with video conferencing service; here the need for awareness of cybersecurity comes into action. Since the entire population is depended on the information technology, all age people without awareness of securing themselves from cyberattack use the technology which creates lots of problem for the end user and the provider of that service. This paper considers the statistics on the cybersecurity awareness on video conferencing service from the different level of users of different age group."
Source: Springer Link

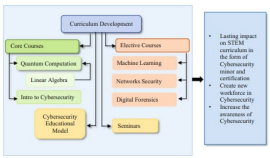
AUTOMOTIVE

Cybersecurity in Automotive: An Intrusion Detection System in Connected Vehicles

"Today's modern vehicles are connected to a network and are considered smart objects of IoT, thanks to the capability to send and receive data from the network. One of the greatest challenges in the automotive sector is to make the vehicle secure and reliable. In fact, there are more connected instruments on a vehicle, such as the infotainment system and/or data interchange systems. Indeed, with the advent of new paradigms, such as Smart City and Smart Road, the vision of Internet of Things has evolved substantially. Today, we talk about the V2X systems in which the vehicle is strongly connected with the rest of the world. In this scenario, the main aim of all connected vehicles vendors is to provide a secure system to guarantee the safety of the drive and persons against a possible cyber-attack. So, in this paper, an embedded Intrusion Detection System (IDS) for the automotive sector is introduced. It works by adopting a two-step algorithm that provides detection of a possible cyber-attack. In the first step, the methodology provides a filter of all the messages on the Controller Area Network (CAN-Bus) thanks to the use of a spatial and temporal analysis; if a set of messages are possibly malicious, these are analyzed by a Bayesian network, which gives the probability that a given event can be classified as an attack."

Source: MDPI

TRAINING



Enhancing the Cybersecurity Education Curricula Through Quantum Computation

"Governmental and corporate networks are increasingly at risk, malicious acts are escalating abruptly, and organized crime and terrorist groups are expanding and improving their cyber capabilities. Individuals and countries have initiated attacks against others, including the public and private sectors. Hiring qualified cybersecurity experts is currently considered to be the highest priority in the United

States. Quantum computation is a revolutionary technology for Cybersecurity education. The traditional digital computers run on encoded data according to the standard binary system 0 or 1. With the emerging of quantum computation, quantum computers run qubits or quantum bits instead of binary data 0 and 1. Quantum computation is vital for Cybersecurity education. The overarching goal of this chapter is to present a cybersecurity educational model with a focus on quantum computation. The given education model is designed according to the National Institute of Standard and Technology (NIST), and the industry's expectations regarding the knowledge, training, and skills that cybersecurity experts should possess."
Source: Springer Link

Evaluation Strategies for Cybersecurity Training Methods: A Literature Review

"The human aspect of cybersecurity continues to present challenges to researchers and practitioners worldwide. While measures are being taken to improve the situation, a vast majority of security incidents can be attributed to user behavior. Security and Awareness Training (SAT) has been available for several decades and is commonly given as a suggestion for improving the cybersecurity behavior of end-users. However, attackers continue to exploit the human factor suggesting that current SAT methods are not enough. Researchers argue that providing knowledge alone is not enough, and some researchers suggest that many currently used SAT methods are, in fact, not empirically evaluated. This paper aims to examine how SAT has been evaluated in recent research using a structured literature review. The result is an overview of evaluation methods which describes what results that can be obtained using them."
Source: Springer Link

Minimizing Cognitive Overload in Cybersecurity Learning Materials: An Experimental Study Using Eye-Tracking

"Cybersecurity education is critical in addressing the global cyber crisis. However, cybersecurity is inherently complex and teaching cyber can lead to cognitive overload among students. Cognitive load includes: 1) intrinsic load (IL- due to inherent difficulty of the topic), 2) extraneous (EL- due to presentation of material), and 3) germane (GL- due to extra effort put in for learning). The challenge is to minimize IL and EL and maximize GL. We propose a model to develop cybersecurity learning

materials that incorporate both the Bloom's taxonomy cognitive framework and the design principles of content segmentation and interactivity. We conducted a randomized control/treatment group study to test the proposed model by measuring cognitive load using two eye-tracking metrics (fixation duration and pupil size) between two cybersecurity learning modalitie."
Source: Springer Link

Securing CHEESEHub: A Cloud-based, Containerized Cybersecurity Education Platform

"The Cyber Human Ecosystem for Engaged Security Education (CHEESEHub) is an open web platform that hosts community-contributed containerized demonstrations of cybersecurity concepts. In order to maximize flexibility, scalability, and utilization, CHEESEHub is currently hosted in a Kubernetes cluster on the Jetstream academic cloud. In this short paper, we describe the security model of CHEESEHub and specifically the various Kubernetes security features that have been leveraged to secure CHEESEHub. This ensures that the various cybersecurity exploits hosted in the containers cannot be misused, and that potential malicious users of the platform are cordoned off from impacting not just other legitimate users, but also the underlying hosting cloud."
Source: ACM Digital Library