SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN

10 March - 21 April 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

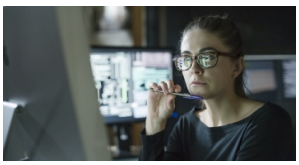
WOMEN IN CYBERSECURITY

Meet the women in IBM Research securing your digital future

"This is our fifth and final blog post in a series for Women's History Month 2020 focused on women innovating the future of IBM Research…They're developing technologies that promise to transform entire industries, from medicine to mobility, and solve our thorniest problems. And yet the tremendous power of digital technology also introduces risk. If it's hacked, or falls into the wrong hands, it can be used against us. That's why security research is indispensable. And the four women we meet here represent every aspect of it, from blockchain and open source defense to erecting cloud-based fortifications around digital crown jewels.."

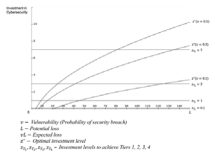
Source: IBM

SECURITY



academic

STANDARDS



Integrating cost–benefit analysis into the NIST Cybersecurity Framework via the Gordon–Loeb Model

"Distinguished Professor Alan Mantooth of the University of Arkansas received a $3.6 million award from the U.S. Department of Energy Solar Energy Technologies Office to advance technologies that integrate solar power systems to the national power grid."

Source: Journal of Cybersecurity

Nudging personalized password policies by understanding users' personality

"Password composition policies are used to prevent users from picking weak passwords. A website usually provides a unified password policy for each user but ignores the fact that people have a variety of preferences due to individual differences, which makes it difficult to achieve the expected strong password goals. In order to improve the effectiveness of password composition policies, we propose a dynamic personalized password

reports

REVIEW

Threat Roundup for April 10 to April 17

"Talos is publishing a glimpse into the most prevalent threats we've observed between April 10 and April 17. As with previous roundups, this post isn't meant to be an in-depth analysis. Instead, this post will summarize the threats we've observed by highlighting key behavioral characteristics, indicators of compromise, and discussing how our customers are automatically protected from these threats."

Source: CISCO

INDUSTRY INSIGHTS

Global; Product Leadership Award - IoT Cybersecurity

"Frost & Sullivan predicts that the overall number of IoT devices will steadily increase from approximately 30 million devices in 2020 to around

TA505 Continues to Infect Networks With SDBbot RAT

"

IBM X-Force Incident Response and Intelligence Services (IRIS) responds to security incidents around the globe. During analysis and comparison of malicious activity on enterprise networks, our team identified attacks likely linked to Hive0065, also known as TA505. We observed that Hive0065 continues to spread the SDBbot remote-access Trojan (RAT) alongside other custom malware and continues to display tactics used against companies within the past year."
Source: Security Intelligence

APT41 Distributing Speculoos Backdoor in New Attack Campaign

"Security researchers discovered an attack campaign in which APT41 distributed the Speculoos backdoor by exploiting CVE-2019-19781.."
Source: Security Intelligence

Promising Results for Post-Quantum Certificates in TLS 1.3

"Quantum Computers could threaten the security of TLS key exchange and authentication. To assess the performance of post-quantum certificates TLS 1.3, we evaluated NIST Round 2 signature algorithms and concluded that two of them offer acceptable speeds. We also analyzed other implications of post-quantum certs in TLS."
Source: CISCO

ITG08 (aka FIN6) Partners With TrickBot Gang, Uses Anchor Framework

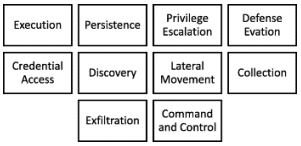
"The past two years have borne witness to the increasing collaboration between organized cybercrime groups to avoid duplication of efforts and maximize profits...In a new and dangerous twist to this trend, IBM X-Force Incident Response and Intelligence Services (IRIS) research believes that the elite cybercriminal threat actor ITG08, also known as FIN6, has partnered with the malware gang behind one of the most active Trojans — TrickBot — to use TrickBot's new malware framework dubbed "Anchor" against organizations for financial profit..."
Source: Security Intelligence

policy (DPPP), which can personally recommend different password policies according to the user's personality traits."
Source: Computers & Security

Optimal Filter Assignment Policy Against Distributed Denial-of-Service Attack

"In this paper, we propose a DDoS attack protection system by using the filter router. The victim needs to wisely select and send filters to a subset of filter routers to minimize attack traffic and blockage of legitimate users (LUs). Many filters can minimize the attack traffic and blockage of LUs easily, but it is costly to the victim. So, we formulate two problems with different settings for selecting filter routers given a constraint on the number of filters. We propose a dynamic programming solution for both problems. Both problems consider the blockage of all attack traffic before it reaches the victim. We conduct extensive simulation to support our solutions."
Source: IEEE Transactions on Dependable and Secure Computing

RULE OF LAW



Under false flag: using technical artifacts for cyber attack attribution

"The attribution of cyber attacks is often neglected. The consensus still is that little can be done to prosecute the perpetrators – and unfortunately, this might be right in many cases. What is however only of limited interest for the private industry is in the center of interest for nation states... In this paper we provide an overview of prominent attack techniques along the cyber kill chain. We investigate traces left by attack techniques and which questions in course of the attribution process are answered by investigating these traces. Eventually, we assess how easily traces can be spoofed and rate their relevancy with respect to identifying false flag campaigns.."
Source: Journal of Cybersecurity

THREAT DETECTION & PREDICTION

50 billion devices in 2023, at a global compound annual growth rate of 17.2%, with building automation and security systems responsible for over 50% of all IoT devices within this period.1 However, the promise of IoT cannot be realized unless the market addresses emerging threats presented by the increased interconnectedness between users, devices, and systems."
Source: Frost & Sullivan

Israel; Product Leadership Award - Mobile Cybersecurity Solutions

"Founded in 2016 and headquartered in Israel, FirstPoint Mobile Guard (FirstPoint) began with a vision of providing comprehensive solutions tailored to cellular cyber protection. FirstPoint set out to deliver cutting-edge solutions that identify mobile communication privacy issues ranging from smart devices to the most basic operating systems or even very simple devices with no operating system at all. The company recognized the growing threat from hacker groups, business competitors and state-sponsored attacks; with the knowledge of how and when attacks occur, FirstPoint pinpointed the need to protect the people and critical devices of the world from malicious attacks.."
Source: Frost & Sullivan

North America; Technology Innovation Award - ICS Cybersecurity Solution

"Founded in 1994, Verve Industrial Protection (Verve) leverages its background in control systems engineering to develop game-changing ICS cybersecurity solutions. The company serves clients globally in the chemical, industrial, manufacturing, pharmaceutical, and utilities industries to protect their IIoT systems against the ever-evolving hacker model. Frost & Sullivan recognized Verve as the 2018 North America Growth Excellence Leader in the industrial cybersecurity market and remains impressed with the company's continuing innovation, customer-centric design, and exceptional ICS cybersecurity solutions and services."
Source: Frost & Sullivan

Europe; Technology

The CSO guide to top security conferences, 2020

"Tracking postponements, cancellations, and conferences gone virtual — CSO Online's calendar of upcoming security conferences makes it easy to find the events that matter the most to you."
Source: CSO

Breaking the Ice: A Deep Dive Into the IcedID Banking Trojan's New Major Version Release

"This post will delve into the technical details of IcedID version 12 (0xC in hexadecimal). Before we delve into the technical details, here are the components that saw changes applied in this new version... In this post, you will also find information on IcedID's naming algorithms that are used for creating names for its various files, events, and resources. We also mention how to find and extract the malware's internal version number."
Source: Security Intelligence

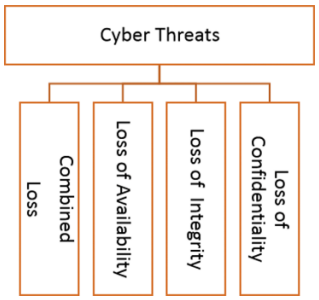
You Can Now Check If Your ISP Uses Basic Security Measures

"FOR MORE THAN an hour at the beginning of April, major sites like Google and Facebook sputtered for large swaths of people. The culprit wasn't a hack or a bug. It was problems with the internet data routing standard known as the Border Gateway Protocol, which had allowed significant amounts of web traffic to take an unexpected detour through a Russian telecom. For Cloudflare CEO Matthew Prince, it was the last straw."
Source: Wired

Google enters zero-trust market with BeyondCorp Remote Access offering

"Google is launching a commercial zero-trust remote access service that will allow companies to enable their work-from-home employees to access internal web-based applications without the need of virtual private networks (VPNs)"
Source: CSO

Google enters zero-trust market with BeyondCorp



Review and insight on the behavioral aspects of cybersecurity

"Stories of cyber attacks are becoming a routine in which cyber attackers show new levels of intention by sophisticated attacks on networks. Unfortunately, cybercriminals have figured out profitable business models and they take advantage of the online anonymity. A serious situation that needs to improve for networks' defenders. Therefore, a paradigm shift is essential to the effectiveness of current techniques and practices. Since the majority of cyber incidents are human enabled, this shift requires expanding research to underexplored areas such as behavioral aspects of cybersecurity."
Source: Cybersecurity

Predicting individuals' vulnerability to social engineering in social networks

"The popularity of social networking sites has attracted billions of users to engage and share their information on these networks. The vast amount of circulating data and information expose these networks to several security risks... Identifying the most vulnerable users in order to target them for these training programs is desirable for increasing the effectiveness of such programs. 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

Process-Aware Model-based Intrusion Detection System on Filtering Approach: Further Investigations

"Based on the S.A.F.E. approach, this

Innovation Award - Behavioral Cyber Threat Detection

"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. The company strives to strengthen organizations with robust cybersecurity solutions. The company's cutting-edge cybersecurity solution, ReaQta-Hive, alleviates the complexity of infrastructure analyses, eliminating the need for additional highly skilled personnel. ReaQta's innovative approach applies artificial intelligence (AI) algorithms to automate and simplify the complete process of detecting and handling new threats."
Source: Frost & Sullivan

Global; Enabling Technology Leadership Award - Endpoint Security Industry

"The complexity and volume of cyber threats continue to mount. For businesses of all sizes, this is a serious problem. The legitimate communication channel they rely on extensively, email, is also the channel-of-choice for delivering malware. Email is still the number one threat vector, and web-borne threats encountered though normal business use of the Internet is the second major threat vector. Combined, these threat vectors are serious avenues of attack on endpoints."
Source: Frost & Sullivan

THREAT DETECTION & PREDICTION

Detect and Stop Advanced Threats Faster to Reduce Security Risk

"As cyber adversaries become more sophisticated, organizations are forced to constantly upgrade their security operations in order to stay a few steps ahead."
Source: Secure Works

Threat Intelligence Executive Report 2020: Vol. 1

"The Secureworks® Counter Threat Unit™ (CTU) research team analyzes security threats and helps organizations protect their systems.

Remote Access offering

"Google is launching a commercial zero-trust remote access service that will allow companies to enable their work-from-home employees to access internal web-based applications without the need of virtual private networks (VPNs)"
Source: CSO

COVID-19

IBM X-Force Threat Intelligence Cybersecurity Brief: Novel Coronavirus (COVID-19)

"Global events such as the novel coronavirus (COVID-19) make all of us attractive targets for cybercriminals. Whether it's phishing emails or new targeted scams, these tactics are meant to take advantage of citizens who are understandably concerned about their health and safety during this challenging time.."
Source: Security Intelligence

9 Best Practices from X-Force Red for Organizations and Employees

"As employers rapidly respond to the need to protect their workforces from potential exposure and spread of the novel coronavirus, also known as COVID-19, many organizations are making the very difficult decision to pivot to a work-from-home model. This means employees will be connecting to corporate networks from whichever device is available: laptops, phones, tablets and even smart watches."
Source: Security Intelligence

IoT

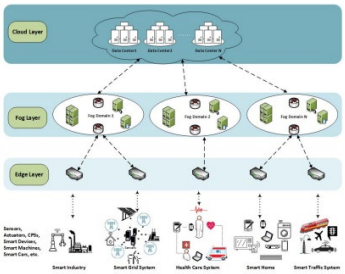
Lock Down Personal Smart Devices to Improve Enterprise IoT Security

"The presence of internet of things (IoT) devices in employee's homes is paper proposes its improvement and novel contributions: a report filter modelling, optimization algorithms for speeding up the computation of the detection indicators and an implementation on a real testbed."
Source: 2020 IEEE International Conference on Industrial Technology (ICIT)

Designing Heavy-Hitter Detection Algorithms for Programmable Switches

"We introduce PRECISION, an algorithm that uses Partial Recirculation to find top flows on a programmable switch. By recirculating a small fraction of packets, PRECISION simplifies the access to stateful memory to conform with RMT limitations and achieves higher accuracy than previous heavy hitter detection algorithms that avoid recirculation. We also evaluate each of the adaptations made by PRECISION and analyze its effect on the measurement accuracy.."
Source: IEEE/ACM Transactions on Networking

IOT SECURITY



Fog-based Attack Detection Framework for Internet of Things Using Deep Learning

"This paper presents a comprehensive attack detection framework of a distributed, robust, and high detection rate to detect several IoT cyber-attacks using DL. The proposed framework implements an attack detector on fog nodes because of its distributed nature, high computational capacity and proximity to edge devices. Six DL models are compared to identify the DL model with the best performance."
Source: IEEE Access

Security Experiences in IoT based applications for Building and Factory Automation

"…this article studies possible security threats and weakness in two case During November and December 2019, CTU™ researchers identified lessons learned and observed notable developments in threat behaviors, the global threat landscape and security trends:."
Source: Secure Works

a neglected item in many enterprise threat models. Caution is certainly warranted here, but it's entirely possible to improve your risk awareness and secure smart devices in a calm and measured way."
Source: Security Intelligence

In 2020, IoT Security Must Be Part of Your Threat Management Strategy

"Internet-enabled devices are emerging more and more in business and personal environments. Often going unnoticed, they simply appear within network infrastructures, using wired or wireless connections and expanding the enterprise attack surface."
Source: Security Intelligence

How microsegmentation architectures differ

"Internet-enabled devices are emerging more and more in business and personal environments. Often going unnoticed, they simply appear within network infrastructures, using wired or wireless connections and expanding the enterprise attack surface."
Source: Security Intelligence

SOLUTIONS

UPDATE 4-18: How enterprise networking is changing with a work-at-home workforce

"Internet-enabled devices are emerging more and more in business and personal environments. Often going unnoticed, they simply appear within network infrastructures, using wired or wireless connections and expanding the enterprise attack surface."
Source: Network world

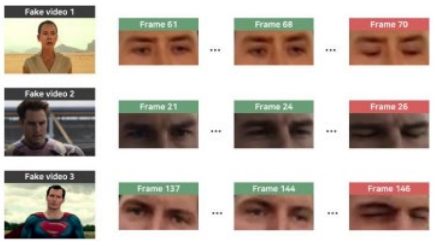
POWER GRID

studies coming from different IoT domains, i.e. building automation and factory automation, while seeking for solutions to improve these systems' security."
Source: 2020 IEEE International Conference on Industrial Technology (ICIT)

Application Layer Key Establishment for End-to-End Security in IoT

"…this article studies possible security threats and weakness in two case studies coming from different IoT domains, i.e. building automation and factory automation, while seeking for solutions to improve these systems' security."
Source: 2020 IEEE International Conference on Industrial Technology (ICIT)

AI



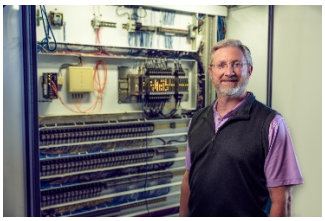
DeepVision: Deepfakes detection using human eye blinking pattern

"In this paper, we propose a new approach to detect Deepfakes generated through the generative adversarial network (GANs) model via an algorithm called DeepVision to analyze a significant change in the pattern of blinking, which is a voluntary and spontaneous action that does not require conscious effort."
Source: Computers & Security

Detecting Stealthy Domain Generation Algorithms Using Heterogeneous Deep Neural Network Framework

"In this paper, we exploit the character-level characteristics of the SDGA domain names and propose a heterogeneous deep neural network framework (HDNN) for detecting SDGA. HDNN employs a proposed improved parallel CNN (IPCNN) architecture with multi-sizes of convolution kernel for extracting multi-scale local features from a domain name."
Source: IEEE Access

An Explainable Machine



Engineers to work on cybersecurity for systems linking solar power to grid

"Distinguished Professor Alan Mantooth of the University of Arkansas received a $3.6 million award from the U.S. Department of Energy Solar Energy Technologies Office to advance technologies that integrate solar power systems to the national power grid."

Source: Eureakalert

Learning Framework for Intrusion Detection Systems

"The framework proposed in this paper leads to improve the transparency of any IDS, and helps the cybersecurity staff have a better understanding of IDSs' judgments. Furthermore, the different interpretations between different kinds of classifiers can also help security experts better design the structures of the IDSs. More importantly, this work is unique in the intrusion detection field, presenting the first use of the SHAP method to give explanations for IDSs."

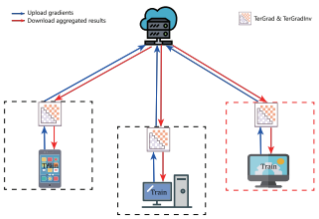
Source: IEEE Access

Machine Learning Security: Threats, Countermeasures, and Evaluations

"In this survey, we systematically analyze the security issues of machine learning, focusing on existing attacks on machine learning systems, corresponding defenses or secure learning techniques, and security evaluation methods. Instead of focusing on one stage or one type of attack, this paper covers all the aspects of machine learning security from the training phase to the test phase."

Source: IEEE Access

PRIVACY

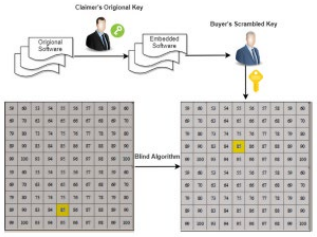


EaSTFLy: Efficient and secure ternary federated learning

"In this paper, firstly, we analyze the privacy leakages of TernGrad. Then, we present our solution-EaSTFLy to solve the privacy issue. More concretely, in EaSTFLy, we combine TernGrad with secret sharing and homomorphic encryption to design our privacy-preserving protocols against semi-honest adversary."

Source: Computers & Security

SOFTWARE SECURITY



KeySplitWatermark: Zero Watermarking Algorithm for Software Protection against Cyber-Attacks

"this paper proposes a novel blind Zero code based Watermark detection approach named KeySplitWatermark, for the protection of software against cyber-attacks. The algorithm adds watermark logically into the code utilizing the inherent properties of code and gives a robust solution. The embedding algorithm uses keywords to make segments of the code to produce a key-dependent on the watermark. The extraction algorithms use this key to remove watermark and detect tampering."

Source: IEEE Access

CLOUD SECURITY

Verifiable Searchable Encryption Framework against Insider Keyword-Guessing Attack in Cloud Storage

"Searchable encryption (SE) allows cloud tenants to retrieve encrypted data while preserving data confidentiality securely. Many SE solutions have been designed to improve efficiency and security, but most of them are still susceptible to insider Keyword-Guessing Attacks (KGA), which implies that the internal attackers can guess the candidate keywords successfully in an off-line manner. Also in existing SE solutions, a semi-honest-but-curious cloud server may deliver incorrect search results by performing only a fraction of retrieval operations honestly (e.g., to save storage space). To address these two challenging issues, we first construct the basic Verifiable SE Framework (VSEF), which can withstand the inside KGA and achieve verifiable searchability."

Source: IEEE Transactions on Cloud Computing (TCC)

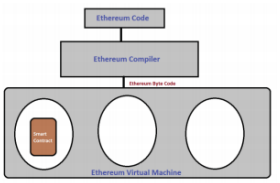
Designing Secure and Efficient

Biometric-Based Secure Access Mechanism for Cloud Services

"The demand for remote data storage and computation services is increasing exponentially in our data-driven society; thus, the need for secure access to such data and services. In this paper, we design a new biometric-based authentication protocol to provide secure access to a remote (cloud) server.."

Source: IEEE Transactions on Cloud Computing

SYSTEM SECURITY



Hybrid Security Framework for Blockchain Platforms

"In this research article, researchers are proposing a more secure and reliable hybrid security framework for Blockchain platforms that can be used as a generalized reference model to counter various security threats in Blockchain platforms.The proposed hybrid security framework can be applied to secure any kind of Blockchain platform. This research could influence future research in the direction of security of Blockchain 1.0, Blockchain 2.0 and beyond."

Source: 2020 First International Conference on Power, Control and Computing Technologies (ICPC2T)

MALWARE

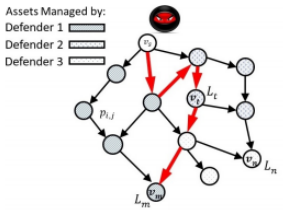
$$\text{Linear kernel } K(\mathbf{u},\mathbf{v}) = \mathbf{u}^T\mathbf{v}$$
$$\text{Polynomial kernel } K(\mathbf{u},\mathbf{v}) = (\gamma\mathbf{u}^T\mathbf{v} + c)^d$$
$$\text{Radial Basis Function kernel } K(\mathbf{u},\mathbf{v}) = \exp\left(-\frac{\|\mathbf{u}-\mathbf{v}\|^2}{2\sigma^2}\right)$$
$$\text{Sigmoid kernel } K(\mathbf{u},\mathbf{v}) = \tanh(k\mathbf{u}^T\mathbf{v} - \delta)$$

Enhanced Android Malware Detection: An SVM-Based Machine Learning Approach

"This paper presents a machine-learning-based approach using Support Vector Machines (SVM) to detect malicious Android applications; the new approach delivers results highly competitive with existing approaches.."

Source: 2020 IEEE International Conference on Big Data and Smart Computing (BigComp)

NETWORKING



Behavioral and Game-Theoretic Security Investments in Interdependent Systems Modeled by Attack Graphs

"We consider a system consisting of multiple interdependent assets, and a set of defenders, each responsible for securing a subset of the assets against an attacker. The interdependencies between the assets are captured by an attack graph, where an edge from one asset to another indicates that if the former asset is compromised, an attack can be launched on the latter asset. Each edge has an associated probability of successful attack, which can be reduced via security investments by the defenders."

Source: IEEE Transactions on Control of Network Systems