SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN

22 April to 16 June 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

UPDATE

Multifactor Authentication: The Next Battleground

"X-Force Incident Response and Intelligence Services (IRIS) has responded to multiple security incidents where multifactor authentication (MFA) was not implemented—but where implementing MFA might have significantly reduced the impact of the incident."
Source: Security Intelligence

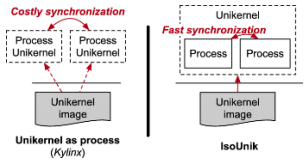
Shift Your Cybersecurity Mindset to Maintain Cyber Resilience

"As the business world navigates the ups and downs of today's economy, a mindset shift is required to maintain cyber resilience. Cybersecurity, often an afterthought in a strong economy, must not be neglected in responding to shifts in the business landscape."
Source: Security Intelligence

Are Current Security Assurance Models Suitable for the Digital World?

"With the constantly transforming cyber landscape, intruders are always finding new ways to exploit weaknesses in organizations' systems and applications. As a result, cyber-related incidents have become one of the top risks to businesses as they

CLOUD



Iso-UniK: lightweight multi-process unikernel through memory protection keys

"Unikernel, specializing a minimalistic libOS with an application, is an attractive design for cloud computing. However, the Achilles' heel of unikernel is the lack of multi-process support, which makes it less flexible and applicable."
Source: Cybersecurity

Multi-dimensional dynamic trust evaluation scheme for cloud environment

"In cloud computing environment, Cloud Customers (CCs) and Cloud Service Providers (CSPs) require to evaluate the trust levels of potential partner prior to appealing in communications. The accurateness of trust evaluation significantly influences the success velocity of the communication."
Source: Computers & Security

Moving target defense in cloud computing: A systematic mapping study

"Moving Target Defense (MTD) consists of applying system reconfiguration (e.g., VM migration, IP shuffling) to dynamically change the available attack surface. MTD makes use of reconfiguration to confuse attackers and nullify their

INDUSTRY INSIGHTS

Post-Pandemic Growth Opportunity in the Global Security Industry

"This research service discusses how security companies can maintain operations and serve customers throughout the crisis; it also analyzes how they will have to adapt to the new normal, which will make its presence felt when the major effects of COVID-19 have passed.."
Source: Frost & Sullivan

Zero Trust—What is it and How to Implement?

"The Frost & Sullivan report presents the concept of Zero Trust Architecture and best practices for CISOs."
Source: Frost & Sullivan

Threat Intelligence Executive Report 2020: Vol. 3

"Review the events and trends from the information security world from March through April 2020."
Source: SecureWorks

FROST RADAR™: Global Web Security Market, 2020

"The Frost Radar™ in the global web security market is an analytical publication that reveals the competitive positioning of 15 web security vendors. The companies' positioning on the Frost Radar™ is

attempt to understand their cyber resilience and exposure to threats.."
Source: Security Intelligence

What the Data Is Telling Us About the Current Rise in Security Threats During the COVID-19 Pandemic

"Cybercriminals, who are notorious for riding trending news and emerging issues, have been watching matters unfold and developing their attacks in context with a large variety of updates and initiatives lined with the current pandemic."
Source: Security Intelligence

WORK FROM HOME

IT Security Specialists Weigh in on the Cyber Strategies of Working at Home

"Consideration of the cyber risks of remote work is nothing new for company IT security professionals. For years, they've advised teleworkers on how to reduce the risk of a cyberattack targeting the corporate IT network from their homes. Never did they expect, however, the mass shift to teleworking nearly overnight."
Source: Dell Technologies

Global VPN use exploded in March

"The VPN market was forecast to grow, even before COVID-19 caused VPN use to skyrocket."
Source: NETWORKEDWORLD

UPDATE 4-28: How enterprise networking is changing with a work-at-home workforce

"Network World updates the latest COVID-19-related networking news "
Source: NETWORKWORLD

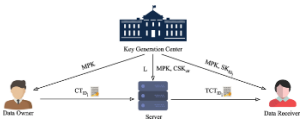
Cyber Threats Rise at Home: An Interview With Tom Kellermann

"As millions of people work from home to reduce the possibility of becoming infected with (and spreading) the coronavirus, they inadvertently increase the risk of a cyberattack targeting their company's IT network and systems."
Source: Dell Technologies

CLOUD

knowledge about the system state."
Source: Computers & Security

IDENTITY VERIFICATION



Server-aided immediate and robust user revocation mechanism for SM9

"As the only approved Identity-Based Encryption scheme in China that is also standardized by ISO, SM9-IBE has been widely adopted in many real-world applications. However, similar to other IBE standard algorithms, SM9-IBE currently lacks revocation mechanism, which is vital for a real system."
Source: Cybersecurity

GTM-CSec: Game theoretic model for cloud security based on IDS and honeypot

"Cloud Computing has been adopted by many leading organizations for storage, processing, sharing and to provide other services. It faces several security challenges from its surroundings in terms of regular and sophisticated attacks... in this paper, a game-theoretic model GTM-CSec has been proposed. The proposed model intelligently selects the most suitable module out of the signature, anomaly, and honeypot based detection to detect the attack."
Source: Computers & Security

REVIEW

Cyber risk at the edge: current and future trends on cyber risk analytics and artificial intelligence in the industrial internet of things and industry 4.0 supply chains

"Digital technologies have changed the way supply chain operations are structured. In this article, we conduct systematic syntheses of literature on the impact of new technologies on supply chains and the related cyber risks."
Source: Cybersecurity

A review and theoretical explanation of the 'Cyberthreat-Intelligence (CTI) capability' that needs to be fostered in information security

determined by their Growth and Innovation scores. Several factors differentiate them from the competition."
Source: Frost & Sullivan

Innovations in Threat Intelligence, Web Security, and IoT Security

"This Cyber Security Technology Opportunity Engine (TOE) provides a snapshot on emerging cyber security solutions powered by cloud, IoT, and artificial intelligence-based 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

FROST RADAR™: Global Transport Layer Security Certificate Market, 2020

"Amid the chaos of the World Wide Web, ensuring brand identity and consumer data protection is of paramount importance to businesses. Digitization of consumer transactions demands heightened security to protect confidential data."
Source: Frost & Sullivan

Global Demand for Biometrics in Security, Forecast to 2025

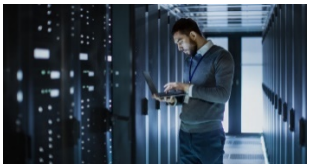
"This study will benefit those who are interested in learning about how the access control and identity market is impacted by biometrics technology, how biometrics is evolving in the security industry, and the potential opportunities in this space."
Source: Frost & Sullivan

North America; New Product Innovation Award - IoT Security

"Founded in 2003 in Alpharetta, Georgia, KORE Wireless provides industry-leading IoT security solutions for customers across industries, e.g., healthcare, life sciences, asset management, fleet management, and industrial IoT. By leveraging its industry-specific security expertise and technology, KORE Wireless delivers proven, seamless security services that have fostered strong customer loyalty."
Source: Frost & Sullivan

Asia-Pacific Network Security Market Q4 2019 Tracker

"The APAC network security market saw a 11.4% growth in Q4 2019. The market is being driven mostly by the firewall segment which grew 14.0%. Top-three revenue contributors remain education, government, and BFSI sectors, with a combined



The Connection Between Cloud Service Providers and Cyber Resilience

"Organizations in both the private and public sectors have increasingly turned to cloud service providers (CSPs) to support their technical infrastructure, primarily to reduce IT costs and increase the efficiency of computing resources. In many cases, CSPs can also offer protection from security threats and increased cyber resilience — though customers often face trade-offs when they rely on cloud providers for these protections."
Source: Security Intelligence

How Threat Actors Are Adapting to the Cloud

"With organizations increasingly moving to cloud environments, cloud security is more critical than ever. Cloud environments often hold large troves of valuable and sensitive data that can put organizations and their customers at risk if they are breached."
Source: Security Intelligence

Use of cloud collaboration tools surges and so do attacks

"Some industries have seen increases in cloud-related threat events rise as much as 1,350% since the COVID-19 crisis began.."
Source: CSO

TRICKBOT

Trickbot Using BazarBackdoor to Gain Full Access to Targeted Networks

"Security researchers observed the Trickbot operators using a new backdoor called "BazarBackdoor" to gain full access to targeted networks."
Source: Security Intelligence

Trickbot Replaces 'Mworm' Propagation Method With New 'Nworm' Module

"In April 2020, Palo Alto Networks' Unit 42 observed Trickbot deploy its new propagation method during an attack on a laboratory environment in which the malware produced nworm on an infected Windows 7 client. Via the use of a Server

practitioners and how this can be accomplished

"Given the global increase in crippling cyberattacks, organizations are increasingly turning to cyberthreat intelligence (CTI).."
Source: Computers & Security

APT datasets and attack modeling for automated detection methods: A review

"This paper provides a review on datasets and their creation for use in APT detection in literature. A special focus is placed on feature engineering, including construction, selection and dimensionality reduction."
Source: Computers & Security

THREAT DETECTION & PREDICTION

Conceptualisation of Cyberattack prediction with deep learning

"The state of the cyberspace portends uncertainty for the future Internet and its accelerated number of users. New paradigms add more concerns with big data collected through device sensors divulging large amounts of information, which can be used for targeted attacks."
Source: Cybersecurity

A comprehensive security assessment framework for software-defined networks

"As Software-Defined Networking (SDN) is getting popular, its security issue is being magnified as a new controversy, and this trend can be found from recent studies of presenting possible security vulnerabilities in SDN.."
Source: Computers & Security

Dynamic facial presentation attack detection for automated border control systems

"Millions of passengers travel every day, border crossing being one of their most common activities. At these points it is extremely important that security is completely guaranteed. However, the maintaining adequate security levels is a very demanding issue."
Source: Computers & Security

Machine Learning Cyberattack and Defense

contribution of 63.3% of market share. Healthcare, government, and manufacturing were the top growing verticals in Q4 2019, registering strong double-digit YoY growth."
Source: Frost & Sullivan

FROST RADAR™: 2020 INNOVATION EXCELLENCE AWARD - Global Web Security Market

"In a field of 30+ global industry participants, Frost & Sullivan has independently ranked the top 15 companies in the above Frost Radar™ analysis."
Source: Frost & Sullivan

Global Managed Detection and Response Market, Forecast to 2024

"The managed detection and response (MDR) market generated $893.8 million in 2019; it is set to grow at a CAGR of 16.4% and reach $1,907.9 million by 2024.."
Source: Frost & Sullivan

Modernizing SecOps With Software-Driven Detection and Investigation (WEBCAST)

"Learn how cloud-native software is transforming security."
Source: Secure Works

Making Sense of MITRE ATT&CK Evaluations to Address Your Cybersecurity Needs (WEBCAST)

"Get a better understanding of the MITRE ATT&CK Framework and evaluations, including our perspective and results as a recent participant."
Source: Secure Works

Modernizing SecOps With Software-Driven Detection and Investigation (WEBCAST)

"The security landscape is more complex than ever. Cybersecurity professionals are challenged by threat detection and response. As organizations confront resource constraints, how can they stay ahead of unknown and emerging cyber threats?."
Source: Secure Works

AWARDS

Europe; Technology Innovation Award - Behavioral Cyber Threat Detection

Message Block (SMB) exploit, the method helped Trickbot move to a Windows domain controller (DC)."
Source: Security Intelligence

TrickBot Campaigns Targeting Users via Department of Labor FMLA Spam

"IBM X-Force monitors billions of spam emails a year, mapping trending, malicious campaigns and their origins. Recent analysis from our spam traps uncovered a new Trickbot campaign that currently targets email recipients with fake messages purporting to come from the U.S. Department of Labor (DoL)."
Source: Security Intelligence

PERSONAL DEVICES

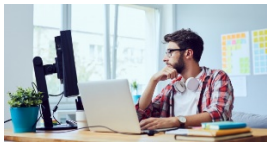
The Latest Mobile Security Threats and How to Prevent Them

"For many of us, the last few months have drastically increased our reliance on mobile capabilities. Through the increased use of corporate mobile apps, virtual private networks (VPNs), hot spots and more, mobile communications are more ubiquitous than ever."
Source: Security Intelligence

Managed Data Activity Monitoring (DAM) Is More Important Than Ever

"he transition to a remote workforce has happened so quickly that many security teams have not had an opportunity to apply desired controls. Organizations are dealing with remote access and execution privileges that were unplanned even a couple of months ago. The use of personal devices and home workspaces has increased potential risks."
Source: Security Intelligence

ZERO TRUST



How Zero Trust Will Change Your Security Design Approach

"Zero Trust is not an architectural model but rather a set of guiding principles that should be applied to existing and new designs. With that said, these principles present a

Strategies

"Cybersecurity is an increasingly important challenge for computer systems. In this work, cyberattacks were modeled using an extension of the well-known Petri net formalism."
Source: Computers & Security

A vulnerability analysis and prediction framework

"In this paper, we propose an integrated data mining framework to automatically describe how vulnerabilities develop over time and detect the evolution of a specific vulnerability. Additionally, our framework has a predictive functionality that can be used to predict specific vulnerabilities or to estimate future appearance probabilities of vulnerability groups."
Source: Computers & Security

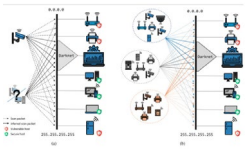
Featureless Discovery of Correlated and False Intrusion Alerts

"Malware and cyber-attacks cause substantial damage to corporations. A common countermeasure is Intrusion Detection Systems (IDSs). Unfortunately, IDSs typically raise many alerts on a single incident, with redundant information, and false alerts that are only noise to analysts."
Source: Emerging Approaches to Cyber Security

Software Vulnerability Detection Using Deep Neural Networks: A Survey

"In this survey, we review the current literature adopting deep-learning-/neural-network-based approaches for detecting software vulnerabilities, aiming at investigating how the state-of-the-art research leverages neural techniques for learning and understanding code semantics to facilitate vulnerability discovery. We also identify the challenges in this new field and share our views of potential research directions."
Source: Proceedings of the IEEE

IOT



On data-driven curation, learning, and analysis for inferring evolving internet-of-Things (IoT) botnets in the wild

"The insecurity of the Internet-of-Things (IoT) paradigm continues to wreak havoc in consumer and critical infrastructures. The highly heterogeneous nature of IoT devices and their widespread deployments

"Founded in 2017 and headquartered in the Netherlands, ReaQta emerged intending to change the landscape of threat intelligence and detection capabilities for all industry sectors."
Source: Frost & Sullivan

Europe; Product Leadership Award - ICS Security for the Energy Industry

"Industrial cybersecurity (ICS) has now become a top priority for companies in the energy industry, and companies want products dedicated to their specific sector as well as comprehensive intelligence, unbiased consulting, and advisory services."
Source: Frost & Sullivan

Industry Guide to Cloud Workload Security in Asia-Pacific

"The awareness of cloud security has significantly improved among businesses, largely driven by industry regulations and in-country cybersecurity laws. Many businesses state that security and privacy are their biggest concerns when moving to the cloud."
Source: Frost & Sullivan

North America; Technology Innovation Award - Secure Data Access Solution for the Hybrid IT Infrastructure Industry

"Founded in 2011, Ionic Security Inc, an Atlanta-based start-up, has developed an innovative data and resource access protection engine called Ionic Machina that completely secures enterprise access across legacy in-house and cloud-based infrastructure. Machina serves as a unified service layer for securing and enforcing access policy across traditional data silos."
Source: Frost & Sullivan

SECURITY SERVICES MARKET

Indian Managed Security Services Market, Forecast to 2023

"The Indian managed security services (MSS) market is witnessing an increase in MSS adoption due to the trend of widespread digitization and increasingly pervasive cyber threats. Following the continuation of the 'Digital India' initiative while remaining cyber-safe, the Indian

number of architectural patterns or use cases that can serve as a starting point for implementation."
Source: Security Intelligence

It's Time to Take a Fresh Look at Zero Trust

"With millions of employees across the U.S. experimenting with work-at-home scenarios for the first time, many organizations are taking a fresh look at a Zero Trust security strategy."
Source: Security Intelligence

When Implementing Zero Trust, Context Is Everything

"Context is an essential element in everything we do. Context is what helps us make decisions…The combination of information provides the context required to make a decision.."
Source: Security Intelligence

AI

Measuring the Effectiveness of AI in the SOC

"According to ISACA's State of Cybersecurity Report, 78 percent of respondents expect the demand for technical cybersecurity roles to increase in the future. The report also mentions that the effects of the skills shortage are going to get worse…This is where AI can step in and help lighten the load considerably."
Source: Security Intelligence

How Chatbots Can Help Bridge Business Continuity and Cybersecurity

"A quick web search for "chatbots and security" brings up results warning you about the security risks of using these virtual agents. Dig a little deeper, however, and you'll find that this artificial intelligence (AI) technology could actually help address many work-from-home cybersecurity challenges — such as secure end-to-end encryption and user authentication — and ensure that your organization continues to prove its data privacy compliance with less direct oversight."
Source: Security Intelligence

has led to the rise of several key security and measurement-based challenges, significantly crippling the process of collecting, analyzing and correlating IoT-centric data."
Source: Computers & Security

An integrity verification scheme of cloud storage for internet-of-things mobile terminal devices

"Because mobile cloud computing has many advantages such as large storage capacity, low cost and scalability, most data owners prefer to store their data on cloud servers to share with other users. However, the shared data in remote cloud servers is out of data owner's control and exposes to lots of security problems such as data integrity."
Source: Computers & Security

On the Implementation of IoT-Based Digital Twin for Networked Microgrids Resiliency Against Cyber Attacks

"This paper provides an IoT-based digital twin (DT) of the cyber-physical system that interacts with the control system to ensure its proper operation. The IoT cloud provision of the energy cyber-physical and the DT are mathematically formulated."
Source: IEEE Transactions on Smart Grid

Deep Transfer Learning for IoT Attack Detection

"In this paper, we propose a novel deep transfer learning (DTL) method that allows to learn from data collected from multiple IoT devices in which not all of them are labeled. Specifically, we develop a DTL model based on two AutoEncoders (AEs)."
Source: IEEE Access

Blockchain for Cybersecurity: A Comprehensive Survey

"This paper provides the blockchain architecture and explains the concept, characteristics, need of Blockchain in Security, how Bitcoin works and to enhance the security in the field of IoT."
Source: 2020 IEEE 9th International Conference on Communication Systems and Network Technologies (CSNT)

Towards Blockchain-Based Architecture for Smart Cities Cyber-Security

"In this work, we analyze the applicability of the Blockchain to ensure the security of the data transmitted and received by the nodes of an IoT network. The purpose of this article is to integrate the Blockchain with IoT to create a secure decentralized architecture to

government introduced the Personal Data Protection Bill in 2019 to better protect the privacy of personal data and regulate its usage."
Source: Frost & Sullivan

ASEAN Managed Security Services Market, Forecast to 2023

"Market trends are analyzed from 2017 to 2023, taking 2018 as the base year. MSS is the key focus area of this study. The vertical segmentation includes government; banking, financial services, and insurance (BFSI); service provider; manufacturing; education; and other sectors (including pharmaceuticals, retail, logistics, oil and gas, energy, mining, agriculture, IT/ITES, eGaming, eCommerce, and BPOs)."
Source: Frost & Sullivan

Japanese Managed Security Services Market, Forecast to 2023

"There were several key market drivers in 2018: increased general information technology (IT) investment in Japanese enterprises for the 2020 Tokyo Olympic Games; Japanese enterprise spending shifting to an 'as a service' instead of 'on-premise' model (despite on-premise being the major revenue contributor); lack of security expertise among the internal IT teams."
Source: Frost & Sullivan

Greater China Managed Security Services Market, Forecast to 2023

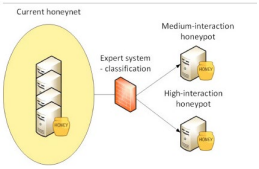
"Cybersecurity compliance and guidance are key initiatives driving the Greater China managed security services (MSS) market. Local governments have placed more emphasis on cybersecurity, thereby raising awareness among both public and private sector enterprises in the region. In the face of tightening regulations, enterprises are increasingly seeking external support to meet the specified requirements and improve their cyber resilience."
Source: Frost & Sullivan

Asia-Pacific Managed Security Services Market, Forecast to 2023

"MSS growth is also driven largely by the lack of skilled cyber professionals in the APAC region. While many large enterprises have set up their own Security Operations Centers (SOCs), they do not have the manpower to staff these centers to their optimal capacity. Small and medium businesses (SMBs) do not usually have the financial leeway for

provide a secure communication platform in a smart city."
Source: 2020 International Conference on Electrical and Information Technologies (ICEIT)

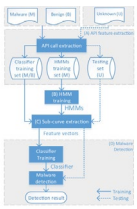
EXPERT SYSTEM



Expert system assessing threat level of attacks on a hybrid SSH honeynet

"This article first analyses the current situation followed by presenting a solution in the form of a system made up of a hybrid honeynet and an expert system. For now, it focuses only on the SSH protocol, as it is widely used for remote system access and is a popular target of attacks."
Source: Computers & Security

MALWARE



Sub-curve HMM: A malware detection approach based on partial analysis of API call sequences

"Malicious software (Malware) plays an important role in penetrating and extracting sensitive information. Based on dynamic program's behavior monitoring, existing solutions have shown that the Hidden Markov Model (HMM) is efficient in detecting malware using sequences of API calls."
Source: Computers & Security

A dynamic Windows malware detection and prediction method based on contextual understanding of API call sequence

"In this paper, we introduce the use of word embedding to understand the contextual relationship that exists between API functions in malware call sequences. We also propose a method that segregating individual functions that have similar contextual traits into clusters.."
Source: Computers & Security

On the use of artificial malicious patterns for android malware detection

"Actually, malware developers this and are thus more reliant on outsourcing their cybersecurity management and operations."
Source: Frost & Sullivan

Indian Managed Security Services (MSS) Industry Outlook, 2020

"This research service analyzes the current state of MSS in India. During the research process, the impact of COVID-19 has been factored in to estimate the market size in 2020 and thereafter. With an aim to provide the readers a comprehensive understanding of the market (current and future), a well-tested step-by-step research methodology has been followed, which is an ideal mix of primary and secondary research."
Source: Frost & Sullivan

South Korean Managed Security Services Market, Forecast to 2023

"The South Korean managed security services (MSS) market is mainly categorized into 2 service types: dispatch professionals to customer sites and monitoring from security operations centers (SOCs). Customer requests for a hybrid of both service types have increased with the growing adoption of security information and event management (SIEM) at the customer site. The lack of professionals to analyze internal log has been the main factor driving this request.."
Source: Frost & Sullivan

usually use obfuscation techniques consisting in a set of transformations that make the code and/or its execution difficult to analyze by hindering both manual and automated inspections. These techniques allow the malware to escape the detection tools, and hence to be seen as a benign program. To solve the obfuscation issue, many researchers have proposed to extract frequent Application Programming Interface (API) call sequences from previously encountered malware programs using pattern mining techniques and hence, build a base of fraudulent behaviors."
Source: Computers & Security

Byte-level malware classification based on markov images and deep learning

"this paper proposes a byte-level malware classification method based on markov images and deep learning referred to as MDMC. The main step in MDMC is converting malware binaries into markov images according to bytes transfer probability matrixs. Then the deep convolutional neural network is used for markov images classification."
Source: Computers & Security

A Preliminary View on Automotive Cyber Security Management Systems

"Cyber security is increasingly recognized as an essential topic for automotive systems, especially in the area of connected and automated driving. Upcoming regulation defines requirements for cyber security on multiple levels in the automotive domain in order to achieve type approval."
Source: Computers & Security

An SUTD Library Service©2020