**George Mason University College of Engineering & Computing**

**Rapid Prototype Research Center (RPRC)**

**1. Introduction**

George Mason University (GMU), renowned for its leadership in innovative research, houses the College of Engineering & Computing (CEC) and its specialized Rapid Prototype Research Center (RPRC). Our mission is to advance knowledge in critical areas including cybersecurity, malware analysis, forensic attribution, and digital forensics, with a focus on creating practical solutions that address national security challenges. This capability statement outlines our expertise, past performance, and capacity to support projects under the IARPA BAA Source Code program and other U.S. Government initiatives.

**2. Core Competencies**

* **Cybersecurity and Threat Intelligence**
  + Advanced research in network security, malware detection, and cyber threat analytics.
  + Development of cybersecurity standards and best practices.
  + Expertise in threat intelligence platforms and adversary behavior analysis.
* **Digital Forensics and Malware Analysis**
  + Leading research in digital forensic techniques for malware attribution and analysis.
  + Development of tools for forensic analysis and threat detection.
  + Expertise in reverse engineering and binary analysis for malware characterization.
* **Forensic Attribution and Incident Response**
  + Pioneering research in cyber attack attribution methodologies.
  + Expertise in identifying and attributing cyber threats through forensic evidence.
  + Development of AI tools for automated forensic analysis and attribution.
* **Rapid Prototyping and Applied Research**
  + Rapid development and testing of prototype solutions for national security applications.
  + Multidisciplinary research teams integrating software engineering, cyber-forensics, and machine learning.
  + Experience in transitioning research innovations to practical applications.

**3. Past Performance**

GMU's CEC and RPRC have a proven track record of delivering high-impact research and solutions in cybersecurity and digital forensics, as highlighted in several key projects and publications:

* **Malware Analysis and Forensics**:
  + **Research on Malware Detection and Analysis**: GMU has been at the forefront of malware detection, digital forensics, and the development of advanced forensic analysis tools​​​​.
  + **Subject Matter Expertise**: Our RPRC provides expert analysis in malware forensic attribution and has developed tools to combat current and emerging malware threats​​.
* **Cybersecurity Initiatives**:
  + **Cybersecurity Research and Development**: GMU has launched initiatives to improve cybersecurity measures, develop threat intelligence analytics, and create tools for combatting cyber threats​​​​.
  + **Cybersecurity Standards**: Participation in developing cybersecurity standards and guidelines through bibliometrics, contributing to setting benchmarks in the field​​.
* **Forensic Attribution**:
  + **Forensic Attribution Techniques**: Extensive research in forensic attribution methods to enhance the identification of cyber attack origins, including the exploration of new forensic approaches​​​​.
  + **Digital Forensics Conferences**: Active participation in international conferences, presenting research on forensic techniques such as authorship attribution and malware analysis​​.
* **Collaborations and Multidisciplinary Expertise**:
  + **Multidisciplinary Research Teams**: GMU fosters collaborations that include experts in binary analysis, software engineering, cyber-forensics, and machine learning, addressing complex challenges in cybersecurity and digital forensics​​​​.

**4. Key Publications**

GMU faculty have published extensively in high-impact journals and conference proceedings, contributing significantly to the fields of cybersecurity, malware analysis, and forensic attribution:

* **Advances in Digital Forensics XI**:
  + **Authors**: Jim Chen and others
  + **Publication**: Springer
  + **Link**: [Advances in Digital Forensics XI](https://link.springer.com/content/pdf/10.1007/978-3-642-41148-9.pdf)
  + **Summary**: This publication explores advancements in digital forensics, including authorship attribution and malware analysis, highlighting the role of digital forensic techniques in cybersecurity and software engineering.
* **Binary Code Fingerprinting for Cybersecurity**:
  + **Authors**: A. Rahimian, L. Nouh, D. Mouheb, H. Huang
  + **Publication**: Springer
  + **Link**: [Binary Code Fingerprinting for Cybersecurity](https://link.springer.com/content/pdf/10.1007/978-3-030-34238-8.pdf)
  + **Summary**: This research focuses on binary code fingerprinting for cybersecurity, particularly in identifying and characterizing malicious code. It emphasizes reverse engineering and malware analysis in digital forensics.
* **Achieving Attribution**:
  + **Authors**: C. Guitton
  + **Publication**: King's College London
  + **Link**: [Achieving Attribution](https://kclpure.kcl.ac.uk/portal/files/179736269/2014_Guitton_Clement_1016638_ethesis.pdf)
  + **Summary**: This thesis discusses the challenges and methodologies of cyber attribution, focusing on the importance of forensic evidence in tracing the origins of cyber attacks and enhancing cyber forensics.
* **International Symposium on Digital Forensics and Security**:
  + **Authors**: A. Varol, M. Karabatak, C. Varol
  + **Publication**: ISDFS
  + **Link**: [International Symposium on Digital Forensics and Security](https://isdfs.org/wp-content/uploads/2023/05/ISDFS2023-ABSTRACT-Book-2023.05.17.pdf)
  + **Summary**: This publication covers topics in digital forensics and security, including malware analysis and threat attribution, and discusses new methodologies for detecting and analyzing cyber threats.
* **Cyber Security Body of Knowledge and Curricula Development**:
  + **Authors**: EM Abu-Taieh, AA Al Faries, ST Alotaibi
  + **Publication**: IntechOpen
  + **Link**: [Cyber Security Body of Knowledge and Curricula Development](https://www.intechopen.com/chapters/61635)
  + **Summary**: This chapter provides an overview of cybersecurity knowledge and curricula development, focusing on digital forensics and cyber crime.

**5. Certifications and Recognitions**

* **Certifications**:
  + Certified Information Systems Security Professional (CISSP)
  + Certified Ethical Hacker (CEH)
  + Certified Computer Forensics Examiner (CCFE)
* **Recognitions**:
  + Recognized by the National Security Agency (NSA) and the Department of Homeland Security (DHS) as a National Center of Academic Excellence in Cyber Defense Education.
  + Recipient of multiple federal research grants for cybersecurity and digital forensics.

**6. Partnerships and Collaborations**

* **Federal Agencies**:
  + Collaborations with the Department of Defense (DoD), Department of Homeland Security (DHS), and the Intelligence Advanced Research Projects Activity (IARPA).
  + Active participation in federally funded research initiatives and consortia.
* **Industry Partnerships**:
  + Partnerships with leading cybersecurity firms and technology companies.
  + Collaborative research projects with industry to develop innovative cybersecurity solutions and tools.
* **Academic Collaborations**:
  + Joint research projects with top universities and research institutions globally.
  + Participation in academic consortia focused on advancing cybersecurity and digital forensics research.

**7. Facilities and Resources**

* **Rapid Prototype Research Center (RPRC)**:
  + State-of-the-art facilities for rapid prototyping and applied research.
  + Equipped with advanced tools for cybersecurity research, digital forensics, and malware analysis.
* **Cybersecurity Labs**:
  + Advanced laboratories for cybersecurity research and experimentation.
  + Facilities for developing and testing cybersecurity solutions, including threat detection and analysis tools.
* **Forensics Labs**:
  + Specialized labs for digital forensics and malware analysis.
  + Equipped with tools for forensic examination and analysis of digital evidence.

**8. Research and Development Capabilities**

* **Cybersecurity Research**:
  + Expertise in developing and testing cybersecurity solutions, including intrusion detection systems and threat intelligence platforms.
  + Research in cybersecurity policy, standards, and best practices.
* **Digital Forensics Research**:
  + Leading research in digital forensics techniques, including malware analysis and forensic attribution.
  + Development of tools for forensic analysis and investigation.
* **Forensic Attribution Research**:
  + Innovative research in cyber attack attribution methodologies.
  + Development of AI tools for automated forensic analysis and attribution.
* **Prototype Development**:
  + Rapid development of prototype solutions for national security applications.
  + Multidisciplinary research teams integrating software engineering, cyber-forensics, and machine learning.

**9. Commitment to Excellence**

George Mason University’s College of Engineering & Computing, through its Rapid Prototype Research Center, is committed to advancing research and innovation in cybersecurity, digital forensics, and forensic attribution. Our expertise, proven track record, and state-of-the-art facilities make us a valuable partner for the U.S. Government and industry in addressing critical national security challenges.

**Appendix: Key Publications and References**

GMU faculty have published extensively in high-impact journals and conference proceedings, contributing significantly to the fields of cybersecurity, malware analysis, and forensic attribution:

* **Advances in Digital Forensics XI**:
  + **Authors**: Jim Chen and others
  + **Publication**: Springer
  + **Link**: [Advances in Digital Forensics XI](https://link.springer.com/content/pdf/10.1007/978-3-642-41148-9.pdf)
  + **Summary**: This publication explores advancements in digital forensics, including authorship attribution and malware analysis, highlighting the role of digital forensic techniques in cybersecurity and software engineering.
* **Binary Code Fingerprinting for Cybersecurity**:
  + **Authors**: A. Rahimian, L. Nouh, D. Mouheb, H. Huang
  + **Publication**: Springer
  + **Link**: [Binary Code Fingerprinting for Cybersecurity](https://link.springer.com/content/pdf/10.1007/978-3-030-34238-8.pdf)
  + **Summary**: This research focuses on binary code fingerprinting for cybersecurity, particularly in identifying and characterizing malicious code. It emphasizes reverse engineering and malware analysis in digital forensics.
* **Achieving Attribution**:
  + **Authors**: C. Guitton
  + **Publication**: King's College London
  + **Link**: [Achieving Attribution](https://kclpure.kcl.ac.uk/portal/files/179736269/2014_Guitton_Clement_1016638_ethesis.pdf)
  + **Summary**: This thesis discusses the challenges and methodologies of cyber attribution, focusing on the importance of forensic evidence in tracing the origins of cyber attacks and enhancing cyber forensics.
* **International Symposium on Digital Forensics and Security**:
  + **Authors**: A. Varol, M. Karabatak, C. Varol
  + **Publication**: ISDFS
  + **Link**: [International Symposium on Digital Forensics and Security](https://isdfs.org/wp-content/uploads/2023/05/ISDFS2023-ABSTRACT-Book-2023.05.17.pdf)
  + **Summary**: This publication covers topics in digital forensics and security, including malware analysis and threat attribution, and discusses new methodologies for detecting and analyzing cyber threats.
* **Cyber Security Body of Knowledge and Curricula Development**:
  + **Authors**: EM Abu-Taieh, AA Al Faries, ST Alotaibi
  + **Publication**: IntechOpen
  + **Link**: [Cyber Security Body of Knowledge and Curricula Development](https://www.intechopen.com/chapters/61635)
  + **Summary**: This chapter provides an overview of cybersecurity knowledge and curricula development, focusing on digital forensics and cyber crime.