SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN

19 FEBRUARY - 22 APRIL 2022

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

Singapore begins licensing cybersecurity service providers

"Singapore launched a new licensing framework for cybersecurity service providers on Monday (Apr 11), giving existing vendors six months to apply for a licence or cease providing such services.

The licensing framework aims to provide greater assurance of security and safety to consumers, said the Cybersecurity Agency of Singapore (CSA) in a press release on Monday."

Source: Channel News Asia

Police introduce new guidelines on online safety to counter cybercrime

"The guidelines were co-developed by SPF and the Asia Internet Coalition (AIC), an association that promotes the understanding and resolution of Internet policy matters in the Asia-Pacific region. "The Guidelines on Online Safety provide a broad overview on the types of crimes and online harms, ranging from scams to terrorism, which members of the public may encounter on the Internet," SPF said in a news release.

They also contain advisories on things that Internet users should look out for, as well as measures that they can take to protect themselves."

Source: Channel News Asia

academic

CYBERSECURITY

Application of cognitive computing in healthcare, cybersecurity, big data and IoT: A literature review

"Human Intelligence is considered superior compared to Artificial Intelligence (AI) because of its ability to adapt faster to changes. Due to increasing data deluge, it is cumbersome for humans to analyse the vast amount of data and hence AI systems are in demand in today's world. However, these AI systems lack self-awareness, social skills, multitasking and faster adaptability. Cognitive Computing (CC), a subset of AI, acts as an effective solution in solving these challenges by serving as an important driver for knowledge-rich automation work. Knowing the latest research and state of the art in CC is one of the initial steps needed for researchers to make progress in this front. Thus, this paper presents a comprehensive survey of prior research in the CC domain along with the challenges, solutions and future research directions."

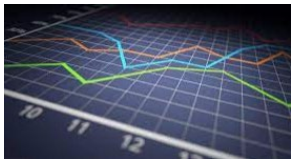
Source: Elsevier

Cybersecurity in the Internet of Things in Industrial Management

"Nowadays, people live amidst the smart home domain, while there are business opportunities in industrial smart cities and healthcare. However,

reports

CYBERSECURITY



Worldwide Automotive Cybersecurity Industry to 2027

"The report on the global automotive cybersecurity market provides qualitative and quantitative analysis for the period from 2019 to 2027. The report predicts the global automotive cybersecurity market to grow with a CAGR of 16% over the forecast period from 2021-2027. The study on automotive cybersecurity market covers the analysis of the leading geographies such as North America, Europe, Asia-Pacific, and RoW for the period of 2019 to 2027. The report on automotive cybersecurity market is a comprehensive study and presentation of drivers, restraints, opportunities, demand factors, market size, forecasts, and trends in the global automotive cybersecurity market over the period of 2019 to 2027. Moreover, the report is a collective presentation of primary and secondary research findings."

Source: Yahoo! Finance

Upstream's 2022 Global Automotive Cybersecurity Report

"This year's annual Global Automotive Cybersecurity Report focuses on the automotive cyber threat landscape in light of the UNECE WP.29 R155 & R156 and ISO/SAE 21434 taking effect. Upstream's report includes an in-depth analysis of over

New Technique Offers Faster Security for Non-Volatile Memory Tech

"Researchers have developed a technique that leverages hardware and software to improve file system security for next-generation memory technologies called non-volatile memories (NVMs). The new encryption technique also permits faster performance than existing software security technologies.

"NVMs are an emerging technology that allows rapid access to the data, and retains data even when a system crashes or loses power," says Amro Awad, senior author of a paper on the work and an assistant professor of electrical and computer engineering at North Carolina State University. "However, the features that give NVMs these attractive characteristics also make it difficult to encrypt files on NVM devices – which raises security concerns. We've developed a way to secure files on NVM devices without sacrificing the speed that makes NVMs attractive.""

Source: NC State University

3 Ways We Can Improve Cybersecurity

"As IT modernizes to support remote work, new customer experiences and evolving business processes, we're seeing attack surfaces expand exponentially. On the one hand, this contributed to a record number of compromises in 2021, while the number of published vulnerabilities surged to an all-time high.

Yet there's another story behind the headlines. For years, we've been talking about the same old paradigm of attacker and victim. In this one-to-one relationship, the attacker targets a victim and either succeeds or doesn't. Today, we're seeing more of what I would call "one-to-many" attacks. Supply chain attacks are nothing new, but we're seeing an uptick in their sophistication and ambition. Attackers have realized they don't need to constantly go one-to-one. They can find a common hub that connects hundreds or even thousands of potential victims and compromise it. For close to the same effort expelled, they have a significant step up in ROI."

Source: Dark Reading

New cyber-security lab launched at ITE to train students and build up tech talent pipeline

"The Institute of Technical Education (ITE) on Wednesday (March 30) launched a new cyber-security facility to train students in an environment modelled after real

there are concerns about security. Security is central for IoT systems to protect sensitive data and infrastructure, whilst security issues have become increasingly expensive, in particular in Industrial Internet of Things (IIoT) domains. Nonetheless, there are some key challenges for dealing with those security issues in IoT domains: Applications operate in distributed environments such as Blockchain, varied smart objects are used, and sensors are limited, as far as machine resources are concerned. In this way, traditional security does not fit in IoT systems. The issue of cybersecurity has become paramount to the Internet of Things (IoT) and the Industrial Internet of Things (IIoT) in mitigating cybersecurity risk for organizations and end users."

Source: MDPI

Organizational science and cybersecurity: abundant opportunities for research at the interface

"Cybersecurity is an ever-present problem for organizations, but organizational science has barely begun to enter the arena of cybersecurity research. As a result, the "human factor" in cybersecurity research is much less studied than its technological counterpart. The current manuscript serves as an introduction and invitation to cybersecurity research by organizational scientists. We define cybersecurity, provide definitions of key cybersecurity constructs relevant to employee behavior, illuminate the unique opportunities available to organizational scientists in the cybersecurity arena (e.g., publication venues that reach new audiences, novel sources of external funding), and provide overall conceptual frameworks of the antecedents of employees' cybersecurity behavior. In so doing, we emphasize both end-users of cybersecurity in organizations and employees focused specifically on cybersecurity work."

Source: Springer Link

Recent Advances on Federated Learning for Cybersecurity and Cybersecurity for Federated Learning for Internet of Things

"Decentralized paradigm in the field of cybersecurity and machine learning (ML) for the emerging Internet of Things (IoT) has gained a lot of attention from the government, academia, and industries in recent years. Federated cybersecurity (FC) is regarded as a revolutionary concept to make the IoT safer and more efficient in the future. This emerging concept has the potential of

900 automotive cybersecurity incidents, compiled by our expert automotive-focused analysts, of the cyber threat landscape from over a decade of connectivity, with an emphasis on 2021.

Download the report to learn:

- Cyber threat trends over the years
- Advanced sophistication of 2021's 240+ attacks
- How new regulations and standards are impacting automotive cybersecurity
- 84.5% of automotive attacks were carried out remotely
- A staggering 40.1% of incidents focused on back-end servers attacks
- A dive into real-life deep and dark web automotive cyber attacks
- Current automotive cybersecurity solutions available today to combat threats and comply with standards and regulations."

Source: Upstream

What's the Current State of Cybersecurity?

"State of Cybersecurity 2022, Global Update on Workforce Efforts, Resources and Cyberoperations reports the results of an eighth annual global study that looks at the following topics and more:

- What are the top cybersecurity hiring challenges today?
- Which cybersecurity skills are in highest demand?
- How can companies improve retention?
- How are cybersecurity budgets changing?
- Which threat vectors are the most concerning?
- How frequently are companies conducting cyber risk assessments?"

Source: ISACA

CYBER-RISK ASSESSMENT

Gartner Identifies Top Security and Risk Management Trends for 2022

"Security and risk management leaders must address seven top trends to protect the ever-expanding digital footprint of modern organizations against new and emerging threats in 2022 and beyond, according to Gartner, Inc.

operational conditions and workflows faced by professionals.
The laboratory, housed in ITE College East, is ITE's first. Similar labs can be found in polytechnics and universities here.
The lab was set up in partnership with cyber-security companies Lumen Technologies, ReaQta, SecureAge and Toffs Technologies, as well as the Cyber Security Agency of Singapore (CSA)."
Source: Straits Times

CYBER ATTACK

Unpatched Bug in RainLoop Webmail Could Give Hackers Access to all Emails

"An unpatched high-severity security flaw has been disclosed in the open-source RainLoop web-based email client that could be weaponized to siphon emails from victims' inboxes.
"The code vulnerability [...] can be easily exploited by an attacker by sending a malicious email to a victim that uses RainLoop as a mail client," SonarSource security researcher Simon Scannell said in a report published this week.
"When the email is viewed by the victim, the attacker gains full control over the session of the victim and can steal any of their emails, including those that contain highly sensitive information such as passwords, documents, and password reset links.""
Source: The Hacker News

A security technique to fool would-be cyber attackers

"Multiple programs running on the same computer may not be able to directly access each other's hidden information, but because they share the same memory hardware, their secrets could be stolen by a malicious program through a "memory timing side-channel attack."
This malicious program notices delays when it tries to access a computer's memory, because the hardware is shared among all programs using the machine. It can then interpret those delays to obtain another program's secrets, like a password or cryptographic key."
Source: MIT

Preparing for Energy Industry Cyberattacks

"The energy industry is especially vulnerable to cyberattacks, according to political leaders and security analysts. Also, attacks on the industry, which includes utilities and

detecting security threats, taking countermeasures, and limiting the spreading of threats over the IoT network system efficiently. An objective of cybersecurity is achieved by forming the federation of the learned and shared model on top of various participants. Federated learning (FL), which is regarded as a privacy-aware machine learning ML model, is particularly useful to secure vulnerable IoT environment. In this paper, we start with background and comparison of centralized learning, distributed on-site learning, and FL which is then followed by a survey of the application of FL to cybersecurity for IoT. This survey primarily focuses on the security aspect but it also discusses several approaches that address the performance issues (e.g. accuracy, latency, resource constraint and others) associated with FL which may impact the security and overall performance of the IoT."
Source: IEEE Xplore

Anomaly Detection in Cybersecurity Datasets via Cooperative Co-evolution-based Feature Selection

"Anomaly detection from Big Cybersecurity Datasets is very important; however, this is a very challenging and computationally expensive task. Feature selection (FS) is an approach to remove irrelevant and redundant features and select a subset of features, which can improve the machine learning algorithms' performance. In fact, FS is an effective preprocessing step of anomaly detection techniques. This article's main objective is to improve and quantify the accuracy and scalability of both supervised and unsupervised anomaly detection techniques. In this effort, a novel anomaly detection approach using FS, called Anomaly Detection Using Feature Selection (ADUFS), has been introduced. Experimental analysis was performed on five different benchmark cybersecurity datasets with and without feature selection and the performance of both supervised and unsupervised anomaly detection techniques were investigated."
Source: ACM Digital Library

Design for Cybersecurity (DfC) Cards: A Creativity-Based Approach to Support Designers' Consideration of Cybersecurity

"As new products exhibit increasing connectivity, cybersecurity will become ever more important to the safety and functionality of these new offerings. Product designers, however, struggle to integrate cybersecurity

"Organizations worldwide are facing sophisticated ransomware, attacks on the digital supply chain and deeply embedded vulnerabilities," said Peter Firstbrook, research vice president at Gartner. "The pandemic accelerated hybrid work and the shift to the cloud, challenging CISOs to secure an increasingly distributed enterprise – all while dealing with a shortage of skilled security staff."
These challenges lend themselves to three overarching trends impacting cybersecurity practices: (i) new responses to sophisticated threats, (ii) the evolution and reframing of the security practice and (iii) rethinking technology."
Source: Gartner

the energy production and distribution sectors, can have a domino effect farbeyond the entities victimized by the breach.
The conflict in Ukraine has put officials on high alert for attacks on the energy sector, both inside Ukraine and elsewhere."
Source: Wall Street Journal

Okta concludes investigation following cyber compromise

"During that time the threat actor accessed two active customer tenants within Okta's SuperUser application. It viewed limited additional information in certain other applications like Slack and Jira that cannot be used to perform actions in Okta customer tenants.
Notably the threat actor was unable to perform many actions including configuration changes, MFA or password resets or customer support impersonation events.
The threat actor was unable to authenticate directly to any Okta accounts."
Source: Cyber Security Hub

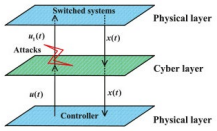
How utilities protect their assets from a potential cyberattack

"The Department of Energy (DOE), the Cybersecurity and Infrastructure Security Agency (CISA) and other federal partners have recently issued alerts to warn that bad actors have shown the ability to access multiple industrial control devices in power systems. By doing so, they could elevate privileges or disrupt critical devices or functions.
"The majority of our nation's critical infrastructure is owned and operated by the private sector – and those owners and operators must take urgent steps to harden their environments," said Eric Goldstein, Executive Assistant Director for Cybersecurity at CISA, in a statement to Clarion Energy.
The federal agencies urged energy companies to enforce multifactor authentication for all remote access to these devices, change all passwords consistently, and to use continuous monitoring solutions to log and alert any malicious activity."
Source: Power Engineering

Mechanical engineering research team identifies methods to predict future cyberattacks

"A UTSA-led research team is investigating ways to accurately predict these attacks. Mechanical Engineering Professor Yusheng Feng and doctoral student Van Trieu-Do in the Margie and Bill Klesse College of Engineering and Integrated Design, in collaboration with professor Shouhuai with other considerations during early-stage design. This paper develops an approach to help designers engage with cybersecurity, articulated as a card-based intervention to support three well-defined modes of engineering design creativity: analysis, generation, and evaluation. Developing cybersecurity support questions for each of those modes across the Research, Analyze, Ideate, Build, and Communicate phases of the human-centered design process, we assemble 15 cards total. A human subjects study using the cards was conducted with 33 students in a design course, validating that novice designers found value in the cards when engaging with a diverse range of design projects. This work adds design creativity to the broad dialogue around cybersecurity education, and forms a foundation for further creativity- and design-process-based interventions in cybersecurity."
Source: Springer Link

CYBER ATTACKS



Adaptive tracking control of switched cyber-physical systems with cyberattacks

"This study investigates the problem of adaptive tracking control for switched cyber-physical systems against cyberattacks. A tracking signal is generated using an exogenous system. An adaptive tracking controller is designed to compensate for the attacks and then stabilize the studied systems. A switching signal is constructed using the mode-dependent average dwell time (MDADT) method. By using the multiple Lyapunov function approach, which is associated with the adaptive estimated signal, the closed-loop error systems with cyberattacks are asymptotically stable under the designed adaptive tracking controller and MDADT switching signal, and the system states can asymptotically track the reference signal."
Source: Elsevier

Heterogeneous traffic flow model under connected vehicles environment considering cyberattacks

"Under the Vehicle-to-Vehicle (V2V) environment, connected vehicles (CVs) can share the traveling information with each other to keep the traffic flow stable. However, the open network cooperation environment makes CVs vulnerable to

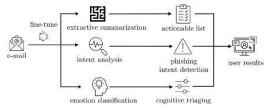
Xu from the Department of Computer Science at the University of Colorado at Colorado Springs, are studying how to use mathematical tools and computer simulation to foresee cyberattacks.

According to a 2019 report by ForgeRock, 2.8 billion consumer data records were breached in 2018, costing more than $654 billion to U.S. organizations, posing a massive industry threat.

The current pervasive security threats motivated the UTSA researchers to develop and use cyber defense tools and sensors to monitor the threats and collect data, which can be used for various purposes in developing defense mechanisms."

Source: The University of Texas at San Antonio

PHISHING



Overview of the system's design. Credit: Kashapov et al.

A model that can help inexperienced users identify phishing emails

"Researchers at Monash University and CSIRO's Data61 in Australia have recently developed a machine learning-based approach that could help users to identify phishing emails, so that they don't inadvertently install malware or send sensitive data to cyber-criminals. This model was introduced in a paper pre-published on arXiv and set to be presented at AsiaCCS 2022, a cyber-security conference.

"We have identified a gap in current phishing research, namely realizing that existing literature focuses on rigorous 'black and white' methods to classify whether something is a phishing email or not," Tingmin (Tina) Wu, one of the researchers who carried out the study, told TechXplore."

Source: Tech Xplore

LinkedIn Becomes the Most Impersonated Brand for Phishing Attacks

"LinkedIn has become by far the most impersonated brand for phishing attacks, according to new research by Check Point Research (CPR).

The cybersecurity vendor's 2022 Q1 Brand Phishing Report revealed that phishing attacks impersonating the professional social networking site made up over half (52%) of all attempts globally in the first quarter of 2022. This represents a 44% increase compared to the previous quarter, Q4 2021, when LinkedIn was the fifth most impersonated brand."

Source: Info Security

cyberattacks, which leads to changes in driving behavior. The existing theories divide cyberattacks into three types: bogus information, replay/delay and collusion cyberattacks. In addition, the mixed flow consisting of truck and car is a common form of road traffic. In order to clarify the potential impact of cyberattacks on mixed traffic flow, this paper proposes an extended car-following model considering cyberattacks under CVs environment. Subsequently, the stability of the model is analyzed theoretically, and the stability condition of the model is obtained."

Source: World Scientific

Design and Emulation of Physics-Centric Cyberattacks on an Electrical Power Transformer

"Malware that attack the electrical power grid consist of exploits and operations modules. The exploits are similar to those of traditional malware. These malware hack into an industrial computer and subsequently deploy operational modules. Some operational modules penetrate the operating system of the compromised industrial computer to take over computing functions and hence facilitate further attacks. Examples include interception of cryptographic keys, and generation of deceptive status data that indicate normal operation of a power transformer, while in reality the transformer is in distress due to the attacks. Other operational modules are designed to recognize and disrupt the physics of the physical equipment."

Source: IEEE Xplore

Studying the Robustness of Anti-adversarial Federated Learning Models Detecting Cyberattacks in IoT Spectrum Sensors

"Device fingerprinting combined with Machine and Deep Learning (ML/DL) report promising performance when detecting cyberattacks targeting data managed by resource-constrained spectrum sensors. However, the amount of data needed to train models and the privacy concerns of such scenarios limit the applicability of centralized ML/DL-based approaches. Federated learning (FL) addresses these limitations by creating federated and privacy-preserving models. However, FL is vulnerable to malicious participants, and the impact of adversarial attacks on federated models detecting spectrum sensing data falsification (SSDF) attacks on spectrum sensors has not been studied. To address this

MALWARE

This devious new malware targets your DVR

"A new variant of the BotenaGo malware that exclusively targets DVR for security camera systems has been spotted in the wild by security researchers.

For those unfamiliar, BotenaGo is a relatively new malware written in Google's open source Golang programming language. While it was originally used to target IoT devices in an effort to create botnets, BotenaGo's source code was leaked online back in October of last year."

Source: Tech Radar

Malware Research Will Create More Secure Online Environment

"A University of Texas at Arlington computer scientist is using a three-year grant worth nearly $500,000 from the National Science Foundation to create virtual "sandbox" environments that allow computer security professionals to analyze Android malware without being detected by the code or its creators.

Jiang Ming, assistant professor of computer science and engineering, is creating container-based virtualization architecture, which allows him to isolate potential malware on up to eight virtual phones in a secure environment for analysis. The goal is to thwart malware that's capable of detecting sandboxes and shutting itself down to prevent analysis.

Ming will create an "out-of-the-box" design to ensure all virtualization activities run outside of the virtual phone."

Source: University of Texas Arlington

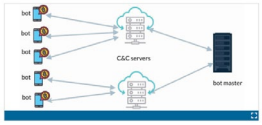
RANSOMWARE

Can you predict ransomware attacks before they happen?

"Along with digital transformation, the arrival of cryptocurrency proved to be a bridge for untraceable payment methods which paved the way to attack and threaten businesses with minimum risk involved. Since 2011, the dynamics have changed from 'if' a business could be breached to 'when' a business will be breached. As vendor networks become more widespread as a result of increased challenge, the first contribution of this work is the creation of a novel dataset suitable for FL and modeling the behavior (usage of CPU, memory, or file system, among others) of resource-constrained spectrum sensors affected by different SSDF attacks. The second contribution is a pool of experiments analyzing and comparing the robustness of federated models according to i) three families of spectrum sensors, ii) eight SSDF attacks, iii) four scenarios dealing with unsupervised (anomaly detection) and supervised (binary classification) federated models, iv) up to 33% of malicious participants implementing data and model poisoning attacks, and v) four aggregation functions acting as anti-adversarial mechanisms to increase the models robustness."

Source: Cornell University

MALWARE



A Survey on Mobile Malware Detection Methods using Machine Learning

"The prevalence of mobile devices (smartphones) along with the availability of high-speed internet access world-wide resulted in a wide variety of mobile applications that carry a large amount of confidential information. Although popular mobile operating systems such as iOS and Android constantly increase their defenses methods, data shows that the number of intrusions and attacks using mobile applications is rising continuously. Experts use techniques to detect malware before the malicious application gets installed, during the runtime or by the network traffic analysis. In this paper, we first present the information about different categories of mobile malware and threats; then, we classify the recent research methods on mobile malware traffic detection."

Source: IEEE Xplore

Mal-Detect: An intelligent visualization approach for malware detection

"Recent outbreaks of pandemics have deepened the adoption and use of IT-based systems. This development has led to an exponential increase in cyberattacks caused by malware. Current approaches (static, dynamic and hybrid) for detecting malware still exhibit low efficiency when subjected to sophisticated malware. This work used an ensemble technique consisting of Deep Convolutional

interdependence, 'buffalo jumping' or 'one-to-many' type of cyber attacks are becoming more commonplace. We have already seen this happen with SolarWinds, Nobelium, and Kaseya. By attacking organisations with deeper pockets and wider networks, adversaries are maximising their financial gain without increasing effort. This may take the form of–but is not limited– to phishing or third-party attacks. The common thread in both is the lack of awareness among the organisation's workforce. According to IBM's X-Force Threat Intelligence Index 2022, phishing operations contributed a significant 41 per cent to running ransomware attacks."
Source: The Indian Express

Leaked documents show notorious ransomware group has an HR department, performance reviews and an 'employee of the month'

- "A huge leak of internal documents — thought to be an act of revenge over Conti's pro-Russia stance — revealed details about the notorious hacker group's size, leadership and operations.
- The messages show that Conti operates much like a regular company, with salaried workers, bonuses, performance reviews and even "employees of the month."
- Cybersecurity experts say some workers were told they were working for an ad company and likely were unaware who was employing them."

Source: CNBC

March ransomware attacks strike finance, government targets

"In March, ransomware reports and disclosures showed a variety of victims, from public schools and county governments to financial services firms and large enterprises."
Source: Tech Target

Report: Many SMBs wouldn't survive a ransomware attack

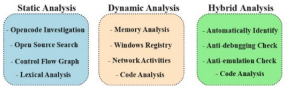
"The report is based on a survey sponsored by CyberCatch and conducted independently by market insights company Momentive. Designed to question SMBs about their susceptibility and resiliency to a ransomware attack, the survey collected responses from 1,200 small- and medium-sized businesses in the U.S. and Canada. The respondents worked for companies with fewer than 500 employees with for-profit

Neural Network and Deep Generative Adversarial Neural Network (Mal-Detect) to analyse, detect, and categorise malware. The proposed Mal-Detect first converts both malware and benign file binaries into RGB binary images. New malware images are then generated using a deep generative adversarial neural network from original malware samples. The generated malware images with original malware and benign files images are pre-processed and trained with Deep Convolutional Neural Networks to extract important features from the dataset."
Source: Journal of King Saud University

Federated learning for malware detection in IoT devices

"Billions of IoT devices lacking proper security mechanisms have been manufactured and deployed for the last years, and more will come with the development of Beyond 5G technologies. Their vulnerability to malware has motivated the need for efficient techniques to detect infected IoT devices inside networks. With data privacy and integrity becoming a major concern in recent years, increasing with the arrival of 5G and Beyond networks, new technologies such as federated learning and blockchain emerged. They allow training machine learning models with decentralized data while preserving its privacy by design. This work investigates the possibilities enabled by federated learning concerning IoT malware detection and studies security issues inherent to this new learning paradigm."
Source: Elsevier

RANSOMWARE

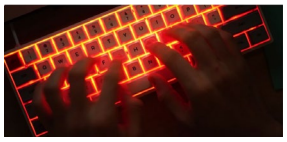


The rise of ransomware: Forensic analysis for windows based ransomware attacks

"While information technologies grow and propagate worldwide, malwares have modified and risen their efficiency towards information system. Recently, the attackers have started to use ransom software (ransomware) as an effective method of cyberattack because of their profitability. Ransomware infiltrate victim systems in various ways, usually encrypt files in the system, and demand a ransom to allow user access to the encrypted files again. Although security mechanisms such as firewalls, anti-virus programs, and automated analysis programs have been developed to combat this threat,

and not-for-profit organizations included. Among those surveyed, 30% said that they don't have a written incident response plan to respond to cyberthreats such as a ransomware attack. Among those that do have this type of plan, 35% last tested it more than six months ago. Some 20% of the respondents said they don't have offline backups of critical data that could be encrypted in an attack. And 34% said they don't give employees phishing tests to determine their exposure to risk."
Source: Tech Republic

MED TECH



Medtech survey finds widespread cybersecurity noncompliance despite rising investment

- "More than half of medical device companies think they are noncompliant with cybersecurity regulations, standards and guidelines, according to a global survey of 150 senior decision makers.
- The poll commissioned by Cybellum, a medtech security company, found that compliance with requirements ranged from 54% for Food and Drug Administration premarket submissions to 37% for International Medical Device Regulators Forum (IMDRF) cybersecurity principles and practices. Many of the surveyed decision-makers plan to become compliant with the various requirements this year.
- Plans to improve compliance are part of a set of evidence that security is becoming a higher priority for medical device manufacturers. More than 80% of respondents see device security as a competitive advantage and almost every polled company increased its security budget this year. However, 78% of those surveyed indicated they are doing the minimum to achieve compliance and 80% view device security as a "necessary evil" imposed by regulators."

Source: Med Tech DIve

these mechanisms have little success and fail to protect the valuable assets stored in local or cloud storage resources. In this study, an effective detection and analysis method against ransomware was proposed, and the proposed method was discussed in detail with a case study."
Source: Elsevier

A Method for Decrypting Data Infected with Hive Ransomware

"Among the many types of malicious codes, ransomware poses a major threat. Ransomware encrypts data and demands a ransom in exchange for decryption. As data recovery is impossible if the encryption key is not obtained, some companies suffer from considerable damage, such as the payment of huge amounts of money or the loss of important data. In this paper, we analyzed Hive ransomware, which appeared in June 2021. Hive ransomware has caused immense harm, leading the FBI to issue an alert about it. To minimize the damage caused by Hive Ransomware and to help victims recover their files, we analyzed Hive Ransomware and studied recovery methods. By analyzing the encryption process of Hive ransomware, we confirmed that vulnerabilities exist by using their own encryption algorithm. We have recovered the master key for generating the file encryption key partially, to enable the decryption of data encrypted by Hive ransomware. We recovered 95% of the master key without the attacker's RSA private key and decrypted the actual infected data."
Source: Cornell University

A Survey of Crypto Ransomware Attack Detection Methodologies: An Evolving Outlook

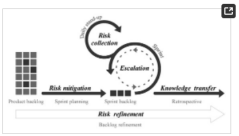
"Recently, ransomware attacks have been among the major threats that target a wide range of Internet and mobile users throughout the world, especially critical cyber physical systems. Due to its unique characteristics, ransomware has attracted the attention of security professionals and researchers toward achieving safer and higher assurance systems that can effectively detect and prevent such attacks. The state-of-the-art crypto ransomware early detection models rely on specific data acquired during the runtime of an attack's lifecycle. However, the evasive mechanisms that these attacks employ to avoid detection often nullify the solutions that are currently in place. More effort is needed to keep up with an attacks' momentum to take the current security defenses to the next level. This

survey is devoted to exploring and analyzing the state-of-the-art in ransomware attack detection toward facilitating the research community that endeavors to disrupt this very critical and escalating ransomware problem. The focus is on crypto ransomware as the most prevalent, destructive, and challenging variation."
Source: MDPI

Evading behavioral classifiers: a comprehensive analysis on evading ransomware detection techniques

"Recent progress in machine learning has led to promising results in behavioral malware detection. Behavioral modeling identifies malicious processes via features derived by their runtime behavior. Behavioral features hold great promise as they are intrinsically related to the functioning of each malware, and are therefore considered difficult to evade. Indeed, while a significant amount of results exists on evasion of static malware features, evasion of dynamic features has seen limited work. This paper examines the robustness of behavioral ransomware detectors to evasion and proposes multiple novel techniques to evade them. Ransomware behavior differs significantly from that of benign processes, making it an ideal best case for behavioral detectors, and a difficult candidate for evasion."
Source: Springer Link

CYBER-RISK ASSESSMENT

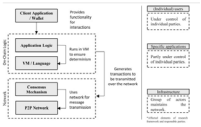


Towards Agile Cybersecurity Risk Management for Autonomous Software Engineering Teams

"In this study, a framework was developed, based on a literature review, to help managers incorporate cybersecurity risk management in agile development projects. The literature review used predefined codes that were developed by extending previously defined challenges in the literature—for developing secure software in agile projects—to include aspects of agile cybersecurity risk management. Five steps were identified based on the insights gained from how the reviewed literature has addressed each of the challenges: (1) risk collection; (2) risk refinement; (3) risk mitigation; (4) knowledge transfer; and (5) escalation. To assess the

appropriateness of the identified steps, and to determine their inclusion or exclusion in the framework, a survey was submitted to 145 software developers using a four-point Likert scale to measure the attitudes towards each step."
Source: MDPI

BLOCK CHAIN



Attacking the trust machine: Developing an information systems research agenda for blockchain cybersecurity

Blockchain-based systems become increasingly attractive targets for cybercrime due to the rising amount of value transacted in respective systems. However, a comprehensive overview of existing attack vectors and a directive discussion of resulting research opportunities are missing. Employing a structured literature review, we extract and analyze 87 relevant attacks on blockchain-based systems and assign them to common attack vectors. We subsequently derive a research framework and agenda for information systems research on the cybersecurity of blockchain-based systems. We structure our framework along the users, developers, and attackers of both blockchain applications and blockchain infrastructure, highlighting the reciprocal relationships between these entities."
Source: Elsevier

MACHINE LEARNING

Applications of Machine Learning Techniques in the Realm of Cybersecurity

"Machine learning (ML) is the latest buzzword growing rapidly across the world, and ML possesses massive potential in numerous domains. ML technology is a subset of Artificial Intelligence (AI) and empowers digital machines with the ability to learn without being explicitly programmed, i.e., the capability to learn from past experiences. Since the last decade, ML technology has been used in various domains because it possesses numerous interesting characteristics such as adaptability, robustness, learnability, and its ability to take instant actions against unexpected challenges. The traditional cybersecurity systems are

built on rules, attack signatures, and fixed algorithms. Thus, the systems can act only upon the '*knowledge*' fed to them and human intervention is continually required for the proper functioning of traditional cybersecurity systems. On the other hand, ML technology can recognize various patterns from past experiences and is capable of predicting or detecting future attacks based on seen or unseen data."
Source: Wiley

AUTONOMOUS VEHICLES

A conceptual system dynamics model for cybersecurity assessment of connected and autonomous vehicles

"Emerging Connected and Autonomous Vehicles (CAVs) technology have a ubiquitous communication framework. It poses security challenges in the form of cyber-attacks, prompting rigorous cybersecurity measures. There is a lack of knowledge on the anticipated cause-effect relationships and mechanisms of CAVs cybersecurity and the possible system behaviour, especially the unintended consequences. Therefore, this study aims to develop a conceptual System Dynamics (SD) model to analyse cybersecurity in the complex, uncertain deployment of CAVs. Specifically, the SD model integrates six critical avenues and maps their respective parameters that either trigger or mitigate cyber-attacks in the operation of CAVs using a systematic theoretical approach."
Source: Elsevier

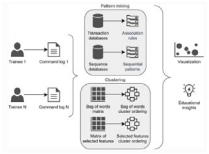
CONSTRUCTIONS

A systemic framework for addressing cybersecurity in construction

"Today, the built environment is designed, built, and managed using digital technology, making it increasingly exposed to cyber security risks. Cybersecurity is a general topic, and the construction sector has been borrowing general solutions and frameworks. However, the construction industry is specific and needs a specialized framework that would assist in understanding and managing cybersecurity. We

have studied general cybersecurity frameworks, cybersecurity standards, research literature, and first principles of systems theory and process engineering. Drawing from that, we developed an original framework that identifies three kinds of wrongful activities: stealing, lying, and harming. It identifies four elements that can be affected by wrongful activities: information asset, material asset, person, and system. It defines cybersecurity as the absence of the three wrongs across the four kinds of elements."
Source: Elsevier

TRAINING



Student assessment in cybersecurity training automated by pattern mining and clustering

"Hands-on cybersecurity training allows students and professionals to practice various tools and improve their technical skills. The training occurs in an interactive learning environment that enables completing sophisticated tasks in full-fledged operating systems, networks, and applications. During the training, the learning environment allows collecting data about trainees' interactions with the environment, such as their usage of command-line tools. These data contain patterns indicative of trainees' learning processes, and revealing them allows to assess the trainees and provide feedback to help them learn. However, automated analysis of these data is challenging. The training tasks feature complex problem-solving, and many different solution approaches are possible. Moreover, the trainees generate vast amounts of interaction data. This paper explores a dataset from 18 cybersecurity training sessions using data mining and machine learning techniques."
Source: Springer Link