SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN

25 DECEMBER 2021 – 18 FEBRUARY 2022

TOPICAL REPORT

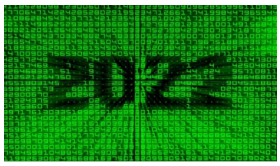
CYBERSECURITY

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



Cybersecurity in 2022 – A Fresh Look at Some Very Alarming Stats

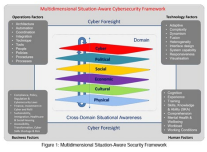
"In retrospect, 2021 was a very trying year for cybersecurity in so many areas. There were high profile breaches such as Solar Winds, Colonial Pipeline and dozens of others that had major economic and security related impact. Ransomware came on with a vengeance targeting many small and medium businesses. Perhaps most worrisome was how critical infrastructure and supply chains security weaknesses were targeted and exploited by adversaries at higher rates than in the past. Since it is only January, we are just starting to learn of some of the statistics that certainly will trend in 2022. By reviewing the topics below, we can learn what we need to fortify and bolster in terms of cybersecurity throughout the coming year."
Source: Forbes

IT Security: Computer Attacks with Laser Light

"Computer systems that are physically isolated from the outside world (air-gapped) can still be attacked. This is demonstrated by IT security experts of the Karlsruhe Institute of Technology (KIT) in the LaserShark project. They show that data can be transmitted to light-emitting diodes of regular office

academic

CYBERSECURITY

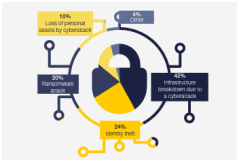


Multidimensional Cybersecurity Framework for Strategic Foresight

"Cybersecurity is now at the forefront of most organisational digital transformative agendas and National economic, social and political programmes. Hence its impact to society can no longer be seen to be one dimensional. The rise in National cybersecurity laws and regulations is a good indicator of its perceived importance to nations. And the recent awakening for social and ethical transparency in society and coupled with sustainability issues demonstrate the need for a paradigm shift in how cybersecurity discourses can now happen. In response to this shift, a multidimensional cybersecurity framework for strategic foresight underpinned on situational awareness is proposed. The conceptual cybersecurity framework comprising six domains such as Physical, Cultural, Economic, Social, Political and Cyber, is discussed. The guiding principles underpinning the framework are outlined, followed by in-depth reflection on the Business, Operational, Technological and Human (BOTH) factors and their implications for strategic foresight for cybersecurity."
Source: Cornell University

reports

CYBERSECURITY



Global Security Outlook 2022

"At the time of writing, digital trends and their exponential proliferation due to the COVID-19 pandemic have thrust the global population onto a new trajectory of digitalization and interconnectedness. One of the starkest and most troubling new consequences of our digitalized existence is the increasingly frequent, costly and damaging occurrence of cyber incidents, sometimes even paralyzing critical services and infrastructure. This trend shows no signs of slowing, notably as sophisticated tools and methods become more widely available to threat actors at relatively low (or in some cases no) cost…Considering these ongoing cyber challenges, the World Economic Forum Centre for Cybersecurity engaged the Cybersecurity Leadership Community consisting of 120 cyber leaders who are senior-most executives from private and public sectors representing 20 countries. The focus of the Centre for Cybersecurity's work was to gather data via a Cyber Outlook Survey and the Cyber Outlook Series (see Appendix) and analyse it to understand cyber leaders' perceptions, and the trajectory of cybersecurity and cyber resilience. The results of the analysis shed light on valuable insights about the state of cyber and perceptions

devices using a directed laser. With this, attackers can secretly communicate with air-gapped computer systems over distances of several meters. In addition to conventional information and communication technology security, critical IT systems need to be protected optically as well."
Source: Karlsruher Institut Für Technologie (KIT)

Cybersecurity and data privacy foresight 2022

"The relentless rate of change in the threat and regulatory environments for cybersecurity and data privacy did not abate in 2021, and we should expect increasing volatility in 2022, necessitating more than ever a forward-looking, risk-based and increasingly globalized strategy. At the same time, exciting new technologies continue to mature and open up new opportunities — and risks. Amidst this complexity and disruption, especially for companies operating in or looking to expand into new jurisdictions and markets around the world, the lessons of the past year can help chart the best course for the year ahead."
Source: Reuters

The Channel Angle: How Cybersecurity Changed Through the Pandemic

"Cyberattacks have been happening for years but have been on an extreme increase in activity since the pandemic began. During the pandemic, cybersecurity was thrust into the spotlight. As an example, SolarWinds and it's environment management technology, was deployed across a large percentage of public and private enterprises, including service providers, when they suffered their own significant security incident. This breach highlighted an important dynamic with our network and security tools and their typically trusted presence throughout environments. When a once trusted solution, was quickly proven untrustworthy, it resulted in organizations around the world needing to perform compromise assessments and to quickly reassess their third-party and fourth-party management strategies. This was previously looked at as an unlikely attack vector to consider to many IT teams, and left those organizations exposed. Further complicating matters is that the very action organizations are instructed to do, keep their software and other solutions up to date, would have been the very path used to compromise so many."
Source: CRN

Cybersecurity in Transit Systems

"Every transit agency should ensure that it has effective cybersecurity practices in place to protect employees, passengers, and infrastructure from cybersecurity events. However, the current environment, together with the COVID-19 pandemic, has produced unforeseen challenges and made it even harder for transit systems to effectively protect their assets, customers, and employees. This synthesis study focuses on cybersecurity of emerging operational technology, such as teleworking/remote worker offices, contactless customer services, real-time service information, and transit-on-demand services, and on cyber resilience practices of transit and other relevant transportation modes. The report is written for transit organization executives and senior managers who would benefit from an understanding of these terms and practices. A literature review and targeted interviews of qualifying organizations that have implemented measures to improve cybersecurity were completed. The synthesis includes multiple, brief case examples that are representative of emerging transit system cybersecurity programs and practices. These examples highlight innovative approaches, successes, challenges, and lessons learned. Gaps in information and future research needs were also identified."
Source: The National Academics of Sciences Engineering Medicine

Intellectual structure of cybersecurity research in enterprise information systems

"Enterprises aspire for ongoing and effective information systems security. Cybersecurity frameworks ensure the availability, confidentiality, and integrity of information. Inspired by the omnipresent challenges and ever-increasing spending by enterprises, we identify the state of research on cybersecurity in enterprises. We employ citation, co-citation, centrality, and citation-path analysis to uncover its intellectual core. Our study reveals five core themes of cybersecurity research: (a) artificial intelligence in cybersecurity, (b) grids, networks, and platform security, (c) algorithms & methods, (d) optimisation & modelling, and (e) cybersecurity management. We discuss the implications for EIS and opportunities for research in each of these themes."
Source: Taylor & Francis Online

about the current path of cyber resilience."
Source: World Economic Forum

Tech Trends 2022

"Despite making significant investments in security technologies, organizations continue to struggle with security breaches: Their adversaries are quick to evolve tactics and stay ahead of the technology curve. Humans may soon be overwhelmed by the sheer volume, sophistication, and difficulty of detecting cyberattacks…Meanwhile, the cost of cybercrime continues to climb; it's expected to double from US$3 trillion in 2015 to US$6 trillion by the end of 2021 and grow to US$10.5 trillion by 2025.1 The average cost of a single data breach in 2021 was US$4.24 million,2 a 10% increase from 2019.3 According to insurer AIG, ransomware claims alone have grown 150% since 2018.4

It's time to call for AI backup. Cyber AI can be a force multiplier that enables organizations not only to respond faster than attackers can move, but also to anticipate these moves and react to them in advance. Cyber AI technology and tools are in the early stages of adoption; the global market is expected to grow by US$19 billion between 2021 and 2025."
Source: Deloitte

Cybersecurity outlook for 2022

"Cyberthreats are in the geopolitical spotlight as conflict over Ukraine has raised alarms about the wider network security risks. The diplomatic standoff puts the threats to operational technology and critical infrastructure in stark relief. This, coupled with the ongoing Log4j remediation, has the security community on high alert. The steady march of cyberthreats, accented by critical vulnerabilities and high-profile ransomware attacks, has come to define the security industry. Log4j succeeds SolarWinds, and it is just a matter of time before another takes its place. Already, industry is racing to patch a trio of SAP CVEs that researchers say would allow attackers to take full control of a system."
Source: Cybersecurity Drive

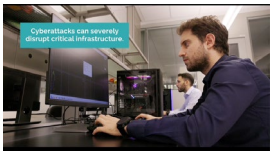
Increasing Sophistication of Attacks and Evolving Threat Landscape Powering Global Industrial Cybersecurity, Outlook 2022

"Cybersecurity attacks increased tremendously in 2020 and 2021, primarily in the frequency and sophistication of attacks. Apart from the growing concerns about signature-less ransomware and

Why are cybersecurity asset management startups so hot right now?

"The cybersecurity industry experienced what is being hailed by some as a "golden year" — funding for cyber startups climbed by 138% to $29.5 billion in 2021 and M&A activity skyrocketed by more than 294% to $77.5 billion. And those focused on securing an organization's internet-facing assets have received more attention than most… Big-name tech giants clearly see the value in this often-overlooked area of the industry, too. Microsoft spent $500 million in July to acquire RiskIQ, a company that provides visibility into what assets, devices and services can be accessed outside of a company's firewall, describing the takeover as a "powerful" addition to its portfolio."
Source: Tech Crunch

CYBER ATTACK



Blocking microgrid cyberattacks to keep the power flowing

"While previous studies into microgrid attacks assumed that attackers have a good knowledge of the power grid's internal components and structure, Zografopoulos and Konstantinou took a more realistic approach. Instead, they adopted a model where the attacker has limited knowledge but is able to design attacks based on historical measured data about the grid's performance.
The researchers considered three different types of attack. Zografopoulos explains, "the first scenario involved altering the measurement data that the microgrid system operator uses to coordinate the power generation of the DGs, the second involved modifying the control signals that regulate power conversion within the DG controllers, while the third involved sudden changes in load, causing grid instabilities."
Source: King Abdullah University of Science & Technology (KAUST)

UTSA researcher part of team protecting EV charging stations from cyberattacks

"As the number of electric cars on the road grows, so does the need for electric vehicle (EV) charging stations and the Internet-based managing systems within those stations. However, these managing systems

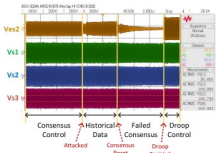
CyberOps: Situational Awareness in Cybersecurity Operations

"Cybersecurity operations, CyberOps, is the use and application of cybersecurity capabilities to a domain, department, organisation or nation. It is fundamentally to protect digital investments, contribute to national economic wellbeing by providing a safe, secure and conducive environment to conduct business and to protect national critical national infrastructures and citizens welfare. In this paper, we investigate operational factors that influence situational awareness of CyberOps, specifically, the features that deals with understanding and comprehension of operational and human factors aspects and that helps with insights on human operator decision making such as cognition, teamwork, knowledge, skills and abilities. The operational factors discussed in this paper range from tools, techniques, integration, architecture to automation, cognition, people, policy, process and procedures."
Source: Cornell University

Guest Editorial Special Section on Cybersecurity of Power Electronics Through Hardware Hardening

"Cybersecurity is becoming a household word in all parts of the developed world because of the headline-grabbing incidents that have occurred over the past five years. These incidents have been perpetrated on the retail industry, banking, health care, water supply, electric power grid, and many more. The term ransomware, where the ultimate attack is coupled with a monetary demand before the attacker releases a locked out system, has also become an infamous term associated with cybersecurity. As awareness has increased, so has the sophistication of the attacks."
Source: IEEE Xplore

CYBER ATTACKS



Cyber-Attack Detection and Countermeasure for Distributed Electric Springs for Smart Grid Applications

"With increasing installations of grid-connected power electronic converters in the distribution network, there is a new trend of using

ransomware-as-a-service, attackers also use artificial intelligence and machine learning to scale up attacks. To this end, many governments acknowledge the serious threat of industrial cybersecurity attacks and propose effective defense policies. However, a shortage of OT security expertise remains a critical issue that needs to be addressed. From an industry standpoint, critical infrastructures are no longer the only targets. Apolitical and financially motivated attacks are now common across all industries, increasingly prompting industry participants to strengthen their awareness in building an effective OT security posture. In addition to critical infrastructures (e.g., power) and the oil and gas sector, industries such as manufacturing, transportation, and logistics also present growth opportunities. While the power sector is ahead in cybermaturity and typically has a higher budget, sectors such as water are challenged with lower budget and resource shortages."
Source: Frost & Sullivan

RANSOMWARE

State of Ransomware Attacks Report

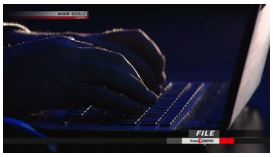
"Ransomware attacks have targeted and inflicted damage at all levels of the government and across varying industries. Local government, healthcare, energy, and financial services are just a few examples of the many sectors hit with ransomware attacks. Valuable industries like critical infrastructure organizations are targeted. Since they provide vital services, organizations are more likely to pay the ransom to protect the stolen data and restore provided services. According to a poll on ransomware, 44% of respondents in the education industry reported a ransomware event. 34% of respondents in the financial services sector and local government reported a ransomware attack."
Source: CyberSaint

face their own issues: cybersecurity attacks.
Elias Bou-Harb, director of the UTSA Cyber Center for Security and Analytics, and his colleagues—Claud Fachkha of the University of Dubai and Tony Nasr, Sadegh Torabi and Chadi Assi of Concordia University in Montreal—are shedding light on the vulnerabilities of these cyber systems. The researchers are also recommending measures that would protect them from harm.
The systems built into electric cars perform critical duties over the Internet, including remote monitoring and customer billing, as do a growing number of internet-enabled EV charging stations."
Source: University of Texas At San Antonio

Identity is the first pillar of zero trust

"The recent increase in high-profile cyberattacks has shown that the federal government can no longer depend on the traditional perimeter-based defenses to defend their networks. Agencies are beginning to realize that they must adapt and adjust their strategies as new malicious tactics and technologies emerge. Earlier this year, President Biden took a step in helping agencies keep up with the ever-changing cyber landscape with his May Executive Order, calling for a revamp in the cybersecurity and Zero Trust process.
Since May, several organizations have followed suit by releasing their own guidelines and publications designed to help advance the effort toward zero trust. In September, the Cybersecurity and Infrastructure Security Agency released its Zero Trust Maturity Model draft guidance, listing "identity" as the first pillar in a successful zero trust model. The National Institute of Standards and Technology also released its zero trust special publication SP-800-207. At the same time, the National Cybersecurity Center of Excellence has started work on a zero trust use case of "building blocks" that provide clear, use-case based examples of how zero trust can be adopted and deployed into agency networks."
Source: Federal News Network

MALWARE



Cyber security experts: Emotet malware rampant again

"Cyber security experts are warning that the resurfaced Emotet malware is spreading rapidly. The Japan distributed control in a cyber layer to coordinate the operations of these power converters for improving power system stability. However, cyber-attacks remain a threat to such distributed control. This paper addresses the cyber-attack detection and a countermeasure of distributed electric springs (ESs) that have emerged as a fast demand-response technology. A fully distributed model-based architecture for cyber-attack detection in the communication network is developed. Based on a dynamic model of ES with consensus control, a local state estimator is proposed and practically implemented to monitor the system. The estimator is fully distributed because only local and neighboring information is necessary. A countermeasure for the distributed ESs to ride through the cyber-attack and maintain regulatory services in a microgrid is demonstrated successfully. Experimental results are provided to verify the effectiveness of the proposed cyber-attack detection method and its ride-through capability."
Source: IEEE Xplore

Cyberattack and Fraud Detection Using Ensemble Stacking

"Smart devices are used in the era of the Internet of Things (IoT) to provide efficient and reliable access to services. IoT technology can recognize comprehensive information, reliably deliver information, and intelligently process that information. Modern industrial systems have become increasingly dependent on data networks, control systems, and sensors. The number of IoT devices and the protocols they use has increased, which has led to an increase in attacks. Global operations can be disrupted, and substantial economic losses can be incurred due to these attacks. Cyberattacks have been detected using various techniques, such as deep learning and machine learning. In this paper, we propose an ensemble staking method to effectively reveal cyberattacks in the IoT with high performance. Experiments were conducted on three different datasets: credit card, NSL-KDD, and UNSW datasets. The proposed stacked ensemble classifier outperformed the individual base model classifiers."
Source: MDPI

Cyber-Attack Detection in Cyber-Physical Systems Using Supervised Machine Learning

"Cyber-Physical Systems (CPS) are where the physical processes are controlled by computation and other

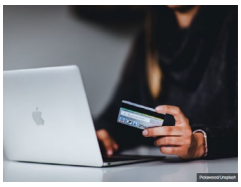
Computer Emergency Response Team Coordination Center says the average daily number of Japan-based email addresses that may be compromised by the malware was around 70. But the number has surged since late January, reaching 1,230 as of February 8. That is close to the figure seen in September 2020, when infections were most widespread. Emotet infects computers through files attached to emails. It steals the content of address books and other data, and sends fake emails to infect other devices."
Source: NHK World

RANSOMWARE

Backup Plays Key Role in Ransomware Response, But Not a Complete Solution

"Ransomware attacks have increased in volume, sophistication and ransom demanded consistently over the last few years. According to published records, the education and retail industries are the most targeted."
Source: Security Week

PHISHING



3 key questions in the wake of OCBC phishing scam

"There are three separate questions we need to ask in order to move forward. First, prevention: What can be done to prevent people from falling victim to such scams and who should be doing it? Second, accountability: Who should be held accountable when a scam occurs and how can victims vindicate their rights? Third, loss allocation: In situations where no one is at fault, besides the scammers, who should bear the loss?"
Source: Today Online

ARTIFICIAL INTELLIGENCE

Putting AI to Practical Use in Cybersecurity

technology components. Although, the collaboration of the computer with traditional physical infrastructure can improve the efficiency of such facility-based systems. However, it increases the scope of attack from physical security to a cybersecurity perspective. Thus, it becomes critical for authorities of such systems to be able to identify the cyber-attacks on such systems and can impact the functioning of such geographically distributed systems. Machine learning techniques have been used to accurately parse such data of Cyber-physical systems to detect attacks. In this paper, we use four different supervised machine learning algorithms to build models to detect cyber-attack activities on a CPS water treatment plant. The result of the four classification models K-Nearest Neighbors (KNN), Support Vector Machine (SVM), Decision Tree (DT), and Random Forest (RF) are compared on the basis of evaluation matrices to perform the comparative analysis. The comparative analysis results show that the DT model performs better than the other models with an overall accuracy of 99.9% and other improved evaluation metrics."
Source: Springer Link

Dynamic Event-Triggered Output Feedback Control for Load Frequency Control in Power Systems With Multiple Cyber Attacks

"This article presents a novel dynamic event-triggered scheme for the load frequency regulation with periodic denial-of-service (DoS) attacks and deception attacks via decentralized output-based control algorithm. Compared with the existing event-triggered strategy, the proposed one automatically changes the parameters of the triggered condition by detecting the frequency trend of the DoS attack to change the release frequency, which can ensure the stability of the power system while increasing the probability of effective transmission subject to DoS attack and thus, reducing network bandwidth usage. First, the proposed dynamic event-triggered strategy combined with the decentralized output-based controller is presented in a unified framework to deal with deception attacks and DoS attacks in the multiarea power system. Then, we utilize the Lyapunov stability theory to analyze the exponential stability in the mean-square sense and the robustness of the power system. By solving a set of linear matrix inequalities (LMIs), a procedure is given for the design of output-based load frequency controllers. Finally, a three-area power system is exploited

"The shortcomings of artificial intelligence (AI) tools in the cybersecurity world have drawn a lot of attention. But does the bad press mean that AI isn't working? Or is AI just getting slammed for failing to meet overinflated expectations. It's time to take a hard look at what AI is accomplishing before kicking it to the curb.

Where Cyber AI Is Winning

There has never been a superhero who hasn't gone to the dark side or fallen off their pedestal. AI is no different. But if you know where AI performs well, you'll have a better idea of how to test vendors' AI claims "Machine learning [and] AI technologies have been influencing information security for a long time," says Alexandra Murzina, a machine learning engineer and data scientist at cybersecurity firm Positive Technologies. "Spam detection or preventing fraudulent transactions are just two of many examples of successful AI applications in security today.""

Source: Dark Reading

HEALTHCARE

There's no 'magic bullet' to enhance cybersecurity, say experts

"Cybersecurity has taken on increased importance in the healthcare industry, particularly as domestic and international incidents continue to dominate the headlines. Amid this dynamic environment, experts stress that an organization's defensive strategy should be flexible and adaptable. At HIMSS22, panelists from the National Cybersecurity Center of Excellence (NCCoE) and affiliated federal agencies will offer their perspectives on the evolving threat landscapes – and examine how various strategies can address cyber risk. "Healthcare continues to be plagued with cyber threats that include ransomware, malware and phishing," observed Nakia Grayson, IT security specialist at the National Institute of Standards and Technology."

Source: Healthcare IT News

ELECTRIC VEHICLE

as a simulation to verify the effectiveness of the proposed results."

Source: IEEE Xplore

MALWARE

IoT Malware Detection Architecture using a Novel Channel Boosted and Squeezed CNN

"Interaction between devices, people, and the Internet has given birth to a new digital communication model, the Internet of Things (IoT). The seamless network of these smart devices is the core of this IoT model. However, on the other hand, integrating smart devices to constitute a network introduces many security challenges. These connected devices have created a security blind spot, where cybercriminals can easily launch an attack to compromise the devices using malware proliferation techniques. Therefore, malware detection is considered a lifeline for the survival of IoT devices against cyberattacks. This study proposes a novel IoT Malware Detection Architecture (iMDA) using squeezing and boosting dilated convolutional neural network (CNN). The proposed architecture exploits the concepts of edge and smoothing, multi-path dilated convolutional operations, channel squeezing, and boosting in CNN. Edge and smoothing operations are employed with split-transform-merge (STM) blocks to extract local structure and minor contrast variation in the malware images. STM blocks performed multi-path dilated convolutional operations, which helped recognize the global structure of malware patterns. Additionally, channel squeezing and merging helped to get the prominent reduced and diverse feature maps, respectively."

Source: Cornell University

A Survey on DNS Encryption: Current Development, Malware Misuse, and Inference Techniques

"The domain name system (DNS) that maps alphabetic names to numeric Internet Protocol (IP) addresses plays a foundational role for Internet communications. By default, DNS queries and responses are exchanged in unencrypted plaintext, and hence, can be read and/or hijacked by third parties. To protect user privacy, the networking community has proposed standard encryption technologies such as DNS

Electric vehicle charging stations are a new focus for Concordia cybersecurity researchers

"In a paper published in the journal Computers & Security, a Concordia-led team of researchers studied the vulnerabilities found in some of the EV charging station industry's biggest manufacturers. They found significant weaknesses that can leave those systems open to cyberattacks, with consequences affecting users, the stations themselves and even the power grid they connect to.

The researchers at the Gina Cody School of Engineering and Computer Science's Security Research Centre used several techniques to assess the security of 16 EV charging station management systems (EVCSMS), including system lookup and collection, reverse engineering and penetration testing techniques. They identified the leading products and discovered vulnerabilities in them by assessing their security measures, then discussed the implications of successful cyberattacks that may leverage them and simulated the impact of potential cyberattacks on the power grid."

Source: University of Concordia

PHONE SECURITY

First real-world study shows the potential of gait authentication to enhance smartphone security

"Real-world tests have shown that gait authentication could be a viable means of protecting smartphones and other mobile devices from cyber crime, according to new research.

A study led by the University of Plymouth asked smartphone users to go about their daily activities while motion sensors within their mobile devices captured data about their stride patterns.

The results showed the system was on average around 85% accurate in recognising an individual's gait, with that figure rising to almost 90% when they were walking normally and fast walking."

Source: University of Plymouth

SOFTWARE

over TLS (DoT), DNS over HTTPS (DoH), and DNS over QUIC (DoQ) for DNS communications, enabling clients to perform secure and private domain name lookups. We survey the DNS encryption literature published since 2016, focusing on its current landscape and how it is misused by malware, and highlighting the existing techniques developed to make inferences from encrypted DNS traffic. First, we provide an overview of various standards developed in the space of DNS encryption and their adoption status, performance, benefits, and security issues. Second, we highlight ways that various malware families can exploit DNS encryption to their advantage for botnet communications and/or data exfiltration. Third, we discuss existing inference methods for profiling normal patterns and/or detecting malicious encrypted DNS traffic. Several directions are presented to motivate future research in enhancing the performance and security of DNS encryption."

Source: Cornell University

Android Malware Detection using Feature Ranking of Permissions

"We investigate the use of Android permissions as the vehicle to allow for quick and effective differentiation between benign and malware apps. To this end, we extract all Android permissions, eliminating those that have zero impact, and apply two feature ranking algorithms namely Chi-Square test and Fisher's Exact test to rank and additionally filter them, resulting in a comparatively small set of relevant permissions. Then we use Decision Tree, Support Vector Machine, and Random Forest Classifier algorithms to detect malware apps. Our analysis indicates that this approach can result in better accuracy and F-score value than other reported approaches. In particular, when random forest is used as the classifier with the combination of Fisher's Exact test, we achieve 99.34\% in accuracy and 92.17\% in F-score with the false positive rate of 0.56\% for the dataset in question, with results improving to 99.82\% in accuracy and 95.28\% in F-score with the false positive rate as low as 0.05\% when only malware from three most popular malware families are considered."

Source: Cornell University

Agent-based modeling and simulation for malware spreading in D2D networks

"This paper presents a new multi-agent model for simulating malware propagation in device-to-device (D2D) 5G networks. This model allows

Researchers develop automated approach to extract security policies from software

"Unlike traditional software models, the agile software development process is meant to produce software at a faster pace, eliminating the need to spend time on comprehensive documents and changing software requirements. User stories, the specifications that define the software's requirements, are the only required documentation. However, the practices innate to this process, such as constant changes in code, limit the ability to conduct security assurance reviews.

"The basic idea of addressing this disconnect between security policies and agile software development came from happenstance conversation with software leaders in the industry," Krishnan said. "We were able to assemble a team of faculty and students with expertise in cybersecurity, software engineering and machine learning to start investigating this problem and develop a practical solution.""

Source: University of Texas At San Antonio

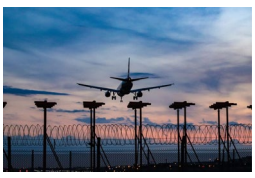
HIGHER EDUCATION

Data Science, Cybersecurity and the Metaverse Future of Higher Education

"Higher education is evolving continuously with the new age of digital exploration. Even though metaverse has been in existence for decades, it is now gaining heavy traction. Along with that, data science and cybersecurity are trends and have also captured the attention of the IT world. Cybersecurity, data science, and the metaverse are exponential markets, where the global market size of cybersecurity is estimated to reach around $370 billion by 2028 growing at a CAGR of 12% from $153.16 billion in 2020, while the global data science market is expected to value a little over $80 billion by 2027 with a CAGR of 11.1% and the global metaverse market is predicted to expand at a CAGR of 41.7% from 2021 to 2030."

Source: Tech Graph

AVIATION



to understand and analyze mobile malware-spreading dynamics in such highly dynamical networks. Additionally, we present a theoretical study to validate and benchmark our proposed approach for some basic scenarios that are less complicated to model mathematically and also to highlight the key parameters of the model. Our simulations identify critical thresholds for "no propagation" and for "maximum malware propagation" and make predictions on the malware-spread velocity as well as device-infection rates. To the best of our knowledge, this paper is the first study applying agent-based simulations for malware propagation in D2D."

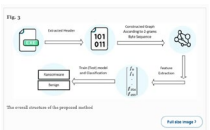
Source: Cornell University

A comprehensive survey on machine learning approaches for malware detection in IoT-based enterprise information system

"The Internet of Things (IoT) is a relatively new technology that has piqued academics' and business information systems' attention in recent years. The Internet of Things establishes a network that enables smart devices in an organisational information system to connect to one another and exchange data with the central storage. Android apps are placed on Android apps to enhance the user-friendliness of IoT devices in business information systems, making them more interactive and user-friendly. However, the usage of Android apps makes IoT devices susceptible to all forms of malware attacks, including those that attempt to hack into IoT devices and get access to sensitive information stored in the corporate information system. The researchers offered a variety of attack mitigation approaches for detecting harmful malware embedded in an Android application operating on an IoT device. In this context, machine learning offered the most promising strategies to detect malware attacks in IoT-based enterprise information systems because of its better accuracy and precision. Its capacity to adapt to new forms of malware attacks is a result of its learning capabilities."

Source: Taylor & Francis Online

RANSOMWARE



A novel approach for ransomware detection based

Why Cybersecurity Remains The Top Tech Investment For Airlines In 2022

"Despite the aviation industry going through a considerable transformation over the last few years, certain priorities remain the same. With a new chapter underway, cybersecurity continues to be the top airline technology investment. SITA, the IT provider for the air transport industry, released findings from industry surveys conducted last year. The research looks into developing IT trends and the role of technology in aiding the market's recovery from the global health crisis.

While sectors such as biometrics, sustainability, and digital verification remain high on the agenda, cybersecurity remains the top priority for aviation stakeholders."

Source: Simply Flying

on PE header using graph embedding

"The development of cryptocurrency has led to an increase in a type of malware called ransomware. Ransomware is a family of malware that uses malicious techniques to prevent users from accessing their systems or data. Ransomware threatens all industries, from health and hospitals to banks, training centers, and manufacturers of goods. Therefore, early ransomware detection is critical. Most researchers try to identify ransomware by examining the behavior of the software at runtime. Therefore, these approaches are costly and require resources to run every software. In this paper, ransomware detection is conducted without running the software and without any special pre-processing, only using the headers of the executable file. In the proposed approach, a graph is created using the headers of executable files (specifically portable executable files) and then the graph is mapped in an eigenspace using the "Power Iteration" method."

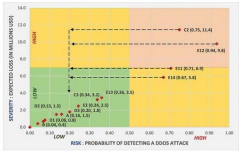
Source: Springer Link

Bitcoin Ransomware Detection Employing Rule-Based Algorithms

"Cryptocurrencies have completely altered the digital transaction process all over the globe. Almost a decade after Satoshi Nakamoto generated the first Bitcoin block; many cryptocurrencies have been established. The Ransomware attack is a type of cybercrime and a class of malware that encrypts the files and prevents users from accessing their data or systems and demands payment for decrypting and retrieving access to their files. Ransomware data classification using present data mining and machine learning methods is difficult because predictions aren't always correct. We aim to build two models that effectively address these challenges and can diagnose and classify Ransomware attacks accurately, then compare the performance of the models. In this paper, we investigated the use of Rule-Based algorithms for mining Bitcoin Ransomware Data to classify Ransomware attacks in Bitcoin transactions. Employing Rule-Based techniques in detecting Bitcoin data is beneficial because the algorithms effectively classify non-linear datasets."

Source: Science Journal of University of Zakho

CYBER-RISK ASSESSMENT



Kernel naïve Bayes classifier-based cyber-risk assessment and mitigation framework for online gaming platforms

"Recently, the number and intensity of cyberattacks against massively multiplayer online (MMO) gaming platforms have increased; up to 74% of distributed denial-of-service (DDoS) attacks on MMO gaming (MMOG) firms have been launched by hackers. These malicious attacks affect gamers' experience and MMOG firms' revenue model. Along with financial losses, MMOG firms' reputation also suffers from these attacks. Therefore, in this study, we devised a framework to quantify and mitigate cyber-risk for MMOG firms using a hybrid learning method, namely, a kernel naïve Bayes classifier. Our kernel naïve Bayes classifier-based cyber-risk assessment and mitigation (KB-CRAM) framework included the DDoS attack traits. Subsequently, it outputs (i) the probability of DDoS attacks; (ii) the expected financial losses; and (iii) cyber-risk mitigation strategies, such as self-protection (technology, compliance, and legal deterrence), self-insurance, or cyber-insurance. Our study contributes to field-relevant literature by providing managers with a tool to improve game performance. This framework also suggests ways in which MMOG firms can hedge losses against repeated attacks from unethical hackers."
Source: Taylor & Francis Online

Cyber-risk Management Framework for Online Gaming Firms: an Artificial Neural Network Approach

"Hackers have used Distributed-Denial-of-Service attacks to overwhelm a firm's cyber-resources resulting in disrupted access to legitimate end-users. Globally, DDoS attacks cost firms between US$ 120 K to US$ 2 M for each incident. Apart from the monetary loss, they also disrupt service quality and damage the brand reputation of firms. In 2018-2019, Massively Multiplayer Online Gaming (MMOG) firms witnessed 74% of the total DDoS attacks. MMOG firms form a lucrative segment for hackers because of their large customer base and the massive incentive to cause disruptions and losses. Our Feedforward Neural Network-based Cyber-risk Assessment and Mitigation (FNN-CRAM) model consists of three modules: assessment, quantification, and mitigation. The

cyber-risk assessment module uses FNN, which takes seven inputs comprising DDoS attack intensity and duration for five DDoS attack types, vulnerability data (i.e., their counts and score), and the vulnerability trends over time. This layer is connected to a ten-neuron hidden layer and one neuron output layer that estimates the probability of these attacks."
Source: Springer Link