SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN

21 AUGUST – 22 OCTOBER 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 | academic | reports

CYBERSECURITY

New govt cyber-security tool being developed to protect Singaporeans' phones from hackers

"A new mobile tool for Singaporeans to secure their smartphones from cyber-security threats is being developed by the Government and industry partners.

This comes amid growing cases of cyber criminals targeting mobile devices as people are becoming more reliant on these gadgets, said the Cyber Security Agency of Singapore (CSA).

The tool is one of the initiatives outlined in Singapore's new cyber-security strategy that was announced on Tuesday (Oct 5) by Senior Minister and Coordinating Minister for National Security Teo Chee Hean."

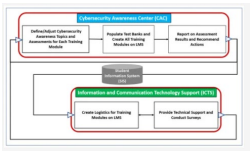
Source: Straits Times

New regional cybersecurity training centre opens in Singapore

"A new regional cybersecurity training centre that will see ASEAN member states work together to conduct research, share knowledge and train to respond to cyber threats, opened on Wednesday (Oct 6), three years after it was first announced.

Located in the city centre at North Bridge Road, the ASEAN-Singapore Cybersecurity Centre of Excellence

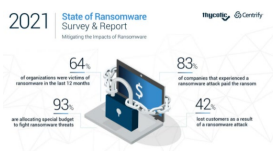
CYBERSECURITY



Cybersecurity Awareness Framework for Academia

"Cybersecurity is a multifaceted global phenomenon representing complex socio-technical challenges for governments and private sectors. With technology constantly evolving, the types and numbers of cyberattacks affect different users in different ways. The majority of recorded cyberattacks can be traced to human errors. Despite being both knowledge- and environment-dependent, studies show that increasing users' cybersecurity awareness is found to be one of the most effective protective approaches... This work proposes a conceptual Cybersecurity Awareness Framework to guide the implementation of systems to improve the cybersecurity awareness of graduates in any academic institution. This framework comprises constituents designed to continuously improve the development, integration, delivery, and assessment of cybersecurity knowledge into the curriculum of a university across different disciplines and majors; this framework would thus lead to a better awareness among all university graduates, the future workforce. This framework may be adjusted to serve as a blueprint that, once adjusted by academic institutions to accommodate their missions, guides

CYBERSECURITY



2021 State of Ransomware Survey & Report

"The odds of your organization experiencing a ransomware attack are growing every day. This new research report from ThycoticCentrify reveals two out of three companies surveyed were victims of a cyberattack in the last 12 months—and more than four out of five felt they had no choice but to pay the ransom demands.

The 2021 State of Ransomware Survey & Report will help you:

- Understand the risks of extended dwell time—the time from the point of breach until actual ransomware attack launch
- See where companies are increasing their cyber security budgets in response
- Prioritize prevention and incident response to contain the threat and limit damage."

Source: Thycotic

The Singapore Cybersecurity Strategy 2021

"The Singapore Cybersecurity Strategy 2021 outlines Singapore's updated goals and approach to adapt to a rapidly evolving strategic and technological environment. Potential disruptive technologies such as edge computing and quantum

(ASCCE) has two training labs that can hold up to 100 participants, and other conference rooms and amenities to facilitate capacity building efforts."
Source: Channel News Asia

Google, Microsoft and Oracle amassed the most cybersecurity vulnerabilities in the first half of 2021

"In the first six months of 2021, Google and Microsoft have "accumulated the most vulnerabilities," according to Atlas VPN findings based on a recent Telefonica Tech report. Among companies with the most accumulated security vulnerabilities to start 2021, Google claimed the top spot with 547; followed by Microsoft with 432, per AtlasVPN.
In a post, author of the report and cybersecurity researcher William S. said "exploiting Google products like Chrome is popular among cybercriminals," making note of the large user base, "meaning that more internet users can become victims of the exploits." As for runner-up Microsoft, William S. said that "state-sponsored threat actors from China abused Microsoft Exchange Server vulnerabilities to carry out ransomware attacks," adding that "other attackers would drop cryptocurrency miners from the post-exploit web shells."
Source: Tech Republic

Google launches Cybersecurity Action Team

"Google announced this week the launch of its Cybersecurity Action Team, aimed at assisting governments, critical infrastructure organizations, enterprises and small businesses.
The team's goal will be to guide customers through the cycle of security transformation, including creating a road map, increasing cyber-resilience preparedness and engineering new solutions in response to changing circumstances.
The effort will begin within Google Cloud, eventually expanding to more organizations."
Source: Healthcare IT News

Why cyber security and regulatory compliance are one and the same

"Cyber security and regulatory compliance have long been considered two largely separate issues. Regulatory compliance involves following a set of tangible and distinct guidelines and ensuring the company meets deadlines for new rules. In contrast, cyber security largely involves preparing for the institutions in developing or amending their policies and procedures for the design and assessment of cybersecurity awareness."
Source: MDPI

Cybersecurity and Fatigue: Does fatigue from visual contrast impact our ability to correctly classify emails?

"Email phishing schemes represent a constant threat to personal and organizational security. To combat this threat, it is critical to develop a firm understanding of the factors that affect email classification performance. One such factor might be fatigue. Work performance research shows that fatigue impairs information processing, shortens attention span, and slows reaction times. Studies have demonstrated that elevated screen use can induce fatigue that leads to such impairments (Jeong, 2012; Lin et al., 2008). Specifically, Bhattacharyya et al. (2014) showed that changes in text-background contrast induce fatigue. The current study examined whether fatigue impacts email classification performance. Participants first read a series of text-excerpts on a computer screen and answered comprehension questions, after which they classified 100 emails (4 blocks; 25 emails per block) as either legitimate or non-legitimate (50% legitimate; see Sarno et al., 2020)."
Source: Journal of Vision

Digital Transformation and Cybersecurity of Critical Infrastructures

"Critical infrastructures are vital assets for public safety, economic welfare, and the national security of nations. Vulnerabilities of critical infrastructures have increased with the widespread use of information technologies. As Critical National Infrastructures are becoming more vulnerable to cyberattacks, their protection becomes a significant issue for any organization as well as nation. The risks to continued operations from failing to upgrade ageing infrastructures or not meeting mandated regulatory regimes are considered higher given the demonstrable impact of such circumstances.
Due to the rapid increase in sophisticated cyber threats targeting critical infrastructures with significant destructive effects, cyber security of critical infrastructures has become an agenda item for academics, practitioners, and policy makers. In recent years, cyber attacks, especially those targeting systems that keep or process sensitive information, are becoming more sophisticated. Attacks to such critical technologies are on the horizon. Threat actors are becoming more sophisticated and taking advantage of increasingly ubiquitous connectivity to launch more cyberattacks. Singapore thus reviewed and refreshed its cybersecurity strategy, which was first launched in 2016.
Cybersecurity is a team sport, and everyone has a part to play. Developed in consultation with multiple stakeholders, including industry, and local and overseas academia, Strategy 2021 seeks to actively defend our cyberspace, simplify cybersecurity for end-users, and promote the development of international cyber norms and standards. Workforce and ecosystem development are the foundations of this strategy."
Source: CSA Singapore

Allianz: Companies need to strengthen cyber controls to counter ransomware pandemic

"During the Covid-19 crisis another outbreak has happened in cyber space: a digital pandemic driven by ransomware. Malware attacks that encrypt company data and systems and demand a ransom payment for release are surging globally. The increasing frequency and severity of ransomware incidents is driven by several factors: the growing number of different attack patterns such as 'double' and 'triple' extortion campaigns; a criminal business model around 'ransomware as a service' and cryptocurrencies; the recent skyrocketing of ransom demands; and the rise of supply chain attacks. In a new report, cyber insurer Allianz Global Corporate & Specialty(AGCS) analyzes the latest risk developments around ransomware and outlines how companies can strengthen their defenses with good cyber hygiene and IT security practices."
Source: Allianz

US Healthcare Cybersecurity Growth Opportunities

"The research service will provide an overview of the US healthcare cybersecurity market from 2021 to 2026. Healthcare cybersecurity includes those systems, applications, and IT-enabled services that assess third-party vendor risks, safeguard data networks, privatize cloud-based access management, and ensure the state-of-the-art security of all IT systems, medical devices, and IoT-based sensors connected through centralized wireframes.
The report provides a detailed segment analysis of the healthcare cybersecurity market. It covers industry challenges and various

unknown and future challenges that may face a business.
As a result, regulatory compliance is often prioritised over cyber security because it is seen as more urgent. Adopting this approach is misguided as a lack of adequate preparation for cyber attacks can lead to all manner of compliance issues in the future.
As the challenges facing leaders continue to mount, businesses need to remodel their approach, and consider both cyber security and compliance as being two sides of the same coin."
Source: Continuity Central

CYBER ATTACK

Cyber-attack Response Takes More than Two Working Days

"Organizations around the world take on average more than two business days to respond to a cyber-attack, according to new research by American cybersecurity company Deep Instinct.
The finding was published in the company's second bi-annual *Voice of SecOps Report*, which was based on a survey of 1,500 senior cybersecurity professionals in 11 countries who work for businesses with more than 1,000 employees and annual revenue north of $500m.
The survey revealed the average global response time to a cyber-assault to be 20.09 hours. Companies within the financial sector were faster to respond, taking on average 16 hours to react.
Larger companies also answered threats faster, clocking up an average response time of 15 hours. Smaller companies were found to be slower at responding, taking an average of 25 hours to make their move."
Source: Info Security

The real-world impacts of cyberattacks

"Gartner predicts that by 2025 cyberattackers will have weaponized operational technology environments to successfully harm or kill humans. Ambulances rerouted. Gas supplies were disrupted, leading to days of long lines and high prices. Disruption to food suppliers causing shortages.
These are the real-life impacts of cyberattacks. Cyberattacks are seemingly in the news every day, and while sometimes they merely cause inconvenience, they often also have dire consequences. Cyberattacks in critical infrastructure and healthcare sectors don't just affect data – they systems include penetrations to their network and the installation of malicious tools or programs that can reveal sensitive data or alter the behaviour of specific physical equipment. A holistic view, which covers technical, policy, human, and behavioural aspects, is essential to handle the the cyber security of critical infrastructures effectively."
Source: MDPI

Four-Factor Authentication with Emerging Cybersecurity for Mobile Transactions

"Cybersecurity is very much essential for Mobile Transactions to complete seamlessly. Mobile Commerce (Mcom.) is the very basic transaction type, which is very commonly used (two in five people use mobile as transaction medium). To secure this, there are various technologies used by this research. The four "factors" formally known as Multi-Factor-Authentication are: two of them are Traditional methods (User Login password and One Time Password (aka OTP)) with addition of Geolocation and Facial Recognition. All the data is converted to a text file, which is hidden in an image (using Babushka algorithm). The end-point then decrypts the image using the same algorithm."
Source: Springer Link

A primer on insider threats in cybersecurity

"Though human factors are increasingly being acknowledged as a contributor to cybersecurity incidents, this domain is not widely understood by those in technical and applied disciplines. Humans can be influenced, are not always rational or predictable, and must be studied through psychology rather than technology. Consequently, this domain may represent uncharted territory for the technical practitioner leaving many promising areas of research and practice unexplored. This paper provides a broad primer on human factors in cybersecurity, specifically focusing on the threat posed by organizational insiders. We emphasize the pivotal role that users play in determining overall system security and aim to introduce non-experts to this field, stimulating new interest in this intersection of humans and computers."
Source: Taylor & Francis

A Search Engine for Scientific Publications: A Cybersecurity Case Study

"Cybersecurity is a very challenging topic of research nowadays, as digitalization increases the interaction of people, software and services on promising technologies, vendors, business models, and growth opportunities that are expected to influence the market dynamics during the study period. The market forecast for this study will involve an application-wise regional breakdown for the United States healthcare cybersecurity market."
Source: Frost & Sullivan

RISK MANAGEMENT

White Paper: Powerful New Ideas in Risk Management

"Risk management is an essential element of high-performing supply chains. An intentional and deliberate approach to minimizing supply chain risk will lead to lower total costs, improved customer satisfaction and an overall competitive advantage. Shippers are counting on emerging technologies, improved data and advanced analytics to help them mitigate risks and improve customer experience while growing their business.
FreightWaves partnered with BlueGrace Logistics to survey shippers about types of risks, volatility and disruption that could impact the performance of their supply chain."
Source: Freight Waves

Prioritizing Cybersecurity Risk for Enterprise Risk Management

"This report continues an in-depth discussion of the concepts introduced in NISTIR 8286, Integrating Cybersecurity and Enterprise Risk Management (ERM), with a focus on the use of enterprise objectives to prioritize, optimize, and respond to cybersecurity risks.
The NISTIR 8286 series of documents is intended to help organizations better implement cybersecurity risk management (CSRM) as an integral part of ERM – both taking its direction from ERM and informing it. The increasing frequency, creativity, and severity of cybersecurity attacks mean that all enterprises should ensure that cybersecurity risk is receiving appropriate attention within their ERM programs and that the CSRM program is anchored within the context of ERM.
This publication draws upon processes and templates described in NISTIR 8286A, Identifying and Estimating Cybersecurity Risk for Enterprise Risk Management (ERM), and on feedback received on public comment drafts of that report. Draft NISTIR 8286B extends the use of

can also wreak havoc in the physical world.
The wave of recent cyberattacks has impacted everything from oil pipelines to hospitals and shows no sign of stopping. Even worse than that, they may soon turn deadly. The cyber battlefield has expanded, and the stakes are higher than ever before."
Source: Security Magazine

Smart buildings emerging as targets of cyberattacks

"With buildings getting smarter through technology designed to make them more efficient, myriad new cybersecurity risks have opened up for real estate owners and developers investing in and implementing the latest building automation systems (BAS). There is no question that the benefits of BAS outweigh the inherent risk, but developing a risk management strategy is imperative for owners and tenants alike.
The retail, hospitality, and financial services industries, to name a few, have long been plagued with cyberattack incidents. However, companies that hold personally identifiable consumer information are no longer the only ones at risk for a major cyber incident. Cyberthreat actors are honing their craft and shifting their focus to more financially lucrative targets. Ransomware attacks have increased significantly in severity and sophistication in recent years, and cybercriminals are pursuing all industries, including commercial real estate and smart buildings."
Source: Biz Journals

Singapore Government-funded software creates cyber attack fixes for utilities and more

"Water treatment is important to societies globally but glaring leaks in the cyber defences of systems controlling water plants have been in the spotlight in recent months.
In January, a hacker gained access to a water plant in San Francisco and deleted programs linked to water treatment. This came to light only in June."
Source: The Straits Times

MALWARE

New malware seizes on COVID-19 to target Android users

the Internet by means of technology devices and networks connected to it. The field is broad and has a lot of unexplored ground under numerous disciplines such as management, psychology, and data science. Its large disciplinary spectrum and many significant research topics generate a considerable amount of information, making it hard for us to find what we are looking for when researching a particular subject. This work proposes a new search engine for scientific publications which combines both information retrieval and reading comprehension algorithms to extract answers from a collection of domain-specific documents. The proposed solution although being applied to the context of cybersecurity exhibited great generalization capabilities and can be easily adapted to perform under other distinct knowledge domains."
Source: Springer Link

The Development of a Cyber Safety Culture

"A rise in catastrophic events as a result of poor safety management (e.g. the capsizing of the Herald of Free Enterprise and Costa Concordia), has driven the maritime sector to seek improvements in its safety management. This paper will explore the vital role of the human element within safety management, and why, as part of that safety management companies must foster a safety culture. The development of safety cultures is not new to the maritime sector. However, the increase in connected systems within the sector (e.g. satellite communications etc.) means these safety cultures must now consider the risks posed by digital systems. Therefore, the paper will consider what the core elements of a cyber safety culture are, and how a company can nurture its development. The paper will then conclude by discussing the various benefits of developing a robust cyber safety culture, including demonstrable compliance to the International Maritime Organization's (IMO) cyber regulations, Resolution MSC.428(98)."
Source: University of Plymouth

CYBER ATTACKS

Enabling Cyber-attack Mitigation Techniques in a Software Defined Network

Software Defined Networking (SDN) is an innovative technology, which can

stakeholders' risk appetite and risk tolerance statements to define risk expectations. It further describes the use of the risk register and risk detail report templates to communicate and coordinate activity."
Source: Computer Security Resource Center

THREAT REPORT

Advanced Threat Research Report October 2021

"Ransomware's Increasing Prevalence
As 2021 progressed through its second quarter and into the third, cyber criminals introduced new—and updated—threats and tactics in campaigns targeting prominent sectors. Ransomware campaigns maintained their prevalence while evolving their business models to extract valuable data and millions in ransoms from enterprises big and small.
DarkSide's highly publicized attack on Colonial Pipeline's gas distribution dominated cybersecurity headlines in May. MVISION Insights quickly identified DarkSide's early prevalence of targets within the United States, primarily Legal Services, Wholesale and Manufacturing, Oil, Gas, and Chemical sectors."
Source: McAfee

4th October – Threat Intelligence Report

"Top Attacks and Breaches
Check Point Research has discovered cyber attacks against the users of PIX, the instant payment solution created and managed by the Brazilian Central Bank. The attackers distributed two different variants of banking malware, named PixStealer and MalRhino, through two separate malicious applications on Google's Play Store to carry out their attacks. Both malicious applications were designed to steal money of victims through user interaction and the original PIX application."
Source: Checkpoint Research

"A new form of malware that experts are referring to as "TangleBot" is relying on interest in COVID-19 to trick Android users in the U.S and Canada into clicking on a link that will infect their cell phones, according to analysts at the mobile and email security company Cloudmark.
Cloudmark says the "clever and complicated" malware sends Android users a text message claiming to have the latest COVID-19 guidance in their area or informs them that their third COVID-19 vaccine appointment has been scheduled. When users click on the link provided, they're prompted to update their phone's Adobe Flash player, which instead installs the virus on their phone, according to Cloudmark."
Source: CBS News

Over 10M Android Phones Infected With GriftHorse Malware

"A new, and very successful piece of Android malware has been discovered that's managed to infect over 10 million devices in more than 70 countries.
As The Record reports, the malware is called GriftHorse and it was discovered by researchers at mobile security company Zimperium. The sheer scale of infected devices that have flown under the radar until now is due to the method of distribution, which relies on "benign-looking apps" available to download through the Google Play store. It also helps that no anti-virus vendors detected the malware they contained."
Source: PC Mag

RANSOMWARE

How to proactively detect and prevent ransomware attacks

"The key to combating any type of cyberattack is to prevent it before it happens, or at least before it's able to cause significant damage. That's especially true with ransomware. Once an attacker gets their hands on your sensitive data, they can prevent you from accessing it and can even leak it publicly. That's why many organizations hit by ransomware choose to pay the ransom. For that reason, detecting and preventing an attack in the first place should still be your ultimate goal."
Source: Tech Republic

BlackByte ransomware decryptor released

"A new form of malware found in a recent IT incident appears to have be applied in a plethora of applications and areas. Recently, SDN has been identified as one of the most promising solutions for industrial applications as well. The key features of SDN include the decoupling of the control plane from the data plane and the programmability of the network through application development. Researchers are looking at these features in order to enhance the Quality of Service (QoS) provisioning of modern network applications. To this end, the following work presents the development of an SDN application, capable of mitigating attacks and maximizing the network's QoS, by implementing mixed integer linear programming but also using genetic algorithms. Furthermore, a low-cost, physical SDN testbed was developed in order to evaluate the aforementioned application in a more realistic environment other than only using simulation tools."
Source: IEEE Xplore

Behavioral responses to a cyber attack in a hospital environment

"Technical and organizational steps are necessary to mitigate cyber threats and reduce risks. Human behavior is the last line of defense for many hospitals and is considered as equally important as technical security. Medical staff must be properly trained to perform such procedures. This paper presents the first qualitative, interdisciplinary research on how members of an intermediate care unit react to a cyberattack against their patient monitoring equipment. We conducted a simulation in a hospital training environment with 20 intensive care nurses. By the end of the experiment, 12 of the 20 participants realized the monitors' incorrect behavior. We present a qualitative behavior analysis of high performing participants (HPP) and low performing participants (LPP). The HPP showed fewer signs of stress, were easier on their colleagues, and used analog systems more often than the LPP. With 40% of our participants not recognizing the attack, we see room for improvements through the use of proper tools and provision of adequate training to prepare staff for potential attacks in the future."
Source: Nature Scientific Reports

Cyber-attack detection via non-linear prediction of IP addresses: an innovative big data analytics approach

"Computer network systems are often subject to several types of attacks. For example, an excessive traffic load sent to a web server for making it

been inspired by other strains known to reap their operators' huge financial rewards -- but is likely the work of amateurs. Dubbed BlackByte and discovered by Trustwave, the Windows-based ransomware is considered "odd" due to some of the design and function decisions made by its creators.
In a set of technical advisories published last week (1,2), the cybersecurity firm says the malware only targets systems that are not based on Russian or ex-USSR languages -- a common trend in ransomware believed to be of Russian origin."
Source: ZD Net

PHISHING

Tech support scams top list of latest phishing threats

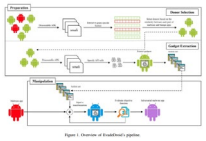
"Tech support hoaxes topped Norton's list of phishing threats for 13 consecutive weeks from July 1 through Sept. 30. These scams are designed to trick you into believing that your computer is facing some dire security risk. In reality, the criminals behind these con games want to steal your personal information, gain access to your bank account or install malware on your PC. Many scammers will employ standard phishing tactics by impersonating the names of major technology companies such as Microsoft, Google and Apple."
Source: Tech Republic

Cybersecurity awareness month: Fight the phish!

Unfortunately, anti-phishing advice often seems to fall on deaf ears, because phishing is an old cybercrime trick, and lots of people seem to think it's what computer scientists or mathematical analysts call a solved game.
Tic-tac-toe (noughts and crosses outside North America), for example, is a solved game, because it's easy to create a list of every possible play, and figure out the best possible move from every game position on the list. (If neither player makes a mistake then the game will always be a draw.) Even games that are enormously more complex have been "solved" in this way too, such as checkers (draughts)…and in comparison to playing checkers, spotting phishing scams feels like an easy contest that the recipient of the message should always win.
And if phishing is a "solved game", surely it's not worth worrying about any more?"

unusable is the main technique introduced by the Distributed Denial of Service (DDoS) attack. A well-known method for detecting attacks consists in analyzing the sequence of source IP addresses for detecting possible anomalies. With the aim of predicting the next IP address, the Probability Density Function of the IP address sequence is estimated. Anomalous requests are detected via predicting source's IP addresses in future accesses to the server. Thus, when an access to the server occurs, the server accepts only the requests from the predicted IP addresses and it blocks all the others. The approaches used to estimate the Probability Density Function of IP addresses range from the sequence of IP addresses seen previously and stored in a database to address clustering, for instance via the K-Means algorithm. Instead, the sequence of IP addresses is considered as a numerical sequence in this paper, and non-linear analysis of this numerical sequence is applied. In particular, we exploited non-linear analysis based on Volterra Kernels and Hammerstein models."
Source: Springer Link

MALWARE



EvadeDroid: A Practical Evasion Attack on Machine Learning for Black-box Android Malware Detection

"Over the last decade, several studies have investigated the weaknesses of Android malware detectors against adversarial examples by proposing novel evasion attacks; however, the practicality of most studies in manipulating real-world malware is arguable. The majority of studies have assumed attackers know the details of the target classifiers used for malware detection, while in real life, malicious actors have limited access to the target classifiers. This paper presents a practical evasion attack, EvadeDroid, to circumvent black-box Android malware detectors."
Source: Cornell University

Malware Detection with Directed Cyclic Graph and Weight Merging

"Malware is a severe threat to the computing system and there's a long history of the battle between malware detection and anti-detection. Most traditional detection methods are based on static analysis with signature matching and dynamic analysis methods that are

Source: APN News

RISK MANAGEMENT

What does it take to develop a good risk management strategy?

"Ensuring that risks are well managed is vital to the smooth running of every organisation, but it is also an area that a lot of business owners might prefer to avoid - something which can result in a significant increase in risk exposures, and a higher chance of taking a financial hit.

One of the organisations looking to increase the understanding of risk management is RiskNZ, a non-profit group which aims to help businesses develop risk management skills, and to stay on top of current issues.

At the helm of RiskNZ is managing director David Turner, who has over 20 years' experience as an adviser in the risk sector. When it comes to developing a good risk strategy, Turner said that his ultimate goal is to enable everyone within a business to be able to confidently talk about and assess risk."

Source: Insurance Business Magazine

Tsinghua University Reports Findings in Risk Management (Analysis and prediction of intersection traffic violations using automated enforcement system data): Risk Management

"New research on Risk Management is the subject of a report. According to news reporting out of Beijing, People's Republic of China, by NewsRx editors, research stated, "The automated enforcement system (AES) is an effective way of supplementing traditional traffic enforcement, and the traffic violation data from AES can also be effectively used for safety research. In this study, traffic violation data were used to analyze the influencing factors associated with traffic violations and to predict the probability of violations at intersections."

Financial supporters for this research include National Key Research and Development Program of China Stem Cell and Translational Research, National Key Research and Development Program of China."

Source: Insurance News Net

CYBERSECURITY SKILLS

focused on sensitive behaviors. However, the usual detections have only limited effect when meeting the development of malware, so that the manual update for feature sets is essential. Besides, most of these methods match target samples with the usual feature database, which ignored the characteristics of the sample itself. In this paper, we propose a new malware detection method that could combine the features of a single sample and the general features of malware. Firstly, a structure of Directed Cyclic Graph (DCG) is adopted to extract features from samples. Then the sensitivity of each API call is computed with Markov Chain. Afterward, the graph is merged with the chain to get the final features. Finally, the detectors based on machine learning or deep learning are devised for identification. To evaluate the effect and robustness of our approach, several experiments were adopted. The results showed that the proposed method had a good performance in most tests, and the approach also had stability with the development and growth of malware."

Source: EbscoHost

Falcon: Malware Detection and Categorization with Network Traffic Images

"Android is the most popular smartphone operating system. At the same time, miscreants have already created malicious apps to find new victims and infect them. Unfortunately, existing anti-malware procedures have become obsolete, and thus novel Android malware techniques are in high demand. In this paper, we present Falcon, an Android malware detection and categorization framework. More specifically, we treat the network traffic classification task as a 2D image sequence classification and handle each network packet as a 2D image. Furthermore, we use a bidirectional LSTM network to process the converted 2D images to obtain the network vectors. We then utilize those converted vectors to detect and categorize the malware. Our results reveal that Falcon could be an accurate and viable solution as we get 97.16% accuracy on average for the malware detection and 88.32% accuracy for the malware categorization."

Source: Springer Link

Hawk: Rapid Android Malware Detection Through Heterogeneous Graph Attention Networks

"Android is undergoing unprecedented malicious threats daily, but the existing methods for

Here's how to become an in-demand cybersecurity expert

"Tech giant Cisco has such a significant share of networking technologies on the market, so the Cisco 210-260 IINS: Implementing Cisco Network Security course is a logical choice for anyone already familiar with the company's systems. But the bundle's other classes are vendor-neutral.

Entry- to mid-level IT professionals will benefit from the Certified Information Systems Auditor (CISA) course. It will give you the skills to gain certifications required for positions that include monitoring, assessing, auditing and controlling business and IT systems for a company."

Source: Tech Republic

A Career in Cybersecurity is for Everyone

"It's National Cyber Security Awareness Month (NCSAM), created as a collaborative effort between government and industry to ensure that everyone has the resources they need to stay safe and secure online. Now in its 18th year, NCSAM has grown exponentially, reaching consumers, small businesses, corporations, educational institutions, and young people across the globe.

This week, NCSAM focuses on cybersecurity careers with the Explore. Experience. Share. campaign. The cybersecurity field is growing rapidly, and it has something for everyone."

Source: Yahoo! Finance

CLOUD SECURITY

Cloud Security Should Be the CEO's Wheelhouse Too

"Cybersecurity is hot on the minds of corporations as the workforce is still partially digitally based, as are the security concerns that this situation creates. Increasing ransomware attacks and generalized hacking continue to be on the rise, creating an environment in which businesses of all sizes need to ensure that they have firm protections in place within digital spaces. In an article for Entrepreneur, Stu Sjouwerman, founder and CEO of KnowBe4, a platform that offers security awareness training as well as simulated phishing, argues that CEOs need to be the driving force for cybersecurity within their cloud systems. CEOs should be

malware detection often fail to cope with evolving camouflage in malware. To address this issue, we present Hawk, a new malware detection framework for evolutionary Android applications. We model Android entities and behavioral relationships as a heterogeneous information network (HIN), exploiting its rich semantic meta-structures for specifying implicit higher order relationships. An incremental learning model is created to handle the applications that manifest dynamically, without the need for reconstructing the whole HIN and the subsequent embedding model. The model can pinpoint rapidly the proximity between a new application and existing in-sample applications and aggregate their numerical embeddings under various semantics."

Source: IEEE Xplore

Hybrid Malware Detection Based on Bi-LSTM and SPP-Net for Smart IoT

"We propose the hybrid malware detection scheme, HyMalD, with bidirectional long short-term memory (Bi-LSTM) and the spatial pyramid pooling network (SPP-Net). Its purpose is to protect IoT devices and minimize the damage caused by infection through obfuscated malware. HyMalD performs the static and dynamic analyses logically simultaneously detects obfuscated malware, which is impossible to do using static analysis alone. First, it extracts static features of the opcode sequence using a reconstructed dataset according to the obfuscation, and extracts the application programming interface (API) call sequence dynamically. The extracted features are trained through the Bi-LSTM and SPP-Net models, which HyMalD uses to detect and classify IoT malware. The performance of HyMalD was evaluated, and its detection accuracy was 92.5%. False-negative rate (FNR) of HyMalD was 7.67%. Thus, HyMalD detects IoT malware more accurately and with a lower FNR than static analysis, which had a 92.09% detection accuracy and a 9.97% FNR."

Source: IEEE Xplore

RISK MANAGEMENT

Human Capital Vulnerability and Cybersecurity Risk Management: An Integrated Approach

knowledgeable and involved in the day-to-day operations of the IT department when it pertains to cloud security."
Source: Nasdaq

Cloud Security: Report Finds 68% of Malware Delivered From Cloud Apps

"Cloud apps are now the most common way digital attackers distribute malware. In the second quarter of 2021, researchers found that 68% of malware downloads originated from cloud apps, reported ZDNet. In order to keep your cloud security up, it's important to know where problems might come from. Specifically, cloud-based misconfigurations could often be a contributing factor. Read on to learn what types of apps factored into these attacks."
Source: Security Intelligence

Lacework and Snowflake Partner to Enable Better Cloud Security Analytics and Insights

"Lacework, the data-driven cloud security company and Snowflake, the Data Cloud company, today announced a product integration and go-to-market partnership. Making Lacework data easily available in the Snowflake Data Cloud enables organizations to quickly and cost-effectively analyze and report on risk and threats across their cloud and container environments.
Lacework is a data-driven security platform built natively on top of Snowflake that takes tens of billions of security data points and — through intelligent automation and a patented analytics engine — surfaces the handful of security events that matter most in a given day. This visibility gives overloaded and under-resourced security and developer organizations the insights they need to remediate the most pressing security and performance issues quickly, without impacting the agility of the business."
Source: PR News Wire

"There is a long-standing claim that cybersecurity and digital information system protection is primarily a technological issue falling into the information technology domain. However, empirical evidence demonstrates that human and behavioural factors are usually the main vulnerability causing cybersecurity accidents. This chapter examines the role of the human capital of being both a vulnerability and strength in cybersecurity risk management. It provides recommendations to align firms' corporate governance and internal control systems to human-related cybersecurity risk."
Source: Springer Link

DATA SCIENCE

Cybersecurity for Data Science: Issues, Opportunities, and Challenges

"Cybersecurity (CS) is one of the critical concerns in today's fast-paced and interconnected world. Advancement in IoT and other computing technologies had made human life and business easy on one hand, while many security breaches are reported daily. These security breaches cost millions of dollars loss for individuals as well as organizations. Various datasets for cybersecurity are available on the Internet. There is a need to benefit from these datasets by extracting useful information from them to improve cybersecurity. The combination of data science (DS) and machine learning (ML) techniques can improve cybersecurity as machine learning techniques help extract useful information from raw data. In this paper, we have combined DS and ML for improving cybersecurity. We will use the CS dataset, and ML techniques will be applied to these datasets to identify the issues, opportunities, and cybersecurity challenges. As a contribution to research, we have provided a framework that will provide insight into ML and DS's use for protecting cyberspace from CS attacks."
Source: Springer Link

Data-driven insight into the puzzle-based cybersecurity training

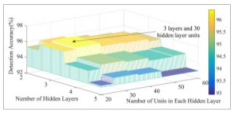
"Puzzle-based training is a common type of hands-on activity accompanying formal and informal cybersecurity education, much like programming or other IT skills. However, there is a lack of tools to

help the educators with the post-training data analysis. Through a visualization design study, we designed the Training Analysis Tool that supports learning analysis of a single hands-on session. It allows an in-depth trainee comparison and enables the identification of flaws in puzzle assignments. We also performed a qualitative evaluation with cybersecurity experts and students. The participants apprised the positive influence of the tool on their workflows. Our insights and recommendations could aid the design of future tools supporting educators, even beyond cyber security."
Source: Harvard

Big Data Tools: A Solution To Cyber Security

"In this global world huge amount of data gets generated every day. Securing such data from
attackers is the challenge in front of cyber security officials. The 3 V"s of big data –Variety,
Velocity & Volume can be used to fix cyber security problems efficiently. This paper highlights
types of cyber security threats. Also this paper tries to elaborate the use of big data tools in
handling cyber security problem. In this paper author have enlisted different tools which can be
used to detect & prevent attacks in real time. To complete the research systematic review
approach was adopted and objectives of this paper were used as a research questions."
Source: Episteme

ARTIFICIAL INTELLIGENCE



A deep learning-based classification scheme for cyber-attack detection in power system

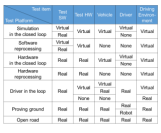
"A smart grid improves power grid efficiency by using modern information and communication technologies. However, at the same time, the system might become increasingly vulnerable to cyberattacks. Among various emerging security problems, a false data injection attack (FDIA) is a new type of attack against the state estimation. In this article, a deep learning-based identification scheme is developed to detect and mitigate information corruption. The scheme implements a Conditional Deep Belief Network to analyse time-series input data and leverages captured features to detect the FDIA. The

performance of the detection mechanism is validated by using the IEEE standard test system for simulation. Different attack scenarios and parameters are set to demonstrate the feasibility and effectiveness of the developed scheme. Compared with the support vector machine and the multilayer perceptrons, the experimental analyses indicate that the results of the proposed detection mechanism are better than those of the other two in terms of FDIA detection accuracy and robustness."
Source: IET Research

Deep Learning Applications on Cybersecurity

"Security has always been one of the biggest challenges faced by computer systems, recent developments in the field of Machine Learning are affecting almost all aspects of computer science and Cybersecurity is no different. In this paper, we have focused on studying the possible application of deep learning techniques to three different problems faced by Cybersecurity: SPAM filtering, malware detection and adult content detection in order to showcase the benefits of applying them. We have tested a wide variety of techniques, we have applied LSTMs for spam filtering, then, we have used DNNs for malware detection and finally, CNNs in combination with Transfer Learning for adult content detection, as well as applying image augmentation techniques to improve our dataset. We have managed to reach an AUC over 0.9 on all cases, demonstrating that it is possible to build cost-effective solutions with excellent performance without complex architectures."
Source: Springer Link

AUTONOMOUS CAR



Design and Verification Standard for Safety and Cybersecurity of Autonomous Cars: ISO/TR 4804

"This paper describes ISO/TR 4804, an international standard to describe how to design and verify autonomous cars to ensure safety and cybersecurity. Goals of ISO/TR 4804 are (1) positive risk balance and (2) avoidance of unreasonable risk. It also 12 principles of safety and cybersecurity to achieve these goals. In the design procedures, it describes (1) 13 capabilities to achieve these safety and cybersecurity principles, (2) hardware and software elements

to achieve these capabilities, and (3) a generic logical architecture to combine these elements. In the verification procedures, it describes (1) 5 challenges to ensure safety and cybersecurity, (2) test goals, platforms, and solutions to achieve these challenges, (3) simulation and field operation methods, and (4) verification methods for hardware and software elements. Especially, it regards deep neural network as a software component and it describe design and verification methods of autonomous cars."
Source: Korea Science

GAMIFICATION

Evaluation of HackLearn COFELET Game User Experience for Cybersecurity Education

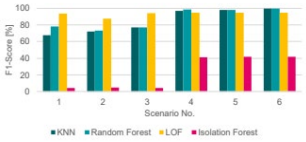
"HackLearn is a scenario-based hacking simulation game for teaching cybersecurity concepts while providing hands-on hacking experiences to the learners. HackLearn design is based on the COFELET framework, which assimilates modern learning theories, well-known cybersecurity standards, and built-in scaffolding and assessment features. Aiming at evaluating the user experience perceived by HackLearn's users, we describe the process of adopting it in a real educational environment based on the didactic framework for simulation games. Additionally, we present the evaluation methodology elaborated, based on the serious games' quality characteristics framework. We discuss the evaluation results which indicate that HackLearn is engaging, motivating, usable and effective in teaching cybersecurity concepts and hacking strategies and techniques. The evaluation results revealed the HackLearn's aspects that can be improved such as the scaffolding feature and the communication mechanism with the game's back-end facility."
Source: International Journal of Serious Games

Assessing the Effects of Gamification on Enhancing Information Security Awareness Knowledge

"Information security awareness (ISA) has become a vital issue, as security breaches often attributed to humans lead to losses for individuals and organizations. Information security (IS) education may be an effective strategy to improve students' ISA; however, studies associated with the

relationships between teaching effects and information security learning are few. This study adopted gamification practice and examined its effect on students' ISA knowledge enhancement, attitude and intention of security compliance, and willingness for continuous IS education. This study also examined the gender difference in a gamified learning system. One hundred ten undergraduates participated in a quasi-experimental study. The results indicated that students within a gamified class performed better than students within a lecture-based instructional group. We found significant gamification effects on the three security focus areas of password management, Internet use, and information handling. Gamification did not significantly impact the attitude and intention of participants' security compliance and students' willingness for continuous IS learning. Gender difference in the effect of gamification on ISA knowledge enhancement was not observed as well. The research provides theoretical and practical contributions by incorporating gamification into IS learning and suggests gamification as an effective means to enhance students' knowledge acquisition in an engaging, timely, economical, and repeated manner."
Source: MDPI

SMART SYSTEMS



An Approach of Replicating Multi-Staged Cyber-Attacks and Countermeasures in a Smart Grid Co-Simulation Environment

"While the digitization of power distribution grids brings many benefits, it also introduces new vulnerabilities for cyber-attacks. To maintain secure operations in the emerging threat landscape, detecting and implementing countermeasures against cyber-attacks are paramount. However, due to the lack of publicly available attack data against Smart Grids (SGs) for countermeasure development, simulation-based data generation approaches offer the potential to provide the needed data foundation. Therefore, our proposed approach provides flexible and scalable replication of multi-staged cyber-attacks in an SG Co-Simulation Environment (COSE). The COSE consists of an energy grid simulator,

simulators for Operation Technology (OT) devices, and a network emulator for realistic IT process networks. Focusing on defensive and offensive use cases in COSE, our simulated attacker can perform network scans, find vulnerabilities, exploit them, gain administrative privileges, and execute malicious commands on OT devices. As an exemplary countermeasure, we present a built-in Intrusion Detection System (IDS) that analyzes generated network traffic using anomaly detection with Machine Learning (ML) approaches. In this work, we provide an overview of the SG COSE, present a multi-stage attack model with the potential to disrupt grid operations, and show exemplary performance evaluations of the IDS in specific scenarios."
Source: Cornell University

Role of Cyber-Security in Smart Energy Management Systems

"Cyber-security is the most fundamental requirement of digital enterprises. Cyber-security helps an organization to monitor, detect, report, and counter cyber-attacks to maintain data confidentiality. The adoption of cyber-security solutions is expected to grow with emerging technologies such as the Internet of Things, big data, cloud computing, supply chains, etc…The monitor and control functions are known as SCADA (which stands for supervisory control and data acquisition), and the optimization packages are often referred to as advanced applications. Thus, a communication infrastructure is necessary to integrate the smart energy management system. To counter possible disruption, a highly reliable, secure, robust, and cost-effective information and communications technology infrastructure is absolutely essential. Most of the materials in this chapter cover baseline concepts with which all security professionals and experts will develop smart energy management."
Source: AIP

HEALTHCARE

Cybersecurity in the Internet of Medical Things

"Background
The Internet of Things has spawned a new fleet of medical devices replete with improved sensing and actuating capabilities. Preemptive mitigation of the cyber risks that arise in this hyperconnected space is needed to ensure continued patient safety.

Objective
The aim of this paper is to analyse the robustness of existing policy measures in securing the Internet of Medical Things technologies. The regulatory ecosystem in the US is primarily discussed herein and includes regulatory frameworks for industry, public-private partnerships, and transparency initiatives.
Methods
A qualitative review of the medical cybersecurity literature was performed with collation of federal and international legal documents, policy reports, industry frameworks, cyberbreach analyses, and scientific journal articles."
Source: Elsevier