International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 11 Issue 06, June-2022

Integration of Malware Analysis Concepts, Techniques, and Tools in Undergraduate Cybersecurity Programs

Evolving Education to Counter Evolving Cyber Threats

Matthew A. Chapman, Ph.D.
Professor of Computer Science & Cybersecurity
University of Hawaii – West Oahu, United States

***Abstract*— Cybersecurity is one of the fastest growing technical career fields in the country. Due to the increasing threat to both government and industry information systems, it is necessary for cybersecurity programs to produce graduates that can react to the increasingly complex attempts by hostile actors to exploit computer networks. To respond to these growing threats, it is critical for graduates of cybersecurity undergraduate programs to have knowledge of the concepts, techniques, and tools to break down and analyze malicious software used by hostile actors, and understand evolving cyber-attack tactics, techniques, and procedures. Malware analysis is typically an advanced cyber security topic covered in cybersecurity graduate degree programs or specialized training; however, with the rapidly evolving threat, malware analysis must be incorporated into undergraduate cybersecurity degree programs in a significant level of detail. A curriculum is necessary that includes a survey of the socio-cultural aspects impacting the cyber threat landscape, fundamentals of traditional and cloud network architecture and services, and a detailed study into the fundamentals of both static and dynamic malware analysis.**

Keywords—Cybersecurity; cyber threats; malware analysis; socio-cultural; cloud computing; education

I. INTRODUCTION

The occupational outlook for Information Security Analysts is much higher than average, currently with a 33% increase and a typical entry requirement of a bachelor's degree [1]. According to a cybersecurity workforce study by (ISC)2, there is a global shortage of 2.72 million cybersecurity professionals. To address this gap, employers are investing in cybersecurity education and training [2]. The same study highlights that employers' top professional development areas include cyber threat analysis, cloud computing security, and security analysis [2]. This global shortage in the cybersecurity workforce may be a result of socio-cultural changes, including the evolution of digital currency, an increase in cloud computing, and the success of ransomware attacks by cyber threat actors.

As the demand for training the cybersecurity workforce increases, our education system must keep pace and evolve to both meet this demand and counter highly sophisticated, evolving cyber threats. While malware analysis is typically an advanced cybersecurity topic covered in graduate degree programs or specialized training, the rapidly evolving threat requires a significant coverage of malware analysis concepts and techniques in undergraduate cybersecurity degree programs. A curriculum is necessary that includes a survey of the socio-cultural aspects impacting the cyber threat landscape, the fundamentals of traditional and cloud network architecture and services, and a detailed study of the fundamentals of both static and dynamic malware analysis.

II. SOCIAL-CULTURAL CHANGES

Over the past several years, we have observed a significant increase by both industry and critical infrastructure sectors to focus on cybersecurity concerns. Socio-cultural changes are driving organizations to adjust cybersecurity practices and rethink their approach to meeting growing cybersecurity workforce requirements. Taking a page from our colleagues in anthropology and archeology, quite literally in this instance, socio-cultural changes help describe the processes by which societies change. Specifically, both economic factors and technology are significant factors in socio-cultural change [3].

A. Virtual Currency

Virtual currency is just that, a digital representation of value that can be stored, traded, and transferred electronically. It is accepted as payment, but it is generally not issued by a central back or authority. The use of virtual currencies and cryptocurrencies has dramatically increased for both legitimate and illegitimate purposes [4].

Cryptocurrencies are a specific type of virtual currency based on cryptographic properties, algorithms, or protocols. Cryptocurrencies, such as Bitcoin, have gained increasing momentum with their decentralized authority, where users trust the anonymity and security of their transactions. This has led to the popularity of cryptocurrencies in illegal activities such as payments to criminals and cyber threat actors [4].

Considering projections for 2022, the popularity and use of cryptocurrencies are expected to see even wider public acceptance and success. Cryptocurrencies, including Bitcoin, Ethereum, and crypto dollars, have a limited supply, and are expected to see increasing yields in 2022 [5].

B. Moving to the Cloud

Considering the professional development topics sited earlier in the $(ISC)^2$ cybersecurity workforce study, the highest-ranking area was cloud computing security, included by 40% of their respondents [2].

Organizations transitioned information technology and data processing requirements to cloud-based solutions increasingly

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 11 Issue 06, June-2022

over the past decade. These solutions include three major types of cloud computing services: infrastructure as a service, platform as a service, and software as a service. Depending on the needs of the organization, services may include remote networks, virtual machines, data centers, and end-user applications. Services can be deployed completely in the cloud, in a hybrid architecture with physical infrastructure connected to remote cloud services, or on-premises as a private cloud [6].

One of the major cloud service providers is Amazon Web Services (AWS), which began offering information technology infrastructure as a service in 2006 [6]. Considering AWS as a sample cloud provider, it is important to review the organization's cybersecurity model, in this case, the Shared Responsibility Model. There are three key concepts related to risk and compliance in this model. First, AWS manages the cybersecurity 'of the cloud.' Second, it is the customers' responsibility to manage cybersecurity 'in the cloud.' Finally, compliance is a shared responsibility [7]. In this case, the cybersecurity model clearly states that the customer retains the responsibility for cybersecurity of their assets in the cloud, regardless of the type of service or deployment model. The implication of moving to a cloud-based solution is that the organization requires cybersecurity professionals that understand operations and security concerns of cloud services.

C. *Ransomware is Trending*

In the United States in 2021, we observed a couple of very high-profile ransomware attacks. Hackers gained access to Colonial Pipeline networks on April 29th, 2021, through a compromised password and exploited a virtual private network access point. Network resources were encrypted and close to 100 gigabytes of data was compromised. A ransom note was discovered demanding cryptocurrency, and services were disrupted. This impacted the production of about 2.5 million barrels of fuel a day. Colonial paid the hackers a $4.4 million ransom [8]; although, U.S. federal authorities later recovered a majority of the bitcoin [9]. A few weeks later in June 2021, Reuters reported that operations at JBS Meatpacking were disrupted, and a ransom was paid of about $11 million. A spokesperson for JBS stated that the ransom was paid in bitcoin [10].

Overall, there has been a significant increase in the number of ransomware attacks and ransomware as a service (RaaS). REvil and Conti are two specific variants of ransomware that were widespread in 2020-2021 [11]. Analysis of how cyber threat actors employ these types of tools, and how software variants are designed and executed, can bring significant insight into efforts to stop or negate the effects of these attacks [11].

D. *A New Reality*

February 24th, 2022, was the beginning of a new global crisis, with the Russian offensive against Ukraine. Russian President Vladimir Putin announced on that date the beginning of a special military operation that saw combat forces cross into Ukraine [12]. However, several days before the start of movement across the border and the attack of physical forces, Ukraine was the victim of cyber-attacks, likely as the first signal of hostilities [13].

More destructive cyber-attacks were detected by Microsoft's Threat Intelligence Center a few hours before the attack by Russian ground forces. Within just three hours, the new malware was named "FoxBlade," Ukraine cyber defense authorities were notified, and automated detection and prevention systems were updated to block destructive malware that appeared to be targeting Ukraine government ministries and financial institutions [14]. In this new reality, where actions in cyberspace are integrated into multi-domain operations, malware analysis and professional cybersecurity teams emerged as a key component to security and stability.

E. *Implications*

These economic and technological changes made a significant impact on society over the past decade. The evolution of virtual currency and the expanding ability to maintain anonymity in financial transitions can be very appealing to cyber threat actors. The difficulty tracing these funds and identifying the people linked to these virtual currency accounts, also seems very favorable to cybercrime groups [4].

At the same time, we observed a significant trend in migrating from conventional information technology architecture to cloud-based solutions. Although there may be significant cybersecurity benefits to migrating to cloud services, there is still a shared responsibility model between security 'of the cloud' and security 'in the cloud' [7]. Considering this model, a vulnerability to the cloud itself may lead to vulnerabilities to many of the cloud services and organizations involved. A misunderstanding of security requirements by the customer 'in the cloud' may lead to opportunities for exploitation of individual instances.

The growing success in ransomware attacks demonstrated that the associated tactics and techniques can be very profitable to cyber threat actors, as targets with the funding and will to pay large ransoms are available. Finally, the most significant and possibly the most dangerous development in cyber operations was observed as the precursor to Russian aggression into Ukraine. Highly skilled malware analysts demonstrated that cyber defense professionals can have a significant impact in boosting security from nation-state aggression [14].

The impacts of these socio-cultural changes and implications are reflected in the gap in cybersecurity workforce requirements with the current global shortage of 2.72 million cybersecurity professionals [1][2].

III. MALWARE ANALYSIS

To help equip the cybersecurity workforce to meet global cybersecurity requirements, specifically cyber threat analysis and security analysis [2], we consider both a broad coverage and the technical aspects of malware analysis. Major topics here include static and dynamic malware analysis, associated practices and tools, and considerations for developing proficiency.

A. *Static Analysis*

Static analysis is basically a process to understand a program by reading through the code; static analysis does not include the execution of the code [15]. The complexity of programming languages has evolved over several decades, and the term *generation* is commonly used to define the stages of this evolution. IBM lists up to eight generations, but the most significant of these for malware analysis are the first three [16].

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 11 Issue 06, June-2022

1) Generations of Programming Languages

The lowest form of programming languages are first-generation languages (1GL). These are programs in the most basic, directly machine executable form, a sequence of ones and zeros. These 1GL can be referred to as machine language, byte code, or binaries. Binaries are typically viewed by a programmer or analyst in hexadecimal, or hex, for readability. As writing programs at this level is difficult, prone to error, and not portable to other computer architectures, evolution moved to second-generational languages [17].

Second-generation languages (2GL) are a bit easier to read and construct. These languages map the 1GL bit patterns to operation codes, or opcodes. These opcodes are instructions for a specific computer architecture. These assembly languages are still very complex and time-consuming, and programmers primarily use higher-level languages [15][17].

Third-generation languages (3GL) use keywords and constructs. These are a step closer to what we would consider a natural language [15]. These are procedural, general purpose, high-level programming languages. They are much easier to understand, and take advantage of variable names, sequences of commands, selection constructs, and iteration [17].

2) Assembly and Disassembly

Compilers, assemblers, and linkers are all used to create an executable program from a 3GL or higher-level programming language. In general terms, 3GL programs are translated into assembly language by a compiler, 2GL programs are translated into 1GL binaries using an assembler, and external resources are resolved and included using a compiler and/or assembly linker; although, modern compilers may include all of this functionality [15].

3) Topics

Engaging in static analysis involves a breadth of foundational skills. These include programming, file structure, network traffic analysis, operating system theory, disassembly methods, and the use of publicly available resources.

a) Programming skills may be the most significant here, as by definition, the process and assembly/disassembly and compiling/decompiling requires comfort and proficiency working between 2GL and 3GL. Within the domain of programming, emphasis is required in interpreting the use of variables and data structures, implementation of function calls and libraries, debugging, and code obfuscation. This includes the identification of global and local variables, impacts of function parameters and modified values, the management of variables directly in memory, the run-time stack, and considerations for various hardware architectures. Most of these topics can be studied in great detail, so the balance of breadth versus depth is a significant consideration for malware analysis education, particularly at the undergrade level.

b) File structure is important in malware analysis, as malware may be designed to target a particular system or architecture. Microsoft specifications describe Portable Executable (PE) and Common Object File Format (COFF) files. These have specific structures, including file headers, sections tables, section data, symbol tables, and data contents [18]. Similarly, the Executable and Linkable Format (ELF) in Linux has a structure that includes a program header table, section header table, and data [19]. Familiarity with the formats for identification, deconstruction, and data analysis is a good starting point for analyzing malware.

c) Network Traffic Analysis and log analysis involve intercepting, recording, and analyzing network traffic to determine how the system or network was impacted [20]. Network traffic analysis can be used to identify malicious network traffic as well. There are some implicit prerequisites to studying network traffic analysis, to include comfort working in binary and hex, a good understanding of basic networking, and familiarity with various networking protocols. Although internet traffic is fundamentally based on the Transmission Control Protocol/Internet Protocol (TCP/IP) stack, many other public and proprietary protocols are also implemented, particularly when capturing traffic relating to critical infrastructure sectors and services.

d) Operating Systems have different implementations of functionality, architecture, and design based on the developer. Computer networks at almost every level commonly have a mix of operating systems that provide services and sustain operations. At the most basic level, operating system software implements memory management, processor management, device management, file management, and network management. This functionality is linked to a user interface that allows the user to issue commands [21]. The malware analyst should be able to research the impacts of malware across these management systems in a diverse deployment of operating systems.

e) Disassembly can be considered a four-step process. The first step is to identify the program code in the 1GL. At times, it may be difficult to distinguish between program code and program data. Second, is a process of matching binary values to assembly level opcodes. Third, these opcodes are matched with the associated operands and translated into assembly code. Finally, the process is repeated based upon the chosen algorithm [15].

Disassembly methods can produce various results based on the chosen algorithm. There are two general categories of disassembly algorithms, linear sweep disassembly and recursive descent disassembly, with various implementations and combinations of the two. The recursive descent algorithms have advantages over the liner methods, as the recursive algorithms consider the impacts of flow control and branching [15]. These disassembly algorithms are important for the malware analyst to understand, in order to determine the best approach to disassemble the code and to help the analyst decipher the disassembly output and recognize potential misinterpretations.

f) Publicly available resources may provide the best insight into malware behavior. Malware analysts and cybersecurity professionals worldwide maintain online repositories of malware artifacts, behavior, and very detailed analysis. These sites include results of both static and dynamic analysis and can be both detailed and timely.

One of the most popular sites is VirusTotal. Users at this site can upload malware, signatures of malware, and uniform

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 11 Issue 06, June-2022

resource locators (URLs) for inspection by over 70 scanners and services. Results can be publicly shared, and the aggregated data and search capability results in raising the global cybersecurity level through sharing [22].

A suite of resources is also available from the *abuse.ch* website, a research project hosted at Bern University of Applied Sciences in Switzerland. These include the tools listed below [23]:

- *Malware Bazaar* provides shared malware samples [24].
- *Feodo Tracker* provides tracking associated with botnet infrastructure [25].
- *SSL Blacklist* provides lists of malicious Secure Socket Layer (SSL) certificates and related resources for detecting malicious SSL connections [26].
- *URL Haus* provides a collection of malware distribution sites [27].
- *Threat Fox* provides a collection of indicators of compromise (IOC) for threat analysis [28].

A quick web search will reveal that there are numerous other malware analysis and threat intelligence sites available today that provide free, open-source malware analysis support. Below are only a few of these resources, and these do not include sandboxes and dynamic analysis tools, which are discussed in a following section. These resources may also contain very robust government and industry tools as well (not always free or open-source). Malware analysts should track sites that provide meaningful and current malware analysis resources and that support their research style and malware analysis techniques. A few select sites include:

- VirusShare [29]
- Malware-Traffic-Analysis.net [30]
- AZORult Tracker [31]
- ViriBack C2 Tracker [32]
- Cryptolaemus Pastedump [33]
- OTX AlienVault [34]

4) Tools: There are many tools available to support static analysis, assembly, and disassembly. These include classification tools, summary tools, and deep inspection tools [35]. Building a toolkit to support malware analysis depends upon personal preference, comfort working with the software, and the capabilities of each tool. A few of these are included here for experimentation and further research.

- *Programing Skills* and preferences for integrated development environments (IDEs) are generally established by the time a cybersecurity professional or student begins to study malware analysis. A few select IDEs include:

  Python – Integrated Development and Learning Environment (IDLE) [36], PyCharm [37], and Visual Studio Code [38].

  Java/JavaScript – Eclipse [39], NetBeans [40], Xcode [41], and Visual Studio Code [38].

  C/C++ - GNU Compiler Collection (GCC) [42] and Visual Studio Code [38].

  Hex – Hex editors are readily available for various operating systems. A few select options include *010-Editor*, *ghex*, *hexedit*, *hexer*, *hexyl*, *HxD*, *wxHexEditor*, and *xxd* [43] [44] [45].

- *File structure* tools that support analysis of ELF files include *readelf* (displays information on ELF files), *elfdump* (viewing ELF file information), *objdump* (information on ELF and other file formats), *strings*, and *file* (displays information on file architecture) [19]. Additional tools that support analysis of Windows files include *PE Tools*, *PEiD*, *PEview*, *resource Hacker*, *PE Explorer*, and the *dumpbin* utility that is part of the Visual Studio tool suite [15][46]. Many of these tools have functionality to support disassembly as well.

- *Network traffic analysis* is generally conducted using *Wireshark* [47]. Other popular tools include *The Elastic Stack* [48], *TCPdump* [49], and various commercial products.

- *Disassembly* tools include a couple of very popular and powerful tool suites, the Interactive Disassembler (IDA) from hex-rays [50] and Ghidra, developed by the Research Directorate of the National Security Agency in the United States [51]. These tools have very robust capabilities, but students and researchers alike should note that it may take a significant amount of time to understand each set of tools and develop proficiency; however, it is worth the investment.

B. Dynamic Analysis

The goal of malware dynamic analysis is to gain an understanding of the malicious software by observing the details of its execution; this promotes the ability to identify, defeat, and eliminate the threat [46].

Dynamic analysis requires a strictly controlled computing environment, as dynamic analysis is accomplished by actually running the code [15]. Executing malware can be quite dangerous and even have legal consequences if the malware escapes the analysis platform. Control processes must be in place to contain malicious behavior inside the analysis environment and keep it from causing impacts outside of the controlled system or network.

This process includes collecting a malware sample, which again requires very strict controls to avoid escaping the analysis environment. Samples may be collected through network captures, transferred files, and many publicly available websites that post malware samples for analysis.

1) Setting up a Safe Environment

There are a few options to consider when determining the setup of the malware analysis environment. Basic options

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 11 Issue 06, June-2022

include using dedicated hardware, virtual machines, or cloud-based dynamic analysis platforms. Overall, the selection of the analysis network or platform should be focused on containing the malware and managing risk [52].

a) Dedicated hardware has both its advantages and disadvantages. When a dynamic malware analysis platform is built on physical hardware, it will likely avoid virtual machine detection, implemented by advanced malware designers. This is a feature by which malware will attempt to detect a virtual machine environment and not execute malicious portions of the code. Disadvantages include high cost and the lack of flexibility to restore the system to a previous state, depending on the software and operating system implemented [53].

b) Virtual machines are commonly selected for dynamic malware analysis and are generally preferred over dedicated hardware platforms. A virtual environment can replicate the behavior of an entire system, including the processor, memory, and attached devices. This type of full-system emulation can be contained and isolated in a sandbox environment [54]. Other advantages include cost, resiliency in cloning, saving snap-shots, maintenance, and energy savings [55]. Full malware analysis sandbox software, such as Cockoo Sandbox, can be downloaded for local environments [56].

c) Cloud-based analysis platforms may be the best option available for conducting dynamic malware analysis, particularly in an academic setting. Not only are the risks greatly reduced for inadvertent escape of the malware off the platform, but these cloud-based platforms allow access to dynamic malware analysis results by some very skilled professionals. In addition, malware samples may already be loaded into cloud-based solutions for analysis and collaboration to promote global cybersecurity. Samples of these types of online platforms and sandbox environments include:

- *Any.Run* malware analysis sandbox, supporting a large database, public submissions, and over 100,000 individual users and corporations [57].
- *JoeSandbox Cloud* [58].
- *Hatching Triage* malware analysis sandbox [59].

2) Malware Samples

Samples of malware can be collected from many resources, including live network captures. Samples appropriate for practicing dynamic malware analysis skills and samples of actual malware executables can be downloaded for analysis from online repositories and portals. These include academic postings [46][60][52] and websites specifically built to share malware for analysis [23][24].

An additional resource for working with malware samples is also an irreplaceable tool for practicing both static and dynamic malware analysis - *cyber competitions*. Many organizations, corporations, and state/national agencies have a vested interest in educating cyber professionals. This has led to a very robust offering of cyber competitions nationally in the United States. These are tailored to both beginner and advanced malware students and practitioners [20][61][62][63].

3) Topics

Engaging in dynamic analysis involves specific skills related to the previously mentioned foundational skills for dynamic analysis. These include program debugging, monitoring and management of network traffic, memory management, and the leveraging of publicly available online tools and sandboxes.

a) Program debugging skills may be the most important aspect of dynamic malware analysis, as debugging can provide information on malware that can not be learned through static analysis and disassembly. The significant capability in debugging is that the malware analyst can observe code execution at runtime and examine states of memory, variable and register management, flow control, and overall process control. Process control, such as pausing or stepping through program execution, allows the malware analyst to observe the malware in action, monitor specific debugging events, and better analyze the impact of code execution [46][64].

b) Network traffic monitoring and management supports the ability of the analyst to discover external resources used in the execution of the malware. As discussed above, network traffic recording and log analysis provide detailed information supporting malware analysis [20]. Network traffic monitoring and management is closely related to network traffic analysis, but highlighted here, as it more closely relates to malware at execution time and indications of an active attack. Visibility and management of internal network traffic and monitoring of the network perimeter can provide insight into external intrusions, exfiltrated data, and attacks in progress. Enabled services, open ports, external connections, and network traffic alerts can be indicators of active intrusions [65].

c) Memory management has a key role in malware execution, as many types of malware target specific operating systems, particular versions of software applications, and various memory management techniques. Although the allocation and management of memory can be interpreted and predicted using static analysis, its actual use and values can be directly observed using dynamic analysis. Memory management or memory manipulation can be observed by following the assignment of register values, the manipulation of the run-time stack, and portions of both executable and nonexecutable memory.

d) Publicly available platforms may provide the best available resource for dynamic malware analysis. International malware analysts contribute samples and recorded captures of malware execution on platforms accessible to the public. In some instances, access to these resources requires a subscription. These online repositories provide malware artifacts, examine the behavior of the malware at runtime, and provide analysis products. These sites include results of both static and dynamic analysis and can be both detailed and timely [22][23][24][29][34].

4) Tools: There are many tools available to support program debugging, network traffic monitoring and management, and memory management. Selection and construction of a personal toolkit depends on personal preference, comfort working with the software, and capabilities of each tool on your selected operating system(s). A few of these are included here for experimentation and further research.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 11 Issue 06, June-2022

- *Program Debugging* tools may be developed for specific or multiple operating systems. Debuggers are designed to debug at the source level and/or assembly level. Debugging tools include:

  Windows - WinDbg, OllyDbg, and Kernel Debugger [46][64]

  Linux - the GNU Project debugger [66] and LLDB [67].

  Multiple operating systems - IDA Pro [35] and Ghidra 10.1.3 [51].

- *Network traffic monitoring and management* tools are provided by many reputable cybersecurity organizations. A few examples are extended detection and response (XDR); security, information, and event management (SIEM) systems offered by Rapid7 [65]; Crowdstrike [68] products, and Splunk [69]. There are also many open-source or free tools available, including Cacti [70], Prometheus [71], Suricata [72], and Spiceworks [73].

- *Memory Management* and program debugging tools listed above are important in setting breakpoints to pause execution, observing memory contents, dumping memory, and editing values for analysis. There are also several other memory management and analysis tools available including memdump [74], Volatility [75], and Autopsy [76].

IV. Integration of Malware Analysis Techniques in Undergraduate Cybersecurity Programs

Considering the significance of socio-cultural changes and the robust scope of malware analysis topics covered here, both static and dynamic, it quickly becomes evident that the integration of malware analysis techniques in undergraduate programs is much more robust then developing a new course. It is a reassessment of the entire undergraduate cybersecurity program and curriculum to build both the foundational and core student learning outcomes (SLOs) necessary to meet workforce demands and counter a rapidly evolving cyber threat.

Although the topics and outcomes listed below use specific language and word choice, outcomes should be adjusted to meet the program specific vision and mission for each institution. It is important to keep the focus on the foundational and core outcomes required to integrate malware analysis concepts, techniques, and tools into undergraduate cybersecurity programs. It is also important to note that this is not a comprehensive list of SLOs for a cybersecurity degree program, but a list of SLOs that support the integration of malware analysis requirements into undergraduate cybersecurity programs. These outcomes are a product of the analysis and decomposition of malware analysis topics and requirements discussed in detail above.

A. Foundational Malware Analysis SLOs

SLOs at the foundational level are necessary to prepare students to be successful in meeting core malware analysis learning outcomes. However, at the same time, these foundational skills can be important in supporting the development of information technology and computer science students. Achieving these outcomes may have a very wide application at both the program and college / university level. Foundational requirements address both strategic and technical requirements.

Strategic

1) Describe socio-cultural factors that impact global cybersecurity requirements.
2) Discuss the evolution and use of virtual currencies and cryptocurrencies.
3) Explain the implications of ransomware attacks on industry and public services.
4) Explain the implications of cloud computing and cloud services.
5) List key skills needed for cybersecurity professions to meet expanding cybersecurity workforce requirements.
6) Explain cyber threat analysis and available threat analysis resources.
7) Explain the implications of modern cyber conflicts.

Technical

8) Design, implement, and manage a network.
9) Design, implement, and manage a cloud-based computing system or network.
10) Conduct analysis of network traffic artifacts.
11) Conduct a cybersecurity vulnerability analysis of a computing system or network.
12) Demonstrate proficiency in the fundamentals of computer programming.
13) Compare modern programming languages.
14) Demonstrate the deployment and management of major operating system implementations.
15) Demonstrate proficiency in the fundamentals of databases.
16) Implement and manage a virtual machine.

B. Core Malware Analysis SLOs

More specific SLOs at the core level build upon foundational skills to better educate the undergraduate cybersecurity student in malware analysis requirements. These SLOs are more specific to malware analysis; however, they also support the success of information technology and computer science students, prepared for more advanced analysis and research.

1) Demonstrate the ability to program and debug first and second generation languages.
2) Obtain malware samples for analysis.
3) Describe the elements of file structure.
4) Analyze code using a disassembler.
5) Analyze malware using publicly available resources.
6) Design and implement a secure malware analysis platform using virtual machines.
7) Identify and describe cloud computing security issues.
8) Complete dynamic analysis of malware using a cloud-based malware analysis platform.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 11 Issue 06, June-2022

9) Use network traffic monitoring and management to recognize malware.

10) Analyze malware during executing using a debugger.

11) Inspect and interpret memory management during malware execution.

12) Practice malware analysis using static analysis tools and techniques.

13) Practice malware analysis using dynamic analysis tools and techniques.

14) Prepare a malware evaluation report based on completed static and dynamic malware analysis.

C. Continuing Evolution

Cybersecurity is a highly technical and evolving field. This trend and need for cybersecurity professionals will likely be a challenge for many years, due to socio-cultural changes and the dependency of industry and critical services on interconnected networks.

As technology and malicious cyber threat actors continue to evolve, so must the approach to educate undergraduates and prepare them to join the global cybersecurity workforce. This research is analysis of one aspect of cybersecurity at a specific time in history. To keep cybersecurity education programs current, the cycle of observing and studying global cyber issues and assessing cybersecurity programs is continuous and evolving.

ACKNOWLEDGMENT

The intent of this research is to offer analysis, and hopefully a bit of insight, of the requirements to integrate malware analysis concepts, techniques, and tools into undergraduate cybersecurity programs. This analysis is intended to contribute to continuous improvement of cybersecurity programs, and at the same time, offer a resource for colleges and universities seeking to design new degree programs.

Contributions in this field include generations of researchers, operators, and scientists. Not only are these professionals providing exceptional career opportunities for graduates, but these efforts directly promote the success of industry and the ability to safely provide critical services to the population. Thank you for your hard work, dedication, and keen intellect. Finally, thank you to my dad, Hal Chapman, an Aerospace Engineer, who started me off so many years ago with a brand-new Apple II+ and a cassette tape recorder. Technology evolves so quicky.

REFERENCES

[1] U.S. Bureau of Labor Statistics. "Occupational Outlook Handbook." 15 September 2021. www.bls.gov. 25 January 2022.

[2] (ISC)^2. "A Resilient Cybersecurity Profession Charts the Path Forward." 2021. *www.isc2.org*. 25 January 2022. pp16-24.

[3] Bard, Kathryn A. *An Introduction to the Archeology of Ancient Egypt*. second. Chichester, West Sussex: Wiley-Blackwell, 2015. p.21.

[4] Baron, Joshua, et al. National Security Implications of Virtual Currency. Santa Monica: RAND Corporation, 2015.

[5] Bloomberg. "Global Cryptocurrencies 2022 Outlook." December 2021. https://assets.bbhub.io. 2 February 2022.

[6] Amazon Web Services. "Overview of Amazon Web Services - AWS Whitepaper." 12 January 2022. *www.docs.aws.amazon.com*. 4 January 2022.

[7] Amazon Web Services. "Amazon Web Services: Risk and Compliance." 11 March 2021. *www.docs.aws.amazon.com*. 4 January 2022.

[8] Turton, William and Kartikay Mehrotra. "Hackers Breached Colonial Pipeline Using Compromised Password." 4 June 2021. www.bloomberg.com. article. 29 01 2022.

[9] Johnson, Kevin and Josh Meyer. "Majority of $4.4 million cryptocurrency ransom payment in Colonial Pipeline hack recovered." 7 June 2021. *www.usatoday.com*. 30 January 2022.

[10] Reuters. "Meatpacker JBS says it paid equivalent of $11 million in ransomware attack." 10 June 2021. *www.reuters.com*. 30 January 2022.

[11] Smith, Randy Franklin, et al. *Using the MITRE ATT&CK Framework to Boost Ransomware Defenses*. Boulder: LogRhythm Inc., 2022.

[12] BBC News Visual Journalism Team. "Ukraine conflict: Simple visual guide to the Russian Invasion." 26 02 2022. *www.bbc.com*. 01 03 2022.

[13] Tsvetkova, Maria, Dmitry Antonov and Andrea Shalal. "Ukraine hit by cyber attack as U.S. questions Russian troop pullback." 15 02 2022. *www.reuters.com*. 01 03 2022.

[14] Sanger, David E, Julian E Barnes and Kate Conger. "As Tanks Rolled into Ukraine, so did Malware. Then Microsoft Entered the War." 28 02 2022. *www.nytimes.com*. 01 03 2022.

[15] [15] Eagle, Chris and Kara Nance. *The Ghidra Book*. San Francisco: No Starch Press, 2020.

[16] [16] IBM. "Application programming on z/OS." 2010. *www.ibm.com*. 12 January 2022.

[17] O'Regan, Gerard. "Computer Programming Languages." O'Regan, Gerard. *A Brief History of Computing*. London: Springer, 2008.

[18] Microsoft. "PE Format." 11 November 2021. *docs.microsoft.com*. 18 February 2022.

[19] Tool Interface Standard (TIS) Committee. "Tool Interface Standard (TIS) Executable and Linking Format (ELF) Specification Version 1.2." 1995.

[20] National Cyber League. "Network Traffic Analysis." n.d. www.nationalcyberleague.org/categories/network-traffic-analysis. 22 February 2022.

[21] McHoes, Ann McIver and Ida M Flynn. *Understanding Operating Systems*. Sixth. Boston: Course Technology, Cengage Learning, 2011.

[22] VirusTotal. *www.virustotal.com*. n.d. 03 03 2022.

[23] abuse.ch. *Fighting Malware and Botnets: Our Mission*. 2021. 07 03 2022.

[24] bazaar.abuse.ch. *MalwareBazaar*. 2022. 07 03 2022

[25] feodotracker.abuse.ch. *Feodo Tracker*. 2022. 07 03 2022+

[26] sslbl.abuse.ch. *SSLBL*. 2022. 07 03 2022

[27] urlhaus.abuse.ch. *URLhaus*. 2022. 07 03 2022

[28] threatfox.abuse.ch. *ThreatFox*. 2022. 07 03 2022

[29] virusshare.com. *VirusShare*. 2022. 07 03 2022

[30] malware-traffic-analysis.net. 2022. 07 03 2022

[31] azorult-tracker.net. *AZORult Tracker*. 2022. 07 03 2022

[32] tracker.viriback.com. *C2 Tracker*. 2022. 07 03 2022

[33] paste.cryptolaemus.com. *Cryptolaemus Pastedump*. 2022. 07 03 2022

[34] otx.alienvault.com. The World's First Truly Open Threat Intelligence Community. Alienvault, Inc. 2022. 07 03 2022

[35] Eagle, Chris. *The IDA Pro Book*. San Francisco: No Starch Press, 2011.

[36] python.org. "IDLE." 21 03 2022. *docs.python.org/3/library/idel.html*. 21 03 2022.

[37] "PyCharm: The Python IDE for Professional Developers." 21 03 2022. *jetbrains.com/pycharm*.

[38] "Visual Studio Code: Code editing redefined." 21 03 2022. *code.visualstudio.com*.

[39] "The Community for Open Innovation and Collaboration." 21 03 2022. *eclipse.org*.

[40] "Apache NetBeans." 21 03 2022. *netbeans.apache.org*.

[41] "Xcode." 21 03 2022. *Developer.apple.com/documentation/xcode*.

[42] "GCC, the GNU Compiler Collection." 21 03 0200. *Gcc.gnu.org*.

[43] "How to install and use Hex editor on Kali Linux." 23 03 2022. *Linuxconfig.org*.

[44] "Top 10 Hex Editors for Linux." 23 03 2022. *geeksforgeek.org*.

[45] "What are the best hex editors?" 23 03 2022. *slant.co*.

[46] Sikorski, Michael and Andrew Honig. *Practical Malware Analysis*. San Francisco: No Starch Press, 2012.

[47] "Wireshark." 21 03 2022. *wireshark.org*.

[48] "The Elastic Stack." 21 03 2022. *elastic.co*.

[49] "TCPdump & Libpcap." 21 03 2022. *tcpdump.org*.

[50] "Solutions: Hex-Rays tools are used to solve critical problems in the software industry." 23 03 2022. *hex-rays.com/solutions/*.

[51] "Ghidra: A software reverse engineering (SRE) suite of tools developed by the NSA's Research Directorate in support of the Cybersecurity mission." 23 03 2022. *ghidra-sre.org*.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 11 Issue 06, June-2022

[52] “Practical Malware Analysis.” 24 03 22. *nostarch.com/malware.*
[53] Kirat, Dhilung, Giovanni Vigna and Christopher Kruegel. "BareBox: efficient malware analysis on bare-metal." *In Proceedings of the 27th Annual Computer Security Applications Conference (ACSAC '11). Association for Computing Machinery* (2011): 403-412.
[54] “What is Malware Analysis.” 29 03 2022. VMware, Inc. *www.vmware.com.*
[55] “5 Benefits of Virtualization.” 29 03 2022. IBM. *www.ibm.com/cloud/blog/5-benefits-of-virtualization.*
[56] Cockoo Automated Malware Analysis.” 04 01 2022. Stichting Cuckoo Foundation. *https://cuckoosandbox.org/*.
[57] “Malware Research with Any.Run.” 01 04 2022. Any.Run. *https://any.run/why-us*.
[58] “JoeSandbox Cloud.” 01 04 2022. Joe Security LCC. *https://www.joesandbox.com*.
[59] “Welcome to Triage.” 01 04 2022. Hatching B.V. *https://tria.ge/*.
[60] “Running the Gauntlet.” 24 03 2022. *practicalmalwareanalysis.com/labs/.*
[61] “President’s Cup Cybersecurity Competition.” 04 05 2022. Cybersecurity & Infrastructure Security Agency. *cisa.gov/presidentscup*.
[62] “US CyberQuests.” 04 05 2022. *uscc.cyberquests.org*.
[63] “Air Force Association’s CyberPatriot.” 05 04 2022. Northrop Grumman Foundation. *uscyberpatiot.org*.
[64] Dang, et al. *Practical Reverse Engineering*. Indianapolis: John Wiley & Sons, Inc., 2014.
[65] “Network Traffic Analysis: The importance of network traffic analysis and monitoring in your cybersecurity program.” 04 05 2022. Rapid7. *https://www.rapid7.com/fundamentals/network-traffic-analysis/.*
[66] “GDB: The GNU Project Debugger.” 03 05 2022. Free Software Foundation, Inc. *https://www.sourceware.org/gdb/.*
[67] “The LLDB Debugger.” 03 05 2022. The LLDB Team. *https://lldb.llvm.org/*.
[68] “VDR vs SIEM vs SOAR.” 04 05 2022. Crowdstrike. *https://www.rapid7.com/fundamentals/network-traffic-analysis/.*
[69] “Splunk Security.” 04 05 2022. Splunk Inc. *https://www.splunk.com/en_us/software/cyber-security.html*.
[70] “About Cacti.” 04 05 2022. The Cacti Group, Inc. *https://www.cacti.net/*.
[71] “From metrics to insight.” 04 05 2022. Prometheus Authors. *https://prometheus.io/*.
[72] “Suricata: Community Driven. Always Alert.” 04 05 2022. Open Information Security Foundation (OISF). *https://suricata.io/*.
[73] “Spiceworks IT Tools for IT Pros.” 04 05 2022. Spiceworks. *https://community.spiceworks.com/tools*.
[74] “Memdump.” 05 05 2022. OffSec Services Limited. *https://www.kali.org/tools/memdump/*.
[75] “Volatility Foundation.” 05 05 2022. The Volatility Foundation. *https://www.volatilityfoundation.org/*.
[76] “Autopsy.” 05 05 2022. Basis Technology. *https://www.autopsy.com/about/*.