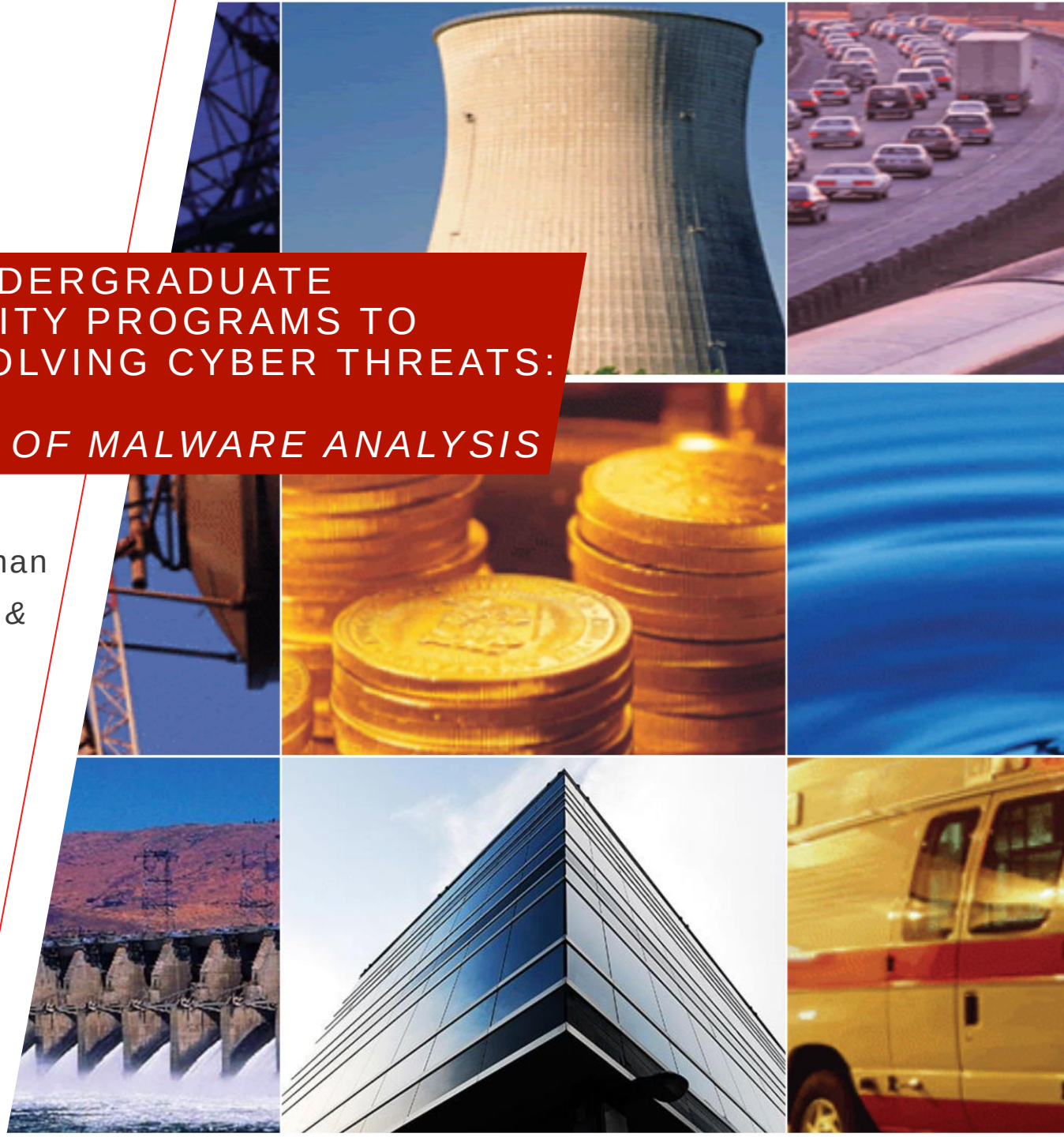
EVOLVING UNDERGRADUATE CYBERSECURITY PROGRAMS TO COUNTER EVOLVING CYBER THREATS:

INTEGRATION OF MALWARE ANALYSIS

Dr. Matthew A. Chapman

Computer Science & Cybersecurity



OCCUPATIONAL OUTLOOK FOR CYBERSECURITY PROFESSIONALS

- Global Shortage of Cybersecurity Professionals (2.72 million)[1]
- The need for cybersecurity professionals with a bachelor's degree is increasing by 33% [2]

"Demand for information security analysts is expected to be very high. Cyberattacks have grown in frequency, and analysts will be needed to come up with innovative solutions to prevent hackers from stealing critical information or creating problems for computer networks."

[1] (ISC)2. "A Resilient Cybersecurity Profession Charts the Path Forward." 2021. www.isc2.org. 25 January 2022. pp16-24.
[2] U.S. Bureau of Labor Statistics. "Occupational Outlook Handbook." 15 September 2021. www.bls.gov. 25 January 2022.

CAE IN CYBERSECURITY COMMUNITY

SOCIAL – CULTURAL CHANGES

VIRTUAL CURRENCY

- A digital representation of value (stored, traded, transferred electronically)[3]
- Generally, not issued by a central bank[3]
- Cryptocurrencies are a specific kind of virtual currency[3]
  - Bitcoin, Ethereum, Crypto Dollars
  - Gained momentum with decentralized authority and anonymity

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

MOVING TO THE CLOUD

- Organizations transitioned information technology and data processing requirements to cloud-based solutions increasingly over the past decade.
- Cloud Computing Services
  - Infrastructure as a service
  - Platform as a service
  - Software as a service

- Security: Amazon Web Services (AWS) “Shared Responsibility Model”[4]
  - AWS manages the cybersecurity ‘of the cloud.’
  - It is the customers’ responsibility to manage cybersecurity ‘in the cloud.’

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

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 with a paid ransom of $4.4 million[5].
  - June 2021, Reuters reported that operations at **JBS Meatpacking** were disrupted, and a ransom was paid of about $11 million[6].

[5] Turton, William and Kartikay Mehrotra. "Hackers Breached Colonial Pipeline Using Compromised Password." 4 June 2021. www.bloomberg.com. article. 29 01 2022.
[6] Reuters. "Meatpacker JBS says it paid equivalent of $11 million in ransomware attack." 10 June 2021. www.reuters.com. 30 January 2022.

A NEW REALITY

- February 24th, 2022, was the beginning of a new global crisis, with the Russian offensive against Ukraine[7].
- 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 the first signal of hostilities[8].

[7] BBC News Visual Journalism Team. "Ukraine conflict: Simple visual guide to the Russian Invasion." 26 02 2022. www.bbc.com. 01 03 2022.
[8] 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.

A NEW REALITY

- 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[9].

[9] 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.

IMPLICATIONS OF SOCIAL – CULTURAL CHANGES

- Virtual currency and cryptocurrency
  - Anonymity in financial transitions can be very appealing to cyber threat actors. Difficulty tracing funds and identifying people linked to virtual currency accounts, also seems very favorable to cybercrime groups.
- Cloud-based computing solutions
  - A vulnerability to the cloud itself may lead to vulnerabilities in 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.
- Ransomware
  - 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.
- Cyber operations in a multi-domain operation
  - 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.

IMPLICATIONS TO CYBER WORKFORCE DEVELOPMENT

- The impacts of 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].
- The same workforce study highlights employers' top professional development areas[1]:
  - Cyber Threat Analysis
  - Cloud Computing security
  - Security Analysis

EVOLVING UNDERGRADUATE CYBERSECURITY PROGRAMS TO COUNTER EVOLVING CYBER THREATS

- Equipping the cybersecurity workforce to meet global cybersecurity requirements requires both a broad coverage of international cyber issues and the technical aspects of malware and threat analysis.

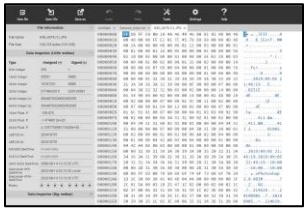
  - Social-cultural changes
  - Modern cyber conflicts
  - **Static malware analysis**
  - **Dynamic malware analysis**
  - Associated practices and tools

STATIC MALWARE ANALYSIS

CAE IN CYBERSECURITY COMMUNITY

PROGRAMMING SKILLS

- Binaries
- Assembly
- 3rd – Gen languages



FILE STRUCTURE AND FORMATS

- Portable Executable (PE) files
- Common Object File Format (COFF)
- Executable and Linkable Format (ELF)

NETWORK TRAFFIC ANALYSIS

- Intercept
- Record
- Analyze

OPERATING SYSTEMS

Management of:

- Memory
- Processor
- Devices
- Files
- Network

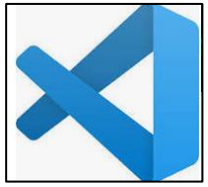
ASSEMBLY AND DISASSEMBLY

- Compliers
- Assemblers
- Linkers
- Disassembly

DYNAMIC MALWARE ANALYSIS

PROGRAMMING DEBUGGING

- Observe code execution
- Examine memory and variables
- Observe flow control
- Observe internal and external actions

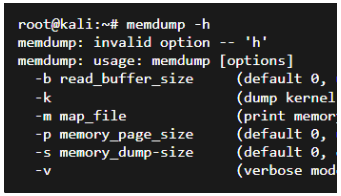


NETWORK TRAFFIC MONITORING AND MANAGEMENT

- Find external components
- Inbound and outbound traffic
- Enables services
- External connections

MEMORY MANAGEMENT

- Allocation of memory
- Memory manipulation
- Run-time stack



ANALYSIS PLATFORMS

- Setting-up a safe environment
- Dedicated hardware
- Virtual machines
- Cloud-based platforms

EVOLVING UNDERGRADUATE CYBERSECURITY PROGRAMS TO COUNTER EVOLVING CYBER THREATS[10]

- Cyber workforce development and education require a set of both foundational and core leaning outcomes to meet demands of industry and crucial service providers.
- New requirements should be integrated into current curriculum or continuing education programs.
- https://www.ijert.org/integration-of-malware-analysis-concepts-techniques-and-tools-in-undergraduate-cybersecurity-programs
  - Foundational outcomes
    - Strategic (7)
    - Technical (9)
  - Core malware analysis outcomes (14)

[10] Matthew A. Chapman, 2022, Integration of Malware Analysis Concepts, Techniques, and Tools in Undergraduate Cybersecurity Programs, INTERNATIONAL JOURNAL OF ENGINEERING RESEARCH & TECHNOLOGY (IJERT) Volume 11, Issue 06 (June 2022)

EVOLVING UNDERGRADUATE CYBERSECURITY PROGRAMS TO COUNTER EVOLVING CYBER THREATS[10]

Foundations – 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.

[10] Matthew A. Chapman, 2022, Integration of Malware Analysis Concepts, Techniques, and Tools in Undergraduate Cybersecurity Programs, INTERNATIONAL JOURNAL OF ENGINEERING RESEARCH & TECHNOLOGY (IJERT) Volume 11, Issue 06 (June 2022)

EVOLVING UNDERGRADUATE CYBERSECURITY PROGRAMS TO COUNTER EVOLVING CYBER THREATS[10]

Foundations – Technical

1. Design, implement, and manage a network.
2. Design, implement, and manage a cloud-based computing system or network.
3. Conduct analysis of network traffic artifacts.
4. Conduct a cybersecurity vulnerability analysis of a computing system or network.
5. Demonstrate proficiency in the fundamentals of computer programming.
6. Compare modern programming languages.
7. Demonstrate the deployment and management of major operating system implementations.
8. Demonstrate proficiency in the fundamentals of databases.
9. Implement and manage a virtual machine.

[10] Matthew A. Chapman, 2022, Integration of Malware Analysis Concepts, Techniques, and Tools in Undergraduate Cybersecurity Programs, INTERNATIONAL JOURNAL OF ENGINEERING RESEARCH & TECHNOLOGY (IJERT) Volume 11, Issue 06 (June 2022)

INTEGRATION OF MALWARE ANALYSIS[10]

Core Malware Analysis Outcomes

1. Demonstrate the ability to program and debug first and second gen. 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 analysis platform.
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

[10] Matthew A. Chapman, 2022, Integration of Malware Analysis Concepts, Techniques, and Tools in Undergraduate Cybersecurity Programs, INTERNATIONAL JOURNAL OF ENGINEERING RESEARCH & TECHNOLOGY (IJERT) Volume 11, Issue 06 (June 2022)

QUESTIONS

Dr. Matthew A. Chapman

Computer Science & Cybersecurity