E-COMMERCE & DIGITAL SECURITY
Assignment-11

N Ravinder Reddy
Roll No: 2406CYS106

Unit 3 - DIGITAL DEVICES SECURITY

Assignment Questions.

Syllabus:

Device and Mobile Security: End Point device and Mobile phone security, Password policy, Security patch management, Data backup, Downloading and management of third-party software, and Device security policy.

Tools and Technologies for Cyber Security: Authentication tools, firewalls, intrusion detection systems, and antivirus and encryption software.

Cyber Security Best Practices: Cyber Security best practices, Significance of host firewall and Anti-virus, Management of host firewall and Anti-virus, Wi-Fi security, Configuration of basic security policy and permissions.

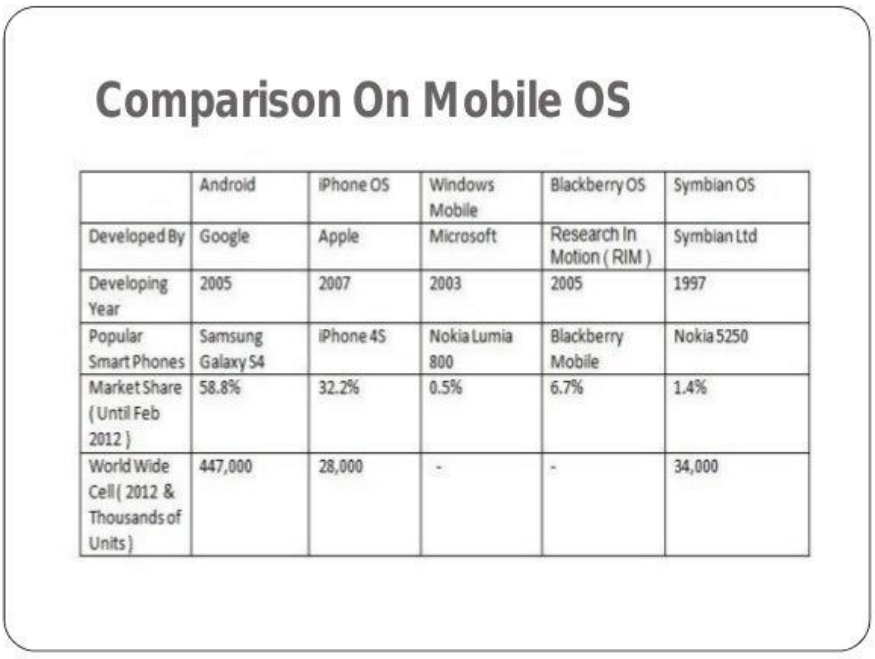
Device and Mobile Security:

Research Question:

Q. Conduct a comparative analysis of different mobile operating systems (e.g., Android, iOS) in terms of their security features and vulnerabilities. Investigate the security architectures, patching mechanisms, and app permission models employed by each operating system to protect user data and privacy. Evaluate the effectiveness of these security measures in mitigating common threats such as malware, unauthorized access, and data leakage. Furthermore, examine the impact of device fragmentation and software update practices on the overall security posture of mobile ecosystems. Based on your analysis, propose recommendations for improving the security of mobile devices across different platforms. Tools and Technologies for Cyber Security:

Ans: Smartphone usage has increased exponentially in recent years. Android and iOS are the most popular smartphone platforms, while the ease of use along with the computational power to handle a wide array of applications attracts millions of users worldwide, and also raises the security concerns on these platforms. This paper presents a comparative analysis between Android and iOS on a wide range of security aspects. It analyzes data for the period 2015-2019 and gives a detailed snapshot of not only the quantum of vulnerabilities but also their impact. In addition, the paper

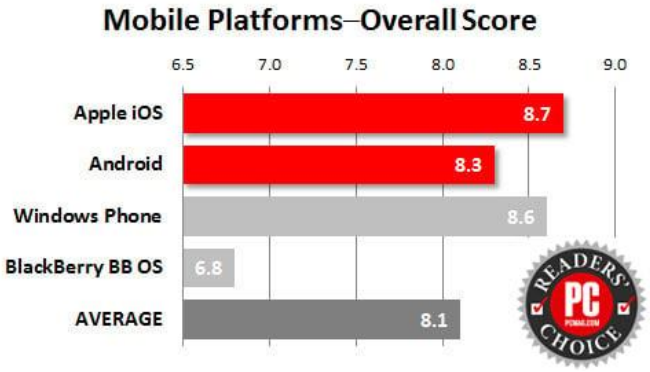
leverages the well-established security triad i.e. CIA (Confidentiality, Integrity, Availability) to compare both operating systems. The comprehensive and pragmatic approach taken in the paper makes it easier to infer that Android is more susceptible to security breaches and malware attacks as compared to iOS. Hence, researchers should divert their efforts and focus on finding solutions to problems with Android. The paper concludes by laying down future research directions and scope of work, which can be leveraged not only by application developers but also by researchers. This will help make Android safer for users and will further increase its demand as a mobile operating system.



Comparison On Mobile OS

	Android	iPhone OS	Windows Mobile	Blackberry OS	Symbian OS
Developed By	Google	Apple	Microsoft	Research In Motion (RIM)	Symbian Ltd
Developing Year	2005	2007	2003	2005	1997
Popular Smart Phones	Samsung Galaxy S4	iPhone 4S	Nokia Lumia 800	Blackberry Mobile	Nokia 5250
Market Share (Until Feb 2012)	58.8%	32.2%	0.5%	6.7%	1.4%
World Wide Cell (2012 & Thousands of Units)	447,000	28,000	-	-	34,000

Due to the ever increasing capabilities of current generation smartphones, they are quickly becoming more attractive targets for malicious attackers. The potential of porting attacks and malware from modern computers to these mobile devices is becoming a reality. In this paper, we explore the possibility of staging some attacks on the 802.11 network interface which is common to all smartphones. We begin by explaining and carrying out the exploitation of the SSH vulnerability on jailbroken iPhones that was discovered in late 2009. This paper then looks at simple network flooding attacks with the intention of causing a simple denial of service by depleting the battery life of the device. It is also our intention to show that these flooding attacks can be carried out utilizing a smartphone as the aggressor in order to attack other mobile devices and that the procedure for such attacks is not difficult. A simple tool is developed in order to carry out these attacks and to show that even though these attacks are relatively simple, they can have profound effects.



Emphasis is to carry out a comparative study of the following operating systems: Windows, UNIX, Linux, Mac, Android and iOS. Issues of concern are Computer Architecture Supported, Target System Type, File System Supported, User Friendly for Lay Users, Integrated Firewall, Security Threats, Shell Terminal, Kernel Type, Reliability, and Compatibility. Also, the advantages and limitations of each of the operating systems were listed. The comparison of the operating systems based on features and functionalities is presented in Table.

	Windows	Linux	Mac	UNIX	Android	iOS
Manufacturer	Microsoft Inc.	Linux is developed as open source OS under the GNU project by the Originator, Linus Torvalds and many others.	Apple Inc. for their Macintosh line of computer systems.	Three biggest distributions are Solaris running (Oracle), AIXon (IBM) & HP-UX Hewlett Packard. And Apple Makes OSX, an Unix based OS	Open source OS designed &developed by Android Inc. Google is now the current owner	Apple Inc. closed, with components that are source openly
Development and Distribution	Developed and distributed by Microsoft.	Linux is Open Sourced and distributed by various vendors.	Mac OS was designed only to be deployed by Apple Computers.	Unix system has various flavors, most ofwhich are developed by AT&T with other commercial vendors and non-profit orgs.	OHA (Open Handset Allianc e)	Apple Inc. developed and distributed iOS
Computer Architecture Supported	x86, x86-64	x86, x86-64, PowerPC, SPARC, Alpha, Others	68k, PowerPC	Available on PA-RISC and Itanium machines. Solaris also available for x86/x64 based systems. OSX is PowerPC(10.0 - 10.5)/x86(10.4)/x64 (10.5-10.8)	Android-x86 powered by AMD and Intelx86 processors.	ARM
Target System Type	Workstation, Personal Computer, Media Centre, Tablet PC, Embedded.	Desktop/ Server Depends on Distribution	Workstation, Personal Computer, embedded	8086 UNIX system, PDP-11/70 system	Consumer, Enterprise, education	Smartphone, music system player, Tablet system/ comput

						er
File System Supported	NTFS, FAT & exFAT with ISO 9660; UDF, 3rd Party driver that supports file system ext2, and ext3, ReiserFS, and HFS	ext2, ext3, ex4,ReiserFS ,FAT, ISO 9660,UDF, NFS, and others.	HFS+, HFS, MFS (Mac OS 8.0 and before) AFP, with ISO 9660, FAT, UDF	jfs, gpfs, hfs, hfs+, ufs, xfs, zfs format	Ext4	HFS+, FTP
User Friendly for Lay Users	Very User Friendly	Depends on Distribution. More friendlier to users than Unix	Very User Friendly	Unix is user-friendly. It's just choosy about who its friends are	Very User Friendly	Very User Friendly
Integrated Firewall	Windows Firewall	Chroot capability-based security, [s 5] seccomp, SELinux	Application Firewall	IPFilter	iptables	Firewall-IP for iOS
Security Threats	Huge	Negligible	Negligible	Mild	Negligible	Negligible
Shell Terminal	CMD	Bash shell powerful shell with many features	BASH	Originally the Bourne Shell. Now it's compatible with many others including BASH, Korn & C.	Mosh	Blink Shell
Kernel Type	Hybrid	Monolithic with modules	Monolithic with modules	Monolithic with modules	Linux kernel	XNU kernel of Darwin

Reliability	Great	Great	Greatest	Greater	Could be unstable	More than Android
Compatibility	Can coexist on local networks with Windows, BSD, Macs, and other Unix-like systems. More compatible.	Linux has few programs and games like Windows. But is more compatible and scalable than Unix	Only few programs will run on Mac	Unix does not have as many programs and games as Windows	Better than iOS	Compatibility is fair

Merits of Windows OS

i. Technical/Maintenance support: Support is made available either online or offline because of its general acceptability by so many users.
ii. Compatibility: Windows accommodates almost every application, game works, and different types of drivers.
iii. Enormous quantity of functions: Getting used to Windows, one would realize that there are many functions one can do almost anything quite easily with when called up.

Demerits of Windows OS

iv. Viruses: Need to purchase an antivirus programs that needs to be activated frequently, and this can be done on Auto or Manual mode, although free antivirus exist but with limitations.
v. Slow: Windows operating system, particularly Vista and Windows 7 needs a lot of system resources like registers, cache, main memory, processor, disk space, and this makes the system runs slower.
vi. Price: The cost of purchasing Windows operating system is high and very few users can afford it and this necessitate cracking and makes pirated software version available.

Android Operating System

The original creator of the platform is Android Inc., Google later bought it over and released the OS as AOSP (Android Open Source Project) in 2007. This new development was complemented by the founding of the OHA (Open Handset Alliance), a consortium saddled with the responsibility to develop and distribute Android. The software, which is now been released under the Apache license is tagged among others, a free open source license. Android releases a new version every few months as a result of the available huge developer communities who regularly updates and create

applications using custom-built version of Java.

The OHA group is a consortium of several software, hardware and telecom companies, T-Mobile, Intel, Qualcomm, NVIDIA, HTC, Motorola and Google Inc., for which Android provides their software platform. Their main objective of OHA is to develop available technologies that will considerably lower the cost and time of developing and distributing mobile devices and services.

Merits of Android OS

vii. Open Source Platform supported by a wide-range of mobile device manufacturer and communities
viii. Easy access to many free and premium app from communities of app developers that support Android OS
ix. Multitasking: The Android Operating system has the capability of running many applications and processes within the same available time
x. Fast and easy notification of SMS, email or RSS reader alert
xi. Widget zed home screen allows easy access to settings of phones without wasting time and with ease
xii. The continuous upgrades in appearance and features might shortly leave other iOS far behind soon.
xiii. Good for programmers who like to jumble with Linux Kernel for making alterations in OS.

Demerits of Android OS

xiv. Unstable and disposed to crashes compared to other OS.
xv. Being open source, so many apps are created. Very few of these applications might have bugs that can be abused by hackers or viral infections.
xvi. To sign in as an administrator for advanced settings, one needs to get acquainted with Linux commands.
xvii. Frequent updates on the OS could make one upgrade to the latest, and this is called rooting. Rooting should be done carefully, otherwise, one could end up in trouble.
xviii. The majority of Applications require internet connections for operation which sometimes is a disadvantage.
xix. Poor battery backup management.

iPhone Operating System (iOS)

iOS, which is a mobile OS, is designed and owned by Apple Inc. It was designed and developed for iPhone, but later extended support for iPad and Apple TV. iOS root comes from Mac OS X, hence it is UNIX based OS. Like other OS, iOS is frequently updated starting from iOS version 4.0 and the latest is iOS version 5.1.The Core OS layer resides in the bottom of the iPhone OS architecture[19].

The core services layer of iOS architecture encompasses an additional abstraction layer, cocoa touch layer, and media. The Core OS layer contains the scheduler inclusively, Mach kernel, file system, and hardware drivers and controls the memory system, network, and inter-

process communication and security framework to secure the system and program data. As confirmed the core services layer of the OS has an abstraction setup. It also contains nonstop accessibility to the network availability, basic framework for objective-C programming, state of mobile device, access to location information, and address book. As of March 2012, 550,000 iOS apps are available in Apple store (Anup, Raman et al 2015). iOS has many benefits and non-benefits as stated below.

Merits of iOS

xx. Stable and safe Operating System for mobile phones
xxi. Probably the most loved interface for any mobile OS in the market. Good-looking desktop and app icons go hand to hand with the stunning looks of Apple devices.
xxii. Minimal viruses and safe OS with the consideration of very high standard when applications were developed and when updates were also made.
xxiii. High adherence to current web standard and procedures.
xxiv. High consideration for cloud storage technology.
xxv. Easy access to free and premium apps from Apple store.

Demerits of iOS

xxvi. iOS only support Apple Hardware, and less operability
xxvii. Very costly

DEDUCTIONS

a. Windows 10 had 0.04 malware file present while Windows 7 machine was 0.08.
b. Higher % of mobile malware target Androids than iOS.
c. Windows 10, Linux, UNIX and Mac OS are more secured and reliable.
d. Windows and Android are more popular, user- friendly, easy to use and allow more application program than Mac OS.
e. Linux and Android are free while Windows is moderately costly and Mac OS highly costly.
f. Except for Mac and iOS others allow compatibility. Windows 10 and Mac OS integrated firewall.

The comparative analysis and market share analysis between August 2018 and June 2020 showed that Android and Windows OS are very high compare to other OS. Android and Windows have 38.3% and 36.55% respectively.

Research topics and methods used in mobile device security:

Based on their content, we synthesized that current Mobile Device Security research focuses on four topics with their methods, ie:

1. Malware and Intrusion Detection: This type of work employs the service monitor method (Salehi et al, 2019), machine classification with

analysis tools and algorithms (Zhang et al, 2019), machine learning, neural networks, and deep learning (Fournier et al, 2020, D'Angelo et al, 2020, Millar et al, 2017, Jensen et al, 2017), IRS metric (Deypir & Horri, 2018), NATICUSdroid (Mathur et al, 2021), semantic dynamic (Bhandari et al, 2018)), and computational intelligence (CI) (Shahab et al, 2020), among others.

2. Cryptography: Lightweight cryptography techniques (Shahbodin et al, 2019), openkeychain (Schürmann et al, 2017), location-based cryptography (AES + location coordinate) (Mondal & Bours, 2018), and RSA and ECC cryptographic swarm optimization simplified (Mullai & Mani, 2020) are all used in this kind of research.

3. Authentication: This type of work uses combined kernel function artificial intelligence algorithm, seamless secure anonymous (Deebak et al, 2020), token-based authentication framework (Niewolski et al, 2021), proposed D2D security (Edris et al, 2021), gait-based authentication (Zeng et al, 2021, Axente et al, 2020), and lightweight deep learning model secure authentication (Zeroual et al, 2021).

4. Information Invasion: This type of work uses implicit evasive information invasion with sound, called SonicEvasion (Pattani & Gautam, 2021).

Of the four focuses, it can be said that the method most frequently encountered and used is artificial intelligence. Artificial intelligence is currently one of the best methods of automating digital transformation which is always evolving and is increasingly needed in human life.

The dataset is used for a certain purpose.

A set of training data is the collection of data put into a system of machine learning, which is analyzed and creates a useful model from it. A set of tests or evaluation data is a collection of data to assess a learning system of the model. The training and test set data include distinct data sources. According to a review process, contemporary Mobile Device Security research employs a variety of datasets, including

• Private datasets (Wang & Fang, 2019, Trigo et al, 2020, Ali et al, 2020, Shahbodin et al, 2019,

Schürmann et al, 2017, Mullai & Mani, 2020, Niewolski et al, 2021, Edris et al, 2021, Pattani & Gautam, 2021, MoreGimeno et al, 2018, Guo et al, 2018, Yan et al, 2018).

• Malicious application from different families and resources (Salehi et al, 2019, Zhan et al, 2019, Fournier et al, 2020, Millar et al, 2017, Deypir & Horri, 2018, Mathur et al, 2021, Bhandari et al, 2018, Hijawi et al, 2021).

• Malgenome contagio minidump (D'Angelo et al, 2020). • Public mobile biometrics (Mondal & Bours, 2018)

. • UCI machine learning repository (Axente et al, 2020).

• ORL and extended yale (Zeroual et al, 2021).

• Sparks dataset APIs (Lima et al, 2020).

• Enron email datasets (Li et al, 2021).

• Call detail records (Forte et al, 2019).

• Public natural landscape images and facial images (Saharan et al, 2021).

From the explanation of the grouping of datasets above, it can be concluded that the use of public datasets is higher than that of private datasets. Thus, the research that has been carried out has indications that it can be applied by the general public or other researchers who have similar problems or case studies. Fig. 5 depicts the entire mind map, which summarizes the findings of the SLR on the mobile devices security. Mind maps were also used to study connections between ideas and different parts of a debate and come up with problem-solving solutions. It gives us a fresh way of looking at things by viewing all of the crucial concerns and weighing our options in light of the big picture (Buzan & Griffiths, 2013). It also facilitates effectively organizing knowledge and absorbing new information.

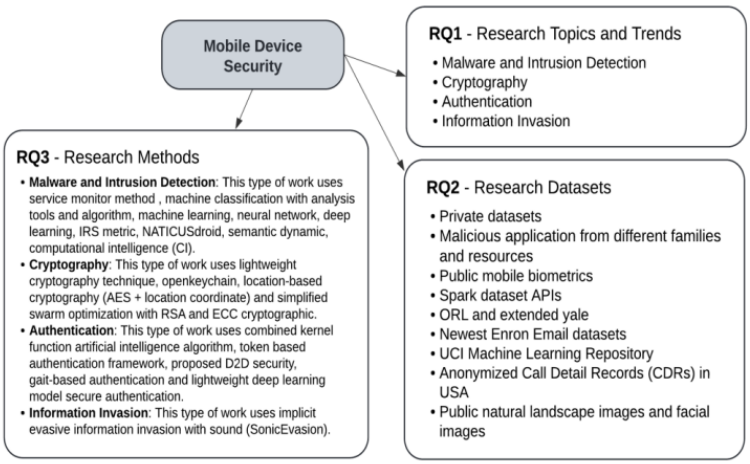


Fig. 5: The complete mind map of the results of SLR on mobile device security

This SLR aims to determine and evaluate the trends, methods, and datasets utilized in Mobile Device Security research between 2017 and 2021. Finally, based on the exclusion and inclusion criteria, 33 Mobile Device Security research issued around January 2017 until December 2021 were kept to be analyzed. This review was carried out systematically. An SLR is a strategy to locate, assess, and understand all research information that is accessible in a position to respond to the specific research question. Based on the results, it can be concluded that current Mobile Device Security research focus on four themes, i.e., malware and intrusion detection, cryptography, authentication, and information invasion. Of the four focuses, it can be said that the method most frequently encountered and used is artificial

intelligence. In addition, 60.61 percent of research papers utilized public datasets, whereas 39.39 percent used private datasets. We managed to find four themes in the Mobile Device Security research. We also identify methods and datasets that can be used. Those results contribute to both the academic side for further research and can become a guidance to the practitioner on the practical side.

References

Ali, G., Dida, M. A. & Sam, A. E. (2020). Two-factor authentication scheme for mobile money: A review of threat models and countermeasures. MDPI Future Internet, 12, 160.

Alimardani, H. & Nazeh, M. (2018). A taxonomy on recent mobile malware: features, analysis methods, and detection techniques. In Proceedings of the 2018 International Conference on E-business and Mobile Commerce, ICEMC 2018, 44-49.

Axente, M. -S., Dobre, C., Raluca, R –l. C. & Purtan, P. (2020). Gait recognition as an authentication method for mobile devices. MDPI Sensors, 20(15), 4110.

Berguig, O. & Abdelbaki, N. (2021). Impact of quality of work life's dimensions on turnover intention: a systematic literature review. Journal of System and Management Sciences, 11(2), 134-254.

Bhandari, S., Panihar, R., Naval, S., Laxmi, V., Zemmari, A. & Gaur, M. S. (2018). SWORD: semantic aware android malware detector. Journal of Information Security and Applications, 42, 46-56.

Buzan, T. & Griffiths, C. (2013). Mind maps for business: Using the ultimate thinking tool to revolutionise how you work (2nd Edition).

FT Press. Byeon, G. & Yu, S. (2022). Mobile AR contents production technique for long distance collaboration. Journal of System and Management Sciences, 12(1), 129-142.

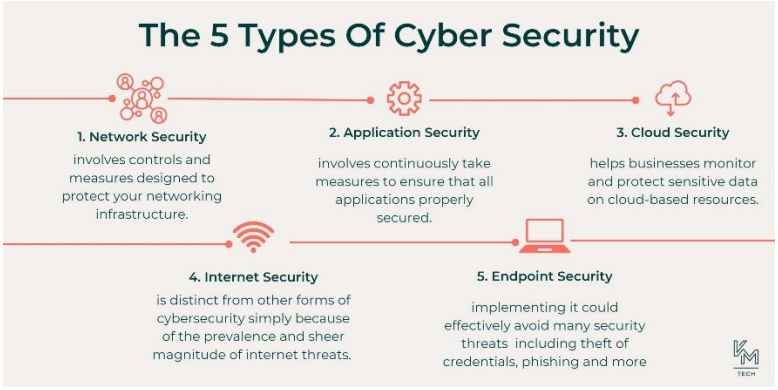
Chan, J. H. and Hong, J. L. (2016). Mobile Security and its Application. International Journal of Security and Its Applications, NADIA, 10(10); 89-106, http://dx.doi.org/10.14257/ijsia.2016.10.10.10

Research Question:

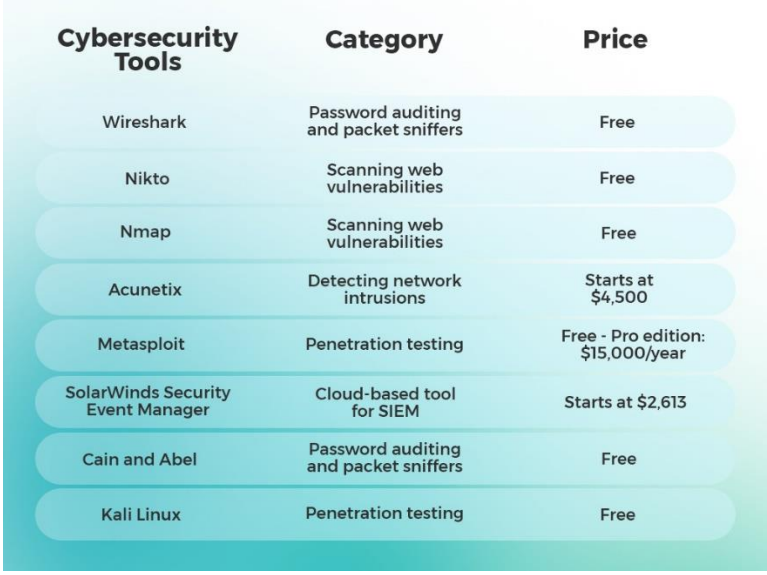
Q. Investigate and compare different categories of cybersecurity tools and technologies used for threat detection, prevention, and incident response. Choose three categories (e.g., antivirus software, intrusion detection systems, threat intelligence platforms) and analyze the key features, functionalities, and deployment considerations for each category. Evaluate the strengths and limitations of popular tools within each category, considering factors such as scalability, ease of use, and integration capabilities. Finally, discuss emerging

trends in cybersecurity technology, such as artificial intelligence and machine learning, and their potential impact on the effectiveness of cyber defense strategies.

Ans: One of the weakest points in actual security detection and monitoring systems is the data retrieval from Open Source Intelligence (OSINT), as well as how this kind of information should be processed and normalized, considering their unstructured nature. This cybersecurity related information (e.g., Indicator of Compromise - IoC) is obtained from diverse and different sources and collected by Threat Intelligence Platforms (TIPs). In order to improve its quality, such information should be correlated with real-time data coming from the monitored infrastructure, before being further analyzed and shared.



In this way, it could be prioritized, allowing a faster incident detection and response. This paper presents an Enriched Threat Intelligence Platform as a way to extend import, quality assessment processes, and information sharing capabilities in current TIPs. The platform receives structured cyber threat information from multiple sources, and performs the correlation among them with both static and dynamic data coming from the monitored infrastructure. This allows the evaluation of a threat score through heuristic-based analysis, used for enriching the information received from OSINT and other sources. The final result, expressed in a well defined format, is sent to external entities, which is further used for monitoring and detecting incidents (e.g., SIEMs), or for more in-depth analysis, and shared with trusted organizations.



Cybersecurity Tools	Category	Price
Wireshark	Password auditing and packet sniffers	Free
Nikto	Scanning web vulnerabilities	Free
Nmap	Scanning web vulnerabilities	Free
Acunetix	Detecting network intrusions	Starts at $4,500
Metasploit	Penetration testing	Free - Pro edition: $15,000/year
SolarWinds Security Event Manager	Cloud-based tool for SIEM	Starts at $2,613
Cain and Abel	Password auditing and packet sniffers	Free
Kali Linux	Penetration testing	Free

The number and the impact of cyber attacks has drastically increased during the last years, as revealed by reports written by governments and companies, especially in terms of how much these threats could harm them from an economical point of view. The Council of the Economic Advisers of the United States1 estimated that malicious cyber activity had an economic impact in the U.S. economy between 57 billion and 109 billion dollars in 2016 (CEA, 2018). Cybersecurity Ventures2 identified cyber crime as the ”greatest threat to every company in the world”, predicting that it will cost the world more than six trillion dollars annually by 2021 (Ventures, 2017). Moreover, the global management consulting firm Accenture3 , during a study conducted in 2017 (Accenture, 2017), affirmed that cyber crime, on an annual average, is costing organizations 11.7 million dollars, more or less 23 percent more than the previous year. These successful incursions potentially allow groups of attackers to acquire valuable intellectual properties and secrets. With the aim of facing these menaces, it is crucial to have timely access to relevant, accurate information about them, for protecting precious internal and sensitive data as well as critical assets.

Collecting and processing Open Source Intelligence (OSINT) information is becoming a fundamental approach for obtaining cybersecurity threat awareness. Recently, the research community has demonstrated that useful information and Indicators of Compromise (IoC) can be obtained from OSINT (Liao et al., 2016; Sabottke et al., 2015). Besides the research oriented efforts, all Security Operation Centre (SOC) analysts get updated about new threats against their IT infrastructures by collecting and analyzing cybersecurity OSINT data. Nevertheless, skimming through various news feeds is a time-consuming task for any security analyst.

Several standard formats have been proposed to facilitate cyber intelligence sharing among platforms. Examples of such formats are the Open

Indicators of Compromise (OpenIoC4), Structured Threat Information eXpression (STIX5), Trusted Automated eXchange of Indicator Information (TAXII6). Few studies of existing threat intelligence platforms (TIPs) have been identified. Tounsi and Rais (Tounsi and Rais, 2018) provides a survey about open source threat intelligence platforms, including the Malware Information Sharing Platform (MISP)7 , the Collective Intelligence Framework (CIF)8 , the Collaborative Research Into Threats (CRITs)9 , and Soltra Edge10. Sauerwein et al. (Sauerwein et al., 2017), provide an exploratory study of software vendors and research perspectives of threat intelligence sharing platform, and conclude that the market for threat intelligence sharing is still developing.

Moreover, also ENISA provides an updated report about opportunities and limitations of actual TIPs (ENISA, 2017), suggesting various guidelines that should be followed for overcoming them. Owen (Owen, 2015) proposes Moat, a powerful tool that covers known bad actors and consume data from multiple sources such as vulnerability systems and port scanners. Moat has been integrated with SIEMs using STIX and XML formats for sharing purposes but it is not yet defined for other well-known standards such as TAXII. Some commercial SIEMs (e.g., LogRhythm11) have added security intelligence to its SIEMs and analytic platforms. Their approach uses rich context enabled by threat intelligence from STIX/TAXIIcompliant providers, commercial and open-source feeds, as well as internal honeypots. As a result, the platform uses these data to reduce false-positives, detect hidden threats, and prioritize concerning alarms.

To the best of our knowledge, more research is needed about threat intelligence sharing platforms, and their integration with other security tools. Our approach suggests the use of a platform for collecting and aggregating cyber security related information from OSINT, relying on MISP for storing and managing the resultant IoCs, which will be further enriched with a threat score, for prioritizing possible defence actions. The outcome of this platform will feed systems, like SIEMs and IDS, with actionable information that will improve the detection of cyber threats, and could also be shared, in an automated way, with internal SOCs and CSIRTs, as well as with other trusted organizations.

Threat Intelligence Platforms

Many companies started relying on Threat Intelligence Platforms (TIPs) for overcoming gaps and limitations of actual detection and monitoring systems, especially SIEMs (ThreatConnect, 2018). They are in charge of retrieving structured and unstructured data from diverse external sources, and perform various complex operations, such as filtering, aggregation, normalization, detection, analysis and enrichment, as well as the injection of results into SIEMs. However, their implementation and usage are still in their infancy and, as stated in (Sauerwein et al., 2017), many drawbacks have to

be addressed, for instance, in terms of dynamic trust assessment of external sources and advanced analysis capabilities, where manual work is still needed, especially for making the retrieved information effectively actionable.

TIPs are ideal tools for data collection, storage, sharing, and for integration with external entities, that could be other security platforms and tools, as well as specific groups for handling incident response and threat management (e.g., SOC, CSIRTs). Several TIPs are available in the market (most of them under commercial license). In terms of open-source solutions, we have identified the following:

1. The Malware Information Sharing Platform (MISP),

2. The Collective Intelligence Framework (CIF),

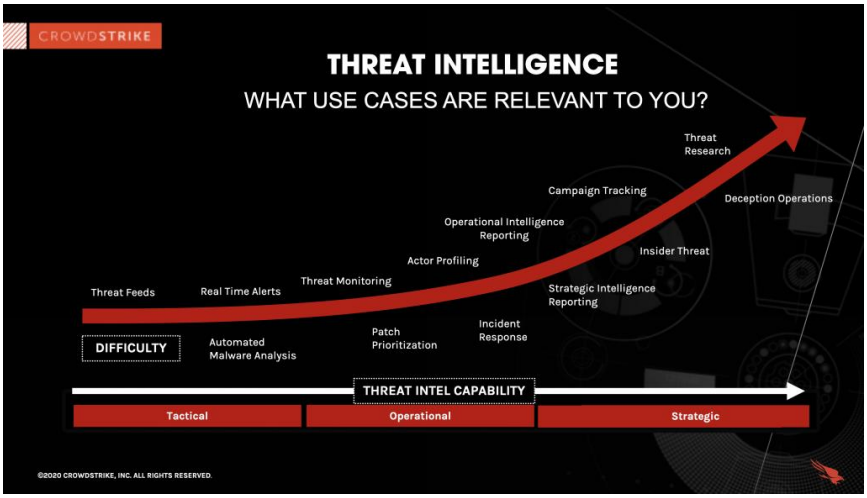
3. The Collaborative Research Into Threats (CRITs), and

4. SoltraEdge (SE), but only a limited version is available with this kind of license. The comparison among them is summarized in Table 1, and has been performed taking into account the following criteria, mainly based on the study conducted by Tounsi et al. (Tounsi and Rais, 2018), together with some personal considerations, especially about hardware requirements:

Table 1: Comparison of Threat Intelligence Platforms

Evaluated Criteria	MISP	CIF	CRITs	SE
Import/Export Format	•	◦	•	–
Integration Capabilities	•	•	◦	◦
Data Exchange Std.	•	◦	◦	◦
Support of Collaboration	•	•	◦	◦
Analysis Capabilities	◦	◦	•	◦
Graph Generation	◦	◦	•	◦
License	•	•	•	◦
Hardware Requirements	•	–	•	•

–Low/Basic ◦ Medium/Average • High/Advanced



Threat Score (TS) Evaluation

The threat score evaluation is part of the heuristic component that uses a threat score function (detailed in Section 5.1) to compute the relevance of the received data. The process performs an analysis methodology composed of the following steps:

1. Source Identification: during this phase, we search and identify all possible sources of information. Examples of these sources are security logs, databases, report data, OSINT data sources, IoCs, etc.

2. Heuristics Identification: different features (e.g., heuristics) are identified from the input data. Such features provide relevant information about the infrastructure (e.g., vulnerabilities, events, faults, errors, etc.) useful in the threat analysis and classification process. Examples of heuristics are CVE, IP source, IP destination, port source, port destination, timestamp, etc.

3. Threshold Definition: for each heuristic, minimum and maximum possible values are defined based on characteristics associated with the instance. We checked, for instance, if the input data contains or not a CVE for the detected threat. A threshold (e.g., 0-5) is assigned to cover all possible results.

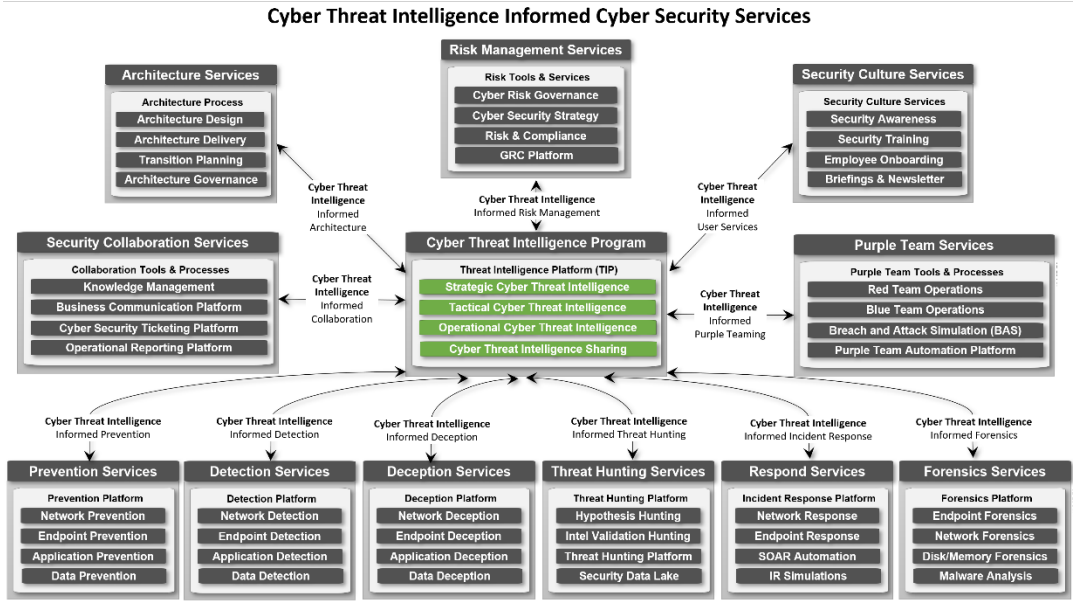
4. Score Computation: for each possible instance of the identified heuristic, a score value is assigned based on expert knowledge. All individual scores are then aggregated and a final score is computed. The resulting value will indicate the priority and relevance of the security information coming from OSINT data sources and the monitored infrastructure.

5. Training Period: a set of preliminary tests need to be performed during a training process to evaluate the performance of the engine. The tests include real data to analyze the score obtained individually (for each heuristic)

and globally (for the whole event) which helps to analyze false positive and negative rates.

6. Engine Calibration: to minimize deviations (e.g., reduce the number of false positives, and false negatives) the engine must be calibrated by analyzing the obtained results, adding other heuristics, and/or modifying the assigned values to current attributes.

7. Final Tests: Once the engine is calibrated, we can repeat previous tests or add new ones to evaluate the performance of the tool.



Cybercriminals use malware and other attack vectors to compromise vulnerable machines. The conventional machine learning malware detection and classification algorithms uses static features of malware for the training purpose. The features extracted by the static analysis is text-based, i.e. signature [7], Opcode sequence [9], control flow graph [4], bytecode [3], and n-gram [9]; therefore, only the subset of malware sample data is included in the training process. Hence, it will degrade the accuracy of the machine learning or deep learning algorithms and is time-consuming compared to the approach that uses complete information of malware samples in the form of visual features.

Various machine learning and deep learning methods such as M-CNN [5], NSGA-II [2], Deep CNN [10], CNN BiGRU [16], IMCFN [15] and CapsNet [1] have been used in the literature to detect malware using visual features. The machine learning algorithms are required to process malware datasets and the inevitable work of features engineering. At the same time, deep learning shows promising results to classify malware images [1, 2, 5, 10, 15, 16].

Thus, we propose a novel MCFT-CNN model to address the above issues and trained with only visual features. We have achieved 99.18% accuracy and 5.14ms prediction time on the MalImg dataset [6]. The model shows significant improvement over a larger dataset (Microsoft Malware Challenge [8]) with 98.63% accuracy and 5.15ms prediction time. Our model performs significantly better than the existing state-of-art [14]. Similarly, in intrusion detection and botnet detection, we have used machine learning algorithms to efficiently classify intrusions and botnet attacks. We have also proposed an incident handling and response process in case of a fileless malware attack to analyze the attack and behavior of the fileless malware. The proposed models perform significantly better than other models available in the literature [1–5, 7, 9, 10, 15, 16].

Our main contributions to cybersecurity research based on machine learning and deep learning are listed in the following points-

• A novel deep learning model has been proposed to classify the malware using visual features without feature engineering and prior knowledge of binary code analysis or reverse engineering.

• A novel investigative model of incident handling and response has been proposed, especially in file less malware. The model includes all the phases with memory forensic, analysis and investigation of such incidents.

• A machine learning model has been proposed to classify web intrusion attacks. The model uses a univariate feature selection technique on the intrusion dataset (CIC-IDS2017).

• A lightweight machine learning model has been proposed to classify botnet attacks in IoT networks.

References

[1] Aykut Çayır, Uğur Ünal, and Hasan Dağ. 2021. Random CapsNet forest model for imbalanced malware type classification task. Computers & Security 102 (2021), 102133.

[2] Zhihua Cui, Lei Du, Penghong Wang, Xingjuan Cai, and Wensheng Zhang. 2019. Malicious code detection based on CNNs and multiobjective algorithm. J. Parallel and Distrib. Comput. 129 (2019), 50–58.

[3] Jake Drew, Michael Hahsler, and Tyler Moore. 2017. Polymorphic malware detection using sequence classification methods and ensembles. EURASIP Journal on Information Security 2017, 1 (2017), 1–12.

[4] Mehadi Hassen and Philip K Chan. 2017. Scalable function call graphbased malware classification. In Proceedings of the Seventh ACM on Conference on Data and Application Security and Privacy. 239–248.

[5] Mahmoud Kalash, Mrigank Rochan, Noman Mohammed, Neil DB Bruce, Yang Wang, and Farkhund Iqbal. 2018. Malware classification with deep

convolutional neural networks. In 2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS). IEEE, 1–5.

[6] Lakshmanan Nataraj, Sreejith Karthikeyan, Gregoire Jacob, and Bangalore S Manjunath. 2011. Malware images: visualization and automatic classification. In Proceedings of the 8th international symposium on visualization for cyber security. 1–7.

[7] Edward Raff and Charles Nicholas. 2018. Lempel-Ziv Jaccard Distance, an effective alternative to ssdeep and sdhash. Digital Investigation 24 (2018), 34–49.

[8] Royi Ronen, Marian Radu, Corina Feuerstein, Elad Yom-Tov, and Mansour Ahmadi. 2018. Microsoft malware classification challenge. arXiv preprint arXiv:1802.10135 (2018).

[9] Asaf Shabtai, Robert Moskovitch, Clint Feher, Shlomi Dolev, and Yuval Elovici. 2012. Detecting unknown malicious code by applying classification techniques on opcode patterns. Security Informatics 1, 1 (2012), 1–22.

[10] Ajay Singh, Anand Handa, Nitesh Kumar, and Sandeep Kumar Shukla. 2019. Malware classification using image representation. In International Symposium on Cyber Security Cryptography and Machine Learning. Springer, 75–92.

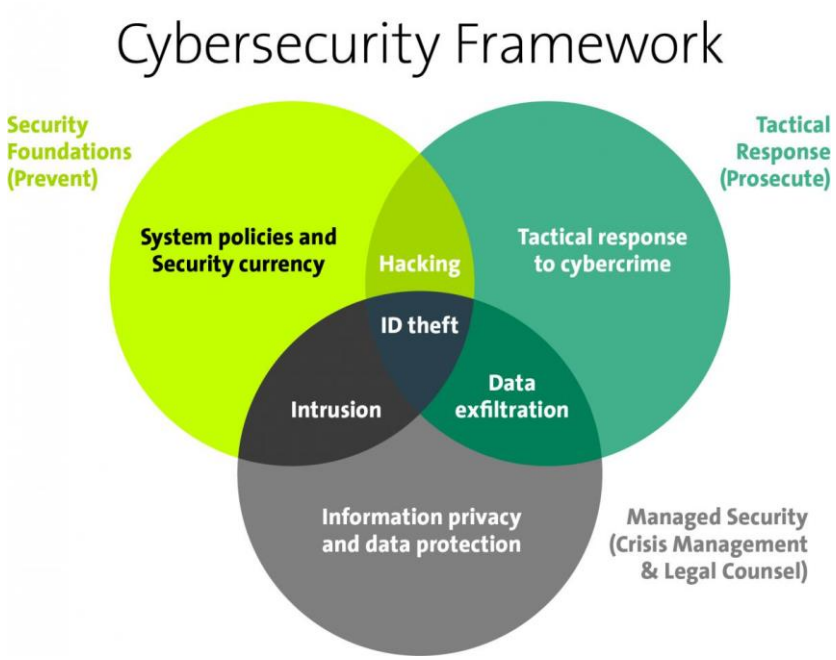
Cyber Security Best Practices:

1Q. Policy Development Question:

Q. Imagine you are tasked with developing a comprehensive cyber security policy for a medium-sized organization. Outline the key components that should be included in the policy, such as access control, data protection, incident response, and employee training. Discuss the importance of each component and provide examples of specific policies or procedures that could be implemented to mitigate cyber security risks. Additionally, address the challenges of policy enforcement and compliance monitoring within the organization. Finally, propose strategies for ensuring the ongoing effectiveness of the cyber security policy in the face of evolving threats and technologies.

Ans:

Six steps to Building a Cyber Security Policy for small and medium-sized Enterprises



Developing a robust cyber security policy is crucial to protect your business's valuable data, maintain customer trust, and ensure business continuity. This article outlines six key steps for SMEs to create an effective cyber security policy that mitigates risks and safeguards their operations.

1. Assess your vulnerabilities through regular IT auditing

Start by conducting a thorough assessment of your business's unique cybersecurity vulnerabilities. Regular IT system audits identify potential entry points for cyberattacks, such as outdated software, weak passwords, or inadequate employee training. Consider the types of data you handle, including customer and supply chain information, financial records, and intellectual property. Understanding your vulnerabilities will guide your policy development and help prioritize security measures.

2. Set clear goals and objectives

Establish clear goals and objectives for your cyber security policy. Define what you aim to achieve, such as protecting sensitive data, ensuring regulatory compliance, and minimising business disruptions. Ensure that your policy aligns with industry best practices and relevant compliance standards, such as the General Data Protection Regulation (GDPR). Setting specific objectives provides a framework for policy implementation and evaluation.

3. Define roles and responsibilities

Clearly define the roles and responsibilities for each employee regarding cyber security within your business. Identify who will be responsible for policy development, implementation, monitoring, and incident response. Assign specific individuals or teams to oversee cyber security tasks and establish reporting protocols to ensure accountability. Clearly defining roles helps

ensure that everyone understands their responsibilities and ensures your business fosters a culture of cyber security awareness.

4. Establish best practices

Develop best practices that address the specific vulnerabilities you identified during the assessment and audit stage. This may include enforcing strong password policies, implementing multi-factor authentication, regularly updating software and systems, and securing network infrastructure. Employee education surrounding safe browsing habits, phishing awareness, and social engineering tactics. Implement measures to protect against malware, including firewalls, antivirus software, and intrusion detection systems.

5. Employee training and awareness

One of the most critical elements of a cyber security policy is employee training and awareness. Conduct regular training sessions to educate employees about the importance of cyber security, common threats, and best practices. Emphasise the significance of identifying and reporting potential security incidents promptly. Encourage a culture of cyber security awareness by promoting ongoing education and providing resources such as posters, newsletters, and awareness campaigns.

6. Incident response and recovery

Develop a cyber response plan that outlines the steps to be taken in the event of a cyber security incident. This plan should include procedures for containing and mitigating the incident, notifying relevant parties, preserving evidence, and initiating recovery processes. Regularly test and update your plan, using ‘playbooks’ to ensure its effectiveness.

Building a cyber security policy is a proactive step that SMEs must take to protect their operations, customers, supply chain and reputation. By assessing vulnerabilities, setting clear goals, defining roles, implementing security controls, training employees, and preparing for incident response and recovery, SMEs can establish a strong foundation for cyber security.

Figure 2. Cyber security approach as set out in the guidelines

Remember that cyber security is an ongoing concern, and regular review and updates to your policy are essential to keep up with evolving threats. If you need support with any of the points raised in this article, please get in touch with one of our engineers. We're happy to have a conversation about how you can better protect your business.