SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN

12 February – 9 March 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 | academic | reports

CYBER AWARENESS

How to Protect People against Phishing and Other Scams

"For electronic health, teach your users basic digital hygiene, but commit your budget and time to staying a step ahead of the enemy in the technical arms race that is impossible to avoid."
Source: Scientific American

Attackers can impersonate other mobile phone users

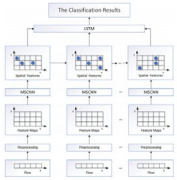
"They can thus start a subscription at the expense of others or publish secret company documents under someone else's identity."
Source: Ruhr-Universität Bochum

Cyber-security label for smart home devices

"A cyber-security label similar to the energy-efficiency labels on home appliances will be rolled out to help buyers of smart devices better judge how exposed they are to cyber risks. This label will be stuck on Wi-Fi routers and smart home hubs for a start, as part of Singapore's new Safer Cyberspace Masterplan designed to protect consumers and small firms."
Source: The Straits Times

SKILLS GAP

THREAT DETECTION & PREDICTION



Model of the intrusion detection system based on the integration of spatial-temporal features

"In this paper, we propose a unified model combining Multiscale Convolutional Neural Network with Long Short-Term Memory (MSCNN-LSTM) … Compared with the model based on the conventional neural networks, the MSCNN-LSTM model has better accuracy, false alarm rate and false negative rate."
Source: Computers & Security

On High-Speed Flow-based Intrusion Detection using Snort-compatible Signatures

"Signature-based Network Intrusion Detection Systems (NIDS) have become state-of-the-art in modern network security solutions. However, most systems are not designed for modern high-speed network links. In the field of network monitoring, an alternative solution has become the choice for such high-speed networks. Flow-monitoring, typically based on the Internet Protocol Flow Information Export (IPFIX) standard, now goes well beyond collecting statistical information about network connections … We now present our improved version of the IPFIX-based

REVIEW

X-Force Threat Intelligence Index 2020

"IBM Security releases the IBM X-Force Threat Intelligence Index annually, summarizing the year past in terms of the most prominent threats raised by our various research teams to provide security teams with information that can help better secure their organizations."
Source: IBM

OUTLOOK

Asia-Pacific Integrated Cybersecurity Framework Industry Guide, 2020

"An integrated cybersecurity framework is an offering by leading vendors aimed at the future of cybersecurity … The study acknowledges that there are several disincentives to swapping to the integrated security framework as highly regulated organizations, especially banks and governments, tend to prefer best-of-breed solutions."

Career and Management Advice to Improve Diversity From 21 Leading Women in Cybersecurity

"The diversity problem is too big for any individual or organization to tackle alone. Creating an inclusive industry is going to require collaboration and radically different approaches. Luckily, 21 women in cyber have offered some advice on how to create better equity in hiring, management and retention efforts, as well as advice for women starting out their cybersecurity careers."
Source: Security Intelligence

SOLUTIONS

Hottest new cybersecurity products at RSA Conference 2020

"The annual RSA Conference is a key venue for companies to showcase their new cybersecurity products. Here are some of the more interesting tools to check out."
Source: CSO

Computer Scientists' New Tool Fools Hackers into Sharing Keys for Better Cybersecurity

"Instead of blocking hackers, a new cybersecurity defense approach developed by University of Texas at Dallas computer scientists actually welcomes them. The method, called DEEP-Dig (DEcEPtion DIGging), ushers intruders into a decoy site so the computer can learn from hackers' tactics. The information is then used to train the computer to recognize and stop future attacks."
Source: University of Texas at Dallas

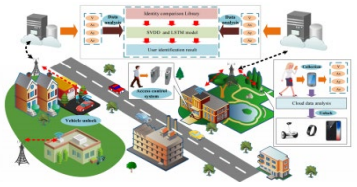
Cryptographic "tag of everything" could protect the supply chain

"MIT researchers' millimeter-sized ID chip integrates a cryptographic processor, an antenna array that transmits data in the high terahertz range, and photovoltaic diodes for power."
Source: MIT News

Mixed-signal hardware security thwarts powerful Signature-based Intrusion Detection System (FIXIDS)."

Source: IEEE Transactions on Dependable and Secure Computing

IOT SECURITY



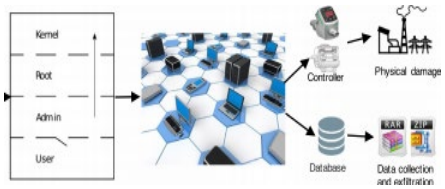
Gait Learning Based Authentication for Intelligent Things

"Identity authentication plays an important role for the safety of smart terminals. Most existing schemes use biological features such as the iris and the fingerprint for identity authentication, which can not implement real-time and continuous identification of user identity. In light of this, we propose a feature extraction and fine-grained authentication scheme based on gait data in this paper …"
Source: IEEE Transactions on Vehicular Technology

Integration of a Threat Traceability Solution in the Industrial Internet of Things

"In this paper, we aim to analyze its applicability in the IIoT from a technical point of view, by studying its deployment over different IIoT architectures and defining a common framework for the acquisition of data considering the computational constraints involved. The result is a beneficial insight that demonstrates the feasibility of this approach when applied to upcoming IIoT infrastructures."
Source: IEEE Transactions on Industrial Informatics

CYBER PHYSICAL SYSTEMS



A dynamic games approach to proactive defense strategies against Advanced Persistent Threats in cyber-physical systems

"Advanced Persistent Threats (APTs) have recently emerged as a significant security challenge for a cyber-physical system due to their stealthy, dynamic and adaptive nature. Proactive dynamic defenses provide a strategic and holistic security mechanism to increase the costs of attacks and mitigate the
Source: Frost & Sullivan

2020 Cybersecurity Outlook Report

"Using the MITRE ATT&CK™ framework as the backdrop for our research, this report uncovers the top attack tactics, techniques, and procedures (TTPs) seen over the last year and provides specific guidance on ransomware, commodity malware, wipers, access mining, and destructive attacks."
Source: Carbon Black

Cybersecurity Trends 2020

"In the Cybersecurity Trends 2020 report, we explore the expanding relationship between cybercrime and our physical safety, potential impacts on society, and risks to the environment. The rapidly increasing number of cyber-physical systems connecting to our digital lives represent a material cyber-kinetic threat."
Source: TÜV Rheinland

INDUSTRY INSIGHTS

Securing What's Now and What's Next: 20 Cybersecurity Considerations for 2020

"By conducting our sixth annual survey of 2,800 IT decision makers from 13 countries, we've continued our annual tradition of going deep into your world to compile key benchmark statistics. We also spoke at length to a panel of CISOs to analyze the findings and build a list of 20 considerations for 2020. This report provides valuable takeaways and data you can share with other members of your C-suite, or your board of directors, to make concrete recommendations for improving your organization's security posture."
Source: Cisco

2020 Global Threat Report

"This report provides a front-line view and greater insight into the cyber battle CrowdStrike's seasoned security experts are waging against today's most sophisticated adversaries, and offers recommendations for increasing your organization's cybersecurity readiness."
Source: CrowdStrike

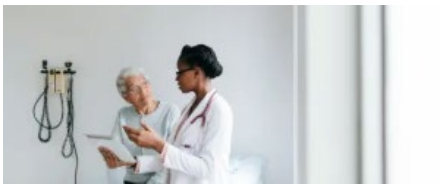
electromagnetic attacks

"Purdue innovators are at Silicon Valley's premier chip-design conference to unveil technology that is 100 times more resilient to electromagnetic attacks to secure Internet of Things devices."
Source: Purdue University

Rice boosts 'internet of things' security — again

"Rice University engineers have one-upped their own technique to increase security for the internet of things … a technique to make security more than 14,000 times better than current state-of-the-art defenses while using far less energy."
Source: Rice University

HEALTHCARE



Measuring Security Risk in a Medical IoT World

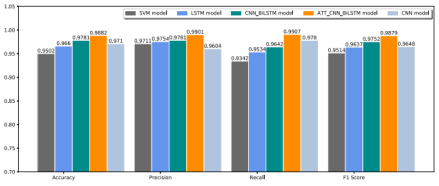
"The medical internet of things (IoT) is no longer a futuristic concept. It is here today, and it includes devices you may have never considered a part of the patient care ecosystem, such as elevators, beds, exit signs and clocks. Between those operational technologies and the devices the U.S. Food and Drug Administration (FDA) has already deemed critical, the healthcare vulnerability landscape continues to expand, with each connected device potentially elevating the risk of an attack."
Source: Security Intelligence

risks. This work proposes a dynamic game framework to model a long-term interaction between a stealthy attacker and a proactive defender."
Source: Computers & Security

Additive Manufacturing Cyber-Physical System: Supply Chain and Risks

"This paper analyzes the general characteristics of Additive Manufacturing (AM) supply chain and proposes three AM supply chain models based on the specific nature of the industry … Throughout the product life cycle of additively manufactured products, the interlacing of the virtual supply chain (digital thread) with the physical supply chain and their operations fundamentally make the AM process a cyber-physical system (CPS). Therefore, the technology brings along with it benefits of a CPS as well as a new class of attack vectors. We discuss the possible attacks (printer, raw material and design level), risks (reverse engineering, counterfeiting and theft) and provide an enhanced risk classification scheme."
Source: IEEE Access

ARTIFICIAL INTELLIGENCE



A DGA domain names detection modeling method based on integrating an attention mechanism and deep neural network

"Considering the randomness of the Domain Generation Algorithm (DGA) domain names, recent research in DGA detection applyed machine learning methods based on features extracting and deep learning architectures to classify domain names. However, these methods are insufficient to handle wordlist-based DGA threats, which generate domain names by randomly concatenating dictionary words according to a special set of rules. In this paper, we proposed a a deep learning framework ATT-CNN-BiLSTM for identifying and detecting DGA domains to alleviate the threat."
Source: Cybersecurity

An improved two-hidden-layer extreme learning machine for malware hunting

"In recent years, there have been attempts to design machine learning techniques to increase the success of existing automated malware

detection and analysis. In this paper, we build a modified Two-hidden-layered Extreme Learning Machine (TELM), which uses the dependency of malware sequence elements in addition to having the advantage of avoiding backpropagation when training neural networks."
Source: Computers & Security

A novel method for malware detection on ML-based visualization technique

"Many machine learning (ML)-based malware detection methods are proposed to address this problem. However, considering the attacks from adversarial examples (AEs) and exponential increase in the malware variant thriving nowadays, malware detection is still an active field of research. To overcome the current limitation, we proposed a novel method using data visualization and adversarial training on ML-based detectors to efficiently detect the different types of malwares and their variants."
Source: Computers & Security

DL-Droid: Deep learning based android malware detection using real devices

"In this paper, we propose DL-Droid, a deep learning system to detect malicious Android applications through dynamic analysis using stateful input generation. Experiments performed with over 30,000 applications (benign and malware) on real devices are presented … the results highlight the significance of enhanced input generation for dynamic analysis as DL-Droid with the state-based input generation is shown to outperform the existing state-of-the-art approaches."
Source: Computers & Security

CYBER AWARENESS

Source: Britannica ImageQuest

Developing a measure of information seeking about phishing

"In order to understand how current and future interventions regarding phishing may be consumed by users, as well as their potential impact on phishing susceptibility, it is important to conduct theoretically based research that provides a foundation to investigate these issues. This study provides a first step in addressing this

by developing and validating a theoretically based survey measure across two studies centred upon the constructs of protection motivation theory (perceived vulnerability, severity, self-efficacy and response efficacy) to assess the factors that influence whether people choose to keep up to date with protective information about phishing."
Source: Journal of Cybersecurity

Predicting individuals' vulnerability to social engineering in social networks

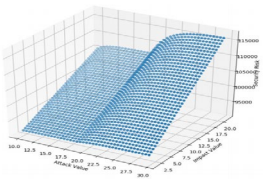
"Few studies have investigated the effect of individuals' characteristics on predicting their vulnerability to social engineering in the context of social networks. To address this gap, the present study developed a novel model to predict user vulnerability based on several perspectives of user characteristics."
Source: Cybersecurity

DATA SCIENCE

Data presentation in security operations centres: exploring the potential for sonification to enhance existing practice

"Sonification in which data are represented as sound, is said to have potential as an approach that could work alongside existing visual data presentation approaches to address some of the unique challenges faced by Security Operations Centres (SOCs) … The perspectives of security practitioners on incorporating sonification into their actual working environments have not yet been examined, however. The aim of this article, therefore, is to address this gap by exploring attitudes to using sonification in SOCs and by identifying the data presentation approaches currently used."
Source: Journal of Cybersecurity

SECURITY EXERCISE



SMART: security model adversarial risk-based tool for systems security design evaluation

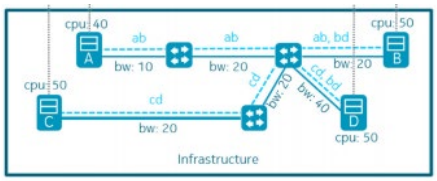
"This work presents a security model adversarial risk-based tool (SMART) for systems security design evaluation. Our tool reads in a systems security model an attack graph and collects the necessary information for the purpose of determining the best solution based on a calculated security risk represented as a monetary amount."
Source: Journal of Cybersecurity

NETWORK SECURITY

Understanding Node Capture Attacks in User Authentication Schemes for Wireless Sensor Networks

"Despite decades of intensive research, it is still challenging to design a practical multi-factor user authentication scheme for wireless sensor networks (WSNs) … Two of the most common security failures are regarding smart card loss attacks and node capture attacks. The former has been extensively investigated in the literature, while little attention has been given to understanding the node capture attacks. To alleviate this undesirable situation, this paper takes a substantial step towards systematically exploring node capture attacks against multi-factor user authentication schemes for WSNs."
Source: IEEE Transactions on Dependable and Secure Computing

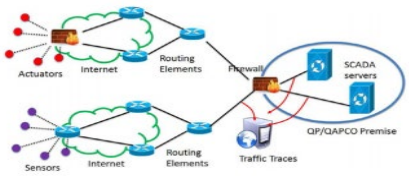
5G



Solving security constraints for 5G slice embedding: A proof-of-concept

"Network slicing is a prominent feature of 5G, which allow tenants to rent network and computing virtual resources from one or more Infrastructure Providers (InPs) … In this paper, we build on our previous work to propose and evaluate a security-aware slice embedding implementation which enables tenants to declare security-oriented requirements, while limiting InP network information disclosure."
Source: Computers & Security

SYSTEM SECURITY

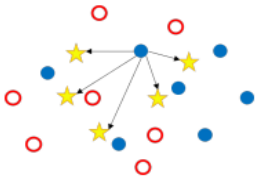


Cybersecurity for industrial control systems: A survey

"In this work, we have a close look at the shift of the Industrial Control System (ICS) from stand-alone systems to cloud-based environments. Then we discuss the major works, from industry and academia towards the development of the secure ICSs, especially applicability of the machine learning techniques for the ICS cyber-security. The work may help to address the challenges of securing industrial processes, particularly while migrating them to the cloud environments."

Source: Computers & Security

MALWARE



Android Malware Detection via (Somewhat) Robust Irreversible Feature Transformations

"We develop FARM, a Feature transformation based AndRoid Malware detector. FARM takes well-known features for Android malware detection and introduces three new types of feature transformations that transform these features irreversibly into a new feature domain."

Source: IEEE Transactions on Information Forensics and Security

---