Sahar Mazloom

✉ sseyedma@gmu.edu
mason.gmu.edu/∼sseyedma

RESEARCH INTEREST

My research interests are two-fold: My primary research interest is on the problem of computation on encrypted data, and how to make the secure solutions more practical and efficient for the real world applications. I am specially focused on the design and development of privacy-preserving machine learning algorithms and secure deep learning techniques. I am leveraging my Artificial Intelligence background, to design machine learning techniques that can train models on encrypted data. My second interest lies in the field of cyber security, threat intelligence, risk and vulnerability assessment, in enterprise environments. Along with my cryptographic and cyber security background, I have hands-on skills in reverse engineering and penetration testing of software and hardware, specially in embedded systems.

EDUCATION

Ph.D., Computer Science (GPA: 3.90)
George Mason University, USA, (Fall 2013-Current).
Advisors: Dr. Samuel Dov Gordon.

M.S., Artificial Intelligence
Azad University, Iran, (Fall 2006-Spring 2009).
Thesis: Novel Chaos-based Color Image Encryption Schemes (Awarded with Distinction)
Advisors: Dr. Amir-Masoud Eftekhari-Moghadam.

B.S., Computer Engineering
Azad University, Iran, (Fall 2002-Spring 2006).
Thesis: Design and Implementation of a WAN for a Virtual Private Bank.
Advisor: Dr. Sam Jabbehdari.

CERTIFICATION

GIAC Security Essentials (GSEC), March 2019 – March 2023.

RESEARCH EXPERIENCE

Research Assistant and Member of Security Lab, George Mason University. Supervisor: Dr. Dov Gordon, Working on multi-party secure computation (MPC) and privacy-preserving machine learning algorithms, Summer 2016-Current
Research Assistant and Member of Security Lab, George Mason University. Supervisor: Dr. Damon McCoy. Working on Security analysis on In-Vehicle Infotainment System (IVI), Fall 2013-Fall 2015.
Research Assistant and Member of Internet Lab, New Jersey Institute of Technology. Supervisor: Dr. Christian Borcea. Working on Smart Virtual Machine Placement and Migration in Cloud, Spring 2013.

Research Assistant and Member of iWIN Lab, University of Louisiana at Lafayette. Supervisor: Dr. Miao Jin. Working on Wireless Sensor Network Security. Spring 2012-Fall 2012.
Research Associate and Member of Image Processing Lab, University of Tehran. Supervisor: Prof. H. Soltanian-Zadeh. Working on Soccer Video Analysis Systems for IRIB (Iran Broadcasting Organization), 2009-2010.

TEACHING EXPERIENCE

TA for Undergraduate, Computer Systems Architecture (MIPS Assembly), George Mason University, Fairfax, VA, Spring 2016.
TA for Undergraduate, Computer Programming for Engineers, George Mason University, Fairfax, VA, Spring 2016.
TA for Graduate, Image Processing, New Jersey Institute of Technology, Newark, USA 2013.
TA for Undergraduate, JAVA Programming Language, New Jersey Institute of Technology, Newark, USA 2013.
Instructor for Undergraduate, Assembly and Machine Language, Azad University, Qazvin, Iran 2009-2010.
Instructor for Undergraduate, Advanced Computer Programming in C C++, Azad University, Qazvin, Iran 2009-2010.
Instructor for Undergraduate, Artificial Intelligence, Payam-Noor University, Tehran, Iran 2009.
Instructor for Undergraduate, Advanced Computer Programming, Payam-Noor University, Tehran, Iran 2009.
Instructor in a computer programming institute, Programming with C++ and MATLAB, A private Computer Programming Institute, Tehran, Iran 2009.

REVIEWER

Elsevier Information Sciences
Elsevier Optics and Lasers in Engineering
Optics Laser Technology
Optik - International Journal for Light and Electron Optics
Circuits, Systems, and Signal Processing (CSSP)
EURASIP Journal on Advances in Signal Processing
Journal of Computer Science and Technology
Annual Conference of the IEEE Industrial Electronics Society (IECON)
IEEE International Symposium on Industrial Electronics (ISIE)
IET Image Processing journal

PUBLICATION

Conference: *Differentially Private Access Patterns in Secure Computation*, Sahar Mazloom, S. Dov Gordon, ACM Conference on Computer and Communications Security (CCS), Toronto, Canada, October 2018.
Conference: *A Security Analysis of an In Vehicle Infotainment and App Platform*, Sahar Mazloom, Mohammad Rezaeirad, Aaron Hunter, Damon McCoy, USENIX Workshop on Offensive Technologies (WOOT), 2016.
Conference: *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 and Networking Conference (CCNC), 2013.
Conference: *Color Image Cryptosystem using Chaotic Maps*, Sahar Mazloom, Amir-Masud Eftekhari-Moghadam, IEEE Symposium on Computational Intelligence for Multimedia, Signal and Vision Processing (CIMSIVP), 2011.
Journal: *Color image encryption algorithm based on Coupled Nonlinear Chaotic Map*, Sahar Mazloom, Amir-Masud Eftekhari-Moghadam. Journal of Chaos, Solitons & Fractals, Elsevier, vol. 42, Issue. 3, pp. 1745-1754, 2009.

TALKS

Differentially Private Access Patterns in Secure Computation, ACM Conference on Computer and Communications Security (CCS), Toronto, Canada, October 2018.
Differentially Private Access Patterns in Secure Computation, DC-Area Anonymity, Privacy, and Security Seminar, University of Maryland, College Park, USA, October 2017 .

RESEARCH PROJECT

Differentially Private Access Patterns in Secure Computation:
We explore a new security model for secure computation on large datasets and establish a new tradeoff between privacy and efficiency in secure computation by defining a security model in which the adversary is provided some leakage that is proven to preserve differential privacy. We show that this leakage allows us to construct a more efficient protocol for a broad class of computations: those that can be computed in graph-parallel frameworks such as MapReduce. We then evaluate the impact of our relaxation by comparing the performance of our protocol with the best prior implementation of secure computation for graph-parallel frameworks. Our work demonstrates that differentially private leakage is useful, in that it provides opportunity for more efficient protocols. The protocol we present has broad applicability, but we leave open the very interesting question of determining, more precisely, for which class of computations this leakage might be helpful.
Tools: GraphSC, GraphLab, FlexSC, ObliveC.

Security Assessment of In-Vehicle Infotainment (IVI) System:
In this project, 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. We documented and demonstrated insecurities in the MirrorLink protocol and IVI implementation that could potentially enable an attacker with control of a driver's smartphone to send malicious messages on the vehicle's internal network. This work was funded by General Motors and DHS.
Tools: IDA-Pro, Scapy, APKtool, JEB, Smali/baksmali, Dex2jar, Heap Walker, Wireshark, DDMS, beagle usb 480.

Color Image Cryptosystems using Chaos Theory:
During my research on employing chaotic systems in image encryption, I have proposed two novel image cryptosystems designed for color images that are based on chaotic systems. One of them is using my proposed Coupled Nonlinear Chaotic Map for symmetric image encryption and the other one is using three chaotic systems to improve the security and increase the complexity of the designed cryptosystem. The results of several experiments demonstrate the satisfactory security and efficiency of the proposed image encryption schemes for color image encryption and transmission compared with the state of the art chaos based image cryptosystems.

COMPUTER SKILL

Programming Languages & Tools: C/C++, Python, JAVA, x86 Assembly, MIPS Assembly, AWS SageMaker, Apache Spark, Hadoop, MapReduce, GraphLab.
Reverse Engineering and Penetration Testing: IDA-PRO, OllyDbg, Scapy, Malheur, Zer0m0n, DDMS, WifiADB, Bytecode/Sourcecode Visualizer, Dependency Walker, Heap Walker, Immunity Debugger, ChopShop, Calamine, Cuckoo Sandbox, JEB, APKtool, Smali/baksmali, APKManager, androguard, JReversePro, Dex2jar.

AWARDS & HONORS

- Congressional Recognition, April 2017.
- First place in PhD Research Symposium in Computer Science Department at George Mason University, April 2017.
- Travel grant to attend Real World Crypto (RWC), Zurich, Switzerland, January 2018.
- Travel grant to attend DIMACS Workshop, Piscataway, New Jersey, October 2017.
- Google travel grant to attend 38th IEEE Symposium on Security and Privacy (SP), San Jose, California, May 2017.
- Travel grant to attend the GREPSEC III Workshop, San Jose, California, May 2017.
- Travel grant to attend Real World Crypto (RWC) 2017, New York, New York, January 2017.
- Travel grant to attend CRA-W Grad Cohort workshop, Washington, DC, April 2017.
- Travel grant to attend CRA-W Grad Cohort workshop, San Diego, California, April 2016.
- Graduate Research Assistantship from George Mason University, (Fall 2013 - Current).
- Research Assistantship from General Motors, (Fall 2014 - Summer 2015).
- Graduate Assistantship from New Jersey Institute of Technology, (Spring 2013 - Summer 2013).
- Graduate Research Assistantship at University of Louisiana at Lafayette, (Spring 2012-Fall 2012).
- Qualified to continue graduate studies to Ph.D. program, exempted to take the nationwide entrance examination of Iranian Universities, (2010).
- Master thesis qualified as the Premier Research Project in Department of Electrical, Computer and IT Engineering, Qazvin University, (2010).
- Research Grant from IRIB (Republic of Iran Broadcasting), (2009 - 2010).
- Ranked top 1% among Computer Engineering students, Department of Electrical, Computer and IT Engineering, Qazvin University, (2006 - 2009).
- Qualified to continue graduate studies to Master's program, exempted to take the nationwide entrance examination of Iranian Universities, (2006).
- Ranked top 1% among Computer Engineering students, Department of Computer Engineering, Tehran North Branch University, (2002 - 2006).

Professional Network

Linkedin.com	- Professional profile and links.
github.com	- Repositories and project contributions.
twitter.com	- online news and social networking.
Google Scholar	- Papers and publications.