SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN

23 OCTOBER – 24 DECEMBER 2021

TOPICAL REPORT

CYBERSECURITY

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

view past reports | subscribe to others | unsubscribe

news

CYBERSECURITY

IBM Canada, University of Ottawa to establish state-of-the-art Cyber Range to train for cybersecurity threats

"IBM (NYSE: IBM) and the University of Ottawa today announce a multi-year partnership to build and operate a Cyber Range: a fully immersive, interactive, and experiential learning facility that will enable state-of-the-art research and training in cybersecurity and cyber safety. As part of the agreement, IBM is also making a more than $21 million in-kind contribution to the University over five years to support business development and security training, while uOttawa will invest nearly $7 million over the same period."
Source: University of Ottawa

This Tool Protects Your Private Data While You Browse

"A team of computer scientists at the University of California San Diego and Brave Software have developed a tool that will increase protections for users' private data while they browse the web.
The tool, named SugarCoat, targets scripts that harm users' privacy—for example, by tracking their browsing history around the Web—yet are essential for the websites that embed them to function. SugarCoat replaces these scripts with scripts that have the same properties, minus the privacy-

academic

CYBERSECURITY

An Integrated Cybernetic Awareness Strategy to Assess Cybersecurity Attitudes and Behaviours in School Context

"Digital exposure to the Internet among the younger generations, notwithstanding their digital abilities, has increased and raised the alarm regarding the need to intensify the education on cybersecurity in schools. Understanding of the human factor and its influence on children, namely their attitudes and behaviors online, is pivotal to reinforce their awareness towards cyberattacks, and to promote their digital citizenship. This paper aims to present an integrated cybersecurity and cyberawareness strategy composed of three major steps: (1) Cybersecurity attitude and behavior assessment, (2) self-diagnosis, and (3) teaching/learning activities. The following contributions are made: Two questionnaires to assess risky attitudes and behaviors regarding cybersecurity; a self-diagnosis to measure students' skills on cybersecurity; a lesson plan addressing cyberawareness to be applied on Information and Communications Technology (ICT) and citizenship education curricular units."
Source: MDPI

reports

CYBERSECURITY

The state of cybersecurity resilience 2021

"In brief

- Our cybersecurity report shows cyber attacks are up, security investment continues to rise and cloud still has a complex relationship with security.
- We reveal four levels of cyber resilience: Cyber Champions, Business Blockers, Cyber Risk Takers and The Vulnerable.
- Cyber Champions lead; they're among the top 30% in at least three of four cyber resilience criteria and align business strategy and cybersecurity.
- For success, organizations need to give CISOs a seat at the top table, be threat-centric and business aligned and get the most out of secure cloud."

Source: Accenture

Companies may be overlooking the riskiest cyber threats of all

"A majority of companies don't have a handle on their third-party cyber risks – risks obscured by the complexity of their business relationships and vendor/supplier networks. This is the finding of the PwC 2022 Global Digital Trust Insights

harming features. SugarCoat is designed to be integrated into existing privacy-focused browsers like Brave, Firefox, and Tor, and browser extensions like uBlock Origin. SugarCoat is open source and is currently being integrated into the Brave browser."
Source: UC San Diego

Researchers unveil new cyber protections against "logic bombs"

"Cybersecurity researchers at Rutgers University-New Brunswick and the Georgia Institute of Technology have proposed new ways to protect 3D printed objects such as drones, prostheses and medical devices from stealthy "logic bombs."
The researchers will present their paper, titled "Physical Logic Bombs in 3D Printers via Emerging 4D Techniques," at the 2021 Annual Computer Security Applications Conference on Dec. 10."
Source: EurekAlert!

The three horsemen of cyber risks: misinformation, disinformation and fake news

"The fake news "infodemic" that spread alongside the COVID-19 pandemic also affected the finance sector. For instance, during the lockdown period of 2020, there was a huge surge in fake news and illegal activity related to the financial and other markets. Financial firms had to train their staff to deal with fraudulent online schemes and reports.
Deliberate spreading of disinformation has also been responsible for swaying the outcome of elections. Cyber attackers have used misleading information on social media for procuring campaign finances as well as personal and financial information of people and corporations. These actions undermine a nation's security and make them vulnerable to geopolitical risks."
Source: Elsevier

Synthetic identity fraud: What is it, and why is it harmful?

"Digital criminals are creating new and effective ways to con businesses and financial institutions by using synthetic identity fraud. They are having enough success that those in the know at McKinsey and Company are more than a little concerned: "By our estimates, synthetic identity fraud is the fastest-growing type of financial crime in the United States, accounting for ten to fifteen percent of charge-offs in a typical unsecured lending portfolio."
Laura Hoffner, current chief of staff at Concentric and former naval

A rough cut cybersecurity investment using portfolio of security controls with maximum cybersecurity value

"This paper deals with optimisation of cybersecurity investment in supply chains using stochastic programming approach. A classical exponential function of breach probability and the intuitive idea of 'the expected net benefits', originally presented in 2002 by Gordon and Loeb, were applied to introduce the concept of cybersecurity value. The cybersecurity value of security control is defined as the value gained by implementing a single control to secure a subset of components. The cybersecurity value of a control can be seen as a measure of its efficiency in reducing vulnerability of a secured system or component. A mixed binary optimisation problem, next transformed into an unconstrained binary program is developed to maximise total cybersecurity value of control portfolio."
Source: Taylor & Francis Online

Analysis of cybersecurity competencies: Recommendations for telecommunications policy

"The paper aims to analyse and assess cybersecurity competencies and define the recommended solutions to improve the human factor in cybersecurity. The article presents the results of theoretical and empirical research that were carried out in 2019–2021. The research subject constitutes one of the priorities of many countries and international organisations. Cybersecurity is one of the essential foundations for implementing the idea of sustainable development. A cybersecurity analysis using a layered structure was proposed in the theoretical part. Empirical research was conducted using a diagnostic poll method based on a survey. The presentation of the research results includes an analysis of statistical dependencies. The paper presents the research results on cybersecurity competencies in the field of threats to state cyberspace and methods of securing and protecting data."
Source: Elsevier

Cybersecurity Requirements for AM Systems: New Enforcement in DoD Environments, and Resources for Implementation

"The Office of the Inspector General (OIG) for the US Department of Defense (DoD) released Audit of the Cybersecurity of Department of Defense Additive Manufacturing

Survey. The survey of 3,600 CEOs and other C-suite executives globally found that 60% have less than a thorough understanding of the risk of data breaches through third parties, while 20% have little or no understanding at all of these risks.
The findings are a red flag in an environment where 60% of the C-suite respondents anticipate an increase in cyber crime in 2022. They also reflect the challenges organizations face in building trust in their data -- making sure it is accurate, verified and secure, so customers and other stakeholders can trust that their information will be protected.
Notably, 56% of respondents say their organizations expect a rise in breaches via their software supply chain, yet only 34% have formally assessed their enterprise's exposure to this risk. Similarly, 58% expect a jump in attacks on their cloud services, but only 37% profess to have an understanding of cloud risks based on formal assessments."
Source: PWC

MORE Alarming Cybersecurity Stats For 2021!

"Earlier this year I wrote a FORBES article called "**Alarming Cybersecurity Stats: What You Need To Know For 2021."** Alarming Cybersecurity Stats: What You Need To Know For 2021 (forbes.com) It included an assortment of stats on the increase in threats to our digital wellness as companies, governments, and consumers. The article was based on the backdrop of a spate of high-profile cyber-attacks such as Solar Winds, and Colonial Pipeline and had painted a dire assessment of the 2021 first half status of the cyber-threat ecosystem. Now we have reached the second half of 2021. Just when we thought it could not get much worse from a cybersecurity stat perspective, it did."
Source: Forbes

134 Cybersecurity Statistics and Trends for 2022

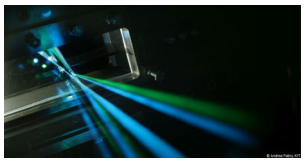
"Cybersecurity issues are becoming a day-to-day struggle for businesses.
Recent trends, side effects of a global pandemic and cybersecurity statistics reveal a huge increase in hacked and breached data from sources that are increasingly common in the workplace, like mobile and IoT devices. On top of this, COVID-19 has ramped up remote workforces, making inroads for cyber attacks.
Additionally, recent security research suggests most companies have unprotected data and poor cybersecurity practices in place, making them vulnerable to data loss. To successfully fight against malicious intent, it's imperative that companies

intelligence officer, is also concerned. "We're seeing a huge increase in synthetic identity fraud — the process of combining real and fake personal information to create an identity and commit fraud," Hoffner said during an email conversation. "It's really growing, fueled by easy criminal access to corporate networks and Ransomware as a Service (RaaS) tools."."
Source: Tech Republic

Squid Game Used as Lure for Malware Campaigns, Phishing Attacks

"Kaspersky uncovered dozens of different malicious files related to Squid Game between September and October 2021, reported PC Mag. In one of those attack instances, a user came across an animated version of the first game depicted in Netflix's series. What the user didn't know is that the campaign downloaded a trojan in the background. Once launched, that threat stole the user's data from their web browser and exfiltrated it to a server under the attackers' control."
Source: Security Intelligence

CYBER ATTACK



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 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: Karlsruhe Institute of Technology

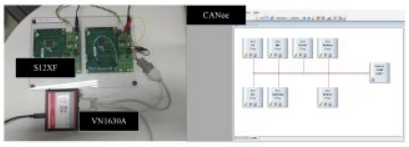
14 new attacks on web browsers detected

"IT security experts have identified 14 new types of attacks on web browsers that are known as cross-site leaks, or XS-Leaks. Using XS-Leaks, a malicious website can grab personal data from visitors by interacting with other websites in the background. The researchers from Ruhr-Universität Bochum (RUB) and Niederrhein Systems (DODIG-2021-098) [1] in July 2021, to determine "whether DoD [sites] secured additive manufacturing (AM) systems to prevent unauthorized changes and ensure the integrity of the design data." The audit report recommends requiring "all AM systems to obtain an authority to operate in accordance with DoD policy before their use" [1], and requiring "AM system owners to immediately identify and implement security controls to minimize risk until obtaining an authority to operate." The DoD Chief Information Officer (CIO) responded that existing DoD regulations require both of these for "all IT systems, including AM systems"."
Source: ACM Digital Library

A Comparison of SONA and MTurk for Cybersecurity Surveys

"For almost every online account, people are required to create a password to protect their information online. Since many people have many accounts, they tend to create insecure passwords and re-use passwords. These insecure passwords are often easy to guess, which can lead to compromised data. It is well-known that every person has a different personality type, which can be determined using personality models such as Big Five and True Colors. This research examines if there is a link between personality type and password security among a variety of participants in two groups of participants: SONA and MTurk. Each participant in both surveys answered questions based on password security and their personality type. Our results show that participants in the MTurk survey were more likely to choose a strong password and to exhibit better security behaviors and knowledge than participants in the SONA survey."
Source: ACM Digital Library

CYBER ATTACKS



Cyber-attack detection for automotive cyber-physical systems

"To provide a high level of security for automotive cyber-physical systems, we propose a new in-vehicle security protocol (IVSP) detecting various cyber-attacks based on a symmetric key. In the IVSP, the complex key distribution mechanism is not required, and a key exposed problem does not occur as the IVSP does not exchange the used secret key between sender and receiver nodes

make cybersecurity awareness, prevention and security best practices a part of their culture.
In order to give you a better idea of the current state of overall security, we've compiled over 100 cybersecurity statistics for 2022. Hopefully, this will help show the prevalence and need for cybersecurity in all facets of business. This includes data breaches, hacking stats, different types of cybercrime, industry-specific stats, spending, costs and the cybersecurity career field."
Source: Varonis

CYBER SURVEY

2021 Future of cyber survey

"Amid the acceleration of digital transformation, 69% of global leaders surveyed noted a significant increase in cyberattacks at their companies this year. However, despite the elevated risk environment, leaders plan to continue to invest heavily in digital transformation—with 94% of chief financial officer (CFO) respondents looking to move their financial systems or Enterprise Resource Planning (ERP) to the cloud. That's according to a new Deloitte Global survey released today, which reveals that while there is no simple solution, there are a number of measures, which, when taken together, can enable organisations to embed cyber in every aspect of their business.
Deloitte Global's 2021 Future of Cyber Survey analyses responses from nearly 600 global C-level executives who have visibility into the cybersecurity functions of their organisations, with the hope of increasing communication around embedding cyber into the core of every business, while providing insights on how organisations can increase visibility into complex technological ecosystems and implement best practices to better prepare for an unpredictable cyber future.
"Over the last year, businesses have been working overtime to remain competitive amid rapid technological change as accelerated digital transformation has drastically increased organisations' vulnerability to cyberattacks," says Emily Mossburg, Deloitte Global Cyber Leader. "As the complexities of integrated environments continue to grow, leaders must prioritise incorporating cyber into every part of their business or risk the consequences of inadequate cyber protections."."
Source: Deloitte

University of Applied Sciences tested how well 56 combinations of browsers and operating systems are protected against 34 different XS-Leaks. To this end, they developed the website XSinator.com, which allowed them to automatically scan browsers for these leaks. Popular browsers such as Chrome and Firefox, for example, were vulnerable to a large number of XS-Leaks. "XS-Leaks are often browser bugs that have to be fixed by the manufacturer," says Lukas Knittel, one of the Bochum authors of the paper."
Source: Ruhr Universitat Bochum

Deeper defense against cyber attacks

"To address the growing threat of cyberattacks on industrial control systems, a KAUST team including Fouzi Harrou, Wu Wang and led by Ying Sun has developed an improved method for detecting malicious intrusions.
Internet-based industrial control systems are widely used to monitor and operate factories and critical infrastructure. In the past, these systems relied on expensive dedicated networks; however, moving them online has made them cheaper and easier to access. But it has also made them more vulnerable to attack, a danger that is growing alongside the increasing adoption of internet of things (IoT) technology."
Source: KAUST Discovery

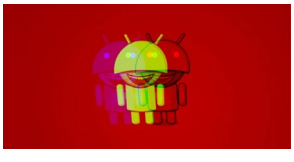
Grinch bots hijack all kinds of holiday shopping, from gift cards to hype drop sales

"All-in-one Grinch bots are working over time this holiday season and using automation to steal gift cards and scoop up limited quantities of in-demand products. The Kasada Threat Intelligence Team identified these bad bot trends during the online holiday shopping season, based on data from the company's e-commerce customers.
The analysis identified these activity patterns:

- 4x increase in automated online gift card lookup attempts
- 10x increase in malicious login attempts via credential stuffing
- Discovery of a new and more efficient all-in-one bot often used during hype drop sales"

Source: Tech Republic

MALWARE



for key synchronization. Our preliminary result shows that the proposed IVSP achieves the good performance in terms of the cyber-attack detection rate."
Source: ACM Digital Library

Digital Transformation and emerging ICS/OT cyber attacks - Imminent Threats to Our Society

"Cyberspace has become kind of war zone as geopolitical tensions are on the rise and digital transformation is rapidly making its way into our societies by connecting everything from power plants to drones to medical devices worn by patients. Once limited to opportunistic cyber criminals and hacktivists, cyber-attacks are now becoming a key weapon for nation states for espionage campaigns and destructive actions against their adversaries in the event of conflicts.
In the era of smart devices and hyperconnected things (internet of things-IoT), bits are becoming more powerful than bullets and malware is taking place of militias. Cyber-attacks could be leveraged by adversaries as a potentially powerful means to a wide variety of political, military, and economic goals and have potential threat to our societies."
Source: ACM Digital Library

A Novel Approach for Detection and Location of Cyber-Attacks in Water Distribution Networks

"Most scientific contributions addressing cyber-security issues in water distribution networks present proposals of detection systems and very few propose location systems. A novel methodology for detection and location of cyber-attacks in water distribution networks (WDNs) is proposed in this paper. Structural analysis and autoencoder neural networks are effectively combined with a the control chart Adaptive Exponentially Weighted Moving Average (AEWMA). In the training phase, the proposed detection and location framework only requires data from normal operating conditions and knowledge about the behavioral model of the system which represents an advantage over previous works that demand for additional data of cyber-attacks. Among other advantages of the proposed methodology are the high performance in the effective, robust and early detection and the effectiveness of the location strategy. The proposal was evaluated with the known case study BATADAL."
Source: Springer Link

RANSOMWARE

Insights for CISOs: Ransomware

"Ransomware has evolved into a top security concern for organizations, and the escalating number of attacks have validated the harmful impact this type of malware can cause across numerous sectors and industries. Cyber-attacks involving ransomware were originally viewed as a novelty that creative criminals came up with, but this type of malware attack has grown into an immense criminal enterprise with significant economic and financial implications. While ransomware is not a new issue, it is now a more prevalent, sophisticated, and damaging concern to a variety of organizations and critical infrastructure entities with a fear factor that it could cost millions of dollars to regain control of data. A rehashed phenomenon with greater defense challenges, ransomware is now used as a digital terrorism tactic, and has been declared a national security issue by the National Security Agency (NSA) in the United States."
Source: Frost & Sullivan

SUPPLY CHAIN ATTACKS

Insights for CISOs: Improving Resilience in the Face of Supply Chain Attacks

"At the end of 2020, FireEye discovered malware distributed through software updates to the Orion Platform, a popular IT management product. SolarWinds, the platform supplier, was breached earlier that year and failed to detect hackers in its environment for several months. Because of the widespread usage of the SolarWinds software, victims of this attack include thousands of high-profile businesses, governments, and law enforcement agencies.
Large-scale data breaches brought to light security considerations of the increasing reliance on third-party technology and services. Because of that, there are growing calls for solutions and strategies that could help organizations mitigate risk stemming from reliance on digital supply chains. Although there is a wide range of solutions that can

Over 500,000 Android Users Downloaded a New Joker Malware App from Play Store

"A malicious Android app with more than 500,000 downloads from the Google Play app store has been found hosting malware that stealthily exfiltrates users' contact lists to an attacker-controlled server and signs up users to unwanted paid premium subscriptions without their knowledge. The latest Joker malware was found in a messaging-focused app named Color Message ("com.guo.smscolor.amessage"), which has since been removed from the official app marketplace. In addition, it has been observed simulating clicks in order to generate revenue from malicious ads and connecting to servers located in Russia."
Source: The Hacker News

Experts warn Emotet malware is back

"Cyber security experts say the Emotet malware has returned, warning that it could spread during New Year holidays. Japan's Information-technology Promotion Agency says the malware was confirmed to be active again in November.
Emotet has infected computers around the world for several years.
Law enforcement authorities from Europe and several other countries announced in January this year that they had taken down the malware infrastructure.
Emotet steals data from infected computers and spreads to other devices through emails."
Source: NHK Japan

Malware removal on Android: how to clean up your smartphone

"Is your Android smartphone playing up? Maybe it's running sluggishly all of a sudden, perhaps popping up ads here and there, or just being randomly a bit weird. It may be because you have a problem with malware, or a Potentially Unwanted Program (PUP).
So what's the best way to check for any malware on your device?
It's simple: grab yourself an anti-malware tool and it won't take long to install the app, get it going and run a scan. In this guide, we will take you through the process of cleaning house and getting rid of any potential malware on your Android device, with clear and concise explanations in step-by-step fashion."
Source: Tech Radar

Neutralizing Cyber Attacks: Techniques of Neutralization and Willingness to Commit Cyber Attacks

"Cyber attacks on critical infrastructure by ideology-based hackers may have both significant financial costs and public safety consequences. Scholars have been increasingly using Sykes and Matza's (1957) techniques of neutralization to better understand the commission of various forms of cybercrime, including that of computer hacking. This study examines the effects of techniques of neutralization on college students' willingness to commit cyber attacks, specifically defacing websites and compromising financial and government servers, against both domestic and foreign targets. An overall techniques of neutralization scale significantly predicted being willing to commit all examined forms of cyber attacks even after controlling for peer behavior, computer skills, time spent online, and being male. The strongest support was found for the techniques of condemnation of the condemners and claim of entitlement."
Source: Springer Link

Dynamic Event-Triggered Output Feedback Control for Networked Systems Subject to Multiple Cyber Attacks

"This article is concerned with the problem of the H∞ output feedback control for a class of event-triggered networked systems subject to multiple cyber attacks. Two dynamic event-triggered generators are equipped at sensor and observer sides, respectively, to lower the frequency of unnecessary data transmission. The sensor-to-observer (STO) channel and observer-to-controller (OTC) channel are subject to deception attacks and Denial-of-Service (DoS) attacks, respectively. The aim of the addressed problem is to design an output feedback controller, with the consideration of the effects of dynamic event-triggered schemes (DETSs) and multiple cyber attacks. Sufficient condition is derived, which can guarantee that the resulted closed-loop system is asymptotically mean-square stable (AMSS) with a prescribed H∞ performance. Moreover, we provide the desired output feedback controller design method. Finally, the effectiveness of the proposed method is demonstrated by an example."
Source: IEEE Xplore

A comprehensive review study of cyber-attacks and cyber

improve organizations' security posture, the industry lacks a dedicated and comprehensive supply chain security solution."
Source: Frost & Sullivan

New PseudoManuscrypt Malware Infected Over 35,000 Computers in 2021

"Industrial and government organizations, including enterprises in the military-industrial complex and research laboratories, are the targets of a new malware botnet dubbed PseudoManyscrypt that has infected roughly 35,000 Windows computers this year alone.

The name comes from its similarities to the Manuscrypt malware, which is part of the Lazarus APT group's attack toolset, Kaspersky researchers said, characterizing the operation as a "mass-scale spyware attack campaign." The Russian cybersecurity company said it first detected the series of intrusions in June 2021.

At least 7.2% of all computers attacked by the malware are part of industrial control systems (ICS) used by organizations in engineering, building automation, energy, manufacturing, construction, utilities, and water management sectors that are located mainly in India, Vietnam, and Russia. Approximately a third (29.4%) of non-ICS computers are situated in Russia (10.1%), India (10%), and Brazil (9.3%)."

Source: The Hacker News

RANSOMWARE

Conti ransomware is exploiting the Log4Shell vulnerability to the tune of millions

"Log4Shell is the most severe vulnerability hitting systems in the end of 2021. Since its public exposure on the December 9, the security industry has worked hard to try to patch and protect against it. But sure enough, cybercriminals have started using it, and it was only a matter of time before one of the most active ransomware groups began to exploit it too."

Source: Tech Republic

10 of the biggest ransomware attacks in the second half of 2021

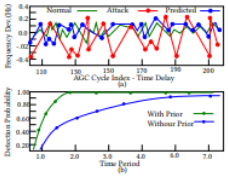
"The World Robotics report shows that Europe is the region with the highest robot density globally, with an average value of 114 units per 10,000 employees in the manufacturing industry. For more facts about robots watch IFR´s video news about Europe in one minute During the first half of 2021, attacks struck critical infrastructure organizations and government agencies, causing

security; Emerging trends and recent developments

"At present, most of the economic, commercial, cultural, social and governmental activities and interactions of countries, at all levels, including individuals, non-governmental organizations and government and governmental institutions, are carried out in cyberspace. Recently, many private companies and government organizations around the world are facing the problem of cyber-attacks and the danger of wireless communication technologies. Today's world is highly dependent on electronic technology, and protecting this data from cyber-attacks is a challenging issue. The purpose of cyber-attacks is to harm companies financially. In some other cases, cyber-attacks can have military or political purposes. Some of these damages are: PC viruses, knowledge breaks, data distribution service (DDS) and other assault vectors. To this end, various organizations use various solutions to prevent damage caused by cyber-attacks."

Source: Elsevier

CYBER RESILIENCE



Optimized Predictive Control for AGC Cyber Resiliency

"Automatic Generation Control (AGC) is used in smart grid systems to maintain the grid's frequency to a nominal value. Cyber-attacks such as time delay and false data injection on the tie-line power flow, frequency measurements, and Area Control Error (ACE) control signals can cause frequency excursion that can trigger load shedding, generators' damage, and blackouts. Therefore, resilience and detection of attacks are of paramount importance in terms of the reliable operation of the grid. In contrast with the previous works that overlook ACE resiliency, this paper proposes an approach for cyber-attack detection and resiliency in the overall AGC process. We propose a state estimation algorithm approach for the AGC system by utilizing prior information based on Gaussian process regression, a non-parametric, Bayesian approach to regression. We evaluate our approach using the PowerWorld simulator based on the three-area New England IEEE 39-bus model."

Source: ACM Digital Library

significant fallout. Ransomware gangs targeted larger organizations with increasingly large ransom demands.
Those trends continued, and no sector was left unturned in the second half of 2021, including cryptocurrency exchanges. Extortion remained a key tactic for ransomware groups and in many cases, data leak sites called attention to attacks even before companies disclosed the incidents. Attackers appeared to follow through on many of those threats by exposing sensitive files."
Source: Tech Target

New Ransomware Variants Flourish Amid Law Enforcement Actions

"Ransomware groups continue to evolve their tactics and techniques to deploy file-encrypting malware on compromised systems, notwithstanding law enforcement's disruptive actions against the cybercrime gangs to prevent them from victimizing additional companies.
"Be it due to law enforcement, infighting amongst groups or people abandoning variants altogether, the RaaS [ransomware-as-a-service] groups dominating the ecosystem at this point in time are completely different than just a few months ago," Intel 471 researchers said in a report published this month. "Yet, even with the shift in the variants, ransomware incidents as a whole are still on the rise."."
Source: The Hacker News

Ransomware attacks soar, hackers set to become more aggressive: Canada spy agency

"Global ransomware attacks increased by 151 per cent in the first half of 2021 compared with 2020 and hackers are set to become increasingly aggressive, Canada's signals intelligence agency said on Monday (Dec 6).
The Communications Security Establishment (CSE), citing attacks on North American health facilities and a United States pipeline, said the scale and scope of ransomware operators represented both security and economic risks to Canada and its allies.
"Ransomware operators will likely become increasingly aggressive in their targeting, including against critical infrastructure," said a report issued by the Canadian Centre for Cyber Security, a unit of CSE."
Source: The Straits Times

RANSOMWARE: DEFEND THE DATA, DEMOLISH THE ROI

Digitalization Capabilities for Sustainable Cyber Resilience: A Conceptual Framework

"Digital transformation is currently an essential condition for companies to operate in most markets, since it provides a whole new set of competitive skills and strategic tools. On the other hand, the same digitalization puts companies in the face of a whole new series of threats coming from the cyber space. The foundation of business sustainability, which is the maintenance of competitiveness while securing business, is no longer a "plus" feature or a captivating sentence but a true and consistent need for all organizations. This article provides a literature analysis on approaches and models for cyber resilience, digitalization capabilities, and a conceptual framework showing how digitalization capabilities drive cyber resilience. Digitalization capabilities are involved in the plan/prepare phase and in the adaptation phase of the cyber resilience process. In particular, online informational capabilities can drive both these phases."
Source: MDPI

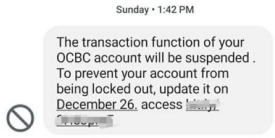
MALWARE

An Ontology-driven Knowledge Graph for Android Malware

"We present MalONT2.0 -- an ontology for malware threat intelligence [4]. New classes (attack patterns, infrastructural resources to enable attacks, malware analysis to incorporate static analysis, and dynamic analysis of binaries) and relations have been added following a broadened scope of core competency questions. MalONT2.0 allows researchers to extensively capture all requisite classes and relations that gather semantic and syntactic characteristics of an android malware attack. This ontology forms the basis for the malware threat intelligence knowledge graph, MalKG, which we exemplify using three different, non-overlapping demonstrations. Malware features have been extracted from openCTI reports on android threat intelligence shared on the Internet and written in the form of unstructured text. Some of these sources are blogs, threat intelligence reports, tweets, and news articles. The smallest unit of information that

"You may have noticed a slight pause in the breathless coverage of ransomware attacks. This is a bad sign: The fact that news of high-profile breaches and other attacks don't dominate the headlines—as they did around this time last year when a global pandemic was already wreaking havoc on business practices—doesn't mean that this odious practice has faded. It might just mean that ransomware is so common that it's no longer newsworthy."
Source: Analytics Insight

PHISHING



At least S$8.5 million lost in December to phishing scams involving OCBC Bank

"According to SPF, victims would receive unsolicited SMSes claiming that there were issues with their banking accounts, asking them to click on a link to resolve the issue.
Upon clicking, victims would be redirected to fake bank websites and asked to key in their iBanking account login details.
They would find out they had been scammed when they received notifications informing them of unauthorised transactions charged to their bank accounts."
Source: Channel News Asia

Hong Kong police to launch free software 'V@nguard' for businesses to fight phishing scams

- "Project, developed with researchers at HKU, is aimed at SMEs, after such scams caused more than HK$1.4 billion in losses last year
- Data confidentiality will be ensured as software will run on companies' servers, with no access for police and developers."

Source: South China Morning Post

Over 300 victims lose $760,000 to phishing scams related to delivery firms

"More than 300 people have fallen prey to phishing scams involving delivery companies amid year-end online shopping events.
There have been at least 341 victims since last month, with losses amounting to at least $759,000, the police said on Monday (Dec 20).
Victims typically received e-mails and text messages from scammers

captures malware features is written as triples comprising head and tail entities, each connected with a relation. In the poster and demonstration, we discuss MalONT2.0 and MalKG."
Source: ACM Digital Library

Investigating Labelless Drift Adaptation for Malware Detection

"The evolution of malware has long plagued machine learning-based detection systems, as malware authors develop innovative strategies to evade detection and chase profits. This induces concept drift as the test distribution diverges from the training, causing performance decay that requires constant monitoring and adaptation.
In this work, we analyze the adaptation strategy used by DroidEvolver, a state-of-the-art learning system that self-updates using pseudo-labels to avoid the high overhead associated with obtaining a new ground truth. After removing sources of experimental bias present in the original evaluation, we identify a number of flaws in the generation and integration of these pseudo-labels, leading to a rapid onset of performance degradation as the model poisons itself. We propose DroidEvolver++, a more robust variant of DroidEvolver, to address these issues and highlight the role of pseudo-labels in addressing concept drift. We test the tolerance of the adaptation strategy versus different degrees of pseudo-label noise and propose the adoption of methods to ensure only high-quality pseudo-labels are used for updates."
Source: ACM Digital Library

Detection Model based on Deep learning through the Characteristics Image of Malware

"Although the internet has gained many conveniences and benefits, it is causing economic and social damage to users due to intelligent malware. Most of the signature-based anti-virus programs are used to detect and defend this, but it is insufficient to prevent malware variants becoming more intelligent. Therefore, we propose a model that detects and defends the intelligent malware that is pouring out in the paper. The proposed model learns by imaging the characteristics of malware based on deep learning, and detects newly detected malware variants using the learned model. It was shown that the proposed model detects not only the existing malware but also most of the variants that transform the existing malware."
Source: Korea Science

impersonating delivery companies such as SingPost."
Source: The Straits TImes

Credential Phishing, Brute Force Attacks Both Increased in H1 2021

"According to Abnormal Security, the volume of brute force attacks grew by 160% starting in May 2021 and ending in mid-June. This means that brute force attacks targeted 26% of all organizations per week on average during that period — more than double the rate (10%) for a typical week.
Some weeks registered a higher volume of attacks than others. In particular, the rate of attacks for the week of June 6 shot up 671% over the previous week's average. Subsequently, nearly a third of all organizations found themselves targeted by brute force attacks that week."
Source: Security Intelligence

RISK MANAGEMENT

Best practices for AI security risk management

"There is a marked interest in securing AI systems from adversaries. Counterfit has been heavily downloaded and explored by organizations of all sizes—from startups to governments and large-scale organizations—to proactively secure their AI systems. From a different vantage point, the Machine Learning Evasion Competition we organized to help security professionals exercise their muscles to defend and attack AI systems in a realistic setting saw record participation, doubling the amount of participants and techniques than the previous year.
This interest demonstrates the growth mindset and opportunity in securing AI systems. But how do we harness interest into action that can raise the security posture of AI systems? When the rubber hits the road, how can a security engineer think about mitigating the risk of an AI system being compromised?."
Source: Microsoft

SMARTPHONE SECURITY

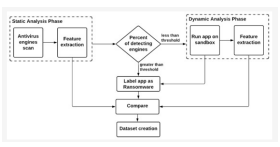
A Novel Monte-Carlo Simulation-Based Model for Malware Detection (eRBCM)

"The use of innovative and sophisticated malware definitions poses a serious threat to computer-based information systems. Such malware is adaptive to the existing security solutions and often works without detection. Once malware completes its malicious activity, it self-destructs and leaves no obvious signature for detection and forensic purposes. The detection of such sophisticated malware is very challenging and a non-trivial task because of the malware's new patterns of exploiting vulnerabilities. Any security solutions require an equal level of sophistication to counter such attacks. In this paper, a novel reinforcement model based on Monte-Carlo simulation called eRBCM is explored to develop a security solution that can detect new and sophisticated network malware definitions. The new model is trained on several kinds of malware and can generalize the malware detection functionality."
Source: MDPI

Time Detection of Malware Threads

"Malware is an unwanted software that performs actions in computers or computer networks, which users might disagree with. One of the worst types of malware is ransomware that affects the victim's data by modifying, deleting, or blocking the access to them. Frequent malware attacks on organizations led to a change in malware detection from external identification (companies were dependent on other organizations or their products) to internal identification. Based on this, the time needed to detect ransomware (dwell time) has significantly decreased. Nowadays, internal detection prevails over the external one. The dwell time differs based on the continent. In the paper, the malware and ransomware descriptions with their variants are provided, and the concept of dwell time is described. Moreover, attention is not only paid to the reduction of dwell time within the recent years but also to how the most used vector attacks are connected."
Source: Springer Link

RANSOMWARE



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

Hybrid-Based Analysis Impact on Ransomware Detection for Android Systems

"Android ransomware is one of the most threatening attacks that is increasing at an alarming rate. Ransomware attacks usually target Android users by either locking their devices or encrypting their data files and then requesting them to pay money to unlock the devices or recover the files back. Existing solutions for detecting ransomware mainly use static analysis. However, limited approaches apply dynamic analysis specifically for ransomware detection. Furthermore, the performance of these approaches is either poor or often fails in the presence of code obfuscation techniques or benign applications that use cryptography methods for their APIs usage. Additionally, most of them are unable to detect ransomware attacks at early stages. Therefore, this paper proposes a hybrid detection system that effectively utilizes both static and dynamic analyses to detect ransomware with high accuracy. For the static analysis, the proposed hybrid system considered more than 70 state-of-the-art antivirus engines. For the dynamic analysis, this research explored the existing dynamic tools and conducted an in-depth comparative study to find the proper tool to integrate it in detecting ransomware whenever needed."

Source: MDPI

Dual Generative Adversarial Networks Based Unknown Encryption Ransomware Attack Detection

"Aiming at unknown or variant ransomware attack encrypted with SSL (Secure Sockets Layer)/ TLS (Transport Layer Security) protocol, a detection framework named TGAN-IDS (Transferred Generating Adversarial Network-Intrusion Detection System) based on dual generative adversarial networks is presented in this paper. In this framework, DCGAN (Deep Convolutional Generative Adversarial Network) is adopted to train a generator which has good performance to generate adversarial sample, and is transferred to the generator of TGAN. A pre-training model named PreD is built based on CNN (Convolutional Neural Network), which has good performance to do binary classification, and is transferred to the discriminator of TGAN. The generator and discriminator of TGAN play games in training process until the discriminator has a strong ability to detection unknown attack, and then it is output as an anomaly detector."

Source: IEEE Xplore

Ransomware Detection, Avoidance, and Mitigation Scheme: A Review and Future Directions

"Ransomware attacks have emerged as a major cyber-security threat wherein user data is encrypted upon system infection. Latest Ransomware strands using advanced obfuscation techniques along with offline C2 Server capabilities are hitting Individual users and big corporations alike. This problem has caused business disruption and, of course, financial loss. Since there is no such consolidated framework that can classify, detect and mitigate Ransomware attacks in one go, we are motivated to present Detection Avoidance Mitigation (DAM), a theoretical framework to review and classify techniques, tools, and strategies to detect, avoid and mitigate Ransomware. We have thoroughly investigated different scenarios and compared already existing state of the art review research against ours. The case study of the infamous Djvu Ransomware is incorporated to illustrate the modus-operandi of the latest Ransomware strands, including some suggestions to contain its spread."

Source: MDPI

Ransomware Detection Using the Dynamic Analysis and Machine Learning: A Survey and Research Directions

"Ransomware is an ill-famed malware that has received recognition because of its lethal and irrevocable effects on its victims. The irreparable loss caused due to ransomware requires the timely detection of these attacks. Several studies including surveys and reviews are conducted on the evolution, taxonomy, trends, threats, and countermeasures of ransomware. Some of these studies were specifically dedicated to IoT and android platforms. However, there is not a single study in the available literature that addresses the significance of dynamic analysis for the ransomware detection studies for all the targeted platforms. This study also provides the information about the datasets collection from its sources, which were utilized in the ransomware detection studies of the diverse platforms."

Source: MDPI

ADDITIVE MANUFACTURING

Defining and Addressing the Cybersecurity Challenges of Additive Manufacturing Platforms

"Additive Manufacturing (AM) Platform is a new technology and commercial business model which enables production of additively made parts through an on-line market of AM designs, services, and manufacturing. Customers who are designing parts to be manufactured with additive technologies can upload their designs to the AM Platform and find a manufacturing partner based on technical capabilities, geographic location, and cost. By providing an easy to use online platform, companies can expect to optimize their cost, quality, and lead-time through a competitive bid process.

This research investigates the cybersecurity issues inherent to an online marketplace and platform which shares data containing Intellectual Property (IP) between multiple companies. Based on currently implemented business models in the AM Platform industry, the most common use cases will be examined to determine any vulnerabilities associated with data and IP sharing between the platform, its customers, and vendors."

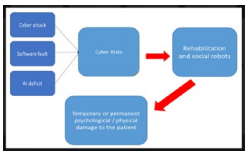
Source: ACM Digital Library

Assessing cyber resilience of additive manufacturing supply chain leveraging data fusion technique: A model to generate cyber resilience index of a supply chain

"The ever-increasing use of technology in manufacturing and other sections of a supply chain make it more susceptible to cyber threats. Perhaps additive manufacturing (AM) supply chains possess higher degrees of threats than other supply chains due to their heavy dependence on technology and information sharing. Therefore, an assessment of the cyber resilience of an additive manufacturing (AM) supply chain is a crucial task to make the AM supply chain safe from the cyber intrusion and to secure competitive business advantages. Consequently, it is essential to develop a strategic decision-making framework to address the vulnerabilities associated with the AM supply chain. The assessment process involves various information sources that are incomplete, subjective, and also

uncertain in type. Therefore, to handle the incomplete, uncertain, and subjective nature of the data, in this study, a data fusion technique named hierarchical evidential reasoning-based approach has been adopted. This study proposes an integrated and comprehensive approach based on Dempster-Shafer (D-S) theory as a methodology of developing a framework for assessing the cyber resilience of an additive manufacturing supply chain."
Source: Elsevier

ROBOTICS



The Cybersecurity and the Care Robots: A Viewpoint on the Open Problems and the Perspectives

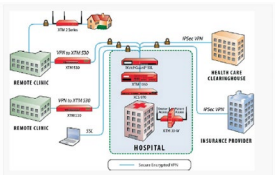
"Care robots represent an opportunity for the health domain. The use of these robots has important implications. They can be used in surgery, rehabilitation, assistance, therapy, and other medical fields. Therefore, care robots (CR)s, have both important physical and psychological implications during their use. Furthermore, these devices, meet important data in clinical applications. These data must be protected. Therefore, cybersecurity (CS) has become a crucial characteristic that concerns all the involved actors. The study investigated the collocation of CRs in the context of CS studies in the health domain. Problems and peculiarities of these devices, with reference to the CS, were faced, investigating in different scientific databases. Highlights, ranging also from ethics implications up to the regulatory legal framework (ensuring safety and cybersecurity) have been reported. Models and cyber-attacks applicable on the CRs have been identified."
Source: MDPI

Cybersecurity of Robotic Systems: Leading Challenges and Robotic System Design Methodology

"Recent years have seen a rapid development of the Internet of Things (IoT) and the growth of autonomous robotic applications which are using network communications. Accordingly, an increasing advancement of intelligent devices with wireless sensors (that means autonomous robotic platforms) operating in challenging environments makes robots a tangible reality in the near future.

Unfortunately, as a result of technical development, security problems emerge, especially when considering human–robot collaboration. Two abnormalities often compromise the basic security of collaborative robotic fleets: (a) Information faults and (b) system failures. This paper attempts to describe the methodology of a control framework design for secure robotic systems aided by the Internet of Things. The suggested concept represents a control system structure using blocks as the components. The structure is designed for the robots expected to interact with humans safely and act connected by communication channels. The properties of the components and relations between them are briefly described."
Source: MDPI

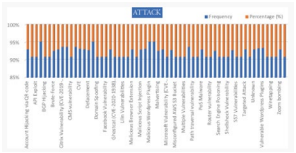
HEALTHCARE



The Impact of Cybersecurity on Healthcare

The advancement of technology in recent times has posed a number of serious threats to the integrity of the systems, networks, and programs utilized in different fields such as Healthcare organizations. Such threats have compounded with the development of cybersecurity, a move which involves protecting the systems from imminent threats that materialize in the form of digital attacks. Inadvertently, cybersecurity has become an important aspect of digital protection from ill-intentioned people who exploit the vulnerability of systems. This paper addresses the impact of cybersecurity in healthcare organizations. While on it, the paper will also present the various types of security threats in the industry and utilizing AES (Advanced Encryption Standard) as a protective measure for health-based organizations."
Source: Springer Link

CYBERSECURITY AND COVID-19



A Descriptive Analytics of the Occurrence and Predictive Analytics of Cyber Attacks During the Pandemic

"The SARS-CoV-2 (Severe acute respiratory syndrome coronavirus 2)

universally and commonly known as COVIT-19 and the across-the-board lockdown measures are having complex and unforeseen effects on intricate social domains, which includes opportunities for offline and online crimes. For some months since March 2020, most countries in the world if not all has been in one lockdown or the other. The lockdown measures have brought increased fear, anxiety, and depression. As if that is not enough, it has also forced the entire world populace to embrace the emergency use of technology to carry out their job functions which was unplanned for in a sit-at-home and work-from-home situation. All these have rendered vast majority of individuals and general populace vulnerable to cyber enabled and cyber dependent crimes."
Source: Springer Link

Cybersecurity post-COVID-19: Lessons learned and policy recommendations

"This article looks at the impact of the novel coronavirus crisis and increased remote work on cybersecurity and the priorities for EU action. Actions should include improving the cybersecurity of businesses, critical infrastructure and users, and creating an EU cybersecurity industry. As more and more aspects of our lives happen online, we are becoming more vulnerable to malicious attacks. This was demonstrated in 2020 when cyber-attacks increasingly disrupted the work of hospitals, service providers, government services and businesses across the globe. The frequency and scale of the attacks created a sense of urgency to improve our cybersecurity resilience. This article argues that the EU should reap the benefits of cybersecurity by pursuing a more ambitious cybersecurity agenda and putting EU values at the core of its approach."
Source: Sage Publications