SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN

24 October – 18 December 2020

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

5 building blocks of a well-developed security culture

"A defined security culture is helping the financial industry, though the fundamentals should apply to any business."
Source: TechRepublic

A better kind of cybersecurity strategy

"New model shows why countries that retaliate too much against online attacks make things worse for themselves."
Source: MIT News

FireEye hack portends a scary era of cyber insecurity

"What happens when a top cyber-security company whose job is to protect its clients from hackers is itself hacked and its tools of the trade stolen?"
Source: Straits Times

New programme to tap educators in updating youth on opportunities in cyber security

"The Cyber Security Agency of Singapore (CSA) is launching the SG Cyber Educators programme, which will equip teachers, school leaders and career guidance counsellors with knowledge on the cyber-security landscape and career options

academic

CYBERSECURITY

Creating Cybersecurity Knowledge Graphs From Malware After Action Reports

"After Action Reports (AARs) provide incisive analysis of cyber-incidents. Extracting cyber-knowledge from these sources would provide security analysts with credible information, which they can use to detect or find patterns indicative of a cyber-attack. In this paper, we describe a system to extract information from AARs, aggregate the extracted information by fusing similar entities together, and represent that extracted information in a Cybersecurity Knowledge Graph (CKG)."
Source: IEEE Xplore

Assessing and Forecasting Cybersecurity Impacts

"Cyberattacks constitute a major threat to most organizations. Beyond financial consequences, they may entail multiple impacts that need to be taken into account when making risk management decisions to allocate the required cybersecurity resources. Experts have traditionally focused on a technical perspective of the problem by considering impacts in relation with the confidentiality, integrity, and availability of information. We adopt a more comprehensive approach identifying a broader set of generic cybersecurity objectives, the

reports

INSIGHT

Report: The Hidden Costs of Cybercrime

"This is our fourth report on the cost of cybercrime. Our reports surveyed publicly available information on national losses, and, in a few cases, we used data from not-for-attribution interviews with cybersecurity officials. Our 2018 report found that cybercrime cost the global economy more than $600 billion. Our new estimate suggests a more than 50% increase in two years."
Source: McAfee

McAfee Labs Threats Reports Nov 2020

"In this report, McAfee® Labs takes a closer look into the threats that surfaced in the second quarter os 2020. After the first quarter that led the world into a pandemic, the second quarter of 2020 saw enterprised continue to adapt to unprecedented levels of employees working from home and the cybersecurity challenges the new normal demands."
Source: McAfee

Future of Secure Remote Work Report

"Pre-COVID, only 19% of organizations from our survey had more than half of their workforce working remotely, compared to 62% now. Download this exclusive report to find out the

through a series of engagements with industry players."
Source: Straits Times

It's Time to Stop Sharing Your Passwords With Your Partner

"You use long passphrases with letters and numbers. You're careful to make sure your passwords are always unique. But there may be one threat to your digital security that you haven't fully considered: love."
Source: WIRED

Top 5 reasons not to use SMS for multi-factor authentication

"Using SMS as an additional means to authenticate your password is better than nothing, but it's not the most reliable approach. Tom Merritt lists five reasons why SMS should not be used for MFA."
Source: TechRepublic

How privacy features in iOS 14 and macOS Big Sur prevent apps and websites from tracking you online

"Apple has new features in iOS 14 and macOS 11 Safari that disable trackers from learning which websites you visit to protect your privacy. Here are tips on how to use these privacy features."
Source: TechRepublic

How to use the Google One VPN on Android

"If you're looking for the best Android VPN, Jack Wallen thinks Google's take on the service might be the perfect fit for those wanting both performance and security."
Source: TechRepublic

CYBER ATTACKS

Smart doorbells 'easy target for hackers' study finds

"Major security flaws in popular smart doorbells are putting consumers at risk of being targeted by hackers inside their homes, according to Which. The consumer group says devices being sold on marketplaces such as Amazon and eBay, could easily be hacked or switched off by criminals."
Source: BBC

Warning after 75,000 'deleted' files found on used USB drives

"Cybersecurity researchers discovered about 75,000 files after buying 100 of the drives on an internet auction site. Some USB drives contained files named "passwords"

corresponding set of attributes, and relevant forecasting and assessment models."
Source: The Institute for Operations Research and the Management Sciences

Electricity system resilience in a world of increased climate change and cybersecurity risk

"A growing array of threats now impact the resilience of the electrical network including digitalisation, cybersecurity, technological changes of the power system, and the potential for climate change to expose the system to more extreme weather events. Whether distributed and renewable electricity systems will be more resilient through multiple pathways and redundancy, or less resilient due to greater cybersecurity risks than a conventional centralised electricity system, is the key focus of this paper."
Source: Elsevier

Cybersecurity of Smart Electric Vehicle Charging: A Power Grid Perspective

"This paper describes and analyzes cyber vulnerabilities that arise at this nexus and points to the current and emerging gaps in the security of the EV charging ecosystem. These vulnerabilities must be addressed as the number of EVs continue to grow worldwide and their impact on the power grid becomes more viable. The purpose of this paper is to list and characterize all backdoors that can be exploited to seriously harm either EV and EVCS equipments, or power grid, or both. The presented issues and challenges intend to ignite research efforts on cybersecurity of smart EV charging and enhancing power grid resiliency against such demand-side cyberattacks in general."
Source: IEEE Xplore

Using event-based method to estimate cybersecurity equilibrium

"This paper initiates the investigation of using the event-based method to estimate the equilibrium in the new application domain of cybersecurity, where equilibrium is an important metric that has no closed-form solutions. More specifically, the paper presents an event-based method for estimating cybersecurity equilibrium in the preventive and reactive cyber defense dynamics, which has been proven globally convergent. The presented study proves that the estimated equilibrium from our trigger rule i) indeed converges to the equilibrium of the dynamics and ii) is Zeno-free, which assures the usefulness of the event-based method."
Source: IEEE Xplore

challenges and threats companies around the world are facing as they embark on this transition, and how you can leverage these insights to help your organization securely adapt and remain resilient."
Source: Cisco Secure

2020 Cyber Threatscape Report

"In this latest report, Accenture Cyber Threat Intelligence, backed by teams from recent acquisitions Context and Deja vu Security, aims to help clients, partners and community members by offering information so that they can stay ahead of threats relevant to their businesses, industries and geographies."
Source: Accenture

Digitalization and Security Convergence are Driving Growth in the Security Industry, 2020

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

Growth opportunities in cloud-, AI-, and IoT-based security

"This Cyber Security Technology Opportunity Engine (TOE) provides a snapshot on emerging cyber security solutions powered by innovations based on cloud, artificial intelligence, and IoT that help companies protect from threats, data breaches, phishing attacks, and defend against modern attacks residing within cloud, endpoints, and various network layers."
Source: Frost & Sullivan

Frost Radar™: Asia-Pacific Web Security Market, 2020

"Web security is an integral component of an enterprise's security posture to detect and filter out malicious or unwanted web content seeking access to the network. The web security market is still in the growth phase in the Asia-Pacific region, with double-digit annual revenue growth common. For the most part, the market is hardware-driven, with most customers preferring end-to-end ownership rather than hosting solutions on the cloud or receiving solutions as-a-service."
Source: Frost & Sullivan

and images with embedded location data."
Source: BBC

Hackers Accessed Covid Vaccine Data Through the EU Regulator

"Information relating to the one of the most promising coronavirus vaccines has been "unlawfully accessed" following a hack on the European regulatory body that's in the final stages of approving it, the firms jointly developing the vaccine"
Source: WIRED

New control architecture defends complex interconnected systems against cyberattacks

"Researchers have developed a novel control architecture that defends complex, interconnected systems previously vulnerable to cyberattacks. Details were published in IEEE/CAA Journal of Automatica Sinica."
Source: EurekAlert!

Individuals may legitimize hacking when angry with system or authority

"Kent research has found that when individuals feel that a system or authority is unresponsive to their demands, they are more likely to legitimise hacker activity at an organisation's expense."
Source: University of Kent

PHISHING

Plenty more phish: Why employees fall for scams and what companies can do about it

"Preventive counter measures to phishing emails may actually increase the likelihood of employees falling for such scams, a new academic study reveals. Protective controls, such as email proxy, anti-malware and anti-phishing technologies, can give employees a false sense of security, causing them to drop their vigilance because they incorrectly assume such measures intercept all phishing emails before they reach their inbox."
Source: University of Sussex

IBM Uncovers Global Phishing Campaign Targeting the COVID-19 Vaccine Cold Chain

Estimating the Cost of Cybersecurity Activities with CAsPeA: A Case Study and Comparative Analysis

"This paper presents new developments on CAsPeA – a method which enables estimating the cost of these activities based on a model derived from the Activity-Based Costing (ABC) and the NIST SP 800-53 guidelines. The application of the method is illustrated by a case study of a civil engineering enterprise. The method's evaluation based on comparative analysis in respect to SQUARE is described."
Source: Springer Link

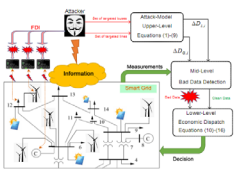
Integrated framework for cybersecurity auditing

"Organizations receive several cyberattacks on their daily operations, thus the need for auditing. However, there is no unified tool to perform cybersecurity audit tasks which are expensive and tedious. In this paper, we build a cybersecurity framework to perform cybersecurity auditing process in organizations. It covers several types of threats and risks by providing the information systems auditors and cybersecurity professionals with several types of controls. Moreover, it illustrates the essential tools and techniques for cybersecurity auditing."
Source: Taylor & Francis Online

Cybersecurity Event Detection with New and Re-emerging Words

"In this paper, we propose a novel event detection system that can quickly identify critical security events, such as new threats and resurgence of an attack or related event, from Twitter regardless of their volume of mentions. Unlike the existing methods, the proposed method triggers events by monitoring new words and re-emerging words, making it possible to narrow down candidate events among several hundreds of events."
Source: Association for Computing Machinery

CYBER ATTACKS



Stealthy Cyberattacks on Loads and Distributed Generation Aimed at Multi-Transmission Line Congestions in Smart Grids

"Developing attack models is the first step to understand cyberattacks in

The 5 biggest cybersecurity threats for the healthcare industry

"Cloud-first security firm Wandera reports that malicious network traffic is the highest cybersecurity risk for hospitals and other healthcare providers and affects 72% of all organizations. This security threat establishes network access from an app to a web service that is known to demonstrate malicious behavior, such as downloading unauthorized software and gathering sensitive data."
Source: TechRepublic

FORECAST

The Future of Cybersecurity: How to Prepare for a Crisis in 2020 and Beyond

"According to the Ponemon Institute and IBM Security's 2020 Cost of a Data Breach Report, enterprises that designated an incident response (IR) team, developed a cybersecurity incident response plan (CSIRP) and tested their plan using tabletop exercises or simulations, saved an average of $2 million in data breach costs. These savings were compared to companies that didn't take these preparatory steps."
Source: Security Intelligence

2021 Security Outcomes Report

"Poised for Success: Proven Factors for Your Security Program. This study will provide you with an extra boost of insight and confidence to get focused for 2021 and beyond."
Source: Cisco Secure

Insights on the Cyber Security Global Market to 2030 - Industry Analysis and Growth Forecast

"The "Cyber Security Market Research Report: By Component, Security Type, Deployment, Enterprise, Use Case, Industry - Global Industry Analysis and Growth Forecast to 2030" report has been added to ResearchAndMarkets.com's offering."
Source: Globe Newswire

WHITE PAPER

The State of Global Phishing

"At the onset of the COVID-19 pandemic, IBM Security X-Force created a threat intelligence task force dedicated to tracking down COVID-19 cyber threats against organizations that are keeping the vaccine supply chain moving. As part of these efforts, our team recently uncovered a global phishing campaign targeting organizations associated with a COVID-19 cold chain."
Source: Security Intelligence

How phishing attacks continue to exploit COVID-19

"These phishing emails promise compensation, test results, and other lures about the coronavirus to trick unsuspecting users, says Armorblox."
Source: TechRepublic

MALWARE

Microsoft Warns Of New Malware That Wants To Infect Your Browser

"Security experts at Microsoft have been tracking a new malware campaign that's targeting Windows computers. It's already claimed tens of thousands of victims and hijacked their web browsers."
Source: Forbes

Malwarebytes: Schools still struggling with connectivity and using last year's antivirus software

"About half of IT decision makers in a new survey say they have not added any cybersecurity training for teachers and students since remote learning started."
Source: TechRepublic

RANSOMWARE

40% Increase in Ransomware Attacks in Q3 2020

"This year cyber attacks have increased many folds as compared to previous years due to new security challenges caused by the Covid-19 pandemic. The third quarter of the year has seen a huge surge in ransomware attacks. Globally, a total of 199.7 million ransomware attacks have been reported in the third quarter of 2020."
Source: Security Boulevard

smart grids and develop countermeasures. In this paper, a three-level nonlinear programming formulation is proposed for false data injection (FDI) cyberattacks that could result in multiple transmission line congestions without being detected by conventional bad data detection (BDD) algorithms. The model is then converted to a mixed integer linear programming (MILP) formulation to guarantee a global optimum exists."
Source: IEEE Xplore

New Challenges in the Design of Microgrid Systems: Communication Networks, Cyberattacks, and Resilience

"Microgrids (MGs), referred to as next-generation power systems, are receiving considerable attention from both industry and academia. Integrated with distributed energy resources (DERs), energy storage systems, and a variety of loads, MGs function as a localized power grid that can be operated independently or connected to utility grids. With the rapid development of technology in communication networks, the framework of MGs tends to be more distributed, intelligent, and tightly integrated with networks. Applications of MGs can be found on the Internet of Things (IoT), Industry 4.0, smart cities, and so on."
Source: IEEE Xplore

Method to Evaluate the Impact of Cyberattacks Against Charging Piles on Distribution Network

"To illustrate the potential impact of cyberattacks to power grid security, this paper proposes two attack scenarios and corresponding attack strategies based on the charging law of electric vehicles. Firstly, a spatial-temporal forecast model of charging loads is established based on the comprehensive analysis of the behaviors of the three types of electric vehicles. Then according to different types of electric vehicle charging laws, corresponding attack scenarios and attack strategies are designed for maximum attack benefits. And then the charging load redistribution model is given."
Source: IEEE Xplore

Cyber Attacks on Power System Automation and Protection and Impact Analysis

"In this paper, we demonstrate the dangerous implications of not securing IEC 61850 standard. Cyber attacks may exploit the vulnerabilities of the Sampled Values (SV) and Generic Object-Oriented Substation Event (GOOSE) protocols of IEC

"Avanan's security scientists analyzed 55.5 million emails to surface key insights on how hackers target Office 365 and Gmail in the 2019 Global Phish Report. It brings clarity to the current phishing-fraught landscape, and suggests how firms can better equip themselves to cope in the future."
Source: Information Week

More Singapore businesses hit by ransomware attacks

"Cyber attacks have intensified in the first 10 months of the year, with many more businesses in Singapore reporting being held to ransom by malware as working from home became a norm amid the pandemic."
Source: Straits Times

Android Ransomware Has Picked Up Some Ominous New Tricks

"While it's still far more common on PCs, mobile ransomware has undergone a worrying evolution, new research shows."
Source: WIRED

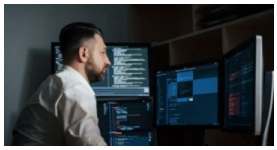
Top 5 business sectors targeted by ransomware

"Any business is subject to ransomware attacks, but some are more hit more than others. Tom Merritt lists five business sectors that are targeted by ransomware."
Source: TechRepublic

Increase in Ransomware Sophistication and Leverage of Legacy Malware Predicted for 2021

"According to the Sophos 2021 Threat Report, there will be a gap between ransomware operators at different ends of the skills and resource spectrum, with big-game hunting ransomware families continuing to refine and change their tactics, techniques and procedures to become more evasive and nation state-like in sophistication."
Source: Info Security

SECURITY MANAGEMENT



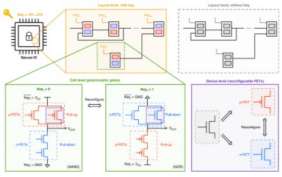
Security Management: Why Companies Need a Unified Cloud Platform

"We must adapt the way we secure data to today's needs. Working from home has increased, forcing entities and their employees to rely more on virtual private networks (VPNs), work with their security operations center (SOC) colleagues remotely and give more attention to data protection."
Source: Security Intelligence

DATA SECURITY

61850. The cyber attacks may be realised by injecting spoofed SV and GOOSE data frames into the substation communication network at the bay level. We demonstrate that such cyber attacks may lead to obstruction or tripping of multiple protective relays."
Source: IEEE Xplore

HARDWARE SECURITY



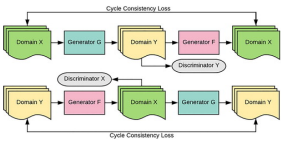
Two-dimensional transistors with reconfigurable polarities for secure circuits

"With the increasing challenges facing the semiconductor industry, interest in out-of-the-box security solutions has grown, even if this implies introducing novel materials such as two-dimensional layered semiconductors. Here, we show that high-performance, low-voltage, two-dimensional black phosphorus field-effect transistors (FETs) that have reconfigurable polarities are suitable for hardware security applications."
Source: Nature Electronics

Design of an Automotive Radar Sensor Firmware Resilient to Cyberattacks

"In this paper, we introduce a novel automotive radar sensor design resilient to cyberattacks. The proposed design can be implemented at the firmware level of the system which provides faster detection of cyberattacks without adding hardware complexity or being computationally expensive. This approach can be combined with any predictive filtering based approach implemented at higher system layers to provide additional security."
Source: IEEE Xplore

DATA NETWORKS



A Review on Application of GANs in Cybersecurity Domain

"Cybersecurity is essential to protect the tremendous increase in data stored on servers and its transmission on networks... At present, a firewall is used to block unknown traffic, antimalware software to detect viruses, trojan, worms and intrusion detection systems to detect attacks. The security professionals are

Break Down Walls in the SOC for Better Data Security

"Data provides businesses the edge they need to unlock their full potential. In turn, employees seek access to data to drive better customer outcomes, become more efficient and increase profits. As these demands for access increase, so too does the need for matching data security controls."
Source: Security Intelligence

ANALYSIS

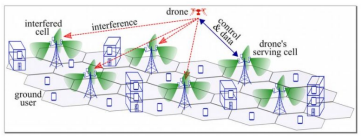
How cybercrime will cost the world $1 trillion this year

"Including both financial losses and cybersecurity spending, the $1 trillion in costs will represent a 50% increase over 2018, says McAfee."
Source: TechRepublic

How the coronavirus outbreak will affect cybersecurity in 2021

"Ensuring security for employees working remotely was cited as the biggest challenge going into the new year, says Check Point."
Source: TechRepublic

UAS



The role of drones in the security of 5G networks

"A work by Giovanni Geraci, a researcher in the Department of Information and Communications Technologies, and researchers at Mississippi State University (USA), which proposes to improve the security of the advanced wireless network against a number of espionage attacks, interference and impersonation."
Source: Pompeu Fabra University Barcelona

ROBOTS

Could Your Vacuum Be Listening to You?

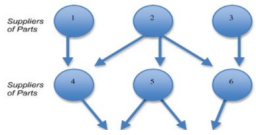
employing Generative Adversarial Networks (GANs) to produce amazing results in fields such as Intrusion Detection, Steganography, Password Cracking, and Anomaly Generation. This paper presents a systematic literature review of GANs applications in the cybersecurity domain, including analysis of specific extended GAN frameworks and currently used stable cybersecurity datasets."
Source: Taylor & Francis Online

CLOUD SECURITY

Cybersecurity management in cloud computing: semantic literature review and conceptual framework proposal

"This paper principally focuses on a comprehensive study of Cloud Computing concerns, security, cybersecurity differences, ISO, and NIST standards. It aims at identifying the policies and the guidelines included in these standards as well as it provides a comprehensive Framework proposal to manage and prevent cyber risks in Cloud Computing taking into consideration the ISO 27,032, ISO 27,001, ISO 27,017 and NIST cybersecurity Framework CSF."
Source: Springer Link

INDUSTRY 4.0



A linear model for optimal cybersecurity investment in Industry 4.0 supply chains

"This paper presents a mixed integer linear programming formulation for optimisation of cybersecurity investment in Industry 4.0 supply chains. Using a recursive linearisation procedure, a complex nonlinear stochastic combinatorial optimisation model with a classical exponential function of breach probability is transformed into its linear equivalent."
Source: Taylor & Francis Online

CYBERSECURITY MANAGEMENT

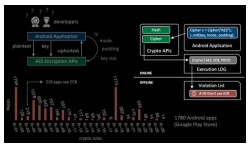
"UMD Researcher Helps Discover Hack of Robotic Cleaners' Navigation Systems to Record Speech and Music"
Source: University of Maryland

IoT

System brings deep learning to "internet of things" devices

"Advance could enable artificial intelligence on household appliances while enhancing data security and energy efficiency."
Source: MIT News

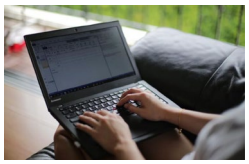
MOBILE SECURITY



New tool detects unsafe security practices in Android apps

"Computer scientists at Columbia Engineering have shown for the first time that it is possible to analyze how thousands of Android apps use cryptography without needing to have the apps' actual codes. The team's new tool, CRYLOGGER, can tell when an Android app uses cryptography incorrectly--it detects the so-called "cryptographic misuses" in Android apps."
Source: EurekAlert!

REMOTE WORKING



New paradigm needed to stay safe online in era of work-from-home, say experts at ST webinar

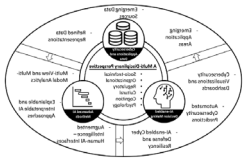
"The World Robotics report shows that Europe is the region with the highest robot density globally, with an average value of 114 units per 10,000 employees in the manufacturing industry. For more facts about robots watch IFR´s video news about Europe in one minute."
Source: Straits Times

HEALTHCARE

Developing cybersecurity culture to influence employee behavior: A practice perspective

"This paper identifies and explains five key initiatives that three Australian organizations have implemented to improve their respective cyber security cultures. The five key initiatives are: identifying key cyber security behaviors, establishing a 'cyber security champion' network, developing a brand for the cyber team, building a cyber security hub, and aligning security awareness activities with internal and external campaigns."
Source: Elsevier

ARTIFICIAL INTELLIGENCE



Trailblazing the Artificial Intelligence for Cybersecurity Discipline: A Multi-Disciplinary Research Roadmap

"Cybersecurity has rapidly emerged as a grand societal challenge of the 21st century. Innovative solutions to proactively tackle emerging cybersecurity challenges are essential to ensuring a safe and secure society. Artificial Intelligence (AI) has rapidly emerged as a viable approach for sifting through terabytes of heterogeneous cybersecurity data to execute fundamental cybersecurity tasks, such as asset prioritization, control allocation, vulnerability management, and threat detection, with unprecedented efficiency and effectiveness."
Source: Association for Computing Machinery

Deep Reinforcement Learning for Cybersecurity Assessment of Wind Integrated Power Systems

"The integration of renewable energy sources (RES) is rapidly increasing in electric power systems (EPS). While the inclusion of intermittent RES coupled with the wide-scale deployment of communication and sensing devices is important towards a fully smart grid, it has also expanded the cyber-threat landscape, effectively making power systems vulnerable to cyberattacks. This article proposes a cybersecurity

How cybercriminals are now exploiting COVID-19 vaccines

"Vaccine-related phishing emails and domains are popping up, while criminals are selling phony vaccines via the Dark Web, says Check Point."
Source: TechRepublic

Healthcare in Crisis: Diagnosing Cybersecurity Shortcomings in Unprecedented Times

"In the early fog of the COVID-19 pandemic, cybersecurity took a back seat to keeping patients alive. Lost in the chaos was IT security."
Source: ThreatPost

Healthcare 2021: Cyberattacks to Center on COVID-19 Spying, Patient Data

"The post-COVID-19 surge in the criticality level of medical infrastructure, coupled with across-the-board digitalization, will be big drivers for medical-sector cyberattacks next year."
Source: ThreatPost

YEAR AHEAD

Cybersecurity Predictions for 2021: Robot Overlords No, Connected Car Hacks Yes

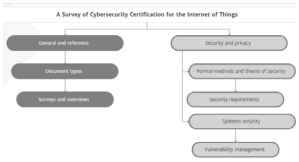
"Gurucul CEO Saryu Nayyar discusses 2021's evolving threats and new challenges — and new tools and technologies that will we hope shift the balance towards the defense."
Source: ThreatPost

assessment approach designed to assess the cyberphysical security of EPS."
Source: IEEE Xplore

Evaluating Explanation Methods for Deep Learning in Security

"In this paper, we introduce criteria for comparing and evaluating explanation methods in the context of computer security. These cover general properties, such as the accuracy of explanations, as well as security-focused aspects, such as the completeness, efficiency, and robustness. Based on our criteria, we investigate six popular explanation methods and assess their utility in security systems for malware detection and vulnerability discovery. We observe significant differences between the methods and build on these to derive general recommendations for selecting and applying explanation methods in computer security."
Source: IEEE Xplore

IoT



A Survey of Cybersecurity Certification for the Internet of Things

"In this survey, we analyze the current cybersecurity certification schemes, as well as the potential challenges to make them applicable for the IoT ecosystem. We also examine current efforts related to risk assessment and testing processes, which are widely recognized as the processes to build a cybersecurity certification framework. Our work provides a multidisciplinary perspective of a possible IoT cybersecurity certification framework by integrating research and technical tools and processes with policies and governance structures, which are analyzed against a set of identified challenges."
Source: Association for Computing Machinery

Forecasting technological positioning through technology knowledge redundancy: Patent citation analysis of IoT, cybersecurity, and Blockchain

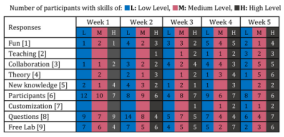
"To understand how the blockchain and IoT can be merged, it is important to have a better understanding of the emerging technologies of IoT, cybersecurity, and blockchain. We used patent analysis, and merged the

patent co-citation analysis (PCA) approach with the patent family to obtain a complete data set analysis. After that, we generated the data using multiple software technologies such as CiteSpace, Pajek, and VOSViewer."
Source: Elsevier

A Multidisciplinary Approach to Internet of Things (IoT) Cybersecurity and Risk Management

"As Internet of Things (IoT) devices and systems become more tightly integrated with our society (e.g., smart city and smart nation) and the citizens (e.g., implantable and insertable medical IoT devices), the need to understand, manage and mitigate cybersecurity risks becomes more pronounced. The ongoing interest in IoT security research is evidenced by the number of submissions we received in this special issue."
Source: Elsevier

CYBERSECURITY & LEARNING


Number of participants with skills of: L: Low Level, M: Medium Level, H: High Level

Responses	Week 1			Week 2			Week 3			Week 4			Week 5		
	L	M	H	L	M	H	L	M	H	L	M	H	L	M	H
Fun [1]	1	2	1	1	2	3	1	1	2	1	1	5	2	1	4
Teaching [2]						1		1	2	1	1	2	2	2	3
Collaboration [3]	1	1	2	3	2	2	1	2	4	2	4	3	2	3	5
Theory [4]		2		2	1	3		1	2	1	3	4	1	5	6
New knowledge [5]	2	1	4	1	3	2	1	2	1	1		3		2	2
Participants [6]	10	10	7	9	9	6	6	8	7	5	6	7	6	7	6
Customization [7]									1		1	2	1	1	2
Questions [8]	2	2	9	14	6	4	2	2	5	2	4	4	4	4	7
Free Lab [9]	2	6	4	2	5	6	2	5	5	2	2	7	2	3	6

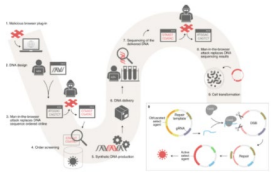
Adapting CTF challenges into virtual cybersecurity learning environments

"This paper aims to highlight the potential of using capture the flag (CTF) challenges, as part of an engaging cybersecurity learning experience for enhancing skills and knowledge acquirement of undergraduate students in academic programs."
Source: Emerald Insight

Estimating the Cost of Cybersecurity Activities with CAsPeA: A Case Study and Comparative Analysis

"This paper presents new developments on CAsPeA – a method which enables estimating the cost of these activities based on a model derived from the Activity-Based Costing (ABC) and the NIST SP 800-53 guidelines. The application of the method is illustrated by a case study of a civil engineering enterprise. The method's evaluation based on comparative analysis in respect to SQUARE is described."
Source: Springer Link

BIOTECHNOLOGY



Increased cyber-biosecurity for DNA synthesis

"Commercial DNA synthesizers sell billions of nucleotides to customers each year, amounting to hundreds of millions of dollars in sales1. As DNA synthesis becomes more widespread, concern is mounting that a cyberattack intervening with synthetic DNA orders could lead to the synthesis of nucleic acids encoding parts of pathogenic organisms or harmful proteins and toxins."
Source: Nature Biotechnology

Cybersecurity Threat Intelligence Augmentation and Embedding Improvement - A Healthcare Usecase

"The implementation of Internet of Things (IoT) devices in medical environments, has introduced a growing list of security vulnerabilities and threats. The lack of an extensible big data resource that captures medical device vulnerabilities limits the use of Artificial Intelligence (AI) based cyber defense systems in capturing, detecting, and preventing known and future attacks. We describe a system that generates a repository of Cyber Threat Intelligence (CTI) about various medical devices and their known vulnerabilities from sources such as manufacturer and ICS-CERT vulnerability alerts."
Source: IEEE Xplore

ETHICS

Ethics in cybersecurity research and practice

"This paper critiques existing governance in cyber-security ethics through providing an overview of some of the ethical issues facing researchers in the cybersecurity community and highlighting shortfalls in governance practice. We separate these issues into those facing the academic research community and those facing the (corporate) practitioner community, drawing on two case studies. While there is overlap between these communities, there are also stark differences."
Source: Elsevier

Scoping the ethical principles of cybersecurity fear appeals

"Fear appeals are used in many domains. Cybersecurity researchers are also starting to experiment with fear appeals, many reporting positive outcomes. Yet there are ethical concerns related to the use of fear to motivate action. In this paper, we explore this aspect from the perspectives of cybersecurity fear appeal deployers and recipients. We commenced our investigation by considering fear appeals from three foundational ethical perspectives."
Source: Springer Link

UAS

Cybersecurity of the Unmanned Aircraft System (UAS)

"This paper will focus on the potential cyber threats against UASs, providing some examples of cyberattacks from the past. Further, the overview of the aviation cybersecurity framework will follow in order to determine the current status of maturity at the international and regional (European Union) levels. The conclusion of the paper will identify the necessary steps to be taken and potential solutions in terms of applying the aviation cybersecurity framework into the operation of UASs."
Source: IEEE Xplore