SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN

21 FEBRUARY – 23 APRIL 2021

TOPICAL REPORT

CYBERSECURITY

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

view past reports | subscribe to others | unsubscribe

news | academic | reports

CYBERSECURITY

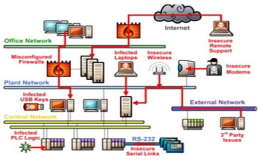
How SASE is Key to 5G Security Success

"Over the past century, there has been a constant demand for change, and wireless networks are central to recent advancements due to trends like IoT, smartphones, tablets and laptops. Now that internet speeds are quicker and users are connecting outside of the office, 4G is becoming a thing in the past as everyone is welcoming 5G.
Since the launch of 5G, the promise of quicker internet speed and faster networks has kept everyone excited, especially organizations in the tech space. 5G provides users and organizations a rapid and more efficient internet while offering lower latency for their employees in and out of the office."
Source: InfoSecurity Magazine

Poppy Gustafsson: the Darktrace tycoon in new cybersecurity era

"It really does feel like we're in this new era of cybersecurity," says Gustafsson, the chief executive of Darktrace. "The arms race will absolutely continue, I really don't think it's very long until this [AI] innovation gets into the hands of attackers, and we will see these very highly targeted and specific attacks that humans won't necessarily be

CYBER ATTACKS



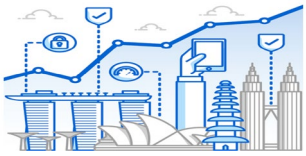
Best ways computation intelligent of face cyber attacks

"The rising of information and communication technologies brought about new challenges that need to be dealt with is the citizens' security is considered. Undoubtedly, the latest well known electronic attacks have indicated the losses that are likely to happen as ICT and security as a field widens. There are several types of electronic attacks like Denial of service, phishing attacks, backdoors, Day-Zero gaps, and technical gaps that facilitate the vulnerabilities that are often taken advantage of by malicious persons. There is a need for cybersecurity because it defines the body of processes, technologies, and practices in terms of how they are designed to help protect various programs, devices, networks, and data from the malicious persons who perform unauthorized access and damage these resources."
Source: Materials Today

Anomaly-Based Intrusion Detection by Machine Learning: A Case Study on Probing Attacks to an Institutional Network

"Cyber attacks constitute a significant threat to organizations with

INSIGHT



3 Trends to Track in the Developing Digital Economy and What They Mean for Your Business

"We have seen a massive upsurge in digitalisation efforts in the business world over the past year as organisations have looked to optimise business processes through technology and digitisation. Catalysed by the pandemic, this trend has resulted in widespread digital transformation across industries for organisations in the Asia Pacific region."
Source: Telstra

HowTo: Improve Your Security Team's Remediation Efficiency

"The impact of the pandemic has left security teams and CISOs with a multitude of security challenges to overcome. Chief among these responsibilities include closing security gaps within critical infrastructure and patching vulnerabilities as necessary. Given that the number of security vulnerabilities reached a record high for a fourth year in a row in 2020, security professionals are presented with a significant task if they hope to meet the growing demands that come with remediating high-risk vulnerabilities to prevent their organization from being attacked."
Source: InfoSecurity Magazine

able to spot and defend themselves from."
Source: Guardian

A Historical Perspective of Cybersecurity Frameworks

"In 2021, cybersecurity risk has become a prominent concern for businesses and governments around the world. The past year has shown that no amount of defensive technology can protect against malicious intent from a variety of adversaries including a new breed of attacker that leverages the financial resources of nation-states and the ingenuity of the world's most advanced cyber criminals. These attacks can cause millions of dollars' worth of damage to companies by compromising valuable data and infrastructure, interrupting business operations, and damaging organizational reputation, sometimes irreparably."
Source: Security Boulevard

Singapore cybersecurity firm launches world's first AI-embedded solid-state drive

"SINGAPORE cybersecurity firm Flexxon on Monday launched the world's first solid-state drive (SSD) embedded with artificial intelligence (AI) data security.
As the "last line of defence" to protect data at the hardware level, the SSD is able to guard against both remote and physical attacks, boasting a range of features including temperature sensors to detect unusual movements that occur."
Source: Business Times

Cybersecurity State Power Struggles

"The 2020 US presidential election made it clear that disinformation remains one of the most powerful tools in sowing doubt into democracy. Foreign actors, most notably from Russia, China and Iran, used disinformation in the US to promote their preferred candidate and cause chaos for voters. Coupled with similar campaigns aimed at election results, it's clear that foreign threats are a considerable force.
Nation state attacks aren't just limited to the US. In mid-September, UK Foreign Secretary Dominic Raab condemned continued Chinese attacks on telecoms, tech and global governments. Following an announcement by the US Department of Justice, along with Malaysian nationals relating to malicious cyber-attacks, he stated the UK would continue to counter bad actors and work with allies in holding them accountable."
Source: InfoSecurity Magazine

implications ranging from economic, reputational, and legal consequences. As cybercriminals' techniques get sophisticated, information security professionals face a more significant challenge to protecting information systems. In today's interconnected realm of computer systems, each attack vector has a network dimension. The present study investigates network intrusion attempts with anomaly-based machine learning models to provide better protection than the conventional misuse-based models. Two models, namely an ensemble learning model and a convolutional neural network model, were built and implemented on a data set gathered from a real-life, institutional production environment. To demonstrate the models' reliability and validity, they were applied to the UNSW-NB15 benchmarking data set. The type of attack was limited to probing attacks to keep the scope of the study manageable. The findings revealed high accuracy rates, the CNN model being slightly more accurate."
Source: IEEE Xplore

Hybrid-triggered-based security controller design for networked control system under multiple cyber attacks

"This paper addresses the hybrid-triggered security control design for the networked control system (NCS) under multiple cyberattacks. A hybrid-triggered scheme (HTS) is introduced to mitigate the burden of the network transmission. Besides, a new model of multiple cyberattacks is built by simultaneously considering deception attacks and DoS attacks. In addition, a novel NCS model based on multiple cyberattacks is established with the hybrid-triggered scheme. Then, based on Lyapunov stability theory, criteria for guaranteeing the closed-loop system stability and achieving hybrid-triggered security controller design are derived. Finally, an illustrative example is given to validate the usefulness of the theoretical results."
Source: Elsevier

Cooperative control for cyber–physical multi-agent networked control systems with unknown false data-injection and replay cyber-attacks

"The paper discusses the cooperative tracking problem of partially known cyber–physical multi-agent networked systems. In this system, there exist two cascaded chances for cyber-attacks. The local agent is of networked system type that is

134 Cybersecurity Statistics and Trends for 2021 UPDATED: 3/16/2021

"In order to give you a better idea of the current state of overall security, we've compiled over 100 cybersecurity statistics for 2021. 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

RESEARCH

Frost Radar™: Global Cyber Threat Intelligence Market, 2021

"Cyber threat intelligence (CTI) is a collection of data, information, and knowledge about past, present, and future cyberattacks. It is the cornerstone of mature cyber defense programs and a sought-after product category that allows organizations to adapt their security posture to the rapidly changing threat landscape. Information about potential attacks enables organizations to thwart attackers' plans by anticipating their next move, and knowledge about past and present campaigns empowers organizations to increase the speed and accuracy of detecting potential breaches."
Source: Frost & Sullivan

Growth Opportunities In Ai-And Cloud-Based Security

"This Cyber Security Technology Opportunity Engine (TOE) provides a snapshot on emerging cyber security solutions powered by artificial intelligence and cloud-based innovations that help companies protect from threats, data breaches, phishing attacks, and defend against modern attacks residing within cloud, endpoints, and various network layers.
Cyber Security TOE's mission is to investigate new and emerging developments that aim to protect the network infrastructure and the resources operating in the network. The TOE offers strategic insights that would help identify new business opportunities and enhance technology portfolio decisions by assessing new developments and product launches in: anti-spam, anti-virus, phishing, identity management, disaster recovery, firewalls, virtual

New RSM Report Reveals Cybersecurity Threats Are Continuing to Grow in the Middle Market

"Middle market companies possess a significant amount of valuable data but continue to lack appropriate levels of protective controls and staffing, according to the RSM US Middle Market Business Index (MMBI) Cybersecurity Special Report released today from RSM US LLP (RSM), in partnership with the U.S. Chamber of Commerce. This year's results revealed that 28% of middle market leaders claimed that their company experienced a data breach in the last year, a sharp rise from 18% in last year's survey and the highest level since RSM began tracking data in 2015. Many leaders attributed this increase to challenges created by COVID-19."
Source: PR Newswire

CYBER ATTACK

Codecov Supply Chain Attack May Hit Thousands: Report

"Experts have urged organizations to reassess cyber-risk in their supply chains as it emerged that hundreds of customers of a software auditing company had their networks accessed illegally… Investigators told Reuters that the attack had already led to hundreds of customers' networks being accessed. Codecov's customer-base of around 29,000 includes many big tech brands such as IBM, Google, GoDaddy and HP, as well as publishers (The Washington Post), consumer goods firms (Procter & Gamble) and many more."
Source: Infosecurity Magazine

Google Patches More Under-Attack Chome Zero-days

"The latest confirmation of this appears today with a new Chrome point-update to patch a pair of security vulnerabilities affecting Windows, MacOS and Linux users. Google said it was aware of reports that both of these vulnerabilities - CVE-2021-21206 and CVE-2021-21220 -- are being exploited in the wild.
As has become normal, Google did not provide any other details on the attacks or provide any IOCs to help organizations find signs of infection."
Source: Security Week

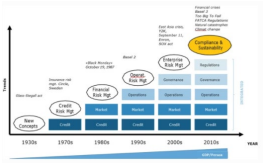
Unearthing the 'Attackability' of Vulnerabilities that Attract Hackers

subjected to unknown false data-injection and replay cyber-attacks that are dissimilar in the sensor-controller and the controller-actuator network parts. The communication between any two agents, if they are connected, is accomplished via a communication network that is subjected to false data-injection cyber-attacks."
Source: Elsevier

Investigating cyber attacks using domain and DNS data

"The majority of cyber attacks leverage the central role that DNS plays in facilitating Internet traffic.
From botnets spreading disinformation and undertaking distributed denial of service (DDoS) attacks to sophisticated spear-phishing campaigns, attackers typically will set up dozens, hundreds or even thousands of malicious domains to stay one step ahead of detection systems and blacklists. These leave a trail that can provide insight into the attackers' real motivations and even lead to the perpetrators, explain Chad Anderson, John 'Turbo' Conwell and Tarik Saleh of DomainTools."
Source: Elsevier

CYBER RESILIENCE



Security as a key contributor to organisational resilience: a bibliometric analysis of enterprise security risk management

"Globalisation and hyperconnectivity affect organisational resilience with threats such as the recent COVID-19 pandemic or large-scale cyberattacks. To strengthen organisational resilience capabilities, a framework such as enterprise risk management (ERM) is necessary so as to enable holistic risk management. Specifically, in this paper, we analyse the role of security, which has great potential in crisis management and makes it possible to follow up businesses integrated in enterprise security risk management (ESRM). This paper examines, for the first time in the literature, the output of scientists on ESRM. After analysing 463 articles from the period between 1986 and 2019, it is concluded that Security Risk Management is a subject area on its own and is closely linked to ERM."
Source: Springer Link

private networks, end-point security, content filtering, Web application security, authentication and access control, intrusion prevention and detection systems, encryption algorithms, cryptographic techniques, and pattern recognition systems for network security."
Source: Frost & Sullivan

INDUSTRY REPORT

Global Cybersecurity Industry Report 2021: With Increasing Adoption of Grid Automation, Cybersecurity will be the Key Concern for Utilities

"The aim of this study is to provide a comprehensive analysis of the cybersecurity industry and to provide insights on trends, threats, and opportunities to global security leaders, businesses, and governments. It illustrates how markets and business models are evolving in the cybersecurity industry and identifies the potential opportunities in the security industry."
Source: Research and Markets

WHITE PAPER

Cybersecurity Key Performance Indicators for Your Security Maturity Level

"Cybersecurity KPIs serve to inform your investment allocations, guide security improvement initiatives and purchase decisions. For business leaders, improving data governance helps navigate the macro uncertainty facing the organization today.
This whitepaper includes a detailed KPI Matrix you can use to up-level your cybersecurity program, covering KPI best practices and how to apply them to cybersecurity."
Source: InfoSecurity Magazine

How UK Companies Are Losing Millions to Cyber-Attacks and What to Do About it

"Every year, cyber-attacks cost companies worldwide, on average, $1.1m – and 90% of those attacks capitalize on one single human error. Losing money to disaster or unforeseen circumstances can be

"In 2020, more than 17,000 vulnerabilities were reported to NIST, and more than 4,000 of these were high priority. Knowing which of these affect you, where they are located in your environment, and which should be tackled first is a challenge.
Randori, a startup that develops an automated red team attack platform, has announced Target Temptation designed to link assets and vulnerabilities. This demonstrates where attackers are likely to strike, and pinpoints the vulnerabilities that should be given the highest priority."
Source: Security Week

CYBER RESILIENCE

Cyber resilience: your last line of defence

"No cyber security defence is impenetrable. We've recently seen breaches on Acer, Microsoft Exchange and SonicWall. A report from Cybint estimates that, on average, there is now a hacker attack every 39 seconds – and the attack vectors are constantly evolving.
In response, organisations around the world are starting to take a new approach to mitigating their cyber risks. A traditional cyber security strategy to try and stop attacks is no longer enough. Instead, organisations must shift from prevention to an 'assumed breach' mentality – operating as though a breach has already happened, and ensuring they can recover fast, with minimal damage to operations."
Source: Information Age

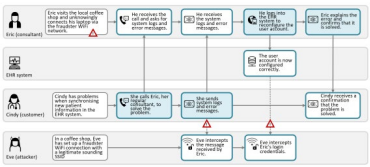
The Different Flavors of Cyber Resilience

"Cyber Resilience Can be Considered a Preventive Measure to Counteract Human Error, Malicious Actions, and Decayed, Insecure Software…The rapid transition to a distributed workforce in response to the COVID-19 pandemic has exacerbated the already challenging situation, widening pre-existing gaps in IT visibility, accountability, and persistence of security controls. It's not surprising to hear more and more CISOs talk about cyber resilience as an emerging measure to assure the ongoing delivery of business operations. But what exactly is cyber resilience and how does it compare to traditional cybersecurity practices?"
Source: Security Week

Emerging Challenges in Smart Grid Cybersecurity Enhancement: A Review

"In this paper, a brief survey of measurable factors affecting the adoption of cybersecurity enhancement methods in the smart grid is provided. From a practical point of view, it is a key point to determine to what degree the cyber resilience of power systems can be improved using cost-effective resilience enhancement methods. Numerous attempts have been made to the vital resilience of the smart grid against cyber-attacks. The recently proposed cybersecurity methods are considered in this paper, and their accuracies, computational time, and robustness against external factors in detecting and identifying False Data Injection (FDI) attacks are evaluated. There is no all-inclusive solution to fit all power systems requirements. Therefore, the recently proposed cyber-attack detection and identification methods are quantitatively compared and discussed."
Source: MDPI

RISK MANAGEMENT



Cybersecurity for SMEs: Introducing the Human Element into Socio-technical Cybersecurity Risk Assessment

"By using a combination of cybersecurity-related visualisations, our goals are: i) to raise awareness about cybersecurity, and ii) to improve communication among IT personnel, security experts, and non-technical personnel. To achieve these goals, we combine two modelling languages: Customer Journey Modelling Language (CJML) is a visual language for modelling and visualisation of work processes in terms of user journeys. System Security Modeller (SSM) is an asset-based risk-analysis tool for socio-technical systems. By demonstrating the languages' supplementary nature through a threat scenario and considering related theories, we believe that there is a sound basis to warrant further validation of CJML and SSM together to raise awareness and handle cyber threats in SMEs."
Source: Scite Press

The Microfoundations of State Cybersecurity: Cyber Risk Perceptions and the Mass Public

written down to bad luck, but in this day and age, it is almost inexcusable to be unprepared for cyber-threats… This white paper, outlines the risks you should be aware of and how you can protect your organization from these possible liabilities."
Source: InfoSecurity Magazine

2021 Cybersecurity Predictions & 2020 in Review

"New threats are constantly emerging in cybersecurity, and in 2020, we saw a dramatically changed attack surface as organizations around the globe shifted to a distributed workforce. There were new threats and high-profile breaches that were representative of the gap in proactive efforts required to remediate known vulnerabilities, and a significant rise in cybercrime complaints.
This white paper examines security learnings from 2020 and how they can be applied to research, tactics and services in 2021."
Source: InfoSecurity Magazine

Employee Privacy and Data Security Training

"Many executives may be surprised to learn that one of the most frequent causes of data breaches is employee error, and not just employees in the IT department. The types of information involved in breaches go beyond payment cards, Social Security numbers and patient medical information, and can include valuable proprietary or trade secret information; privileged or financial data belonging to employees, clients and customers; and sensitive internal email communications. Everyday mishaps like failing to lock a door, using the wrong email address, forgetting a device on a plane, forwarding the wrong attachment or not knowing who is authorized to access data can have catastrophic consequences for a business."
Source: Jackson Lewis

When You Can't Add Cybersecurity Staff Build Cyber-Resiliency Instead

"Worldwide government IT spending was estimated to total $438 billion+ in 2020, a decrease of 0.6% from the year before. While this decrease does not seem significant at first glance, it provides additional context to the cybersecurity talent shortage in government and the public sector. Given this, one of the biggest issues currently facing government IT managers is how to maintain existing, outdated systems without the budgetary resources needed to upgrade them or the labor resources to support them."
Source: Security Boulevard

RISK MANAGEMENT

'Clear and Present Danger': Why Cybersecurity Risk Management Needs to Keep Evolving

"The phrase 'future-proof' is seductive. We want to believe technology prepares us for the future. But with threat actors and developers in an arms race to breach and protect, cybersecurity risk — and cybersecurity risk management — are always changing. As a recent report by World Economic Forum shows, businesses and other entities should know how to keep up with and measure cybersecurity risk. Both are important and ongoing aspects of keeping your digital assets secure.
Source: Security Intelligence

Singapore's ViewQwest debuts security service

"ViewQwest's SecureNet service uses Palo Alto Networks' next-generation firewall with deep packet inspection capabilities to guard against cyber threats… Singapore-based telco ViewQwest has unveiled a new software-defined network security service to help businesses better guard against cyber attacks that have intensified amid the Covid-19 pandemic Dubbed SecureNet, the service makes use of Palo Alto Networks' next-generation firewall, eliminating the need for hardware appliances that enterprises typically install whenever they set up a new branch office."
Source: Computer Weekly

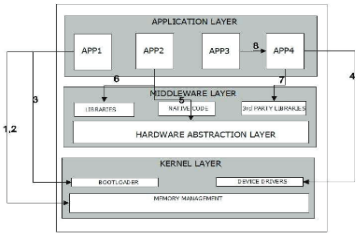
Singapore firm Flexxon unveils computer storage device with

"Using a novel survey experiment, we examine how exposure to different types of data breaches impacts citizens' cyber risk assessments, personal online behavior, and support for various national cybersecurity policies. We find that baseline concerns about cybersecurity and knowledge about safe online practices are very low. However, exposure to a personally relevant data breach heightens risk perception and increases willingness to engage in safer online practices. But these effects are circumscribed—actual online behavior is more resistant to change. These results have important implications for the design of effective state cybersecurity policy."
Source: Oxford Academic

Research on Cybersecurity Risk Prevention and Control of New Infrastructure

"Currently, the new infrastructure has entered the stage of intensive deployment. While driving the integration of innovative applications of new generation information and communication technologies such as 5G, and accelerating the process of digital transformation, new infrastructure is also facing the challenges of complex and diverse cyber attacks and increasingly severe security risks. This paper systematically analyzes the new infrastructure cybersecurity risks, summarizes the new challenges faced by new infrastructure, and proposes a risk prevention and control model METAD which combines monitoring and early warning, threat intelligence sharing, risk assessment, and intelligent defense."
Source: IOP Science

MALWARE



A Review and Case Study on Android Malware: Threat Model, Attacks, Techniques and Tools

"As android devices have increased in number in the past few years, the android operating system has started dominating the smartphone market. The vast spread of android across all the devices has made security an important issue as the android users continue to grow exponentially. The security of android platform has become the need of the hour in view

innovative cybersecurity tech | Video

"Singapore firm Flexxon has unveiled a computer storage device that automatically detects and shuts down threats. It is in trials with Government agencies and industry partners and the device could be rolled out for consumers as early as next year."
Source: Channel News Asia

New cyber security laws to protect smart devices amid pandemic sales surge

- "Apple, Samsung, Google and other manufacturers will say when smartphones, smart speakers and other devices will stop getting security updates
- Easy-to-guess default passwords to be banned on virtually all devices under new law
- Rules will make it easier for people to report software bugs that can be exploited by hackers"

Source: Gov.UK

MALWARE

Trickbot: Attackers Using Traffic Violation Scam to Spread Malware

"Digital attackers launched a new phishing scheme using fake traffic violations to infect victims with Trickbot.
With the prospect of a traffic violation, some people would be scared into opening an attack email. In the aftermath of a successful Trickbot malware infection, the attackers then could load other malware, such as Conti ransomware onto a victim's computer."
Source: Security Intelligence

Collaboration Platforms Increasingly Abused for Malware Distribution, Data Exfiltration

"With the COVID-19 pandemic forcing many organizations to switch to telework, interactive communication platforms such as Discord and Slack saw increased adoption and adversaries didn't wait long to start abusing these tools.
According to Cisco's Talos researchers, the past year has shown a significant increase in the abuse of such platforms as part of malicious of increase in the number of malicious apps and thus several studies have emerged to present the detection approaches. In this paper, we review the android components to propose a threat model that illustrates the possible threats that are present in the android. We also present the attack taxonomy to illustrate the possible attacks at various layers of the android architecture. Experiments demonstrating the feature extraction and classification using machine earning algorithms have also been performed."
Source: Journal of Cyber Security and Mobility

Advances In Malware Detection- An Overview

"This paper describes a literature review of various methods of malware detection. A short description of each method is provided and discusses various studies already done in the advanced malware detection field and their comparison based on the detection method used, accuracy and other parameters. Apart from this we will discuss various malware detection tools, dataset and their sources which can be used in further study. This paper gives you the detailed knowledge of advanced malwares, its detection methods, how you can protect your devices and data from malware attacks and it gives the comparison of different studies on malware detection."
Source: Cornell University

Towards improving detection performance for malware with correntropy-based deep learning method

"In our proposed method for malware detection and analysis, given the success of the mixture correntropy as an effective similarity measure in addressing complex datasets with noise, it is therefore incorporated into a popular deep learning model, i.e., Convolutional Neural Network (CNN), to reconstruct its loss function, with the purpose of further detecting the features of outliers. We present the detailed design process of our method. Furthermore, the proposed method is tested both on a real-world malware dataset and a popular benchmark dataset, to verify its learning performance."
Source: Science Direct

CYBERSECURITY THREATS

attacks. Attackers leveraged these platforms to deliver lures and infect victims with ransomware and other malware."
Source: Security Week

Fake Netflix App Luring Android Users to Malware

"Researchers have discovered new Android malware that uses Netflix as its lure and spreads malware via auto-replies to received WhatsApp messages.
The discovery was reported to Google, and the malware – dubbed FlixOnline – has been removed from Google Play; but the researchers expect the methodology to return and be reused in other malware."
Source: Security Week

Over Half of Malware Delivered via Cloud Applications

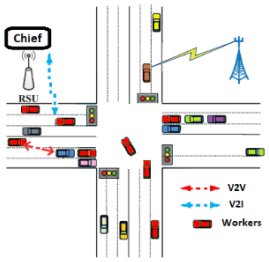
"Malware actors aren't struggling to adapt their attack campaigns to cloud applications. If they were, then they probably wouldn't have sent 61% of their malicious payloads in 2020 via cloud-based apps.
That's up from 48% of malware samples in 2019, according to a study from Netskope. This reveals the extent to which digital attackers are turning to the cloud more and more."
Source: Security Intelligence

PHISHING

URL Phishing Campaign Hides Attack Behind Morse Code

"A very old way to send messages has found new life. Threat actors used Morse code in a new URL phishing campaign detected early in February 2021, according to Bleeping Computer.
Invented by Samuel Morse and Alfred Vail in the 19th century, Morse code was the bedrock of modern communication. It transmits messages over the telegraph using dots and dashes. It's now also a means by which phishers can conceal their malicious URLs in an email attachment to evade detection.
Take a look at how attackers are using this kind of URL phishing and how to prevent it."
Source: Security Intelligence

REMOTE WORKING



Cybersecurity Threats in Connected and Automated Vehicles based Federated Learning Systems

"Federated learning (FL) is a machine learning technique that aims at training an algorithm across decentralized entities holding their local data private. Wireless mobile networks allow users to communicate with other fixed or mobile users. The road traffic network represents an infrastructure-based configuration of a wireless mobile network where the Connected and Automated Vehicles (CAV) represent the communicating entities. Applying FL in a wireless mobile network setting gives rise to a new threat in the mobile environment that is very different from the traditional fixed networks…This paper explores falsified information attacks, which target the FL process that is ongoing at the RSU."
Source: Cornell University

Interorganizational Information Sharing: Collaboration during Cybersecurity Threats

"Information sharing is examined to determine if the willingness to share information relates to the willingness to collaborate in interorganizational actions used to address cybersecurity threats. This study employs ANOVA by placing 85 organizational representatives that participated in a cyber terrorism training exercise into two categories: higher versus lower willingness to share information. The dependent measures in this study are proxies for collaboration measured by willingness to seek assistance from other organizations and willingness to offer assistance to other organizations. There is a significant statistical difference between the two categorizations of organizational representatives. The category that had a lower tendency to share information also had a lower willingness to collaborate with other organizations. This research shows that sharing information is critical when collaborative interorganizational action is required to face cybersecurity threats. Managers of organizations that respond to cybersecurity threats should promote the tendency to share information with other organizations that have the resources to aid in addressing the threat."

6 Cybersecurity Tips for Working from Home

"Here at Tripwire, we, like many others, recently surpassed the one-year anniversary of working from home due to the COVID-19 pandemic. Since March of 2020, we have converted kitchens, spare bedrooms and garages into office spaces. Our pets and children have become our coworkers, and companies are reporting a sudden increase in shirt sales as opposed to pant sales.

This unique transition has required flexibility to adapt to a new environment, and with that new environment has come a different set of security practices. Although many of us have finally established a rhythm when it comes to working from home, it is worth reminding ourselves of some important security practices every remote employee should be implementing."

Source: TripWire

Addressing cybersecurity and it gaps in an ever-changing Workplace: 4 keys to staying safe in your new digital office space

"Cybersecurity has always been tremendously important to organizations. But in the current environment, adequate security measures are harder than ever to implement. Many organizations now manage thousands of laptops, mobile devices, and apps. Moreover, these devices and platforms are being used by employees across a variety of settings, including in their homes, in offices, and even while traveling."

Source: Security Magazine

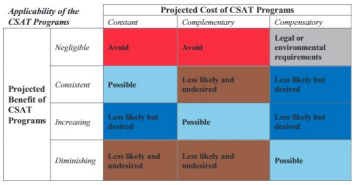
Enhancing Remote Working and Cybersecurity a Top Priority of Asia Pacific

"Across Asia-Pacific (APAC), firms are ramping up their digital transformation efforts, focusing primarily on adopting cloud computing, improving cybersecurity and enhancing remote working, a new survey by Australian telco firm Telstra. The study, conducted in late-2020, polled 420 business decision-makers from various industry verticals spread across seven APAC markets to understand their digital transformation needs and challenges.

Source: FinTech Singapore

Source: Ebscohost

CYBERSECURITY TRAINING



Applicability of the CSAT Programs		Projected Cost of CSAT Programs		
		Constant	Complementary	Compensatory
Projected Benefit of CSAT Programs	Negligible	Avoid	Avoid	Legal or environmental requirements
	Consistent	Possible	Less likely and undesired	Less likely but desired
	Increasing	Less likely but desired	Possible	Less likely but desired
	Diminishing	Less likely and undesired	Less likely and undesired	Possible

Cybersecurity awareness training programs: a cost–benefit analysis framework

"Purpose–Employees must receive proper cybersecurity training so that they can recognize the threats to their organizations and take the appropriate actions to reduce cyber risks. However, many cybersecurity awareness training (CSAT) programs fall short due to their misaligned training focuses.

Design/methodology/approach–To help organizations develop effective CSAT programs, we have developed a theoretical framework for conducting a cost–benefit analysis of those CSAT programs. We differentiate them into three types of CSAT programs (constant, complementary and compensatory) by their costs and into four types of CSAT programs (negligible, consistent, increasing and diminishing) by their benefits. Also, we investigate the impact of CSAT programs with different costs and the benefits on a company's optimal degree of security."

Source: Emerald Insight

"Get a red-hot poker and open up my eyes, it's so boring"1: Employee perceptions of cybersecurity training

"Organisations and security professionals design Security Education, Training, and Awareness (SETA) programs to improve cybersecurity behaviour, but they are often poorly received by employees. To understand employee negative perceptions of SETA programs, we conducted in-depth interviews with 20 Australian employees regarding their experiences with both SETA programs and non-cybersecurity related workplace training."

Source: Elsevier

Red-blue team exercises for cybersecurity training during a pandemic

"The COVID-19 pandemic has given rise to a remote workforce and education system which is vulnerable to a number of unique cybersecurity risks. There is a need for training cybersecurity professionals to deal with cyber threats during the pandemic and its aftermath. We

Mass Monitoring of Remote Workers Drives Shadow IT Risk

"…a third (32%) of workers polled for the study said that the use of monitoring tools would make them less trusting of their manager or team leader, and a similar number (30%) said they would be upset at the invasion of their privacy. Around a quarter (23%) said they would be concerned about potential access to their personal information via this software."

Source: InfoSecurity Information

CYBERSECURITY TRAINING

Cybersecurity Training Company Debuts New Courses (Updated)

"RangeForce, a Manassas, Virginia-based cybersecurity training company, recently announced new remote learning courses to help professionals working in digital security bolster their education… The programs will prepare individuals for different positions including security operations center analysts, threat hunters, web application security, secure coding, cloud security and Microsoft core security."

Source: National Defense

Break Into the Cybersecurity Job Market With This $30 Training Bundle

"When we think of hackers, we instinctively picture cyber-scams conducted in shadowy basements. The truth is, most hackers aren't necessarily the scourge of the internet they once were—and it's not because the requisite skill set has gotten any less impressive. Today, data is currency, and big companies rely on "white hat" hackers and other cybersecurity experts to protect their big data.

It's a surprisingly profitable way to make a living, and best of all, it's completely legal. So how do you find a way into this booming job market? You can start right there in your home with The 2021 All-in-One Ethical Hacking & Penetration Testing Bundle."

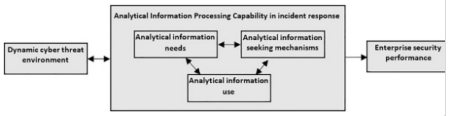
Source: PC Magazine

CLOUD SECURITY

present a series of red-blue team exercises related to pandemic threats, developed for undergraduate cybersecurity students. Implementation and experimental verification of macro virus attacks leveraging social engineering, building command-and-control services and conscripting devices into a botnet, and mitigating man-in-the middle attacks using a Raspberry Pi for website filtering will be discussed."

Source: IEEE Xplore

CYBERSECURITY INCIDENT RESPONSE

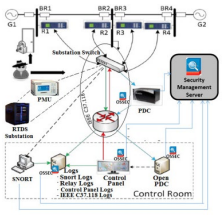


Demystifying analytical information processing capability: The case of cybersecurity incident response

"Little is known about how organizations leverage business analytics (BA) to develop, process, and exploit analytical information in cybersecurity incident response (CSIR). Drawing on information processing theory (IPT), we conducted a field study using a multiple case study design to answer the following research question: How do organizations exploit analytical information in the process of cybersecurity incident response by using business analytics? We developed a theoretical framework that explains how organizations respond to the dynamic cyber threat environment by exploiting analytical information processing capability in the CSIR process."

Source: Elsevier

CYBER PHYSICAL SYSTEMS



Autonomous mitigation of cyber risks in the Cyber–Physical Systems

"The Cyber–Physical Systems (CPS) attacks and vulnerabilities are increasing and the consequences of such attacks can be catastrophic. The CPS needs to be self-resilient to cyber-attacks through a precise autonomous and timely risk mitigation model that can analyze and assess the risk of the CPS and apply a proper response strategy against the ongoing attacks. There is a limited

How to Design and Roll Out a Threat Model for Cloud Security

"Today's cloud security requires a new way of looking at threat models. Making a threat model can support your security teams before problems start. It helps them develop a strategy for handling existing risks, instead of detecting incidents at a later stage. Let's walk through how to create a threat model that works for your cloud landscape.

The Open Web Application Security Project (OWASP) defines threat modeling as "a process for capturing, organizing and analyzing all of the information [that affects the security of an application]."""

Source: Security Intelligence

amount of work on the self-protection of the cyber risks in the CPS. This paper contributes toward the need of advanced security approaches to respond against the attacks across the CPS in an autonomous way, with or without including a system administrator in the loop for troubleshooting based on the criticality of the CPS asset that can be protected, once the alert about a possible intrusion has been raised."

Source: Elsevier

A new enhanced cyber security framework for medical cyber physical systems

"Medical Cyber-Physical Systems (MCPS) are complex, location-aware, networked systems of medical devices that can be used as a piece of the healing center to give the best medical care to patients. Hence, they integrate human, cyber, and physical elements... In this paper, we initially examine the state-of-the-arts of MCPS over the last few decades (1998–2020) and subsequently propose a new framework considering security/privacy for MPCS that incorporates several models that depict various domains of security. An interaction between various models followed with a qualitative assessment of the framework has been carried out to present a detailed description of the proposed framework."

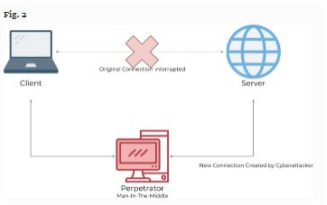
Source: Springer Link

Cooperative control for cyber–physical multi-agent networked control systems with unknown false data-injection and replay cyber-attacks

"The paper discusses the cooperative tracking problem of partially known cyber–physical multi-agent networked systems. In this system, there exist two cascaded chances for cyber-attacks. The local agent is of networked system type that is subjected to unknown false data-injection and replay cyber-attacks that are dissimilar in the sensor-controller and the controller-actuator network parts. The communication between any two agents, if they are connected, is accomplished via a communication network that is subjected to false data-injection cyber-attacks. The problem of the existing two cascaded chances for cyber-attacks is solved in three steps."

Source: Elsevier

ARTIFICIAL INTELLIGENCE



Role of Artificial Intelligence in the Internet of Things (IoT) cybersecurity

"In recent years, the use of the Internet of Things (IoT) has increased exponentially, and cybersecurity concerns have increased along with it. On the cutting edge of cybersecurity is Artificial Intelligence (AI), which is used for the development of complex algorithms to protect networks and systems, including IoT systems. However, cyber-attackers have figured out how to exploit AI and have even begun to use adversarial AI in order to carry out cybersecurity attacks. This review paper compiles information from several other surveys and research papers regarding IoT, AI, and attacks with and against AI and explores the relationship between these three topics with the purpose of comprehensively presenting and summarizing relevant literature in these fields."

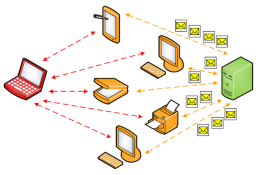
Source: Springer Link

Weaponized AI for cyber attacks

"In this research, we investigated recent cyberattacks that utilize AI-based techniques and identified various mitigation strategies that are helpful in handling such attacks. Further, we identified existing methods and techniques that are used in executing AI-based cyberattacks and what probable future scenarios will be plausible to control such attacks by identifying existing trends in AI-based cyberattacks."

Source: Elsevier

SMART CITY

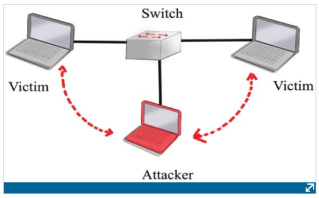


Cybersecurity Risk Assessment in Smart City Infrastructures

"The article is devoted to cybersecurity risk assessment of the dynamic device-to-device networks of a smart city. Analysis of the modern security threats at the IoT/IIoT, VANET, and WSN inter-device infrastructures demonstrates that the main concern is a set of network security threats targeted at the functional sustainability of smart urban

infrastructure, the most common use case of smart networks. As a result of our study, systematization of the existing cybersecurity risk assessment methods has been provided... The experimental study has shown us that the artificial neural network allows us to automatically, unambiguously, and reasonably assess the cyber risk for various object types in the dynamic digital infrastructures of the smart city."
Source: MDPI

HEALTHCARE



Cybersecurity Framework For Healthcare Industry Using NGFW

"In 21 st century due to the advancement in technology and digitalization of healthcare networks, cyber attacks on these networks have advanced and are colossal. The need for protecting healthcare industry from such malice is undeniable. Healthcare information is at risk from malicious actors. Improvements in the state of information security and privacy in the industry are critical to the broad adoption, utilization and confidence in health information systems, medical technologies and electronic exchanges of health information. In this paper a survey on different types of most advanced attacks on healthcare industry and the damage they cause is discussed. Existing approaches to protect healthcare networks is highlighted and a framework for using Next Generation Firewall to detect and prevent cyber attacks is proposed. Additionally configuring the NGFW with a unique hospital network architecture is discussed. The need for an NGFW, its advantages and configuration of such a system is illustrated."
Source: IEEE Xplore

On Medical Device Cybersecurity Compliance in EU

"The medical device products at the European Union market must be safe and effective. To ensure this, medical device manufacturers must comply to the new regulatory requirements brought by the Medical Device Regulation (MDR) and the In Vitro Diagnostic Medical Device Regulation (IVDR)... In this paper, we review the new cybersecurity requirements in the light of currently available guidance documents, and

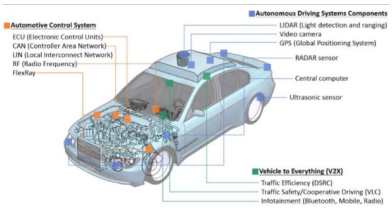
pinpoint four core concepts around which cybersecurity compliance can be built. We argue that these core concepts form a foundations for cybersecurity compliance in the European Union regulatory framework."
Source: Cornell University

SMART DEVICES

Cybersecurity in a post-data environment: Considerations on the regulation of code and the role of producer and consumer liability in smart devices

"This paper outlines the scope of threats which are posed by the hacking of Smart Devices and how these risks can now be physical in nature. The paper then proposes a novel methodology to apportion liability to either the manufacturer or the user, where appropriate. This methodology is based on the principle of negligence, although consumer rights and products liability are also examined from both an American and European perspective. Finally, legislative and judicial shortcomings in relation establishing liability are identified and remedies are proposed, with the intention of establishing a solid legal basis and treatment for cybersecurity."
Source: Elsevier

AUTONOMOUS VEHICLE

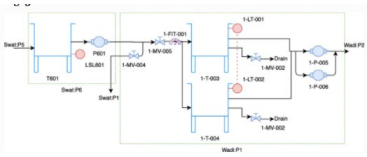


Cybersecurity for autonomous vehicles: Review of attacks and defense

"As technology has evolved, cities have become increasingly smart. Smart mobility is a crucial element in smart cities, and autonomous vehicles are an essential part of smart mobility. However, vulnerabilities in autonomous vehicles can be damaging to quality of life and human safety. For this reason, many security researchers have studied attacks and defenses for autonomous vehicles. However, there has not been systematic research on attacks and defenses for autonomous vehicles. In this survey, we analyzed previously conducted

attack and defense studies described in 151 papers from 2008 to 2019 for a systematic and comprehensive investigation of autonomous vehicles."
Source: Elsevier

CRITICAL INFRASTRUCTURE



Cascading effects of cyber-attacks on interconnected critical infrastructure

"Modern critical infrastructure, such as a water treatment plant, water distribution system, and power grid, are representative of Cyber Physical Systems (CPSs) in which the physical processes are monitored and controlled in real time. One source of complexity in such systems is due to the intra-system interactions and inter-dependencies. Consequently, these systems are a potential target for attackers. When one or more of these infrastructure are attacked, the connected systems may also be affected due to potential cascading effects. In this paper, we report a study to investigate the cascading effects of cyber-attacks on two interdependent critical infrastructure namely, a Secure water treatment plant (SWaT) and a Water Distribution System (WADI)."
Source: Springer Link