CURRICULUM VITAE

Dr. Meera Sridhar

Assistant Professor

Department of Software and Information Systems

University of North Carolina Charlotte

Office: Woodward Hall, 305-B
9201 University City Blvd, Charlotte, NC 28223
Voice: (704) 687-1844
Fax: (704) 687-1652
Email: msridhar@uncc.edu

1 Education

PhD The University of Texas at Dallas, Computer Science, August 2014
Dissertation Title: *Model-checking In-lined Reference Monitors*
Dissertation Research Area: Language-based Security & Formal Methods
Advisor: Kevin W. Hamlen

MS Carnegie Mellon University, Computer Science, August 2004
MS Thesis Title: *Experiments and Analysis Using an Attack Graph Toolkit*
Advisor: Jeannette M. Wing

BS Carnegie Mellon University, Computer Science, December 2002
University and College Honors
Minor in Mathematical Science
Undergraduate Thesis Title: *Formal Verification of Safety Critical Devices*
Advisors: Jeannette M. Wing and Edmund M. Clarke

2 Professional Experience

Aug 2014—Present Assistant Professor, Dept. of Software and Information Systems
University of North Carolina Charlotte, Charlotte, NC

Aug 2007—Aug 2014 Teaching and Research Assistant, Dept. of Computer Science
The University of Texas at Dallas, Richardson, TX

Jun 2012—Dec 2012 Customer Service Applications, Kindle, Intern
Lab126, Cupertino, CA

Jun 2008—Aug 2008 Advanced Technologies Lab, Research Intern
Adobe Systems, Inc., San Jose, CA

3 Career Highlights

- Received $764,754 in funding since appointment at UNCC, including an NSF CISE Research Initiation Initiative (CRII) award as sole-PI ($209,985) in 2016, and an NSF SaTC EDU award as lead-PI ($444,665) in 2020

- As recommended by my 3rd year review, my research since 2016 has evolved to encompass a rapidly emerging new discipline, IoT security, resulting in numerous successes: several publications, student theses/projects, a new lab, and several grant proposal submissions/acceptances

- Successfully graduated 1 PhD student in Spring 2020, supervising 2 PhD students (1 student successfully defended PhD proposal), 3 new incoming PhD students in Fall 2020/Spring 2021, supervising/supervised 19 MS (some multiple semesters), 15 UG (some multiple semesters, 2 co-supervisions), and 2 NSF REU (1 co-supervision) students on various research projects

- Designed and currently Director of the CCI SmartHome Lab, a cutting-edge, *external facing* IoT lab that provides state-of-the-art devices, software, hardware, office equipment and library to faculty and students for facilitating research, education and outreach in related topics

- Established mobile and IoT security, language-based security, and formal methods as core parts of the SIS software security curriculum. Designed a fully online course, two special topics courses and a fully restructured Software Assurance course (ITIS 6150/8150); introduced active-learning exercises across all security and privacy topics in the introductory undergraduate and graduate intro security and privacy courses (ITIS 3200/6200/8200)

4 Publications

4.1 Peer Reviewed Journal Publications

[J4] Phu H. Phung, Rakesh S.V. Reddy, Steven Cap, Anthony Pierce, Abhinav Mohanty, and **Meera Sridhar**. HybridGuard: A Multi-Party, Fine-Grained Permission and Policy Enforcement Framework for Hybrid Mobile Applications. *Journal of Computer Security*, 28(3): 375-404, April 2020.
https://content.iospress.com/articles/journal-of-computer-security/jcs191350

[J3] **Meera Sridhar**, Mounica Chirva, Benjamin Ferrell, Kevin W. Hamlen, and Dhiraj V. Karamchandani. Flash in the Dark: Illuminating the Landscape of ActionScript Web Security Trends and Threats. *Journal of Information System Security (JISSec)*, 13(2): 59—95. Dec 2017.
http://www.jissec.org/Contents/V13/N2/V13N2-Sridhar.html

[J2] Phu H. Phung, Maliheh Monshizadeh, **Meera Sridhar**, Kevin W. Hamlen, and V.N. Venkatakrishnan. Between Worlds: Securing Mixed JavaScript/ActionScript Multi-party Web Content. *IEEE Transactions on Dependable and Secure Computing (TDSC),* 12(4):443—457. July-Aug 2015. [impact factor: 2.296, Scimago Journal and Country Rank h-index: 44]
http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=6894186&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D6894186

[J1] **Meera Sridhar**, Richard Wartell and Kevin W. Hamlen. Hippocratic Binary Instrumentation: First Do No Harm. *Science of Computer Programming (SCP), Special Issue on Invariant Generation*, 93(B):110—124, November 2014. [impact factor: 0.828, Scimago Journal and Country Rank h-index: 51]
http://www.sciencedirect.com/science/article/pii/S0167642314000914

4.2 Peer Reviewed Conference Publications

[C11] Fadi Yilmaz and **Meera Sridhar**. A Survey of In-lined Reference Monitors: Applications and Challenges. In *Proceedings of the 16th ACS/IEEE International Conference on Computer Systems and Applications (AICCSA),* Nov 2019.
https://ieeexplore.ieee.org/document/9035367

[C10] Kelly V. English, Islam Obaidat, and **Meera Sridhar.** Practical Experience Report: Exploiting Memory Corruption Vulnerabilities in Connman for IoT Devices. In *Proceedings of the 49th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, June 2019.
https://ieeexplore.ieee.org/abstract/document/8809506

[C9] **Meera Sridhar**, Abhinav Mohanty, Fadi Yilmaz, Vasant Tendulkar, and Kevin W. Hamlen. Inscription: Thwarting ActionScript Web Attacks from Within. In *Proceedings of the 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, July 2018. https://ieeexplore.ieee.org/document/8455946

[C8] Abhinav Mohanty, Islam Obaidat, Fadi Yilmaz and **Meera Sridhar**. Control hijacking Vulnerabilities in IoT Firmware: A Brief Survey. In *the IEEE International Workshop on Security and Privacy for the Internet-of-Things (IoTSec)*, April 2018.

[C7] Phu H. Phung, Abhinav Mohanty, Rahul Rachapalli, and **Meera Sridhar**. HybridGuard: A Principal-based Permission and Fine-Grained Policy Enforcement Framework for Web-based Mobile Applications. In the *IEEE Workshop on Mobile Security Technologies (MoST)*, May 2017. https://ieeexplore.ieee.org/document/8227301

[C6] **Meera Sridhar**, Abhinav Mohanty, Vasant Tendulkar, Fadi Yilmaz, and Kevin W. Hamlen. In a Flash: An In-lined Reference Monitoring Approach to Flash App Security. In the *12th IEEE Workshop on Foundations of Computer Security (FCS)*, June 2016.

[C5] Kevin W. Hamlen, Micah M. Jones, and **Meera Sridhar**. Aspect-oriented Runtime Monitor Certification. In *Proceedings of the 18th International Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS)*, pp. 126—140, March-April 2012. http://link.springer.com/chapter/10.1007%2F978-3-642-28756-5_10

[C4] **Meera Sridhar** and Kevin W. Hamlen. Flexible In-lined Reference Monitor Certification: Challenges and Future Directions. In *Proceedings of the 5th ACM SIGPLAN Workshop on Programming Languages meets Program Verification (PLPV)*, pp. 55—60, January 2011. http://dl.acm.org/citation.cfm?id=1929537

[C3] **Meera Sridhar** and Kevin W. Hamlen. ActionScript In-lined Reference Monitoring in Prolog. In *Proceedings of the 12th International Symposium on Practical Aspects of Declarative Languages (PADL)*, pp. 149—151, January 2010. http://link.springer.com/chapter/10.1007/978-3-642-11503-5_13

[C2] **Meera Sridhar** and Kevin W. Hamlen. Model-Checking In-Lined Reference Monitors. In *Proceedings of the 11th International Conference on Verification, Model Checking, & Abstract Interpretation (VMCAI)*, pp. 312—327, January 2010. http://link.springer.com/chapter/10.1007%2F978-3-642-11319-2_23

[C1] Brian W. DeVries, Gopal Gupta, Kevin W. Hamlen, Scott Moore, and **Meera Sridhar**. ActionScript Bytecode Verification With Co-Logic Programming. In *Proceedings of the 4th ACM SIGPLAN Workshop on Programming Languages and Analysis for Security (PLAS)*, pp. 9—15, June 2009. http://dl.acm.org/citation.cfm?id=1554342

4.3 Peer Reviewed Posters

[P5] Abhinav Mohanty, Parag Mhatre, and **Meera Sridhar**. Class-sourced Penetration Testing of IoT Devices. Poster presented at the *IEEE Workshop on the Internet of Safe Things (SafeThings)*, May 2020. https://www.ieee-security.org/TC/SPW2020/SafeThings/

[P4] Alek Mieczkowski, Islam Obaidat, K. Virgil English, Glenn Um, Gavin Sroczynski and **Meera Sridhar**. Exploit Delivery to Consumer IoT Devices using WiFi Pineapple. Poster presented at the *IEEE Workshop on the Internet of Safe Things (SafeThings)*, May 2019. https://www.ieee-security.org/TC/SPW2019/SafeThings/

[P3] Phu H. Phung, Abhinav Mohanty, Rahul Rachapalli, and **Meera Sridhar**. HybridGuard: A Principal-based Permission and Fine-Grained Policy Enforcement Framework for Web-based Mobile Applications. Poster presented at the *Network and Distributed System Security Symposium (NDSS)*, February 2018. https://www.ndss-symposium.org/ndss2018/posters/

[P2] Mounica Chirva, **Meera Sridhar**, Vasant Tendulkar, Phu H. Phung, and Mark G. Pleszkoch. Functional eXtraction for Precise Java Malware Detection. Poster presented at the *9th International Symposium on Research in Attacks, Intrusions and Defenses (RAID),* September 2016. http://www.raid2016.org/list-of-accepted-posters/

[P1] Phu H. Phung, Maliheh Monshizadeh, **Meera Sridhar**, Kevin W. Hamlen, and V.N. Venkatakrishnan. FlashJaX: A Framework for Securing Mixed JavaScript/ActionScript Multi-party Web Content. Poster presented at the *USENIX Security Symposium,* August 2016. https://www.usenix.org/conference/usenixsecurity16/poster-session

4.4 Manuscripts Under Review

[M5] Yates Snyder, Yaw Frempong, **Meera Sridhar**, Erfan Al-Hossami, and Samira Shaikh. HIJaX: Human Intent JavaScript XSS Generator. *In Submission*[1], June 2020.

[M4] Abhinav Mohanty and **Meera Sridhar**. Security Evaluation of IoT SmartHome Companion Apps. *In Submission*[1], June 2020.

[M3] Fadi Yilmaz, **Meera Sridhar**, and Wontae Choi. Guide Me to Exploit: Assisted ROP Exploit Generation for ActionScript Virtual Machine. *In Submission*[1], June 2020.

[M2] Islam Obaidat, **Meera Sridhar**, and Phu H. Phung. Jadeite: A Novel Image-Behavior-based Approach for Java Malware Detection using Deep Learning. Submitted to *IEEE Access*, May 2020, in second round review.

[M1] Fadi Yilmaz**, Meera Sridhar**, Kevin W. Hamlen, Abhinav Mohanty, and Vasant Tendulkar. A Fine-Grained Classification and Security Analysis of Web-based Virtual Machine Vulnerabilities. Submitted to *Elsevier Computers & Security*, April 2020, in second round review.

4.5 Other Publications

[T4] **Meera Sridhar**, Abhinav Mohanty, Vasant Tendulkar, Fadi Yilmaz, and Kevin W. Hamlen. Inscription: Thwarting ActionScript Web Attacks From Within. Technical Report SIS-UNCC-17-01, Department of Software and Information Systems, University of North Carolina at Charlotte, March 2017. http://cyberdna.uncc.edu/techreports/sridhar-sis-uncc-17-01.pdf

[T3] **Meera Sridhar**, Mounica Chirva, Benjamin Ferrell, Kevin W. Hamlen, and Dhiraj V. Karamchandani. Flash in the Dark: Illuminating the Landscape of ActionScript Web Security Trends and Threats. Technical Report SIS-UNCC-16-01, Department of Software and Information Systems, University of North Carolina Charlotte, Charlotte, North Carolina, May 2016. http://cyberdna.uncc.edu/techreports/sridhar-uncc-16-01.pdf

[T2] **Meera Sridhar**, Richard Wartell, and Kevin W. Hamlen. Hippocratic Binary Instrumentation: First Do No Harm (Extended Version). Technical Report UTDCS-03-13, Computer Science Department, The University of Texas at Dallas, Richardson, Texas, February 2013. http://webpages.uncc.edu/msridhar/sridhar-utdcs-03-13.pdf

[T1] Kevin W. Hamlen, Micah M. Jones, and **Meera Sridhar**. Chekov: Aspect-oriented

[1] In submission to a conference with double-blind review.

Runtime Monitor Certification via Model-checking (Extended Version). Technical Report UTDCS-16-11, Computer Science Department, The University of Texas at Dallas, Richardson, Texas, May 2011.
http://webpages.uncc.edu/msridhar/hamlen-utdcs-16-11.pdf

5 Extramural Funding

5.1 Peer Reviewed National and International Grants

- **Meera Sridhar** (Lead PI), Harini Ramaprasad (Co-PI). NSF-DGE # 1947295. SaTC:EDU: Enhancing Security Education in Hybrid Mobile and Internet of Things Firmware through Inclusive, Engaging, Learning Modules (E-SHIIELD). January 1, 2020—December 31, 2022, $444,665 (including REU Supplement).
- **Meera Sridhar** (Sole PI). NSF-CNS #1566321. SaTC: CRII: A Language-based Approach to Hybrid Mobile App Security. September 1, 2016—August 31, 2020, $209,985.00.

5.2 Peer Reviewed Institutional Grants

- **Meera Sridhar** (Lead PI), Weichao Wang, (Senior Personnel), Tom Moyer (Senior Personnel), Linquan Bai (Senior Personnel), Badrul Chowdhury (Senior Personnel), Yaosuo Xue (Senior Personnel), Xiaohong Yuan (Senior Personnel), Chen Bo (Senior Personnel). Building Strong Teams for Photovoltaic Systems and Power Grid Resilience and Security. Ignite Planning Grant, UNC Charlotte, April 1, 2020—March 31, 2022, $69,404.
- **Meera Sridhar** (Lead PI), Samira Shaikh (co-PI). Generating Code from Natural Language to Detect and Prevent Cyber-Attacks. Faculty Research Grant, UNC Charlotte, January 1, 2020—May 31, 2021, $16,000.
- **Meera Sridhar** (PI), Weichao Wang (co-PI), David Wilson (co-PI), Nicholas Davis (co-PI), Jinpeng Wei (co-PI). CCI SmartHome IoT Lab. CCI Faculty Innovation Fund. January 1, 2019—June 30th, 2019, $24,700.

6 Student Supervision

6.1 Doctoral Students Supervised

- Fadi Yilmaz. Graduated Spring 2020.
- Abhinav Mohanty. Spring 2015—present. Ph.D. in progress, Ph.D. Proposal Defense completed Dec 2019.
- Islam Obaidat, Spring 2017—present. Ph.D. in progress.
- Nailah Afshan, incoming Fall 2020.

- Ala' Issa Jaraweh, incoming Fall 2020.
- Monzurul Amin, incoming Spring 2021.

6.2 Master's Students Supervised

- Vinmay Nair. Research Assistant, Spring 2015.
- Rishikesh Walawalker. Research Assistant, Spring 2015.
- Mounica Chirva. Research Assistant and Individual Study, Spring 2016.
- Vasant Tendulkar, Research Assistant, Spring 2016.
- David Farthing, Research Assistant, Summer 1, 2016.
- Arun Ramakrishnan, Individual Study, Fall 2016.
- Rahul Rachapalli, Individual Study, Spring 2017; Research Assistant, Summer, Fall 2017.
- Kshitj Gorde, Research Assistant and Individual Study, Spring 2017.
- Shantanu Rajenimbalkar, Fall 2017.
- Archit Khullar, Research Assistant, Spring 2018.
- Karthick Selvaraj, Individual Study, Spring 2018.
- Ram Vinoth Ponnarasu, Research Assistant, Fall 2018, Spring 2019.
- Tabish Gulzar Maniar, Research Assistant, Fall 2018, Spring 2019.
- Arjun Kalidas, Research Assistant, Fall 2018, Spring 2019.
- Parag Mhatre, Research Assistant, Summer 2019, Individual Study, Fall 2019.
- Brian Bahtiarian, Individual Study, Fall 2019.
- Sagar Shah, Individual Study, Fall 2019.
- Amir Payandeh, Individual Study, Spring 2020.
- Hadi Nasrallah, Individual Study, Spring 2020.
- Habib Maizoumbou Dan Aouta, Individual Study, Spring 2020.
-

6.3 Undergraduate Students Supervised

- Glenn Um, Fall 2018
- Jacqueline White, Fall 2018
- Kelly English, Fall 2018, Spring 2019
- Alek Mieczkowski, Fall 2018 & Spring 2019
- Tanvi Patil, Fall 2018, Spring 2019, Fall 2019
- Zachary Taylor, Fall 2018 & Spring 2019
- John Watson, Spring 2019
- Gavin Sroczynski, Spring 2019
- Alex Poloniewicz, Fall 2019
- Cory Martin, Spring 2020

- Seth Schallau, Spring 2020
- Yates Snyder, Spring 2019, Spring 2020, Summer 2020
- Yaw Frempong, Spring 2020, Summer 2020
- Pooja Murarisetty, Summer 2020 (co-supervised with Drs. Harini Ramaprasad & Julio Bahamon)
- Diep Ngoc Nguyen, Summer 2020 (co-supervised with Drs. Harini Ramaprasad & Julio Bahamon)

6.4 NSF Research Experience for Undergraduates (REU) Students Supervised

- Kelly English, Summer 2019
- Yates Snyder, Summer 2020 (co-supervised with Dr. Harini Ramaprasad)

7 Teaching

7.1 Major Accomplishments

- Created a new, fully-online course on Web-based Mobile App and IoT Firmware Security, with state-of-the-art learning materials and activities inspired by the latest research in the fields
- Restructured the introductory Security and Privacy courses (ITIS 3200/6200/8200) to integrate active learning across all security and privacy topics; built a repository of hands-on activities that can be used by all ITIS 3200/6200/8200 instructors
- Established language-based security and formal methods as core parts of the SIS software security curriculum through a Language-based Security research seminar and a fully restructured Software Assurance course (ITIS 6150/8150)
- Actively worked on designing these courses to fit the NSA/DHS National Center of Academic Excellence requirements, enabling them to be integrated into our new MS in Cyber Security and Graduate Certificate in Software Security programs
- Received the *2019-2020 SIS Faculty Development Teaching Award*, and attended the required Connected Learner Summer Institute on active-learning in Summer ’19, and contributed to the ACE-IT! (Advancing Computing Education) program in Summer ‘20

7.2 Courses Taught

7.2.1 Undergraduate Courses

- ITIS 3200: Introduction to Information Security and Privacy
    - Completely restructured course
    - Terms: Spring 2017, Fall 2017, Spring 2018, Spring 2019, Fall 2019

- Average Enrollment: 70
- ITIS 4990: Undergraduate Research
  - New Course
  - Terms: Fall 2018, Spring 2019, Fall 2019
  - Average Enrollment: 5

7.2.2 Graduate Courses

- ITIS 5331: Web-based Mobile and IoT Firmware Security
  - New course
  - Term: Spring 2020
  - Enrollment: 15
- ITIS 6010/8010: Topics in Software and Information Systems: Mobile/IoT Security Workshop
  - New course
  - Term: Spring 2018, Spring 2019
  - Average Enrollment: 11
- ITIS 6150/8150: Software Assurance
  - Completely restructured course
  - Terms: Spring 2016, Spring 2017
  - Average Enrollment: 8
- ITIS 6200/8200: Principles of Information Security and Privacy
  - Completely restructured course
  - Terms: Fall 2014, Fall 2015, Fall 2016, Fall 2019
  - Average Enrollment: 36.5
- ITIS 6010/8010: Topics in Software and Information Systems: Language-Based Security
  - New course
  - Term: Spring 2015
  - Enrollment: 13

8 Service and Outreach

8.1 External Service

8.1.1 Invited Talks

- "Introducing the CCI SmartHome Lab". Invited Talk. Graduate Research Seminar, UNC Charlotte. September 27th, 2019. Charlotte, NC.
- "Runtime Monitors for Hybrid Mobile Apps and Other Stories". Invited Talk. **Static Analysis Team, Google Research**. December 19th, 2018. Sunnyvale, CA.

- "Runtime Monitors for Hybrid Mobile Apps and Other Stories". Invited Tech Talk. **Galois Inc.** December 18th, 2018. Portland, OR.
- "Runtime Monitors for Hybrid Mobile Apps and Other Stories". Invited Talk. **University of California San Diego**. December 14th, 2018. San Diego, CA.
- "Runtime Monitors for Hybrid Mobile Apps and Other Stories". Invited Talk. **University of California Santa Barbara**. December 10th, 2018. Santa Barbara, CA.
- "Runtime Monitors for Hybrid Mobile Apps and Other Stories". Invited Seminar Talk. **University of California Los Angeles**. November 29th, 2018. Los Angeles, CA.
- "Runtime Monitors for Hybrid Mobile Apps and Other Stories". Invited Talk. **University of California Riverside**. November 19th, 2018. Riverside, CA.
- "Language-based Approaches for Securing Cross-Platform Web, Mobile, and IoT Attack Surfaces". Technical Talk. **CyberDNA Seminar, UNC Charlotte**. February 15th, 2018. Charlotte, NC.
- "Language-based Approaches for Securing Cross-Platform Web, Mobile, and IoT Attack Surfaces". Technical Talk. **University of California Irvine**. November 28th, 2017. Irvine, CA.
- "Model-Checking In-lined Reference Monitors". Invited Talk. **Graduate Research Seminar, UNC Charlotte**. October 24th, 2014. Charlotte, NC.
- "Model-Checking In-lined Reference Monitors". **Tech Talk. Galois, Inc**. Feb 5th, 2014, Portland, OR.
- "Creating a more sophisticated security platform for Flash, AIR and others". Invited Talk. **Adobe Systems Inc**. November 19th, 2009. San Francisco, CA.

8.1.2 Journal/Conference Reviewer

- Computers & Security (Elsevier), Reviewer, 2020
- IEEE Transactions on Dependable and Secure Computing (IEEE), Reviewer, 2017
- Computers & Security (Elsevier), Reviewer, 2015
- Runtime Verification (RV), Reviewer, 2014

8.1.3 Program Committees

- ACM Special Interest Group on Computer Science Education Technical Symposium (SIGCSE), 2020
- 20th International Symposium on Practical Aspects of Declarative Languages (PADL), 2018
- 21st International Symposium on Practical Aspects of Declarative Languages (PADL), 2019

8.1.4 Organizing Committees

- Chair: PV Systems and Power Grid Resilience Security: Team Building and Idea Generation Workshop, April 2020
- Volunteer Coordinator/Chair: ACM Conference on Computer and Communications Security (CCS), October 2017

8.1.5 Professional Memberships/Affiliations

- ACM, ACM-W, WiCyS

8.1.6 Community Service

- Panel Reviewer for 2 Panels, National Science Foundation, 2018

8.2 Internal Service

8.2.1 University Committees

- Faculty Competitive Grants Committee, UNCC, August 2016—May 2017

8.2.2 College Committees

- Graduate Education Committee, CCI, UNCC, August 2015—May 2016, Aug 2017—May 2019
- CS Core Courses Subcommittee, CCI, UNCC, Oct 2015
- SIS Department Chair Review Committee, CCI, UNCC, May 2018—Nov 2018
- ITSC2175 Ad Hoc Task Force / Committee (Nov 2019)
- CCI Research Committee, CCI, UNCC, Aug 2019—May 2020

8.2.3 Department Committees

- Faculty Mentor Committee, SIS Department, UNCC, Aug 2018—May 2020
- Graduate Curriculum Committee, SIS Department, UNCC, Aug 2015—May 2016, Aug 2017—May 2020
- Ph.D. Student Steering Committee, SIS Department, UNCC, Aug 2016—May 2018
- Undergraduate Curriculum Committee, SIS Dept, UNCC, Aug 2015—May 2016
- Research Committee, SIS Department, UNCC, Sept 2014—May2015, Aug 2019—May 2020
- Ph.D. Applicant Review Committee, SIS Department, UNCC, Sept 2014—Dec 2014

8.2.4 Ph.D. Dissertation/Master's Thesis/Baccalaureate (Honors) Committees

- Mahmoud Mohammadi, SIS, UNCC, Ph.D.

8.2.5 Other Service

- Faculty Advisor for ACM-W UNCC Chapter, 2018—2019

9 Research Statement

My general research interests reside in developing sophisticated and effective approaches to software security, specifically using programming language theory, program analysis and formal methods. Consequently, my research career has been the amalgamation of the above three domains in the context of software security (popularly known as language-based security). During my Ph.D. and my early years here at UNCC, my research was focused on *in-lined reference monitoring*, especially *certifying in-lined reference monitors.* **As recommended by my 3rd year review, my research since 2016 has evolved to encompass a rapidly emerging new discipline, IoT & CPS security; I have also focused recently on hybrid mobile application security, and security education research.**

IoT & CPS Security Research (2016—present). My research interest in this space lies in building secure defenses for IoT/CPS firmware. My recent works in this space include: a brief survey paper on control-hijacking vulnerabilities in real IoT firmware currently in the market [C8], a practical experience report describing a series of exploits on a buffer-overflow vulnerability in Connman, a network management software used widely in current IoT devices (including crashing and executing arbitrary code, and bypassing W⊕X and ASLR using ret-to-libc and return-oriented programming) [C10], a detailed security analysis of 2082 IoT SmartHome companion mobile apps that analyzes hybrid and native apps across various security vectors [M4], a poster on experiments with WiFi Pineapple to create stealth man-in-the-middle attacks that overcome the need for physical access in consumer IoT devices to allow full control over the entire exploit pathway [P4], and a poster describing class-sourcing penetration testing of a SmartHome router running OpenWrt firmware version 18.06.4, which resulted in the discovery of two zero-day vulnerabilities [P5].

In March 2020, under my leadership, a team consisting of faculty from SIS, SEEM, ECE within UNCC, NCA&T, and ORNL and ANL labs, received the UNCC Ignite Planning grant (2020-2022) to conduct research in the intersection of Photovoltaic system (solar power) and cybersecurity. The grant will bring together a multidisciplinary set of experts, to innovate strategic solutions to difficult cybersecurity challenges, and develop robust defenses for the solar power grid. Through the grant, I will be setting up a Photovoltaic lab in SIS to conduct preliminary experiments, execute team-building workshops, and submit three large-scale external grants including to DoE Solar Energy Technologies Office, NSF Smart & Connected Communities, an NSF Cyber-Physical Systems.

My research efforts in IoT/CPS also include founding and directing the CCI SmartHome Lab, an external-facing lab promoting research, education innovation and outreach in the IoT space. I am also currently supervising one PhD student (Islam Obaidat) in IoT firmware security, and have also supervised seven MS and eight UG individual study projects in IoT firmware security. I also supervised an NSF REU student in Summer 2019 on IoT firmware security that led to a publication in DSN 2019 [C10]. The above projects have contributed

to [C10,C8,P5,P4,M4], and Auto-Fuzz, a tool for automating many of the tasks of fuzzing using AFL with QEMU for IoT firmware.

Hybrid Mobile Application Security (2015—present). In 2016, I received an NSF CRII SaTC grant (2016-2020) for developing language-based security techniques to address critical security and privacy issues in *hybrid mobile apps*. This led to an *In-lined Reference Monitoring* (IRM) framework to enforce useful fine-grained security and privacy policies based on permission for each party in hybrid mobile apps [C7,J4,P3] . In contrast to the conventional permission model in mobile apps, our permission specification is platform-agnostic and context-aware, allowing app developers to customize for different parties over single permission. We integrate our permission specification into an app at the development phase; however, by design, it allows end-users to adjust parameters at runtime to protect their privacy. Together with multi-party permission patterns, we introduce comprehensive classes of fine-grained, stateful policies that developers can deploy in practice. These policy patterns can help to protect the privacy of users and can also mitigate significant types of potential attacks in hybrid apps, evidenced by our real-world evaluation. Our experimental results also demonstrate that the framework is compatible with various hybrid development frameworks over two major mobile platforms, with lightweight overhead.

I am currently supervising one PhD student (Abhinav Mohanty) supported through the CRII grant in hybrid mobile/IoT companion mobile app security. He completed his PhD proposal in Dec 2019, and is expected to graduate in Dec 2020. I have also supervised four MS & three UG students on individual study projects this topic, leading to [C7,J4,P3]. In Summer 2020, I am supervising three UG students on using Natural Language Processing (NLP) techniques to predict web-attacks in hybrid IoT companion mobile apps.

Cybersecurity Education Research (2019—present). In 2020, I received an NSF SaTC EDU grant (2020-2022) for project "E-SHIIELD", a project that proposes developing, deploying, evaluating and disseminating course modules in the areas of hybrid mobile app and IoT firmware security (joint work with Harini Ramaprasad). The course modules will employ state-of-the-art pedagogical strategies aimed towards improved student learning and engagement, and will support multiple class modalities (face-to-face, hybrid, online). The project will develop virtual lab support for application-oriented activities and will develop activity templates to enable adaptability to a rapidly changing field. The course modules will ensure accessibility and inclusivity in the concept, content, delivery, assessment, feedback and review. The courses will be designed as stackable modules for easy integration into existing courses, and broadly disseminated under a Creative Commons license. The project's E-SHIIELD training program will train faculty at five NC universities (including HBCU and community colleges) on the course modules, to deploy them at their universities. The project will also include a K-12 IoT Roadshow at five Title I Charlotte Mecklenburg Schools.

In June 2020, we received an REU supplement on this grant to support two students in the coming year.

In Summer 2020, I am supervising three UG students on this grant on two projects—(1) one NSF REU student, Yates Snyder (co-supervised with Harini Ramaprasad) on redesigning the ITIS 3200/6200 "Stack Smashing Attack" module using the POGIL and visualization pedagogical techniques; and (2) Diep Nguyen & Pooja Murarisetty (co-supervised with Harini Ramaprasad and Julio Bahamon) on creating an AI-enhanced, gamified virtual environment to teach IoT firmware security modules.

In Summer 2020, I submitted/am preparing to submit three grant proposals in cybersecurity education research: (1) an NSF SaTC EDU proposal in the intersection of AI and cybersecurity (joint work with Samira Shaikh) that will develop three novel learning modules that bring techniques from cutting-edge AI research to pressing areas of IoT software security, namely (i) IoT malware & vulnerability classification and analysis, (ii) NLP-guided IoT firmware exploit generation, and (iii) Usable policies for IoT software defense systems; (2) an NSF RET Site proposal (joint work with Harini Ramaprasad) that will provide teachers of high school and community colleges in the Greater Charlotte area research experiences in core cybersecurity areas such as web, mobile, IoT, network, cyber-physical systems security and cryptography; and (3) a UNCC Gambrell Faculty Fellowship proposal (joint work with Audrey Rorrer and Julio Bahamon) that proposes to advance informal learning on the topic of cyber-privacy in computing by delivering game-based informal learning activities directly to Charlotte communities in need.

Guided Exploit Generation (2018—present). In my recent paper [M3], we present GuidExp, a guided (semi-automatic) exploit generation tool for AVM vulnerabilities. GuidExp synthesizes (and produces) an exploit script that exploits a given ActionScript vulnerability. Unlike other *Automated Exploit Generation* (AEG) implementations, GuidExp leverages *exploit deconstruction*, a technique of splitting the exploit script into many smaller code snippets. GuidExp receives hints from security experts and uses them to determine places where the exploit script is split. Thus, GuidExp can concentrate on synthesizing these smaller code snippets in sequence to obtain the exploit script in-stead of synthesizing the entire exploit script at once. GuidExp does not rely on fuzz testers or symbolic execution tools, and adopts four optimization techniques to facilitate the AEG process, including: (1) exploit deconstruction, (2) operand stack verification, (3) instruction tiling, and (4) feedback from the AVM. A running example high-lights how GuidExp synthesizes the exploit script for a real-world AVM use-after-free vulnerability. In addition, GuidExp successful generation of exploits for ten other AVM vulnerabilities is reported.

I received the UNCC Faculty Research Grant award in January 2020 (joint work with Samira Shaikh), for designing, developing and validating novel algorithms capable of predicting (new) cyber-attacks on large-scale urban events that are occurring at increasing frequency in cities across the globe. I will specifically target web-based cyber attacks on event-associated cyber-surfaces, such as the event website and social media pages, mobile apps developed for the event, and IoT surfaces (e.g., security cameras used at the event), since these represent the most accessible/easy form of attack in consumer-facing applications.

While prior research has been conducted on detecting and even predicting cyber-attacks by analyzing text from social media, this project is the first of its kind to propose to develop automated methods that would generate code from natural language descriptions of vulnerabilities gathered from social media.

This grant has led to HIJaX [M5], a novel Natural Language–to–JavaScript generator and syntax validation prototype, that creates workable XSS exploit code from English sentences. We frame our approach to exploit generation by identifying potentially targeted websites with natural language tools, and auto-generating XSS exploits to test website vulnerabilities. We train and test the HIJaX model with a variety of datasets containing benign and malicious intents along with differing numbers of baseline code entries to demonstrate how to best create datasets for XSS code generation. We also examine part-of-speech tagging algorithms and automated dataset expansion scripts to aid the dataset creation and HIJaX model code generation processes. Finally, we demonstrate the feasibility of deploying natural language based auto-generated XSS scripts against a website.

Flash/ActionScript Security (2008—2020). Flash-related vulnerabilities have been widely used in numerous popular exploit kits, including Angler EK, Neutrino, Magnitude, Nuclear, and Hanjuan. Despite the severity of threats, however, ActionScript has been significantly less studied in the scholarly security literature than the other major web scripting language—JavaScript. To fill this void and stimulate future research, my paper [J3,T3] presents a systematic study of Flash security threats and trends, including an in-depth taxonomy of the vulnerable components of Flash Player, vulnerable ActionScript language features, a detailed investigation of 711 Common Vulnerability and Exposure (CVE) articles reported between 2008–2016, and an examination of what makes Flash security challenges unique. The results of these analyses provide researchers, web developers, and security analysts a better sense of this important attack space, and identify the need for stronger security practices and defenses for protecting users.

In [C6,C9], I present an IRM framework for ActionScript 3.0 bytecode, targeting the most heavily exploited vulnerabilities in 2015. Our framework constitutes a complete tool chain for facilitating bytecode-level instrumentation of flexible policies, including parsing, code-generation, and extensible rewriting, capable of monitor instrumentation through wrapper-classes. We design security policies and corresponding IRMs that cure five real classes of vulnerabilities; these vulnerabilities were the top choices for attackers, and were heavily used in popular exploit kits in 2015. Our IRM techniques are easily extensible to untrusted code written in other languages that share similar features (type-safe, object-oriented, bytecode-compiled, no self- modifying code).

My recent work [M1] presents a more thorough, comprehensive and accurate reclassification of web-based VM vulnerabilities to improve web vulnerability analysis and mitigation. Researchers and security engineers depend on well-known, public vulnerability databases that exhaustively collect all discovered vulnerabilities and provide useful information about each vulnerability. However, vulnerability information that is inconsistent or inaccurate hinders diagnosis of vulnerabilities residing in the implementations of web-based virtual machines,

which is one of the crucial prerequisites of building generic, comprehensive security solutions mitigating these vulnerabilities. In [M1], we reclassify vaguely classified "Memory Corruption" and "Unspecified" web-based VM vulnerabilities (a large percentage of CVE web-based VM vulnerabilities) into fine-grained vulnerability sub-classes.

I have supervised one PhD student, Fadi Yilmaz, who graduated in Spring 2020, on this work in Flash security. Fadi's dissertation research contributed to [C6,C9,M1,M3].

Cross-Platform Web Malvertisement Protection (2015). Standard browser security measures do not suffice to protect users from threats to confidentiality of private client data, integrity of publisher and user-owned content, and availability of publisher services, without also disrupting non- malicious ad functionality and other important dynamic web content. My research extends IRM security to web ads that employ cross-platform ActionScript and JavaScript technologies [J2,P1]. My work provides a more flexible, precise enforcement technology that satisfies the security needs of end-users as well as the financial needs of advertisers, without requiring client-browser modification, and addresses threats that specifically target the AS-JS interface.

Certifying In-lined Reference Monitors (IRMs) (2009—2014). An increasingly important family of dynamic analyses is one that modifies untrusted binary code prior to its execution. In-lined reference monitors (IRMs) instrument untrusted code with new operations that perform runtime security checks before potentially dangerous operations. The result is a new program that efficiently self-enforces a customized security policy. Several works of mine have focused on developing elegant, simple, yet provably correct algorithms for certifying IRMs. Automatic certification proving that the new, modified code satisfies soundness (new code satisfies the security policy) and transparency (new code preserves the behavior of the original code if the latter was policy-compliant) not only shrinks the trusted computing base (TCB) of the system, but more importantly, combines the strong formal guarantees of static analysis with the power and flexibility of the dynamic IRM system.

IRM Soundness Certification. My works on model-checking IRM systems [C2,C5] are the first to explore using the powerful paradigm of model-checking for IRM certification. My work on Cheko [C5] extends my earlier approach [C2] to a *full-scale*, *aspect-oriented* IRM framework for Java bytecode, capable of enforcing sophisticated security policies on real-world Java applications. Cheko is the first IRM-certification framework that verifies full, AOP-style IRMs against purely declarative policy specifications without trusting the code that implements the IRM. Cheko uses light-weight model-checking and abstract interpretation for the verification engine, and presents a novel approach to dynamic pointcut verification using Constraint Logic Programming (CLP). Strong proofs of verifier correctness are provided using Cousot's abstract interpretation framework.

IRM Transparency Certification. A correct IRM system must not damage the safe, desired behaviors of good programs as it adds extra security (a property known as *IRM transparency*). The high difficulty of creating fully generalized, program-agnostic IRMs that correctly preserve all safe applications justifies this call for strong evidence of transparency. My work

on IRM transparency [J1], is the first to our knowledge, that has tackled the problem of machine-verifying IRM transparency. My work demonstrates how simple, elegant model-checking algorithms for IRM soundness verification [C2,C5] can be naturally extended to verify transparency; the work presents an untrusted, external invariant-generator which reduces the verifier's state-exploration burden and affords it greater generality than the more specialized rewriting systems it checks; Prolog's unification and Constraint Logic Programming (CLP) keep the verifier implementation simple and closely tied to the underlying verification algorithm; high assurance is provided by proofs of all algorithms.

10 Teaching Statement

Since my appointment at UNCC, I have worked hard to design new courses, bring innovation to existing courses, and mentor UG, MS and PhD students.

New Course Development. I developed a new special topics course "Mobile & IoT Security Workshop" based on my recent research work in hybrid mobile app and IoT firmware security, and taught it in Springs 2018 and 2019. The course was taught in an active-learning, "flipped" style, for which I designed a slew of brand new advanced activities in hybrid mobile app and IoT firmware security, ranging from data exfiltration and tapjacking attacks on a hybrid app to firmware reverse engineering and analysis using binwalk, AFL fuzzing firmware, to stack smashing a firmware. In Spring 2020, I converted the special topics course to a regular course ITIS 5331: "Web-based Mobile and IoT Firmware Security" and offered in fully online, introducing more IoT firmware activities and a semester project involving network, software and web security aspects for an IoT firmware in a smart home router. The course is critical to SIS' MS in Cyber Security and the new Information Security and Privacy Fully Online graduate certificate. I have also designed and taught a Language-based Security research seminar. In this course, I developed substantial material for educating students about both theoretical and practical aspects of language-based enforcement techniques and formal methods such as program analysis, runtime monitoring, model-checking, program-proof co-development using Coq, and type safety.

Education Innovation in Cybersecurity. I regularly teach an introductory breadth course in cybersecurity (graduate and undergraduate). The course includes web/network/software security, cryptography, and authentication. I have invested much time and effort to design the courses to be flipped, with many team-based, active-learning in-class activities, engaging students in state-of- the-art attacks, defenses and tools, such as configuring a Remote Access Tool (RAT) to gain full access to a target machine, using a password recovery tool to retrieve system user passwords from their hashes, buffer overflow simulations, XSS and XSRF attacks using WebGoat, setting up real firewalls, etc.

In the Fall 2019 graduate introductory course, I leveraged the CCI SmartHome Lab to create a cutting-edge project on smart home router security (a TP Link router running OpenWRT firmware). While IoT security is not part of the course syllabus, having an IoT security project got students very excited. Meanwhile, the project had three phases: network

security, web security, and software security, each phase giving students a strong practical experience in that specific domain related to the router, while providing synergy with syllabus topics covered in class. An interesting outcome of this exercise was that my TAs and I discovered a new XSS vulnerability in the OperWRT firmware, and the course students discovered another XSS vulnerability in the firmware, leading us to ethically report to OpenWRT, and receiving two new CVE numbers (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-18992, https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-17367)! We published this work as a poster in *IEEE SafeThings 2020*, describing class-sourcing penetration testing of a SmartHome router running OpenWrt firmware version 18.06.4, which resulted in the discovery of two zero-day vulnerabilities [P5].

I have consistently received overwhelmingly positive feedback from students in my courses about the engaging in-class, hands-on activities and my discussion-oriented teaching style.

I have also taken several efforts towards bringing innovation and improvement in my teaching. These efforts have included writing and receiving an NSF SaTC EDU grant in bringing cutting-edge pedagogical techniques into advanced cybersecurity education (which is currently leading to multiple prototypes, publications and joint, interdisciplinary work in the space), and preparing additional education-related grant proposals (see detailed description above in Section "Cybersecurity Education Research"). The efforts have also included receiving the *2019-2020 SIS Faculty Development Teaching Award*, and attending the associated Connected Learner Summer Institute on active-learning in Summer '19, and participating in the ACE-IT! program in Summer '20, where faculty develop online modules capturing the college's pedagogical best practices, strategies and examples of how they can be applied to different types of computing courses.

Research Supervision Summary. Language-based security research, especially in application areas such as IoT firmware, requires the acquiring of significant theoretical and mathematical background; implementation of these techniques (such as building binary instrumentation engines or abstract interpreters) requires painstaking involvement at the systems level. Both of these contribute to longer than average training cycles for new students. Additionally, as mentioned, IoT security was a new field for me in 2016. Despite the challenges, I have been successful in setting up and running a new language-based security research lab in SIS.

Since my appointment at UNCC, I have successfully graduated 1 PhD student in Spring 2020, I am supervising 2 PhD students (1 student successfully defended PhD proposal and expected to graduate Dec 2020), supervising/supervised 19 MS (some multiple semesters), 15 UG (some multiple semesters, 2 co-supervisions), and 2 NSF REU (1 co-supervision) students on various research projects. My students have all made steady progress towards their degrees, and have produced significant results ([J3,J4,C6-C11,P3-P5,M1-M5,T3,T4]).