Mohammad Rezaeirad

☎ *(225) 439 6424*
✉ *mrezaeir@gmu.edu*
homepage: mason.gmu.edu/∼mrezaeir/Aboutme.htm

RESEARCH INTEREST

I am interested and working in the fields of Cyber-Physical Security. I enjoy developing measurement strategies and tools to evaluate the defense capacity of cyber systems. I particularly excited about studying manually operated malware. The fundamental topics that I have worked on and, influenced my interests are: System Security, Network Security, and Modern Cryptography.

EDUCATION

Ph.D., Information Security and Assurance
George Mason University, USA, (August 2013-Current).
Advisors: Dr. Damon McCoy.

Master of Science, Computer Engineering (GPA: 4.00)
University of Louisiana at Lafayette, USA, (Dec 2012).
Thesis: A Novel Clustering Paradigm for Pre-distribution Key Management for Mobile Homogeneous Wireless Sensor Networks
Advisors: Dr. Magdy Bayoumi & Dr. Dmitri Perkins.

Bachelor of Information Technology (Honours), Security Technology (GPA: 3.28)
Multimedia University, Malaysia, (Jan 2010).
Thesis: An Analysis & Design of An Identity Based Encryption Scheme.
Advisor: Dr. Heng Swee-Huay.

PROJECT

RAT Tarpit Defense: (2018-Current)
Description & Goals: The aim of this project is to measure the operaton viability of RAT operator in facing overwhelming deception.

RATlizer: (2018-Current)
Description & Goals: The aim of this project is to automatically extract RAT protocol behavior and state from RAT traffic.

RAT Ecosystem Study: (2016-2018)
Description & Goals: This project aims to study the various stakeholders in RAT ecosystem (e.g. C&C, threat intelligence companies), and ultimately proposes methods to identify, fingerprint and profile RAT stakeholders, and track and monitor their operations.
My Contributions: Protocol reverse engineering, RAT protocol emulator (sinkhole) development, Threat intelligence analysis.

RAT Operators Behavioral Study: (2015-16)
Description & Goals: This project aimed to shed a light on DarkComet RAT operators from the behavioral perspective. We studied RAT operator life cycle and motivation when engaged with a victim machine.
My Contributions: RAT protocol reverse engineering, Developing network decoder and network signature, Developing behavioral signature, Developing unpacker and RAT configuration extractor, Honeypot development.

Security Assessment of In-Vehicle Infotainment (IVI) System: (2013-15)
Description & Goals: We performed a comprehensive security analysis on an IVI system that is included in at least one 2015 model vehicle from a major automotive manufacturer.
My Contributions: Hardware reverse engineering, Firmware extraction and analysis, Vulnerability analysis, Exploit development, Protocol emulation.

PUBLICATION

Schrödinger's RAT: Profiling the Stakeholders in the Remote Access Trojan Ecosystem
Mohammad Rezaeirad, Brown Farinholt, Hitesh Dharamdasani, Paul Pearce, Kirill Levchenko, Damon McCoy, USENIX Security, (Security 2018).

To Catch a Ratter: Monitoring the Behavior of Amateur DarkComet RAT Operators in the Wild
Brown Farinholt, **Mohammad Rezaeirad**, Paul Pearce, Hitesh Dharamdasani, Haikuo Yin, Stevens LeBlond, Damon McCoy, Kirill Levchenko, IEEE Symposium on Security & Privacy (Oakland 2017).

A Security Analysis of an In-Vehicle Infotainment and App Platform
Sahar Mazloom, **Mohammad Rezaeirad**, Aaron Hunter, Damon McCoy. 10th USENIX Workshop on Offensive Technologies (WOOT 2016).
(Co-first authors)

A novel clustering paradigm for key pre-distribution: Toward a better security in homogenous WSNs
Mohammad Rezaeirad, Mahdi Orooji, Sahar Mazloom, Dmitri Perkins and Magdy Bayoumi. IEEE Consumer Communications & Networking Conference (CCNC 2013).

COMPUTER SKILL

Computer Programming: Python, Assembly (MIPS, x86), C/C++ ,SQL, Node.js
Scripting & Automation: Python, bash, Powershell, Yara, regex
Intel/Data Platform: Virus Total Intelligence, RecordedFuture, FlashPoint, CrowdStrike (Falcon, Hybrid Analysis), MISP, ReversingLabs,IBM xforce, FSISAC, ThreatConnect, Emerging Threat (proofpoint-IQRisk), Farsight, Passive Total (RISKIQ), Malshare.
Threat/Vulnerability Management: Nexpose, Tanium, Kenna, CylancePROJECT, NetWitness, ECAT, Imperva waf.
RE and Pen-testing Tool: IDA-PRO, OllyDbg, Cuckoo(-modified), Zer0m0n, Malheur, Volatility, FTK, Autopsy, Scalpel, Binwalk, WinDbg, Bochs, OpenOCD, Magic16, Rec Studio, Dependency Walker, Bus Pirate, JTAGulator, Wireshark, Nmap, Zmap, Kali Linux, Scapy.
Internet Technology: VMware (vSphere and vCenter), OPNsense, Iptables, Suricata, Squid, Bro,

Amazon-AWS, Cloudra, KVM, Xen, Subversion, Git, PostgreSQL, Redis.
Simulation: MATLAB, QualNet, NetSim, ns2, Magic 8.5, Hspice.
Operating Systems: Linux, macOS.
Work Place: Latex, Adobe, Office, Confluence.

SELECTED COURSE

Research in Digital Forensics, Forensic Artifact Extraction, Malware Reverse-engineering, Operating System Security, Cryptographic Engineering, Secure Software Design, Cloud Computing, Wireless Computing and Computer Networks, Network Protocols Security, Information Theory, Linux Kernel Programming, Data Communications & Networking, Applied Cryptography, Computer Security, Network Security & Management, Database Security, Ethical Hacking & Security Assessment, Password Authentication & Biometrics, System Analysis & Design, Computer Networks, Web Based Computing, Client Server Computing, Digital Watermarking, Operating systems, VLSI Design, Advanced Topics in Computer Architecture, Principle of Computer Architecture.

RESEARCH AFFILIATION & COLLOBURATION

Affiliated Researcher, *International Cyber Center (ICC)*, (2016-Current)
Visiting Researcher, *New York University*, (Summer 2016-7)
Collaborator and Researcher, *Intelligence Operations, DeepSight at Symantec Corporation*, (2014-16)
Affiliated Researcher, *Center for Evidence-based Security Research (CESR)*, (2013-Current)
Research Assistant and Member, *Security Lab at George Mason University*, (2013-Current)
Research Assistant and Member, *Wisper Lab at University of Louisiana at Lafayette*, (2011-13)

PROFESSIONAL EXPERIENCE

Cyber Security Consultant, Vulnerability Intelligence at TransUnion, USA. (Jan 2018 - Now)
Tasks: Conducting research and development. Automation design and development for data collection and processing.
Projects: Automatic vulnerability scoring and prioritization, Automatic application network baselining and lateral movement detection.
Network System Administrator and Security Navigator at The Center of Advanced Computer Studies (CACS), University of Louisiana at Lafayette (ULL), USA, (2010-12).
Network Engineer at Trans-innovation Sdn Bhd, Malaysia, (2009-10).

TEACHING

ISA 562: Information Security, Theory and Practice, TA, by Dr. Dov Gordon, (Fall 2017)
CS 458: Secure Programming and Systems, TA, by Dr Angelos Stavrou, (Fall 2017)
ISA 564: Security Laboratory, Lab Instructor, by Ben Greenberg, (Spring 2017)
ISA 562: Information Security Theory and Practice, TA, by Dr. Arun Sood, (Spring 2017)
CS 469: Security Engineering, TA, by Dr. Arun Sood, (Fall 2016)
CS 262: Introduction to Low-level Programming, Lab Instructor, by Dr. David Nordstrom, (Spring 2014 - Fall 2016)

AWARD & MEMBERSHIP

Awarded with Research Scholarship, NYU, (Summer 2016).
Awarded with Fellowship, General Motors , (2013-2015).

Achieved the second place in 15^{th} annual paper contest at ULL, (April 2012).
Awarded with Certificate of Achievement for Academic Excellence, Honors Convocation, (April 2012).
Awarded with Certificate of Honor Society of Phi Kappa Phi University of Louisiana at Lafayette Chapter, (March 2012).
Member of IEEE-CS at University of Louisiana at Lafayette Student Chapter, (August 2010-Current).
Bachelor Thesis Award Premier Research Project in faculty of Information Science & Technology, MMU, Malaysia, (2009).
Awarded with the YAYASAN TM Scholarship, (2006-09).

Professional Network

Linkedin.com	- Professional profile and links.
github.com	- Repositories and project contributions.