SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN

18 JUNE – 19 AUGUST 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

Thinking like a cyber-attacker to protect user data

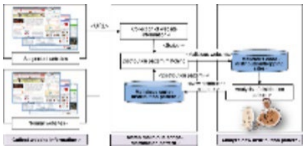
"A component of computer processors that connects different parts of the chip can be exploited by malicious agents who seek to steal secret information from programs running on the computer, MIT researchers have found.
Modern computer processors contain many computing units, called cores, which share the same hardware resources. The on-chip interconnect is the component that enables these cores to communicate with each other. But when programs on multiple cores run simultaneously, there is a chance they can delay one another when they use the interconnect to send data across the chip at the same time."
Source: MIT

Cybersecurity as a sitcom: New TU Graz courses on side channel attacks at edX.org

"Cybersecurity experts at TU Graz have launched an online course designed as a sitcom on side channel attacks, in which physical effects allow inferences to be made about protected data. The first of two new seasons of the educational sitcom will go online on 23 August."
Source: Graz University of Technology

academic

CYBERSECURITY



Malicious script distribution pattern detection technique for image search websites

"Recently, the number of cases of distributing malicious codes by exploiting homepages that provide an image search continues to increase, and malicious codes distributed through homepages are causing personal information infringement accidents and DDoS attacks. Due to the malware spread through web pages, privacy theft and infringement are getting serious and DoS attacks happen frequently. Distribution patterns of hidden malicious codes on the image search website were collected, and patterns of collected malicious codes and malicious scripts were analyzed. We have analyzed the malicious samples and derived some additional distribution patterns of web-based malware. Similar patterns are grouped together and a representative feature is then extracted from each group. Each category of the malicious samples contains malicious script codes and their variants. We have implemented a system to automatically detect malicious web sites using the malicious script patterns. The proposed malicious script pattern is expected to be available for the zero-day attacks."
Source: SPIE

reports

CYBERSECURITY

Cyber security considerations 2022

"CISOs must wear multiple hats simultaneously, but they can't be everywhere at all times. While it's important to remember the oft-heard maxim, "security is everyone's job," it's even more critical to recognise that security is key to building and maintaining customer, client and stakeholder trust. Looking toward 2022 and beyond, we're focusing on eight core topics that we believe CISOs should prioritise at the C-suite and boardroom levels. These themes, along with a focus on the always-fluid regulatory environment, can help executives better understand how cyber can support the business with a security plan based on shared accountability. Whether it's advanced persistent threats, ransomware, backdoor attacks, or something we've yet to see, there will likely always be new perils with which to contend. But if CISOs and their teams adhere to a disciplined set of principles designed with the organisation's key objectives in mind, and if the plan is up to date and flexible, they can position the organisation to mitigate the impact of cyber events."
Source: KPMG

Research offers solution to encrypted messages being hacked before sending or after receipt

"To combat this issue of close location hacking, researchers from Surrey's School of Computer Sciences have created a new end-to-end encryption mechanism called Secure Node End-2-End Encryption (SNE2EE) that protects users' communications at a far higher level than currently experienced on popular applications. Current messaging applications encrypt the data transfer from one device to another, but not the typed or received message on either end."
Source: University of Surrey

A simple tool to make websites more secure and curb hacking

"An international team of researchers has developed a scanning tool to make websites less vulnerable to hacking and cyberattacks."
Source: University of South Australia

How to strengthen the human element of cybersecurity

"KnowBe4, a security awareness training and simulated phishing platform, recently released a resource kit designed to help IT and Infosec professionals improve their human element of security. The organization said that IT professionals are still challenged when it comes to creating a security awareness program.
Carpenter, in contact with TechRepublic, shared the human security lessons he has learned over the past years. He warns that while rising cybersecurity statistics are of great concern, companies should look beyond them."
Source: Tech Republic

Bringing lessons from cybersecurity to the fight against disinformation

"Mary Ellen Zurko remembers the feeling of disappointment. Not long after earning her bachelor's degree from MIT, she was working her first job of evaluating secure computer systems for the U.S. government. The goal was to determine whether systems were compliant with the "Orange Book," the government's authoritative manual on cybersecurity at the time. Were the systems technically secure? Yes. In practice? Not so much.
"There was no concern whatsoever for whether the security demands on end users were at all realistic," says Zurko. "The notion of a secure system was about the technology, and it assumed perfect, obedient humansNow a cybersecurity researcher at MIT Lincoln Laboratory,

Cybersecurity in Supply Chains: Quantifying Risk

"Sharing information in a supply chain can bring benefits to many, if not all, members of the chain; however, the impact of information sharing and information technology (IT) implementation on supply chain risk is not well understood. Reports from corporate board meetings indicate that while concern is expressed over such risk, there are no accepted principles or best practices for quantification of supply chain risk. To increase understanding of cybersecurity risk in supply chains from a more grounded quantitative perspective, we identify four different ways an organization in a chain can be attacked as well as the principal factors putting that firm at risk to each of the four types of attack. Using data from detailed forensic analyses of approximately 2000 companies and/or organizations that experienced attacks, we answer fundamental, data-driven questions both external and internal to a firm belonging to a supply chain."
Source: Taylor & Francis Online

A multi-objective framework for the identification and optimisation of factors affecting cybersecurity in the Industry 4.0 supply chain

"Digital assets are highly vulnerable and always prone to malicious intervention. Identification of causes of such intervention for timely support and assistance remains a key challenge for businesses to remain functional and thrive with the competition. A framework is proposed in this paper for identifying cyber risk, threat, and countermeasure, based on breach databases and textual information processing. Alongside, a multi-objective optimisation of a mixed-integer non-linear problem (MINLP) is made post linearisation to find out a suitable trade-off between cyber risk and investment. The model helps in effective decision-making by finding the proneness of suppliers (as nodes) in the sequence of reducing vulnerability and pairing of categorised factors."
Source: Taylor & Francis Online

Addressing Human Factors in Cybersecurity Leadership

"This article identifies human factors in workplaces that contribute to the challenges faced by cybersecurity leadership within organizations and discusses strategic communication, human–computer interaction, organizational factors, social environments, and security awareness training. Cybersecurity

Gartner Unveils the Top Eight Cybersecurity Predictions for 2022-23

"In the opening keynote at the Gartner Security & Risk Management Summit in Sydney, Richard Addiscott, Senior Director Analyst and Rob McMillan, Managing Vice President at Gartner discussed the top predictions prepared by Gartner cybersecurity experts to help security and risk management leaders be successful in the digital era.
"We can't fall into old habits and try to treat everything the same as we did in the past," said Addiscott. "Most security and risk leaders now recognize that major disruption is only one crisis away. We can't control it, but we can evolve our thinking, our philosophy, our program and our architecture."
Gartner recommends that cybersecurity leaders build the following strategic planning assumptions into their security strategies for the next two years."
Source: Gartner

166 Cybersecurity Statistics and Trends

"Cybersecurity is a day-to-day operation for many businesses.
A lack of data protection, side effects of a global pandemic, and an increase in exploit sophistication have led to a huge incline in hacked and breached data from sources that are increasingly common in the workplace, such as mobile and IoT (internet of things) devices. On top of this, COVID-19 has ramped up remote workforces, making inroads for cyberattacks.
Recent security research suggests most companies have poor cybersecurity practices in place, making them vulnerable to data loss. To successfully fight against malicious intent, it's imperative that companies make cybersecurity awareness, prevention, and security best practices a part of their culture.
To give you a better idea of the current state of overall security, we've compiled more than 160 cybersecurity statistics for 2022. This will help show the prevalence and need for cybersecurity in all facets of business. These stats include data breaches, hacking stats, different types of cybercrime, industry-specific stats, spending, costs, and information about the cybersecurity career field."
Source: Varonis

2022 SonicWall Cyber Threat Report

"As cybercrime continues evolving, we need as much intel as possible. SonicWall is on the front-lines watching every threat and

Zurko is still enmeshed in humans' relationship with computers. Her focus has shifted toward technology to counter influence operations, or attempts by foreign adversaries to deliberately spread false information (disinformation) on social media, with the intent of disrupting U.S. ideals."
Source: MIT

MALWARE

Researchers discover a new hardware vulnerability in the Apple M1 chip

"The M1 chip uses a feature called pointer authentication, which acts as a last line of defense against typical software vulnerabilities. With pointer authentication enabled, bugs that could normally compromise a system or leak private information are stopped dead in their tracks.
Now, researchers from MIT's Computer Science and Artificial Intelligence Laboratory (CSAIL) have found a crack: Their novel hardware attack, called PACMAN, shows that pointer authentication can be defeated without even leaving a trace. Moreover, PACMAN utilizes a hardware mechanism, so no software patch can ever fix it."
Source: MIT

Malicious PyPi packages turn Discord into password-stealing malware

"Python developers are under attack once again, with attackers looking to steal Discord account details along with data stored in various browsers.
Cybersecurity researchers from Snyk have recently spotted a dozen malicious packages, uploaded to PyPi, the biggest Python code repository out there, with more than 600,000 active users.
The packages were uploaded almost a month ago, by a threat actor called "scarycoder". They claim to provide the users with various functionalities, Roblox tools, thread management, and others. Instead, the researchers have found, all the packages do is steal sensitive information."
Source: Tech Radar

Cybercriminals Developing BugDrop Malware to Bypass Android Security Features

"In a sign that malicious actors continue to find ways to work around Google Play Store security protections, researchers have spotted a previously undocumented Android

does not simply focus on information technology systems; it also considers how humans use information systems and susceptible actions leading to vulnerabilities. As cyber leaders begin to identify human behavior and processes and collaborate with individuals of the same mindset, an organization's strategy can improve substantially. Cybersecurity has been an expanding focal point from the viewpoint of human factors. Human inaccuracy can be unintentional due to an inaccurate strategic implementation or accurate unsatisfactory plan implementation. A systematic literature review was conducted to realize unintentional human factors in cybersecurity leadership."
Source: MDPI

Response to Cybersecurity Threats of Informational Infrastructure Based on Conceptual Models

"Response to the threats of information security in conditions of modern organization with a large infrastructure is an area with emergency loaded intensity of the data usage. For a successful exposure and the prevention of computer attacks the construction of complex models of the events and infrastructure is required. In this work, the question of the applicability of ontological models and reasoning for supporting response process is examined. On the basis of built ontology, practical use cases are demonstrated."
Source: Springer Link

Design and Verification of the Arm Confidential Compute Architecture

"The increasing use of sensitive private data in computing is matched by a growing concern regarding data privacy. System software such as hypervisors and operating systems are supposed to protect and isolate applications and their private data, but their large codebases contain many vulnerabilities that can risk data confidentiality and integrity. We introduce Realms, a new abstraction for confidential computing to protect the data confidentiality and integrity of virtual machines. Hardware creates and enforces Realm world, a new physical address space for Realms. Firmware controls the hardware to secure Realms and handles requests from untrusted system software to manage Realms, including creating and running them. Untrusted system software retains control of the dynamic allocation of memory to Realms, but cannot access Realm memory contents, even if run at a

cyberattack. Capture Labs threat researchers collect first-hand data from more than a million global sensors in 215 countries and regions. We provide our valuable cyber threat intelligence in real time.
The world's most quoted ransomware threat intelligence, SonicWall's biannual threat reports are cited by major news outlets worldwide, applied by businesses for cybersecurity planning and trusted by governments. Download the report. Know the threats"
Source: Sonic Wall

METAVERSE

Crime in the metaverse is very real. But how do we police a world with no borders or bodies?

"**Software vulnerabilities and malware**
Malware targeting crypto wallets is already being used to steal people's cryptocurrencies, tokens or NFTs. Cyber extortion and ransomware are some of the most notorious and lucrative cybercrime threats. They may take on different shapes in the metaverse, but will remain a serious risk.
A high percentage of attacks against current Web 3.0 platforms and DeFi protocols are made possible due to vulnerabilities in the underlying software or smart contracts used. For DeFi protocols, in particular, the largest thefts, according to Chainalysis' 2022 Crypto Crime report, are usually the result of code exploits."
Source: The World Economic Forum

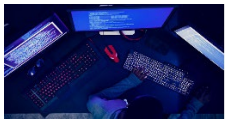
dropper trojan that's currently in development.
"This new malware tries to abuse devices using a novel technique, not seen before in Android malware, to spread the extremely dangerous Xenomorph banking trojan, allowing criminals to perform On-Device Fraud on victim's devices," ThreatFabric's Han Sahin said in a statement shared with The Hacker News."
Source: The Hacker News

TECHNOLOGY

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. The RUB's science magazine Rubin features a report by the team from Ruhr-Universität Bochum (RUB), the Max Planck Institute for Security and Privacy and the IT company PHYSEC."
Source: Ruhr-University Bochum

PHISHING



Conti Cybercrime Cartel Using 'BazarCall' Phishing Attacks as Initial Attack Vector

"A trio of offshoots from the notorious Conti cybercrime cartel have resorted to the technique of call-back phishing as an initial access vector to breach targeted networks. "Three autonomous threat groups have since adopted and independently developed their own targeted phishing tactics derived from the call back phishing methodology," cybersecurity firm AdvIntel said in a Wednesday report.
These targeted campaigns "substantially increased" attacks against entities in finance, technology, legal, and insurance sectors, the company added."
Source: The Hacker News

higher privileged level. To guarantee the security of Realms, we verified the firmware, introducing novel verification techniques that enable us to prove, for the first time, the security and correctness of concurrent software with hand-over-hand locking and dynamically allocated shared page tables, data races in kernel code running on relaxed memory hardware, integrated C and Arm assembly code calling one another, and untrusted software being in full control of allocating system resources. Realms are included in the Arm Confidential Compute Architecture."
Source: Columbia University School of Engineering and Applied Science

A Case for Cybersecurity Awareness Systems

"This Chapter intends to provide the context and environment leading to the development of the CS-AWARE cybersecurity awareness solution, which was comprehensively piloted and evaluated in the local public administration (LPA) use case during the CS-AWARE H2020 European research and innovation project. The Chapter assesses the main factors driving cybersecurity from a holistic multi-angle perspective, and reviews the currently actively developing European legislative cybersecurity environment, which is introducing a multi-level cybersecurity framework centred around awareness and cooperation/collaboration.
Furthermore, this Chapter highlights in more detail the specific cybersecurity requirements for LPAs, which is heavily focused on the critical data they manage, and emphasizes why cybersecurity awareness plays such a crucial role in future collaborative cybersecurity in Europe, and why significant cybersecurity gains can be achieved by introducing awareness and collaboration in the context of cybersecurity management in organizations like LPAs."
Source: Springer Link

MALWARE

Introduction to the Special Issue on Challenges and Trends in Malware Analysis

"Malicious software (malware) has become one of the main threats to Internet security, with a sustained growth in complexity and volume during the last three decades. Malware has experienced an impressive evolution since the 1980s, moving from simple worms,

How credential phishing attacks threaten a host of industries and organizations

"General phishing emails are often a prelude to credential phishing attacks that attempt to compromise an employee's account. Once an attacker has access to an internal account through the stolen credentials, they can launch more dangerous and devastating attacks against entire networks.

For the first half of 2022, email attacks against organizations rose by 48%, according to the report. Out of all those attacks, 68% were credential phishing attempts that contained a link designed to steal sensitive account information. Over the same time, 265 different brands were spoofed in phishing emails."

Source: Tech Republic

QUANTUM COMPUTERS

Quantum digits unlock more computational power with fewer quantum particles

"The team led by Thomas Monz at the Department of Experimental Physics at the University of Innsbruck, now succeeded in developing a quantum computer that can perform arbitrary calculations with so-called quantum digits (qudits), thereby unlocking more computational power with fewer quantum particles."

Source: University of Innsbruck

CRYPTOGRAPHY

Quantum cryptography: Hacking futile

"For exchanging quantum mechanical keys, there are different approaches available. Either light signals are sent by the transmitter to the receiver, or entangled quantum systems are used. In the present experiment, the physicists used two quantum mechanically entangled rubidium atoms, situated in two laboratories located 400 meters from each other on the LMU campus. The two locations are connected via a fiber optic cable 700 meters in length, which runs beneath Geschwister Scholl Square in front of the main building."

Source: Ludwig-Maximilians-Universität München

backdoors, and file-infection viruses to multi-stage campaigns, complex platforms that support a variety of modules, and sophisticated evasion mechanisms that make analysis increasingly difficult [2]. A key reason for this evolution is the fact that the malware industry long ago acquired the role of a commodity [1, 3] in the underground cybercrime economy [4]. This prompted malware developers to continuously improve their arsenal of techniques tailored to make quick money in different ways, from click fraud and spamming to cryptocurrency mining and bank credentials theft.

The increasing sophistication and impact of malware attacks has gone hand-in-hand with a growing interest from both industry and academia in defense and analysis techniques. Traditional signature-based malware detection techniques are easily bypassed by samples using obfuscation, software packing, or other similar techniques."

Source: ACM Digital Library

Identification and Monitoring of Malware with Several Detection System -A Systematic Review

"According to recent studies, Malicious Software is storing itself in the system as a temporary file using a variety of obscuring methods. The detection of malicious software is the first step in system security. In this paper, a comprehensive review of the methods, such as deep learning, and datasets for cyber security intrusion are provided. Numerous researchers have investigated intrusion detection systems to secure the network. Current IDSs are not only challenged by random intrusion categories, but also by the need for massive computational power. The intrusion detection system, or IDS, is utilized to detect network intrusions. IDS may be required to manage multiple distinct audit record types. It is demonstrated that IDS is a significant security tool for detecting computer network and resource attacks. Although there is a vast amount of literature on IDS issues, we aim to obtain a more comprehensive picture in order to provide a thorough review."

Source: Research Gate

Static Malware Analysis Using Machine and Deep Learning

"In the era of digital advancement and innovation, malware (malicious software) still poses major threats to users' privacy and leads to many security breaches. Due to the exponential rise in malware attacks, malware analysis and detection continue to be a hot research topic.

Malware analysis plays a vital role in the malware detection process. Currently, the detection process adopts the malware signatures (static analysis) and behavior patterns (dynamic analysis) that have been proven time-consuming and less effective in identifying unknown malware in real time. Recent malware uses abstraction, packing, encryption, polymorphic, and other cryptic methods to hide and change the malware behavior and its signature which makes the detection process complex. Most of the new malware is the variants of existing malware, where machine learning techniques are effective in identifying such malware. However, the traditional machine learning technique is time-consuming because it requires substantial feature engineering and learning."
Source: Springer Link

Classifying Malware Represented as Assembly and Control Flow Graphs Using Ensemble Learning

"Malware is a serious issue in today's cybersecurity world, and many resources are devoted to malware detection. The features extracted from raw binary files (assembly code) have diverse nature. This makes it hard to make a malware system that employment effectively. To improve performance, we look at novel machine learning algorithms for classifying malware programs based on the type of control flow graphs (CFG) they have. This paper shows a machine learning-based malware classification technique supported static methods for classifying different malware families. We evaluate our proposed system using the BIG 2015 (Microsoft malware) dataset, which comprises over 20 K malware samples. The experimental findings suggest that it can categorize CFG-represented malware programs with comparable performance to approaches applied to raw binary files."
Source: Springer Link

Lightweight CNN-based malware image classification for resource-constrained applications

"Malware (Malicious Software) is a malicious piece of code designed with the intention to enter a computer system to carry out harmful operations. It poses a severe threat to computer and internet users. As the number of new malwares increases, the challenge of identifying and classifying them into appropriate families gets more difficult. During the last couple of years, deep

convolutional neural network (CNN)-based models resulted promising performance on malware classification. However, the existing deep CNN-based approaches require higher resources in terms of storage and computationally heavy training operations for feeding a large number of data to the CNN model. As a result, the existing approaches are not suitable for malware detection in Internet of things (IoT) applications as IoT-based applications are mostly resource-constrained in nature."
Source: Springer Link

RANSOMWARE

Immunizing Files Against Ransomware with Koalafied Immunity

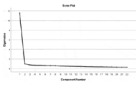
"Without backups, victims of ransomware are often forced to pay a ransom to recover critical files. Some ransomware only encrypts the first 256 K or 1 MB of a file. Could the first 1 MB of a file simply be appended to the end of the file then used to restore files encrypted by these types of ransomware. This paper describes such an approach, called "Koalafied Immunity", and experiments conducted to evaluate the effectiveness of this approach. The disruptive impact on Koalafied Immunity is also examined."
Source: Springer Link

Ransomware Detection Based on PE Header Using Convolutional Neural Networks

"With the spread of information technology in human life, data protection is a critical task. On the other hand, malicious programs are developed, which can manipulate sensitive and critical data and restrict access to this data. Ransomware is an example of such a malicious program that encrypts data, restricts users' access to the system or their data, and then request a ransom payment. Many types of research have been proposed for ransomware detection. Most of these methods attempt to identify ransomware by relying on program behavior during execution. The main weakness of these methods is that it is not explicit how long the program should be monitored to show its real behavior. Therefore, sometimes, these researches cannot detect ransomware early. In this paper, a new method for ransomware detection is proposed that does not need executing the program and uses the PE header of the executable file. To extract

effective features from the PE header file, an image is constructed based on PE header. Then, according to the advantages of convolutional neural networks (CNN) in extracting features from images and classifying them, CNN is used. The proposed method achieves high detection rates. Our results indicate the usefulness and practicality of our method for ransomware detection."
Source: Ebsco Host

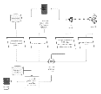
CYBERCRIME AWARENESS



Development of a Scale to Measure Cybercrime-Awareness on Social Media

"This study developed a psychometric scale to measure users' cybercrime awareness level on social media. Psychometric properties of the Cybercrime Awareness on Social Media Scale (CASM-S) were tested based on data collected from 1045 social media users. Exploratory factor analysis (EFA) with principal components analysis was used to identify the underlying factor structure of the scale (N = 545). The results revealed that the scale has a unidimensional factor structure. The scale was found to have a high internal reliability (a = .957). Confirmatory factor analysis (CFA) was conducted to verify factor structure of the CASM-S (N = 500). Results revealed that the one-factor model fits the data well (x2/DF = 2.757, CFI = .939, SRMR = .0366, RMSEA = .059). Further, the study evaluated the concurrent validity of the scale (r = .855, p < .001). The findings revealed that the CASM-S is a reliable and valid tool to measure users' cybercrime awareness level on social media."
Source: Taylor & Francis

IoT



Sandbox Environment for Real Time Malware Analysis of IoT Devices

"The explosion in IoT devices' growth becomes the primary target to attackers. It provides a large attack surface to attackers for Distributed Denial of Service (DDoS), Eavesdropping, Privilege Escalation, etc. With a lack of research in IoT security, there are lake solutions to analyze the advanced malware in a secure environment to understand IoT malware behavior. This paper has proposed a sandbox environment concept model that analyses malware, generates automated

reports, and solves problems with the existing sandbox. Sandbox uses multiple machine-learning algorithms to analyze malware on three basic levels: static malware analysis, real-time malware analysis, and network analysis. Then by consolidating the report from all this analysis, the sandbox environment generates the report. Static analysis is performed by collecting information from shared libraries, ELF, and other binary files using the Convolutional Neural Networks model generated automated analysis report."
Source: Springer Link