SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN

23 APRIL – 17 JUNE 2022

TOPICAL REPORT

CYBERSECURITY

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

view past reports | subscribe to others | unsubscribe

news

CYBERSECURITY

University of Jyväskylä project wants to replace passwords with a more secure solution

"The project aims to develop a secure and user-friendly authentication method.

Password management is crucial not only for the security of everyday users, but also for the security of organizations. The military, the governments, power grids, railway networks and air traffic control also need passwords to maintain their security. The problem, however, is that many users often choose convenience over security when choosing and managing their passwords. "The SAFE Project is developing an authentication method (SAFE Solution) that not only works across all operating systems, services and devices but is also easy to use", Woods describes the project."

Source: University of Jyväskylä

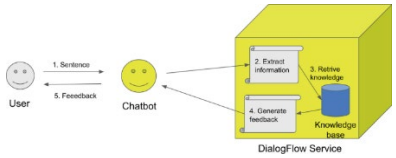
Engineers develop cybersecurity tools to protect solar, wind power on the grid

"Solar panels and wind turbines, now projected to produce 44% of America's electricity by 2050, present cybersecurity challenges.

They have sensors, controllers, actuators or inverters that are directly or indirectly connected to the internet. They're distributed far and

academic

CYBERSECURITY



A Chatbot for Promoting Cybersecurity Awareness

"Cybersecurity is one of the hot topics nowadays. However, not many Internet users know the cyber risks around them. To promote cybersecurity awareness, this paper presents a chatbot that is a cybersecurity expert. It aims to let its users learn more about cybersecurity. It relies on Google Dialogflow, which is a natural language understanding platform. Our chatbot contains a knowledge base on cybersecurity knowledge. Users can make queries to the chatbot to learn definitions and concepts of different cybersecurity terms. Our chatbot also provides self-quizzes for users to test their knowledge on different cybersecurity topics. It also provides suggestions to users on cybersecurity issues such as how to identify and handle phishing emails. In a survey of twenty users, the majority of the users agreed that our chatbot is easy to use and can increase their awareness of cybersecurity issues."

Source: Springer Link

Optimizing Cybersecurity Investments over Time

"In the context of growing vulnerabilities, cyber-risk management cannot rely on a one-off approach, instead calling for a continuous re-assessment of the risk

reports

CYBERSECURITY

X-Force Threat Intelligence Index 2022

"The IBM Security X-Force Threat Intelligence Index maps new trends and attack patterns we observed and analyzed from our data—drawing from billions of datapoints ranging from network and endpoint detection devices, incident response (IR) engagements, domain name tracking and more. This report represents the culmination of that research based on data collected from January to December 2021. We offer these findings as a resource to IBM clients, researchers in the security industry, policy makers, the media and to the broader community of security professionals and business leaders. Given the volatile landscape and the evolution of both threat types and threat vectors, you need threat intelligence insights to stay ahead of attackers and fortify your critical assets more than ever."

Source: IBM

Sophos 2022 Threat Report

"Ransomware-as-a-Service has changed the landscape – find out the impact of this shift

The most significant change Sophos has observed is a shift from bad actors who make their own bespoke ransomware and carry out their own attacks to a model in which one group builds the ransomware and

wide across the country and the countryside. Many have insecure connectivity to legacy electric grid systems. They have complex physics. They're subject to advanced persistent threats. And there will be more and more of them going online."
Source: Iowa State University

Five cybersecurity challenges beyond technology

"In a ransomware attack, a company's computer systems are locked, and the attacker demands a ransom in cryptocurrency in return for unlocking the system. Malware infects a network of objects connected to the Internet of Things to steal the personal data of its users. Talking about cybersecurity is talking about technology. However, it is increasingly common to study cyber risk as part of an interdisciplinary approach. After all, threats are technological, but they also have to do with behavioural, social and ethical factors."
Source: Universitat Oberta De Catalunya

New Technique Offers Faster Security for Non-Volatile Memory Tech

"Researchers have developed a technique that leverages hardware and software to improve file system security for next-generation memory technologies called non-volatile memories (NVMs). The new encryption technique also permits faster performance than existing software security technologies. "NVMs are an emerging technology that allows rapid access to the data, and retains data even when a system crashes or loses power," says Amro Awad, senior author of a paper on the work and an assistant professor of electrical and computer engineering at North Carolina State University."
Source: NC State University

New facility at NTU to help firms with cyber-security evaluation of products

"The facility, known as the National Integrated Centre for Evaluation, will also contribute to research and development in advanced security evaluation techniques, such as those for software and hardware security protection.
The $19.5 million centre, a collaboration between NTU and the Cyber Security Agency of Singapore (CSA), was officially opened last Wednesday (May 18)."
Source: The Straits Times

Singapore and French Regulators Carry Out Joint Cyber Crisis Exercise

and adaptation of risk management strategies. Under the mixed investment–insurance approach, where both risk mitigation and risk transfer are employed, the adaptation implies the re-computation of the optimal amount to invest in security over time. In this paper, we deal with the problem of computing the optimal balance between investment and insurance payments to achieve the minimum overall security expense when the vulnerability grows over time according to a logistic function, adopting a greedy approach, where strategy adaptation is carried out periodically at each investment epoch. We consider three liability degrees, from full liability to partial liability with deductibles. We find that insurance represents by far the dominant component in the mix and may be relied on as a single protection tool when the vulnerability is very low."
Source: MDPI

An approach for detecting LDoS attack based on cloud model

"Cybersecurity has always been the focus of Internet research. An LDoS attack is an intelligent type of DoS attack, which reduces the quality of network service by periodically sending high-speed but short-pulse attack traffic. Because of its concealment and low average rate, the traditional DoS attack detection methods are challenging to be effective. The existing LDoS attack detection methods generally have the problems of high FPR and FNR. A cloud model-based LDoS attack detection method is proposed, and a classifier based on SVM is used to train and classify the feature parameters. The detection method is verified and tested in the NS2 simulation platform and Test-bed network environment. Compared with the existing research results, the proposed method requires fewer samples, and it has lower FPR and FNR."
Source: Springer Link

A High-Quality Entropy Source Using van der Waals Heterojunction for True Random Number Generation

"Generators of random sequences used in high-end applications such as cryptography rely on entropy sources for their indeterminism. Physical processes governed by the laws of quantum mechanics are excellent sources of entropy available in nature. However, extracting enough entropy from such systems for generating truly random sequences is challenging while maintaining the feasibility of the extraction procedure

then leases it out to breaking-and-entering, hands-on-keyboard experts. This has changed the threat landscape in many ways.
In this report you'll find:
The future of ransomware
The impact of Ransomware-as-a-Service
The expanding threat of extortion-style attacks
How misuse of "threat emulation" tools has impacted cybersecurity
AI and its role in 2022 and beyond"
Source: Sophos

European Cybersecurity Responsibility, Spending, and Posture

"The COVID-19 pandemic accelerated the remote working trend by at least 20 years across Europe. To enable remote workers, digital transformation initiatives that were intended to be rolled out over a period of years instead occurred in weeks or months. In the process, security issues were initially pushed aside or ignored altogether in the rush to enable remote workers and protect productivity. That resulted in many organizations unintentionally increasing cyber risk and needing to reexamine security postures.
This study surveyed budget influencing executives in France, Germany, Italy, Spain, and the United Kingdom. The respondent profile is 20% C-level executives, 12% executive management, 34% director-level, 17% middle management, 9% senior management, and 8% manager-level. This research provides a view inside the minds of cybersecurity technology end users to determine what concerns them, what their security posture is, and what is most important to them when making purchasing decisions. It also provides insight on the security implications for European companies as a new and far-reaching second Cold War has erupted between Russia and the democratically aligned European allies."
Source: Frost & Sullivan

"The Monetary Authority of Singapore (MAS), the Banque de France (BdF) and the Autorité de contrôle prudentiel et de résolution (ACPR) had carried out a joint crisis management exercise focused on cybersecurity threats. Backed by the Banque de France, ACPR is the administrative authority that supervises the banking and insurance sectors and ensures financial stability. The exercise follows from the Memorandum of Understanding on Cooperation in Cybersecurity signed between MAS, BdF and ACPR in November 2019. The joint exercise tested the effectiveness of cyber crisis coordination and response by the three financial authorities when managing scenarios such as ransomware, zero-day vulnerabilities and IT supply chain attacks."
Source: FinTech Singapore

Israel and Hong Kong Team Up to Test Digital Currency Cyber Risk

"The Bank of Israel is working with the Hong Kong Monetary Authority on a trial which will test a new digital currency, including against cyber security risks, the Bank of Israel said.
The joint project, which will start in the third quarter, will use a two-tier central bank digital currency (CBDC), it said in a statement. It will be issued by the central bank and then distributed by financial intermediaries like banks."
Source: Bloomberg

Scientific advance leads to a new tool in the fight against hackers

"A new form of security identification could soon see the light of day and help us protect our data from hackers and cybercriminals. Quantum mathematicians at the University of Copenhagen have solved a mathematical riddle that allows for a person's geographical location to be used as a personal ID that is secure against even the most advanced cyber attacks."
Source: University of Copenhagen

RANSOMWARE

New Approach Allows for Faster Ransomware Detection

""Computing systems already make use of a variety of security tools that monitor incoming traffic to detect potential malware and prevent it from compromising the system," says Paul Franzon, co-author of a paper on for real-world applications. Here, we present a compact and an all-electronic van der Waals heterostructure-based device capable of detecting discrete charge fluctuations for extracting entropy from physical processes and use it for the generation of independent and identically distributed true random sequences. We extract a record-high value (>0.98 bits/bit) of min-entropy using the proposed scheme. We demonstrate an entropy generation rate tunable over multiple orders of magnitude and show the persistence of the underlying physical process for temperatures ranging from cryogenic to ambient conditions."
Source: ACS Publications

Metasurface-in-the-Middle Attack: From Theory to Experiment

"Metasurfaces enable controllable manipulation of electromagnetic waves and have been shown to improve wireless communications in many diverse ways. In this paper, we define and experimentally demonstrate for the first time a "MetaSurface-in-the-Middle" (MSITM) attack. In this attack, the adversary Eve places a metasurface in the path of a directive transmission between Alice and Bob and targets to re-direct a portion of the signal towards herself, without being detected. In particular, we show how Eve can design a metasurface that induces abrupt phase changes at the interface of the metasurface to controllably diffract directional links and establish furtive eavesdropping links. We explore the theoretical foundations of the MSITM attack and demonstrate that an effective metasurface can be prototyped in under 5 min at the cost of several cents. We experimentally demonstrate the attack in a THz time-domain system and perform a set of over-the-air experiments."
Source: ACM Digital Library

Leveraging human factors in cybersecurity: an integrated methodological approach

"Computer and Information Security (CIS) is usually approached adopting a technology-centric viewpoint, where the human components of sociotechnical systems are generally considered as their weakest part, with little consideration for the end users' cognitive characteristics, needs and motivations. This paper presents a holistic/Human Factors (HF) approach, where the individual, organisational and technological factors are investigated in pilot healthcare organisations to show how HF vulnerabilities may impact on cybersecurity risks. An overview of

the new ransomware detection approach. "However, the big challenge here is detecting ransomware quickly enough to prevent it from getting a foothold in the system. Because as soon as ransomware enters the system, it begins encrypting files." Franzon is Cirrus Logic Distinguished Professor of Electrical and Computer Engineering at North Carolina State University."
Source: NC State University

This Microsoft 365 flaw could let ransomware hit OneDrive and SharePoint

"A "potentially dangerous" piece of functionality recently discovered in Office 365 could allow threat actors to encrypt cloud-hosted files and make them unrecoverable without a dedicated backup solution, or a decryption key.
Cybersecurity researchers from Proofpoint claim the "AutoSave" feature, which automatically saves documents being worked on to the cloud can be abused by the flaw.
AutoSave is a pretty self-explanatory tool. Every now and then, the documents being worked on get saved to the cloud. The authors, collaborators, and file owners can later access these older versions, giving them a window of opportunity in case of a ransomware(opens in new tab) attack."
Source: Tech Radar

ARTIFICIAL INTELLIGENCE

Keeping web-browsing data safe from hackers

"Researchers at MIT have shown that machine-learning-assisted side-channel attacks are both extremely robust and poorly understood. The use of machine-learning algorithms, which are often impossible to fully comprehend due to their complexity, is a particular challenge. In a new paper, the team studied a documented attack that was thought to work by capturing signals leaked when a computer accesses memory. They found that the mechanisms behind this attack were misidentified, which would prevent researchers from crafting effective defenses."
Source: Massachusetts Institute of Technology

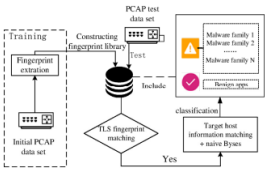
TECHNOLOGY

current challenges in relation to cybersecurity is first provided, followed by the presentation of an integrated top–down and bottom–up methodology using qualitative and quantitative research methods to assess the level of maturity of the pilot organisations with respect to their capability to face and tackle cyber threats and attacks. This approach adopts a user-centred perspective, involving both the organisations' management and employees."
Source: Springer Link

Cybersecurity as illuminator for the future of computing research

"In this column, we suggest that the role of cybersecurity in real-world systems, and the costs of its absence, are making the effects of these forces visible to the cybersecurity research community both particularly clearly and particularly early. Hence, lessons being learned by cybersecurity researchers today can help illuminate the path toward evolution of the larger computing research enterprise tomorrow. To explore this idea, we outline several motivating forces we see at play and some lessons cybersecurity researchers are drawing from them. We then turn to the field more broadly, and propose a series of questions worth asking and exploring in that context.
We start by suggesting that *failing* to fully consider these forces in the context of much past cybersecurity research, development, and deployment has produced disastrous consequences for society. Security continues to be a nonintegrated consideration in the design and operation of many computing systems, addressed narrowly rather than holistically. Equally, security is still viewed by much of the computing research community in a narrow technical context, leading to results poorly aligned with motivating real-world needs. Human factors are poorly understood and insufficiently considered."
Source: ACM Digital Library

MALWARE



An improved fingerprint matching algorithm to detect malware encrypted traffic based on weighted Bayes

"Traffic security is one of the important topic in cyber security of smart city. With the widespread use of

Radio waves for the detection of hardware tampering

"As far as data security is concerned, there is an even greater danger than remote cyberattacks: namely tampering with hardware that can be used to read out information – such as credit card data from a card reader. Researchers in Bochum have developed a new method to detect such manipulations. They monitor the systems with radio waves that react to the slightest changes in the ambient conditions. Unlike conventional methods, they can thus protect entire systems, not just individual components – and they can do it at a lower cost."
Source: Ruhr-University Bochum

Eavesdroppers can hack 6G frequency with DIY metasurface

"Crafty hackers can make a tool to eavesdrop on some 6G wireless signals in as little as five minutes using office paper, an inkjet printer, a metallic foil transfer and a laminator.
The wireless security hack was discovered by engineering researchers from Rice University and Brown University, who will present their findings and demonstrate the attack this week in San Antonio at ACM WiSec 2022, the Association for Computing Machinery's annual conference on security and privacy in wireless and mobile networks… In the study, Knightly, Brown University engineering Professor Daniel Mittleman and colleagues showed an attacker could easily make a sheet of office paper covered with 2D foil symbols — a metasurface — and use it to redirect part of a 150 gigahertz "pencil beam" transmission between two users."
Source: Rice University

PHISHING

Police warn of new phishing scam involving malware installed on victims' phones

"The Singapore Police Force (SPF) on Tuesday (Jun 14) warned of a new phishing scam where victims who received advertisements for cleaning services were led into downloading a mobile phone application believed to contain malware.

encrypted traffic, more and more malware prefers to use encrypted traffic to transmit malicious information. Since the transmission content is not visible, the traditional detection method based on deep packet inspection is not effective anymore. In this paper, by analyzing the protocol and the sessions of malicious encrypted traffic and benign traffic, a weight naive Bayes-based method for detecting malware encrypted traffic and classifying malware family is proposed. The method construct a hybrid fingerprint for each malware family traffic and benign traffic."
Source: SPIE Digital Library

A topic modeling-based approach to executable file malware detection

"Malware is a term that refers to any malicious software used to harm or exploit a device, service, or network. The presence of malware in a system can disrupt operations and the availability of information in networks while also jeopardizing the integrity and confidentiality of such information, which poses a grave issue for sensitive and critical operations. Traditional approaches to malware detection often used by antivirus software are not robust in detecting previously unseen malware. As a result, they can often be circumvented by finding and exploiting vulnerabilities of the detection system. This study involves using natural language processing techniques, considering the recent advancements made in the field in recent years, to analyze the strings present in the executable files of malware."
Source: SPIE Digital Library

Malware distributed collection and pre-classification system using honeypot technology

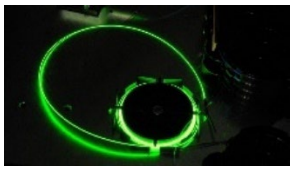
"Malware has become a major threat in the last years due to the ease of spread through the Internet. Malware detection has become difficult with the use of compression, polymorphic methods and techniques to detect and disable security software. Those and other obfuscation techniques pose a problem for detection and classification schemes that analyze malware behavior. In this paper we propose a distributed architecture to improve malware collection using different honeypot technologies to increase the variety of malware collected. We also present a daemon tool developed to grab malware distributed through spam and a pre-classification technique that uses antivirus technology to separate malware in generic classes."
Source: SPIE Digital Library

At least two victims have fallen prey to the scam this month, with losses amounting to at least S$2,000."
Source: Channel News Asia

Phishing Hits All-Time High in Q1 2022

"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: InfoSecurity Magazine

QUANTUM PHYSICS



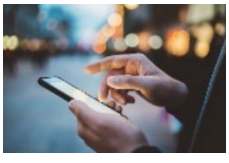
Secure communication with light particles

"While quantum computers offer many novel possibilities, they also pose a threat to internet security since these supercomputers make common encryption methods vulnerable. Based on the so-called quantum key distribution, researchers at TU Darmstadt have developed a new, tap-proof communication network."
Source: Technische Universitat Darmstadt

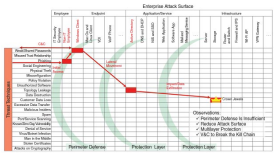
Single-Photon Source Paves the Way for Practical Quantum Encryption

"Researchers have developed a new high-purity single-photon source that can operate at room temperature. The source is an important step toward practical applications of quantum technology, such as highly secure communication based on quantum key distribution (QKD).
"We developed an on-demand way to generate photons with high purity in a scalable and portable system that operates at room temperature," said Helen Zeng, a member of the research team from the University of Technology Sydney in Australia. "Our single-photon source could advance the development of practical QKD systems and can be integrated into a variety of real-world quantum photonic applications.""
Source: Optica

SOCIAL MEDIA



RANSOMWARE



Strategy and Tactics Against Ransomware

"ansomware has become increasingly prevalent in recent years. As one of the primary cyberthreats to enterprises, ransomware can be used to encrypt sensitive files, exfiltrate data, and demand payment in exchange for decryption.3 Recently, the industrial sector of the United States has suffered more than US$20 billion in damages due to ransomware, yet that amount is expected to soar to US$256 billion annually by 2031.1,2 Because campaigns are often accompanied by advanced persistent threats (APTs), the extent of ransomware spread and damage is difficult to accurately measure and forecast. To analyze ransomware and APTs, the Mitre Corporation organized the Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) framework5 as a holistic knowledge base of threat techniques."
Source: IEEE Xplore

Preventive portfolio against data-selling ransomware—A game theory of encryption and deception

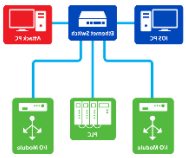
"Ransomware has risen to be among the top cyber threats in recent years. There is an alarming trend of ransomware stealing data in addition to locking files. Compared to traditional ransomware, this new data-selling ransomware can be more harmful to the victims facing the data leakage threat. Traditional wisdom of defensive measures such as data backup is less effective in preventing the attacker from making money by selling data. We propose two preventive measures designed to defend against the data-selling ransomware, i.e., preventive data encryption and preventive data deception. Users may form a preventive portfolio made up of the two preventive measures. We contribute a novel game theoretical model of the data-selling ransomware to study the equilibrium strategies of the attacker and victims."
Source: Elsevier

Ransomware and the Robin Hood effect?: Experimental evidence on Americans'

PITT Prevents Potential Phone Password Plunder

"A recent Pitt-led study found that the Graphics Processing Unit (GPU) in some Android smartphones could be used to eavesdrop on a user's credentials when the user types these credentials using the smartphone's on-screen keyboard, making it an effective target for hacking."
Source: University of Pittsburgh

INDUSTRIAL SYSTEMS



SwRI develops cyber security intrusion detection system for industrial control systems

"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: Southwest Research Institute

GADGETS

Bluetooth Signals Can Be Used to Identify And Track Smartphones

"A team of engineers at the University of California San Diego has demonstrated for the first time that the Bluetooth signals emitted constantly by our mobile phones have a unique fingerprint that can be used to track individuals' movements. Mobile devices, including phones, smartwatches and fitness trackers, constantly transmit signals, known as Bluetooth beacons, at the rate of roughly 500 beacons per minute.These beacons enable features like Apple's "Find My" lost device tracking service; COVID-19 tracing apps; and connect smartphones to other devices such as wireless earphones."
Source: University of California - San Diego

Stronger security for smart devices

"Recently, MIT researchers published a paper in the IEEE Journal of Solid-State Circuits, which demonstrated that analog-to-digital converters in smart devices, which encode real-

willingness to support cyber-extortion

"Ransomware attacks have become a critical security threat worldwide. However, existing research on ransomware has largely ignored public opinion. This initial study identifies patterns in the American public's support for the use of ransomware, specifically when it is framed to provide benefits to others (i.e., in-group members). Drawing on the Robin Hood decision-making literature and Moral Foundations Theory, we offer theoretical predictions regarding ransomware support. In a survey of 1013 Americans, we embedded a split-ballot experiment in which respondents were randomly assigned to indicate their level of support or opposition to one of two sets of six ransomware scenarios. We manipulated the nationality, authority level, and political affiliation of the actors."
Source: Springer Link

A Tale of Two Markets: Investigating the Ransomware Payments Economy

"Ransomware attacks are among the most severe cyber threats. They have made headlines in recent years by threatening the operation of governments, critical infrastructure, and corporations. Collecting and analyzing ransomware data is an important step towards understanding the spread of ransomware and designing effective defense and mitigation mechanisms. We report on our experience operating Ransomwhere, an open crowdsourced ransomware payment tracker to collect information from victims of ransomware attacks. With Ransomwhere, we have gathered 13.5k ransom payments to more than 87 ransomware criminal actors with total payments of more than $101 million. Leveraging the transparent nature of Bitcoin, the cryptocurrency used for most ransomware payments, we characterize the evolving ransomware criminal structure and ransom laundering strategies. Our analysis shows that there are two parallel ransomware criminal markets: commodity ransomware and Ransomware as a Service (RaaS)."
Source: Cornell University

FeSA: Feature selection architecture for ransomware detection under concept drift

"This paper investigates how different genetic and nature-inspired feature selection algorithms operate in systems where the prediction model changes over time in unforeseen ways. As a result, this study proposes a

world signals from sensors into digital values that can be processed computationally, are susceptible to power side-channel attacks. A hacker could measure the power supply current of the analog-to-digital converter and use machine learning to accurately reconstruct output data.

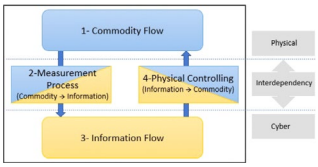
Now, in two new papers, researchers show that analog-to-digital converters are also susceptible to a stealthier form of side-channel attack, and describe techniques that effectively block both attacks. Their techniques are more efficient and less expensive than other security methods."

Source: Massachusetts Institute of Technology

feature section architecture, namely FeSA, independent of the underlying classification algorithm and aims to find a set of features that will improve the longevity of the machine learning classifier. The feature set produced by FeSA is evaluated by creating scenarios in which concept drift is presented to our trained model. Based on our results, the generated feature set remains robust and maintains high detection rates of ransomware malware. Throughout this paper, we will refer to the true-positive rate of ransomware as detection; this is to clearly define what we focus on, as the high true positive rate for ransomware is the main priority. Our architecture is compared to other nature-inspired feature selection algorithms such as evolutionary search, genetic search, harmony search, best-first search and the greedy stepwise feature selection algorithm."

Source: Elsevier

CYBER PHYSICAL SYSTEMS

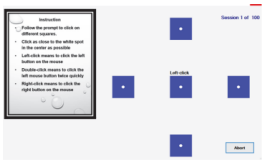


Unified IT&OT Modeling for Cybersecurity Analysis of Cyber-Physical Systems

"Cyber-Physical Systems (CPSs) engineering profoundly relies on modeling methods to represent the system and study the operation and cybersecurity of CPSs. The operation of a CPS is the result of the collaboration between Information Technology (IT) and Operational Technology (OT) components. While OT focuses on the system's process physics, the emphasis of IT is on information flow. Consequently, different system models are utilized to study various aspects of CPSs, which may infer different views of the same system. The increasing complexity of CPSs and the high number of cyberattacks against Industrial Control Systems (ICSs) and CPSs in recent years have highlighted the necessity of considering these interrelations based on a unified model to analyze cybersecurity of CPSs."

Source: IEEE Xplore

ARTIFICIAL INTELLIGENCE



Improving cybersecurity through deep learning on

keystroke and mouse dynamics

"Username, password, and biometrics are three-factor authentication for cybersecurity enhancement. Adding keystroke and mouse biometrics to authentication will definitely improves the cybersecurity. Keystroke dynamics refers to the process of measuring and assessing human's typing rhythm on digital devices. Keystroke timing information such as digraph, dwell time and flight time are used in our experimental datasets. Mouse dynamics records mouse motion (speed), left-, right-, or double-clicking timing information. Our own dataset includes both types of dynamics from same group of subjects. We develop recurrent neural network (RNN) models and support vector machine (SVM) models to represent user's biometrics. Keystroke and mouse dynamics can be used as features fed to the models separately for user verification or identification. Feature fusion is applied to improve the accuracy. "

Source: SPIE Digital Library

Developing Cybersecurity Systems Based on Machine Learning and Deep Learning Algorithms for Protecting Food Security Systems: Industrial Control Systems

"Industrial control systems (ICSs) for critical infrastructure are extensively utilized to provide the fundamental functions of society and are frequently employed in critical infrastructure. Therefore, security of these systems from cyberattacks is essential. Over the years, several proposals have been made for various types of cyberattack detection systems, with each concept using a distinct set of processes and methodologies. However, there is a substantial void in the literature regarding approaches for detecting cyberattacks in ICSs. Identifying cyberattacks in ICSs is the primary aim of this proposed research. Anomaly detection in ICSs based on an artificial intelligence algorithm is presented. The methodology is intended to serve as a guideline for future research in this area. On the one hand, machine learning includes logistic regression, k-nearest neighbors (KNN), linear discriminant analysis (LDA), and decision tree (DT) algorithms, deep learning long short-term memory (LSTM), and the convolution neural network and long short-term memory (CNN-LSTM) network to detect ICS malicious attacks."

Source: MDPI

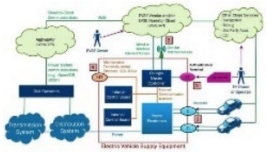
SOCIAL MEDIA

Jettisoning Junk Messaging in the Era of End-to-End Encryption: A Case Study of WhatsApp

"WhatsApp is a popular messaging app used by over a billion users around the globe. Due to this popularity, understanding misbehavior on WhatsApp is an important issue. The sending of unwanted junk messages by unknown contacts via WhatsApp remains understudied by researchers, in part because of the end-to-end encryption offered by the platform. We address this gap by studying junk messaging on a multilingual dataset of 2.6M messages sent to 5K public WhatsApp groups in India. We characterise both junk content and senders. We find that nearly 1 in 10 messages is unwanted content sent by junk senders, and a number of unique strategies are employed to reflect challenges faced on WhatsApp, e.g., the need to change phone numbers regularly. We finally experiment with on-device classification to automate the detection of junk, whilst respecting end-to-end encryption."

Source: Cornell University

ELECTRIC VEHICLE

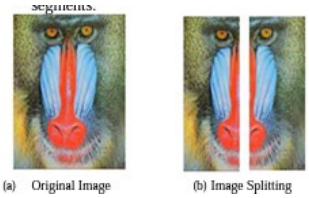


Review of Electric Vehicle Charger Cybersecurity Vulnerabilities, Potential Impacts, and Defenses

"Worldwide growth in electric vehicle use is prompting new installations of private and public electric vehicle supply equipment (EVSE). EVSE devices support the electrification of the transportation industry but also represent a linchpin for power systems and transportation infrastructures. Cybersecurity researchers have recently identified several vulnerabilities that exist in EVSE devices, communications to electric vehicles (EVs), and upstream services, such as EVSE vendor cloud services, third party systems, and grid operators. The potential impact of attacks on these systems stretches from localized, relatively minor effects to long-term national disruptions. Fortunately, there is a strong and expanding collection of information

technology (IT) and operational technology (OT) cybersecurity best practices that may be applied to the EVSE environment to secure this equipment. In this paper, we survey publicly disclosed EVSE vulnerabilities, the impact of EV charger cyberattacks, and proposed security protections for EV charging technologies."
Source: MDPI

FPGA



Implementation Dual Parallelism Cybersecurity Architecture on FPGA

"This paper presents an efficient parallelism architecture that uses a dual-computing engine architecture to better throughput using both spatial and temporal parallelism on FPGA technology. This architecture will enhance the performance in terms of operating frequency and throughput and reduces the power consumption that meets applications with huge data processing such as Internet of Things .in this design, two boards are used, "DE1_Soc and NEEK board" with Altera Quartus Prime 18 for synthesis and simulation. The proposed design architecture gives better resource usage and throughput through fewer hardware redundancies using a frequency of 600MHZ with 64 bits for each engine from the dual-engine. Furthermore, the proposed architecture implementation results show the reduction in the time delay by 40 % and achieves a throughput of 153.6 Gb/s"
Source: Journal of Communications

ETHICS

A framework for assessing AI ethics with applications to cybersecurity

"In the last few years many scholars, public and private organizations have been involved in the definition of guidelines and frameworks for individuating the principles to adopt in the development and deployment of AI systems. Some authors, however, noted that the effectiveness of these guidelines or ethical codes on the

developer's community is very marginal. One of the obstacles that opposes to the effective implementation of ethical principles is the lack of an approach for solving tensions which arise when principles are applied. A possible solution to such an issue could be the adoption of a risk-based approach which is also advocated by many sources. To our knowledge, no concrete proposals have been presented in literature on how to perform a risk-based ethical assessment. In this paper we contribute to close this gap by introducing a framework based on a qualitative risk analysis approach for assessing the ethical impact underneath the introduction of an innovation either technological or organizational in a system."
Source: Springer Link