Muhammad Naveed

440B Gates Hall
343 Campus Rd
Ithaca, NY 14853

Phone: 217-402-4486
Email: naveed2@illinois.edu
Homepage: www.cryptoonline.com

EDUCATION

PhD Candidate – 5th year, Computer Science 2011 – 2016
University of Illinois at Urbana-Champaign
Advisors: Prof. Carl Gunter and Prof. Manoj Prabhakaran

Visiting PhD Student, Computer Science 2015 – 2016
Cornell University
Advisor: Prof. Elaine Shi

Bachelor of Science, Electrical Engineering 2006 – 2010
University of Engineering and Technology, Peshawar, Pakistan

RESEARCH INTERESTS

- *Applied Cryptography:* I analyze cryptographic schemes and build practical yet provably-secure systems.
- *Systems Security:* I explore the fundamental security flaws in popular systems and build defense systems requiring no or minimal changes to the underlying systems.

HONORS AND AWARDS

- Google PhD Fellowship (15 fellows in US/Canada), 2015
- Sohaib and Sara Abbasi Fellowship, UIUC, 2011–2016
- C.W. Gear Outstanding Graduate Student Award, UIUC, 2015
- Feng Chen Memorial Award, UIUC, 2015
- Selected for the Heidelberg Laureate Forum to meet Abel, Fields, and Turing Laureates (12% acceptance rate), 2015
- Fifty for the Future Awardee, Illinois Technology Foundation, 2015
- Google Android Security Team Acknowledgement for contributions to Android (http://goo.gl/oRnOYo)
- $2000 bug bounty from Facebook for our work on cloud push messaging services
- Equipment award from Samsung for our work on Android device driver customization
- Best Paper Award (3rd place among $\approx$ 80 papers) at the NYU CSAW Security Research Competition, 2014
- One of the five finalists at the NYU CSAW Policy Competition (Topic: Internet of Things), 2014
- Emerging Engineer Award, UIUC, 2014
- Best Project Award at Data Sciences Summer Institute (DSSI), UIUC, 2012
- MOL (Hungarian Oil and Gas Company) Technical Scholarship, 2008

TEACHING EXPERIENCE

University of Illinois at Urbana-Champaign Spring 2015
Guest Teaching Assistant for Computer Security II (CS463)

- Lecture 1: Modern Cryptography I (Chapter 1 and 2 of Katz and Lindell book)
- Lecture 2: Modern Cryptography II (Chapter 3 of Katz and Lindell book)
- Designed and graded a course project about private set intersection. See https://github.com/eSMC/PSI for details.

University of Illinois at Urbana-Champaign Spring 2013
Teaching Assistant for Computer Security II (CS463)

- Lecture 1: Security and Privacy Issues of Cloud Computing
- Lecture 2: Confinement and Covert Channels
- Designed and graded course projects where students incrementally built a secure cloud storage system

University of Engineering and Technology, Peshawar, Pakistan Dec 2010 – Jul 2011
Lecturer of Electrical Engineering

- Instructor for a two-semester computer networks lab class

Iqra National University, Peshawar, Pakistan Sep 2010 – Dec 2010
Lecturer of Computer Science

RESEARCH EXPERIENCE

Cornell University Fall 2015, Spring 2016
Visiting Research Assistant (Host: Prof. Elaine Shi)

University of Illinois at Urbana-Champaign Spring 2014, Fall 2014, Spring 2015, Summer 2015
Research Assistant on THaW (www.thaw.org)

Microsoft Research Fall 2014
Research Intern (Host: Dr. Seny Kamara)

Microsoft Research April 2014
Short Research Visit (Host: Dr. Seny Kamara)

University of Illinois at Urbana-Champaign Summer 2012, Fall 2012, Fall 2013
Research Assistant on SHARPS (www.sharps.org)

SRI International Summer 2014
Research Intern (Hosts: Dr. Gabriela Ciocarlie and Dr. Ashish Gehani)

Ecole Polytechnique Federale de Lausanne (EPFL), Switzerland Fall 2013
Research Intern (Host: Prof. Jean-Pierre Hubaux)

University of Virginia Summer 2013
Research Intern (Host: Prof. David Evans)

MENTORING EXPERIENCE

Mentor for Promoting Undergraduate Research (PURE) program at UIUC Spring 2014, Spring 2015

- Nitesh Nath, Project: External Device Security in Apple iOS devices Spring 2014
- Xusheng Zhang, Project: Privacy-Preserving Photo Sharing Spring 2014
- Stephanie Wang, Project: Safety and Security of Internet of Things Spring 2015
- Xinrui Zhu, Project: Safety and Security of Internet of Things Spring 2015

Edward Chou, Undergraduate student (supervised independent study) Spring 2015
Project: Safety and Security of Internet of Things

Peter Fischer, Masters student Summer 2014, Fall 2014, Spring 2014
Project: Secure Cloud Storage

RESEARCH TALKS

Inference Attacks on Property Preserving Encrypted Databases

- Cornell University, *Host: Prof. Elaine Shi* Sep 2015
- Cornell University – Security Class, *Host: Prof. Thomas Ristenpart* Oct 2015
- ACM Conference on Computer and Communications Security (CCS) Oct 2015
- Georgia Institute of Technology, *Host: Prof. Wenke Lee* Nov 2015 (*Upcoming*)
- Princeton University, *Host: Prof. Prateek Mittal* Dec 2015 (*Upcoming*)

Controlled Functional Encryption

- IBM T.J. Watson Research Center, *Hosts: Dr. Salman Baset and Dr. Xin Hu* Oct 2014
- ACM Conference on Computer and Communications Security (CCS) Nov 2014
- Microsoft Research Redmond, *Host: Dr. Bryan Parno* Dec 2014
- University of Washington, *Host: Prof. Tadayoshi Kohno* Dec 2014
- Massachusetts Institute of Technology, *Host: Frank Wang* Feb 2015
- Doctoral Consortium, ACM Richard Tapia Conference Feb 2015
- 10th CSL Student Conference, UIUC Feb 2015
- Dagstuhl Genome Privacy Seminar Oct 2015

Privacy in the Genomic Era

- UIUC THaW Seminar Feb 2014

- Microsoft Research Redmond, *Host: Dr. Bryan Parno* Oct 2014

Cybersecurity Policy Proposal for the Internet of Things (IoTs)

- Finalist talk: CSAW Policy Competition at the New York University Nov 2014

Security and Privacy of Big Data (Cryptographic Approach)

- Dartmouth College Sep 2014

Dynamic Searchable Encryption via Blind Storage

- University of Illinois at Urbana-Champaign March 2014
- Microsoft Research Redmond, *Host: Dr. Seny Kamara* April 2014
- IBM T.J. Watson Research Center, *Host: Dr. Hugo Krawczyk* May 2014
- University of Maryland at College Park, *Prof. Charalampos Papamanthou* May 2014
- IEEE Symposium on Security and Privacy (Oakland) May 2014
- SRI International, *Hosts: Hosts: Dr. Gabriela Ciocarlie and Dr. Ashish Gehani* June 2014
- Stanford University, *Host: Prof. Dan Boneh* July 2014
- Illinois Cyber Security Scholar Program Seminar, *Prof. Masooda Bashir* April 2015

Hurdles for Genomic Data Usage Management

- 5th International Workshop on Data Usage Management (DUMA), (co-located with the IEEE S&P) May 2014

The Peril of Fragmentation: Security Hazards in Android Device Driver Customizations

- Microsoft Research Redmond, *Host: Dr. Seny Kamara* April 2014
- UIUC THaW Seminar April 2014

Inside Job: Understanding and Mitigating the Threat of External Device Misbonding on Android

- ISOC Network and Distributed System Security Symposium (NDSS) Feb 2014

Identity, Location, Disease and More: Inferring Your Secrets from Android Public Resources

- ACM Conference on Computer and Communications Security (CCS) Nov 2013

Genomics and Privacy

- Health Information Technology Center (HITC) Workshop at UIUC Nov 2012

PUBLICATIONS

⋆ 10 original papers in top-tier security conferences (Oakland, CCS, NDSS)
⋆ 1 survey paper in a top-tier computer science journal (ACM Computing Surveys)
⋆ 1 original paper in a top-tier medical informatics conference (AMIA)
⋆ 1 position paper in a workshop

Journal Publications

1. Muhammad Naveed, Erman Ayday, Ellen W. Clayton, Jacques Fellay, Carl A. Gunter, Jean-Pierre Hubaux, Bradley A. Malin, XiaoFeng Wang. *Privacy in the Genomic Era.* ACM Computing Surveys (**CSUR2015**)
   Highlighted paper at the 2015 ACM Conference on Bioinformatics, Computational Biology, and Health Informatics (ACM BCB)

Conference Publications

2. Muhammad Naveed, Seny Kamara, Charles V Wright. *Inference Attacks on Property-Preserving Encrypted Databases.* In ACM Conference on Computer and Communications Security (**CCS2015**).
   Media Coverage: Forbes, Ars Technica, The Register, Golem, and ComputerWorld
3. Vincent Bindschaedler, Muhammad Naveed, Xiaorui Pan, XiaoFeng Wang, Yan Huang. *Practicing Oblivious Access on Cloud Storage: the Gap, the Fallacy, and the New Way Forward.* In ACM Conference on Computer and Communications Security (**CCS2015**).
4. Nan Zhang, Kan Yuan, Muhammad Naveed, Xiaoyong Zhou, XiaoFeng Wang. *Leave Me Alone: App-level Protection Against Runtime Information Gathering on Android.* In IEEE Symposium on Security and Privacy (**Oakland2015**).
   Media Coverage: ComputerWorld
5. Soteris Demetriou, Xiaoyong Zhou, Muhammad Naveed, Yeonjoon Lee, Kan Yuan, XiaoFeng Wang, Carl A. Gunter. *What's in Your Dongle and Bank Account? Mandatory and Discretionary Protection of Android External Resources.* In Network and Distributed System Security Symposium (**NDSS2015**).

6. Muhammad Naveed, Shashank Agrawal, Manoj Prabhakaran, Xiaofeng Wang, Erman Ayday, Jean-Pierre Hubaux and Carl A. Gunter. *Controlled Functional Encryption.* In ACM Conference on Computer and Communications Security (**CCS2014**).
7. Tongxin Li, Xiaoyong Zhou, Luyi Xing, Yeonjoon Lee, Muhammad Naveed, Xiaofeng Wang and Xinhui Han. *Mayhem in the Push Clouds: Understanding and Mitigating Security Hazards in Mobile Push-Messaging Services.* In ACM Conference on Computer and Communications Security (**CCS2014**).
8. Dongjing He, Muhammad Naveed, Carl A. Gunter, Klara Nahrstedt. *Security Concerns in Android mHealth Apps.* In American Medical Informatics Association Annual Symposium (**AMIA2014**).
   Media Coverage: MobiHealthNews, HealthITSecurity
9. Muhammad Naveed, Manoj Prabhakaran, Carl A. Gunter. *Dynamic Searchable Encryption via Blind Storage.* In IEEE Symposium on Security and Privacy (**Oakland2014**).
10. Xiaoyong Zhou, Yeonjoon Lee, Nan Zhang, Muhammad Naveed, XiaoFeng Wang. *The Peril of Fragmentation: Security Hazards in Android Linux Device Customizations.* In IEEE Symposium on Security and Privacy (**Oakland2014**).
    Best Paper Award (3rd place) at the 2014 NYU CSAW Security Research Competition
    Media Coverage: The Register, Tom's Hardware
11. Muhammad Naveed, Xiaoyong Zhou, Soteris Demetriou, XiaoFeng Wang, Carl Gunter. *Inside Job: Understanding and Mitigating the Threat of External Device Misbonding on Android.* In ISOC Network and Distributed System Security Symposium (**NDSS2014**).
12. Xiaoyong Zhou, Soteris Demetriou, Dongjing He, Muhammad Naveed, Xiaorui Pan, XiaoFeng Wang, Carl Gunter, Klara Nahrstedt. *Identity, Location, Disease and More: Inferring Your Secrets from Android Public Resources.* In ACM Conference on Computer and Communications Security (**CCS2013**).

Workshop Publications

13. Muhammad Naveed. *Position paper: Hurdles for Genomic Data Usage Management.* In 5th International Workshop on Data Usage Management (DUMA2014) (co-located with IEEE S&P 2014).

Preprints

14. Christopher Fletcher, Muhammad Naveed, Ling Ren, Elaine Shi, Emil Stefanov. *Bucket ORAM: Single Online Roundtrip, Constant Bandwidth Oblivious RAM.*
15. Muhammad Naveed. *The Fallacy of Composition of Oblivious RAM and Searchable Encryption.*

In submission/preparation

16. Muhammad Naveed. *Viewpoint: Making the World a Better Place with Cryptography.*
17. Muhammad Naveed, Vincent Bindschaedler, Gabriela Ciocarlie, Ashish Gehani, Mariana Raykova. *Reduced Leakage Searchable Encryption*.
18. Muhammad Naveed, Shashank Agrawal, Fardin Abdi, Manoj Prabhakaran. *Highly Scalable Secure Multiparty Computation*

POSTERS

- Muhammad Naveed. *Bridging the Gap between Modern Cryptography and Real World Applications.* In Google PhD Fellowship Summit, 2015; In Usenix Security Symposium, 2015; In 3rd Heidelberg Laureate Forum, 2015.
- Muhammad Naveed, Seny Kamara, Charles V Wright. *Inference Attacks on Encrypted Databases*. In Usenix Security Symposium, 2015; In 3rd Heidelberg Laureate Forum, 2015.
- Muhammad Naveed. *Finalist Poster: Cybersecurity Policy Proposal for the Internet of Things (IoTs).* In CSAW Policy Competition at the New York University, Nov 2014.
- Muhammad Naveed, Shashank Agrawal, Manoj Prabhakaran, Xiaofeng Wang, Erman Ayday, Jean-Pierre Hubaux and Carl A. Gunter. *Controlled Functional Encryption.* In IBM Research Frontiers of Cloud Computing and Big Data Workshop, Feb 2014.
- Muhammad Naveed, XiaoFeng Wang, Carl Gunter. *Privacy Implications of BSSID based Location Services.* In IEEE Symposium on Security and Privacy, 2013.

SOFTWARE

- Blind Storage and Symmetric Searchable Encryption (Oakland2014) – link
- Controlled Functional Encryption (CCS2014) – link
- Bluetooth Attacks and Dabinder (NDSS2014) – link
- CURIOUS and other ORAM Systems (CCS2015) – link
- App Guardian (Oakland2015) – link

SERVICE

- Student PC Member for IEEE S&P (Oakland) 2016
- PC Member for the Workshop on Genome Privacy and Security (GenoPri 2015) – co-located with (Oakland)
- Journal Reviewer: ACM TISSEC, ACM Computing Surveys, IEEE TSDC, IEEE TSC, PLOS ONE
- Invited Reviewer for USENIX Security 2015, ACM CCS 2015, ACM SIGMOD 2015, WWW 2015
- Invited Reviewer for Annual Symposium of American Medical Informatics Association (AMIA 2015)
- External Reviewer for
  - 2016: NDSS, EUROCRYPT
  - 2015: S&P (Oakland), Usenix Security, NDSS, CCS, SIGMOD
  - 2014: S&P (Oakland), Usenix Security, NDSS, CCS, SIGCOMM, ACSAC, CODASPY
  - 2013: SIGCOMM, CRYPTO, CODASPY

PROFESSIONAL CERTIFICATIONS

- Cisco Certified Network Associate – Security (CCNAS), 2010.
- Cisco Certified Network Associate (CCNA), 2009.

TRAINING

Data Sciences Summer Institute (DSSI) Summer 2012
Department of Computer Science, University of Illinois at Urbana-Champaign.

Training in Genomics Fall 2012
Institute of Genomic Biology, University of Illinois at Urbana-Champaign.

System Administration for Linux 2008
Linsol, Islamabad, Pakistan

REFERENCES

Carl Gunter (Advisor)
Professor
Department of Computer Science
University of Illinois at Urbana-Champaign
Email: cgunter@illinois.edu

Manoj Prabhakaran (Advisor)
Associate Professor
Department of Computer Science
University of Illinois at Urbana-Champaign
Email: mmp@illinois.edu

XiaoFeng Wang
Professor
School of Informatics and Computing
Indiana University at Bloomington
Email: xw7@indiana.edu

Elaine Shi
Associate Professor
Department of Computer Science
Cornell University
Email: elaine@cs.cornell.edu

Vitaly Shmatikov
Professor
Department of Computer Science
Cornell University, Cornell Tech NYC
Email: shmat@cs.cornell.edu