SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN

7 January – 11 February 2020

TOPICAL REPORT

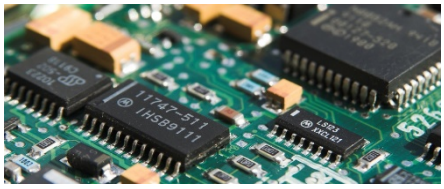
CYBERSECURITY

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

OUTLOOK

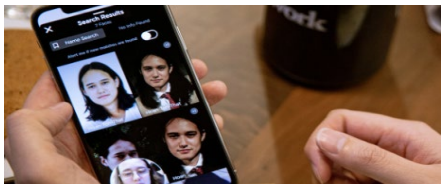


Why 2020 is a turning point for cybersecurity

"In 2020, the drive of the Fourth Industrial Revolution towards ubiquitous connectivity and digitalization will continue. But as new connections and technologies support socio-economic progress, cyberattacks and risks to and stemming from these innovations will increase in frequency and impact. Here's how leaders can adapt and adopt the right strategies, and build effective partnerships to ensure optimal cybersecurity and digital trust."

Source: World Economic Forum

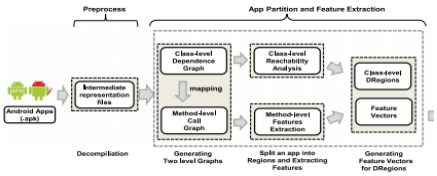
CYBER AWARENESS



The Secretive Company That Might End Privacy as We Know It

"A little-known start-up helps law enforcement match photos of unknown people to their online images — and 'might lead to a dystopian future or something,' a

THREAT DETECTION & PREDICTION



Detection of Repackaged Android Malware with Code-Heterogeneity Features

"During repackaging, malware writers statically inject malcode and modify the control flow to ensure its execution. Repackaged malware is difficult to detect by existing classification techniques, partly because of their behavioral similarities to benign apps. By exploring the app's internal different behaviors, we propose a new Android repackaged malware detection technique based on code heterogeneity analysis."

Source: IEEE Transactions on Dependable and Secure Computing

Real-Time Multistep Attack Prediction Based on Hidden Markov Models

"A novel method based on the Hidden Markov Model is proposed to predict multistep attacks using IDS alerts. We consider the hidden states as similar phases of a particular type of attack. As a result, it can be easily adapted to multistep attacks and foresee the next steps of an attacker. To achieve this goal, a preliminary off-line training phase based on observations will be required."

REVIEW

Innovate for Cyber Resilience: Lessons from Leaders to Master Cybersecurity Execution

"The Third Annual State of Cyber Resilience shows how leaders have mastered cybersecurity execution to drive innovation and grow with confidence."

Source: Accenture

OUTLOOK

2020 Cyber Security Report

"The 2020 Cyber Security Report highlights the trends cyber-criminals use to attack organizations worldwide across all industries, and gives cyber security professionals and C-Level executives the information they need to protect their organizations from fifth-generation cyber attacks and threats."

Source: Check Point

NETWORK SECURITY

backer says."
Click here to register for your NYT account.
Source: The New York Times

Cisco Flaws Put Millions of Workplace Devices at Risk

"Five vulnerabilities in Cisco Discovery Protocol make it possible for a hacker to take over desk phones, routers, and more."
Source: Wired

DEEPFAKE

How Deepfakes Will Make Us Question Everything in 2020

"This concept has been discussed in legal circles and is referred to as the "liar's dividend." If anyone can claim that what they said is the result of a deepfake, how do we distinguish the truth anymore? The ramifications in the political world are significant, but that's another discussion. We must probe this issue from the perspective of enterprise cybersecurity, because there's a lot to chew on."
Source: Security Intelligence

AVIATION

Airport Security Concern As 97% Of World's Top 100 Fail Cybersecurity Test

"When it comes to cybersecurity, 97 of the world's largest 100 airports failed to pass the tests set by one leading web security business. Given that the World Economic Forum (WEF) had flagged emerging cybersecurity challenges facing the aviation industry during its 2020 annual meeting in Davos-Klosters, the timing of this research couldn't be better, or should that be worse?"
Source: Forbes

SECURITY EXERCISE

How to manage cyber risk with a Security by Design

Source: IEEE Transactions on Dependable and Secure Computing

Biometric Face Presentation Attack Detection With Multi-Channel Convolutional Neural Network

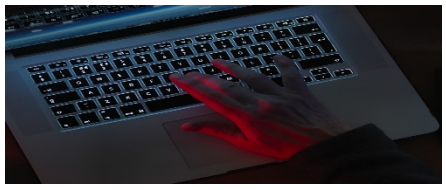
"Face recognition is a mainstream biometric authentication method. However, the vulnerability to presentation attacks (a.k.a. spoofing) limits its usability in unsupervised applications. Even though there are many methods available for tackling presentation attacks (PA), most of them fail to detect sophisticated attacks such as silicone masks. As the quality of presentation attack instruments improves over time, achieving reliable PA detection with visual spectra alone remains very challenging. We argue that analysis in multiple channels might help to address this issue. In this context, we propose a multi-channel Convolutional Neural Network-based approach for presentation attack detection (PAD)."
Source: IEEE Transactions on Information Forensics and Security

Decentralized Detection With Robust Information Privacy Protection

"We consider a decentralized detection network whose aim is to infer a public hypothesis of interest. However, the raw sensor observations also allow the fusion center to infer private hypotheses that we wish to protect. We consider the case where there are an uncountable number of private hypotheses belonging to an uncertainty set, and develop local privacy mappings at every sensor so that the sanitized sensor information minimizes the Bayes error of detecting the public hypothesis at the fusion center while achieving information privacy for all private hypotheses."
Source: IEEE Transactions on Information Forensics and Security

SAI: A Suspicion Assessment-Based Inspection Algorithm to Detect Malicious Users in Smart Grid

"Malicious users can launch cyberattacks to tamper with smart meters anytime and anywhere, mainly for the purpose of stealing electricity. This makes electricity theft much easier to commit and more difficult to detect. Researchers have devised many approaches to identify malicious users. However, these approaches suffer from either poor accuracy or expensive cost of deploying monitoring devices. This paper aims to locate malicious users



Source: Britannica ImageQuest

Asia-Pacific Network Security Market Q3 2019 Tracker

"This tracker provides an analysis of the total network security market in the Asia-Pacific region for Q3 2019 (July to September) period. Market trends such as vendor performance, vertical market splits, and enterprise-size splits are analyzed in this study."
Source: Frost & Sullivan

DDOS ATTACK

APAC Distributed Denial-of-Service Protection and Web Application Firewall Market, Forecast to 2023

"Investments into Web Application Firewall (WAF) and Distributed Denial-of-Service (DDoS) solutions in the Asia-Pacific region continued to increase during 2018, with both markets recording robust growth on a year-on-year (YoY) basis …"
Source: Frost & Sullivan

INNOVATION

Innovations in AI-, Cloud-, and Analytics-based Security

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

MOBILITY

approach

"Security by Design is a new approach to cybersecurity that builds in risk thinking from the onset, enabling global innovation with confidence."
Source: EY

SMART CITIES

Cyber security 2050: hackers to tap smart cities and deep fakes

"Growing connectivity widens scope for large-scale attacks while AI will exploit users."
Click here to register for your FT account.
Source: Financial Times

using a limited number of monitoring devices (called inspectors) within the shortest detection time."
Source: IEEE Transactions on Information Forensics and Security

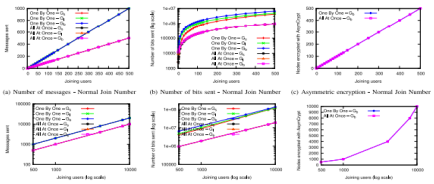
An Intrusion Detection Method for Line Current Differential Relays

"Making protective relays cyber-resilient is a prominent security issue in power networks. Line current differential relays (LCDRs) are among the potentially vulnerable digital relays that are increasingly deployed for protecting critical transmission lines. LCDRs, however, lack the required resiliency against cyber attacks, due to their high dependence on communication systems. This paper unveils that such susceptibilities can result in unwarranted trip signals through false data injection attacks (FDIAs), and so cause instability if several attacks are coordinated."
Source: IEEE Transactions on Information Forensics and Security

Heuristic-based strategy for Phishing prediction: A survey of URL-based approach

"This article focuses on phishing prediction based on a set of features. The purpose of this proposal is to evaluate the static features used and observe their occurrence in the current phishing. Static aspects refer to elements such as keywords and patterns over the phishing URL."
Source: Computers & Security

NETWORK SECURITY



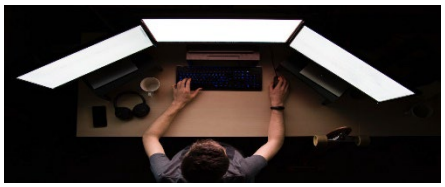
A Logical Key Hierarchy Based Approach to Preserve Content Privacy in Decentralized Online Social Networks

"Distributed Online Social Networks (DOSNs) have been proposed to shift the control over user data from a unique entity, the online social network provider, to the users of the DOSN themselves. In this paper we focus on the problem of preserving the privacy of the contents shared to large groups of users."
Source: IEEE Transactions on Dependable and Secure Computing

CYBER AWARENESS

Upstream Security's 2020 Global Automotive Cybersecurity Report

"The 2020 Global Automotive Cybersecurity report includes an in-depth analysis of the cyber threat landscape over the past ten years, with an emphasis on 2019. Upstream Security's research team has classified and analyzed hundreds of incidents to create a one-of-a-kind report that contains unique insights and statistics to help you be prepared for 2020."
Source: Upstream Security



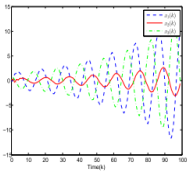
Source: Michigan State University

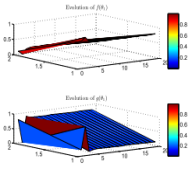
An Examination of Motivation and Routine Activity Theory to Account for Cyberattacks Against Dutch Web Sites

"This study provides a partial test of the relationship between actor motivations and target suitability using a routine activity framework to understand a form of cybercrime called web defacements. Specifically, the relationships between the visibility, inertia, value, and accessibility of the target in online spaces relative to the unique nonmonetary motivations of the attacker were examined."

Source: Criminal Justice and Behavior

DDOS ATTACK



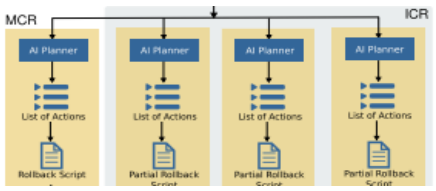


Active Defense-Based Resilient Sliding Mode Control Under Denial-of-Service Attacks

"This paper investigates the problem of the resilient control for cyber-physical systems (CPSs) in the presence of malicious sensor denial-of-service (DoS) attacks, which result in the loss of state information. The concepts of DoS frequency and DoS duration are introduced to describe the DoS attacks. According to the attack situation, that is, whether the attack is successfully implemented or not, the original physical system is rewritten as a switched version. A resilient sliding mode control scheme is designed to guarantee that the physical process is exponentially stable, which is a foundation of the main results."

Source: IEEE Transactions on Information Forensics and Security

CLOUD SECURITY



Rollback Mechanisms for Cloud Management APIs Using AI Planning

"Human-induced faults play a large role in systems reliability. In cloud

platforms, system administrators may inadvertently make catastrophic mistakes, like deleting a virtual disk with important data. Providing rollback for cloud operations can reduce the severity and impact of such mistakes, by allowing to revert to a known, good state. However, in the context of cloud management this is non-trivial, since cloud consumers only have limited visibility and indirect control. In this paper, we present a scalable approach to rollback operations that change the state of a system on proprietary cloud platforms."
Source: IEEE Transactions on Dependable and Secure Computing

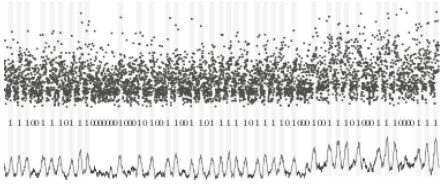
Securing Resources in Decentralized Cloud Storage

"Decentralized cloud storage services represent a promising opportunity for a different cloud market, meeting the supply and demand for IT resources of an extensive community of users. The dynamic and independent nature of the resulting infrastructure introduces security concerns that can represent a slowing factor toward the realization of such an opportunity, otherwise clearly appealing and promising for the expected economic benefits. In this paper, we present an approach enabling resource owners to effectively protect and securely delete their resources while relying on decentralized cloud services for their storage."
Source: IEEE Transactions on Information Forensics and Security

Hypervisor-based cloud intrusion detection through online multivariate statistical change tracking

"Cloud computing is facing a multidimensional and rapidly evolving threat landscape, making intrusion detection more challenging. This paper introduces a new hypervisor-based cloud intrusion detection system (IDS) that uses online multivariate statistical change analysis to detect anomalous network behaviors."
Source: Computers & Security

MALWARE



Malware Guard Extension: abusing Intel SGX to conceal cache attacks

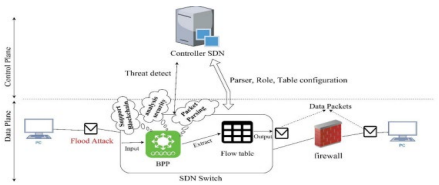
"In a cloud scenario it is crucial that

the hypervisor isolates tenants from other tenants that are co-located on the same physical machine. However, the hypervisor does not protect tenants against the cloud provider and thus, the supplied operating system and hardware. Intel SGX provides a mechanism that addresses this scenario. It aims at protecting user-level software from attacks from other processes, the operating system, and even physical attackers.In this paper, we demonstrate fine-grained software-based side-channel attacks from a malicious SGX enclave targeting co-located enclaves."
Source: Cybersecurity

An emerging threat Fileless malware: a survey and research challenges

"The fileless malware attack is catastrophic for any enterprise because of its persistence, and power to evade any anti-virus solutions. The malware leverages the power of operating systems, trusted tools to accomplish its malicious intent. To analyze such malware, security professionals use forensic tools to trace the attacker, whereas the attacker might use anti-forensics tools to erase their traces. This survey makes a comprehensive analysis of fileless malware and their detection techniques that are available in the literature."
Source: Cybersecurity

BLOCKCHAIN



P4-to-blockchain: A secure blockchain-enabled packet parser for software defined networking

"In this paper, we propose a new packet parser architecture called Blockchain-enabled Packet Parser (BPP) based on the security characteristics of the blockchain and support for data processing functions with the description of Programming Protocol-Independent Packet Processors (P4) language that has the BPP-independent attribute of the protocol. In the proposed architecture, we provide a mathematical model based on a multivariate correlation approach for attack detection from the observed packet traffic."
Source: Computers & Security