Curriculum Vitae

Nitesh Saxena

Affiliations:

Associate Professor, Computer and Information Sciences
Director, Security and Privacy in Emerging Systems (SPIES) group
Co-Director, M.S. Computer Forensics and Security Management (CFSM)
Co-Lead IA Pillar, Center for Information Assurance and Joint Forensics Research (CIA|JFR)

University of Alabama at Birmingham (UAB)

Contact:

Campbell Hall (CH) 133
1300 University Boulevard
Birmingham, Alabama 35294

email: saxena@cis.uab.edu
web: http://cis.uab.edu/saxena
group web: http://spies.cis.uab.edu

Executive Summary / Biography:

Nitesh Saxena is an Associate Professor of Computer and Information Sciences at the University of Alabama at Birmingham (UAB), and the founding director of the Security and Privacy in Emerging Systems (SPIES) group/lab. He works in the broad areas of computer and network security, and applied cryptography, with a keen interest in wireless and mobile device security, and the emerging field of usable security.

Saxena’s current research has been externally supported by multiple grants from NSF, and by gifts/awards/donations from the industry, including Google (2 Google Faculty Research awards), Cisco, Comcast, Intel, Nokia and Research in Motion. He has published over 90 journal, conference and workshop papers, many at top-tier venues in Computer Science, including: IEEE Transactions, ISOC NDSS, ACM CCS, ACM WiSec, ACM CHI, ACM Ubicomp, IEEE Percom, IEEE ICME and IEEE S&P. His work has won the Distinguished Paper Award at NDSS 2014. On the educational/service front, Saxena currently serves as a co-director for UAB’s MS program in Computer Forensics and Security Management. He was also the principal architect and a co-director of the M.S. Program in Cyber-Security at the Polytechnic Institute of New York University (NYU-Poly). Saxena has instructed over a dozen core fundamental courses in Computer Science, including Computer Security, Network Security, Modern Cryptography, and Discrete Structures. Saxena has also advised and graduated numerous graduate (Ph.D. and M.S.) and undergraduate students as well as a few high school students. He is serving as an Associate Editor for flagship security journals, IEEE Transactions on Information Forensics and Security (TIFS), and Springer’s International Journal of Information Security (IJIS). Saxena’s work has received extensive media coverage, for example, at NBC, MSN, Fox, Discovery, ABC, Bloomberg, ZDNet, ACM TechNews, Yahoo! Finance, Communications of ACM, Yahoo News, CNBC, Slashdot, Computer World, Science Daily and Motherboard.

Saxena obtained his Ph.D. in Information and Computer Science from the University of California, Irvine, an M.S. in Computer Science from the University of California, Santa Barbara, and a Bachelor's degree in Mathematics and Computing from the Indian Institute of Technology, Kharagpur, India. Before joining UAB, he was an Assistant Professor in the Department of Computer Science and Engineering at NYU-Poly. He has also previously worked at Nokia Research Center, Finland and at INRIA Rhone-Alpes, France.

1 EDUCATION

- **Ph.D.** in Information and Computer Science
  University of California, Irvine, August 2006
- **M.S.** in Computer Science
  University of California, Santa Barbara, March 2002
- **B.S.** in Mathematics and Computing,
  Indian Institute of Technology (IIT), Kharagpur, India, May 2000

2 RESEARCH INTERESTS

All aspects of information assurance with emphasis on computer and network security, wireless and mobile device security, usable security, privacy, and applied cryptography

3 PROFESSIONAL EXPERIENCE

- Associate Professor (with tenure), Computer and Information Sciences, University of Alabama at Birmingham, June 2013 –
- Assistant Professor, Computer and Information Sciences, University of Alabama at Birmingham, Aug 2011 – May 2013
- Assistant Professor, Computer Science and Engineering, Polytechnic Institute of New York University (formerly Polytechnic University), Sep 2006 – Aug 2011
- Research Intern, INRIA Rhone-Alpes, Grenoble, France, Oct – Dec 2005
- Research Intern, Nokia Research Center, Helsinki, Finland, Jun – Sep 2005
- Research and Teaching Assistant, Information and Computer Science, University of California, Irvine, Sep 2002 – Aug 2006
- Summer Intern, Automated Total Systems Solutions, Santa Ana, California, Jul - Sep 2003
- Teaching Assistant, Computer Science, University of California, Santa Barbara, Sep 2000 – Mar 2002

4 SCHOLARLY WORK

[***91 publications***, *including* ***20 journal***, *and* ***68 conference/workshop papers.]***

4.1 Peer-Reviewed Journal Publications[1]

[*20 journal papers,* *including* *9 IEEE Transactions papers*]

1. B. Shrestha, D. Ma, Y. Zhu, H. Li, and N. Saxena. Tap-Wave-Rub: Lightweight Human Interaction Approach to Curb Emerging Smartphone Malware. In IEEE Transactions on Information Forensics and Security (TIFS), to appear, 2015.

2. N. Saxena, J. Sloan, M. Godbole, J. Cai, M. Georgescu, O. Harper, D. Schwebel. Consumer Perceptions of Mobile and Traditional Point-Of-Sale Credit or Debit Card Systems. In International Journal of Cyber Criminology, Volume 2, Issue 2, 2015.

3. H. Truong, X. Gao, B. Shrestha, N. Saxena, N. Asokan and P. Nurmi. Using Contextual Co-Presence to Strengthen Zero-Interaction Authentication: Design, Integration and Usability. In Elsevier Journal of Pervasive and Mobile Computing (PMC), to appear, 2014.
4. T. Halevi and N. Saxena. Keyboard Acoustic Side Channel Attacks: Exploring Realistic and Security-Sensitive Scenarios. In International Journal of Information Security, to appear, 2014.
5. S. Peddinti and N. Saxena. Web Search Query Privacy: Evaluating Query Obfuscation and Anonymizing Networks. In Journal of Computer Security (JCS), Volume 22, Number 1, January, 2014.
6. T. Halevi, H. Li, D. Ma, N. Saxena, J. Voris, and T. Xiang. Context-Aware Defenses to RFID Unauthorized Reading and Relay Attacks. In IEEE Transactions on Emerging Topics in Computing (TETC), 1(2), 307-318, December 2013.
7. D. Ma, A. K Prasad, N. Saxena, and T. Xiang. Location-Aware and Safer Cards: Enhancing RFID Security and Privacy via Location Sensing. In IEEE Transactions on Dependable and Secure Computing (TDSC), 10(2), 57-69, March 2013.
8. T. Halevi and N. Saxena. Acoustic Eavesdropping Attacks on Constrained Wireless Device Pairing. In IEEE Transactions on Information Forensics and Security (TIFS), Vol 8, Issue 3, 563 – 577, March 2013.
9. S. Jarecki and N. Saxena. Authenticated Key Agreement with Key Re-Use in the Short Authenticated Strings Model. American Mathematical Society, Contemporary Mathematics, Computational and Combinatorial Group Theory and Cryptography, Volume 582, December 2012.
10. T. Perkovic, M. Cagalj, T. Mastelic, N. Saxena, D. Begusic. Secure Initialization of Multiple Constrained Wireless Devices for an Unaided User. IEEE Transactions on Mobile Computing (TMC), Volume 11, Issue 2, 337 – 351, February 2012.

[1] Author's copies for all published papers are available at http://www.cis.uab.edu/saxena/publications.html

11. D. Ma and N. Saxena. A context-aware approach to defend against unauthorized reading and relay attacks in RFID systems. In the International Journal of Security and Communication Networks, Special Issue on "Protecting the Internet of Things", DOI: 10.1002/sec.404, December 2011.
12. N. Saxena and J. Voris. Data Remanence Effects on Memory Based Entropy Collection for RFID Systems. International Journal of Information Security, Volume 10, Number 4, 213-222, July 2011.
13. N. Saxena, J. Ekberg, K. Kostiainen, and N. Asokan. Secure Device Pairing based on a Visual Channel: Design and Usability Study. IEEE Transactions on Information Forensics and Security (TIFS), Volume 6, Issue 1, 28-38, March 2011.
14. T. Halevi, N. Saxena and S. Halevi. Tree-based HB Protocols for Privacy-Preserving Authentication of RFID Tags. Journal of Computer Security (JCS) -- Special Issue on RFID System Security, Volume 19, Issue 2, 343-363, April 2011.
15. S. Jarecki and N. Saxena. On the Insecurity of the Proactive RSA Signature Scheme in the URSA Ad Hoc Network Access Control Protocol. In IEEE Transactions on Information Forensics and Security (TIFS), Volume 5, Issue 4, 739-749, December, 2010.
16. N. Saxena and J. H. Yi. Non-Interactive Self-Certification for Long-Lived Mobile Ad Hoc Networks. In IEEE Transactions on Information Forensics and Security (TIFS), Volume 4, Issue 4, 946-955, December 2009.
17. A. Kumar, N. Saxena, G. Tsudik and E. Uzun. A Comparative Study of Secure Device Pairing Methods. In Elsevier Pervasive and Mobile Computing Journal (PMC), Volume 5, Issue 6, 734-749, December 2009.
18. N. Saxena, G. Tsudik, and J. H. Yi. Efficient Node Admission and Public Key Cryptography in Ad Hoc Networks. In IEEE Transactions on Parallel and Distributed Systems (TPDS), Volume 20, No. 2, 158-170, February 2009
19. N. Saxena, G. Tsudik, and J. H. Yi. Threshold Cryptography in P2P and MANETs: the Case of Access Control. In Elsevier Computer Networks, Volume 51, Issue 12, 3632-3649, Aug 2007
20. C. Castelluccia, N. Saxena, and J. H. Yi. Robust Self-Keying Mobile Ad-Hoc Networks. In Elsevier Computer Networks, Volume 51, Issue 4, 1169-1182, Mar 2007

4.2 Peer-Reviewed Conferences / Workshop Publications

[***68 conference/workshop papers,*** *including* ***3 NDSS; 4 ACM CCS****;* ***1 IEEE S&P****;* ***5 IEEE Percom; 2 ESORICS****;* ***2 ACSAC****;* ***3 ACM WiSec****;* ***1 ACM CHI****;* ***2 ACM Ubicomp****;* ***1 IEEE Infocom****;* ***1 IEEE ICME; 1 IEEE P2P; 1 IEEE ICNP****; and* ***1 IACR TCC papers***]

21. O. Huhta, P. Shrestha, S. Udar, M. Juuti, N. Saxena and N. Asokan. Pitfalls in Designing Zero-Effort Deauthentication: Opportunistic Human Observation Attacks. In the Network and Distributed System Security Symposium (NDSS), February 2016. [acceptance rate = **15.4%** (60/389)]

22. S. Gao, M. Mohamed, N. Saxena, and C. Zhang. Emerging Image Game CAPTCHAs for Resisting Automated and Human-Solver Relay Attacks. In Annual Computer Security Applications Conference (ACSAC), December 2015. [acceptance rate = **24.4%** (47/193)]

23. M. Shirvanian and N. Saxena. On the Security and Usability of Crypto Phones. In Annual Computer Security Applications Conference (ACSAC), December 2015. [acceptance rate = **24.4%** (47/193)

24. A. Neupane, Md. Lutfor Rahman, Nitesh Saxena and Leanne Hirshfield. A Multi-Modal Neuro-Physiological Study of Phishing Detection and Malware Warnings. In ACM Conference on Computer and Communications Security (CCS), October 2015. [acceptance rate = **19.8%** (128/646)]

25. D. Mukhopadhyay, M. Shirvanian and N. Saxena. All Your Voices Are Belong to Us: Stealing Voices to Fool Humans and Machines. In European Symposium on Research in Computer Security (ESORICS), September 2015. [acceptance rate = **19.8%** (58/293)]

26. B. Shrestha, M. Mohamed, A. Borg, N. Saxena and Sandeep Tamrakar. Curbing Mobile Malware based on User-Transparent Hand Movements. International Conference on Pervasive Computing and Communications (PerCom), March 2015. [acceptance rate for full papers = **7.7%** (15/196)]

27. M. Shirvanian and N. Saxena. Wiretapping via Mimicry: Short Voice Imitation Man-in-the-Middle Attacks on Crypto Phones. In ACM Conference on Computer and Communications Security (CCS), November 2014. [acceptance rate = **19.5%** (114/585)]

28. S. Gao, M. Mohamed, N. Saxena, and C. Zhang. Gaming the Game: Defeating a Game CAPTCHA with Efficient and Robust Hybrid Attacks. In the Security and Forensics track, IEEE International Conference on Multimedia and Expo (ICME), July 2014 (full paper; oral presentation). [acceptance rate for full papers = **13.7%** (98/716)]

29. M. Mohamed, N. Sachdeva, M. Georgescu, S. Gao, N. Saxena, C. Zhang, P. Kumaraguru, P. C. V. Oorschot and W. Chen. A Three-Way Investigation of a Game-CAPTCHA: Automated Attacks, Relay Attacks and Usability. In ACM Symposium on Information, Computer and Communications Security (AsiaCCS), June 2014. [acceptance rate for full papers = **16%** (43/260)]

30. M. Mohamed, S. Gao, N. Saxena, and C. Zhang. Dynamic Cognitive Game CAPTCHA Usability and Detection of Streaming-Based Farming. In the Workshop on Usable Security (USEC), co-located with NDSS, February 2014. [acceptance rate = 34% (15/44)]

31. B. Shrestha, N. Saxena, H. Truong and N. Asokan. Drone to the Rescue: Relay-Resilient Authentication using Ambient Multi-Sensing. In Financial Cryptography and Data Security, March 2014. [acceptance rate for full papers = **22.5%** (31/138)]

32. H. Truong, X. Gao, B. Shrestha, N. Saxena, N. Asokan and P. Nurmi. Comparing and Fusing Different Sensor Modalities for Relay Attack Resistance in Zero-Interaction Authentication. International Conference on Pervasive Computing and Communications (PerCom), March 2014. [acceptance rate for full papers = **10.3%** (18/175)]

33. A. Neupane, N. Saxena, K. Kuruvilla, M. Georgescu, and R. Kana. Neural Signatures of User-Centered Security: An fMRI Study of Phishing, and Malware Warnings. In the Network and Distributed System Security Symposium (NDSS), February 2014. (**Distinguished Paper Award**) [acceptance rate = **18.6%** (55/295)]

34. M. Shirvanian, S. Jarecki, N. Saxena and N. Nathan. Two-Factor Authentication Resilient to Server Compromise Using Mix-Bandwidth Devices. In the Network and Distributed System Security Symposium (NDSS), February 2014. [acceptance rate = **18.6%** (55/295)]

35. M. Godbole, J. Cai, M. Georgescu, O. N. Harper, N. Saxena, D. Schwebel, and J. Sloan. Consumer anxiety concerning credit/debit card fraud. In the 122nd American Psychological Association (APA), August 2014.

36. N. Sachdeva, N. Saxena, and Ponnurangam Kumaraguru. On the Viability of CAPTCHAs for Use in Telephony Systems: A Usability Field Study. In Information Security Conference (ISC), to appear, November 2013. [acceptance rate for full papers = **22.8%** (16/70)]

37. B. Shrestha, N. Saxena and J. Harrison. Wave-to-Access: Protecting Sensitive Mobile Device Services via a Hand Waving Gesture. International Conference on Cryptology and Network Security, November 2013.

38. D. Ma, N. Saxena, B. Shrestha, Y. Zhu, and H. Li. Tap-Wave-Rub: Lightweight Malware Prevention for Smartphones using Intuitive Human Gestures. ACM Conference on Wireless Network Security (WiSec), April 2013.

39. R. Hasan, N. Saxena, T. Halevi, S. Zawoad, and D. Rinehart. Sensing-Enabled Channels for Hard-to-Detect Command and Control of Mobile Devices. ACM Symposium on Information, Computer and Communications Security (AsiaCCS), May 2013. [acceptance rate for full papers = **16%** (35/216)]

40. A. Gallego, N. Saxena and J. Voris. Exploring Extrinsic Motivation for Better Security: A Usability Study of Scoring-Enhanced Device Pairing. International Conference on Financial Cryptography and Data Security (FC), April 2013.

41. T. Halevi, D. Ma, N. Saxena and T. Xiang. Secure Proximity Detection for NFC Devices based on Ambient Sensor Data. The European Symposium on Research in Computer Security (ESORICS), 379-396, September 2012. [acceptance rate = **20%** (50/248)]

42. N. Saxena and J. Voris. Exploring Mobile Proxies for Better Password Authentication. International Conference on Information and Communications Security (ICICS), 293-302, October 2012.

43. T. Halevi and N. Saxena. A Closer Look at Keyboard Acoustic Emanations: Random Passwords, Typing Styles and Decoding Techniques. ACM Symposium on Information, Computer and Communications Security (AsiaCCS), May 2012. [acceptance rate = 30%]

44. D. Ma, A. K Prasad, N. Saxena, and T. Xiang. Location-Aware and Safer Cards: Enhancing RFID Security and Privacy via Location Sensing. ACM Conference on Wireless Network Security (WiSec), 51-62, April 2012. [acceptance rate = **26%** (17/63)]

45. T. Halevi, S. Lin, D. Ma, A. K Prasad, N. Saxena, J. Voris and T. Xiang. Sensing-Enabled Defenses to RFID Unauthorized Reading and Relay Attacks without Changing the Usage Model. In International Conference on Pervasive Computing and Communications (PerCom), 227-234, March 2012. [acceptance rate = **18%** (28/150)]

46. R. Dey, C. Tang, K. Ross and N. Saxena. Estimating Age Privacy Leakage in Online Social Networks. In International Conference on Computer Communications (IEEE INFOCOM), 2836-2840, March 2012. [acceptance rate = **24%** (378/1547)]

47. A. Bagherzandi, S. Jarecki, N. Saxena and Y. Liu. Password-Protected Secret Sharing. In ACM Conference on Computer and Communications Security (CCS), 433-444, October 2011. [acceptance rate = **13.9%** (60/429)]

48. S. T. Peddinti, A. Dsouza, and N. Saxena. Cover Locations: Availing Location-Based Services without Revealing the Location. In ACM Workshop on Privacy in the Electronic Society (WPES 2010), co-located with ACM Conference on Computer and Communications Security, October, 143-152, 2011. [acceptance rate for full papers = **16%** (12/73)]

49. S. T. Peddinti and N. Saxena. On the Limitations of Query Obfuscation Techniques for Location Privacy. In International Conference on Ubiquitous Computing (Ubicomp), 483-489, September 2011. [acceptance rate = **16.6%** (50/302)]

50. A. Gallego, N. Saxena, and J. Voris. Playful Security: A Computer Game for Secure Pairing of Wireless Devices. In The 16th International Computer Games Conference (CGames): AI, Animation, Mobile, Interactive Multimedia, Educational & Serious Games, 177 – 184, July 2011.

51. J. Voris, N. Saxena and T. Halevi. Accelerometers and Randomness: Perfect Together. In ACM Conference on Wireless Network Security (WiSec), 115-126, June 2011. [acceptance rate for full papers = **11% (**10/92)]

52. N. Saxena, Md. B. Uddin, J. Voris and N. Asokan. Vibrate-to-Unlock: Mobile Phone Assisted User Authentication to Multiple Personal RFID Tags. In International Conference on Pervasive Computing and Communications (PerCom), 181-188, March 2011. [acceptance rate = **16%** (26/156)]

53. E. Uzun, N. Saxena and A. Kumar. Pairing Devices for Social Interactions: A Comparative Usability Evaluation. ACM Conference on Human Factors in Computing Systems (CHI), 2315-2324, May 2011. [acceptance rate = **26%** (395/1540)]

54. C. Tang, K. W. Ross, N. Saxena and R. Chen. What's in a Name: A Study of Names, Gender Inference, and Gender Behavior in Facebook. International Workshop on Social Networks and Social Media Mining on the Web (SNSMW), co-located with DASFAA, 344-356, April 2011.

55. S. T. Peddinti and N. Saxena. On the Effectiveness of Using Anonymizing Networks for Web Search Privacy. ACM Symposium on Information, Computer and Communications Security (AsiaCCS), 483-489, March 2001. [acceptance rate = **27%** (60/217)]

56. T. Halevi and N. Saxena. On Pairing Constrained Wireless Devices Based on Secrecy of Auxiliary Channels: The Case of Acoustic Eavesdropping. ACM Conference on Computer and Communications Security (CCS), 97-108, October 2010. [acceptance rate = **17%** (55/320)]

57. A. Karole, N. Saxena and N. Christin. A Comparative Usability Evaluation of Traditional Password Managers. International Conference on Information Security and Cryptology (ICISC), 233-251, December 2010. [acceptance rate = **28%** (28/100)]

58. D. Wu, C. Tang, P. Dhungel, N. Saxena and K. W. Ross. On the Privacy of Peer-Assisted Distribution of Security Patches. IEEE International Conference on Peer-to-Peer Computing (P2P), 1-10, August 2010. [acceptance rate for full papers = **19%** (27/143)]

59. S. Jarecki and N. Saxena. Authenticated Key Agreement with Key Re-Use in the Short Authenticated Strings Model. Conference on Security and Cryptography for Networks (SCN), 253-270, September 2010. [acceptance rate = **29%** (27/94)]

60. N. Saxena and J. Voris. Still and Silent: Motion Detection for Enhanced RFID Security and Privacy without Changing the Usage Model. Workshop on RFID Security (RFIDSec), 2-21, June 2010. [acceptance rate = 36% (17/47)]

61. R. Nithyanand, N. Saxena, G. Tsudik and E. Uzun. Groupthink: On the Usability of Secure Group Association of Wireless Devices. International Conference on Ubiquitous Computing (Ubicomp), 331-340, September 2010. [acceptance rate = **19%** (39/202)]

62. S. T. Peddinti and N. Saxena. On the Privacy of Web Search Based on Query Obfuscation: A Case Study of TrackMeNot. Privacy Enhancing Technologies Symposium (PETS), 19-37, July 2010. [acceptance rate = **28%** (16/57)]

63. T. Perkovic, M. Cagalj, and N. Saxena. Shoulder Surfing Safe Login in a Partially Observable Attacker Model. In International Conference on Financial Cryptography and Data Security (FC), 351-358, January 2010. [acceptance rate = **26%** (15/59)]

64. M. Cagalj, N. Saxena and E. Uzun. On the Usability of Secure Association of Wireless Devices Based On Distance Bounding. In International Conference on Cryptology and Network Security (CANS), 443-462, December 2009. [acceptance rate = **29%** (32/109)]

65. N. Saxena and Md. B. Uddin. Blink 'Em All: Secure, Scalable and User-Friendly Initialization of Sensor Nodes. In International Conference on Cryptology and Network Security (CANS), 154-173, December 2009. [acceptance rate = **29%** (32/109)]

66. N. Saxena and J. H. Watt. Authentication Technologies for the Blind or Visually Impaired. In USENIX Workshop on Hot Topics in Security (HotSec), August 2009. [acceptance rate = **26%** (12/46)]

67. N. Saxena and J. Voris. We Can Remember It for You Wholesale: Implications of Data Remanence on the Use of RAM for True Random Number Generation on RFID Tags. In International Workshop on RFID Security (RFIDSec), July 2009.

68. T. Halevi, N. Saxena and S. Halevi. Using HB Family of Protocols for Privacy-Preserving Authentication of RFID Tags in a Population. In International Workshop on RFID Security (RFIDSec), July 2009.

69. A. Karole and N. Saxena. Improving the Robustness of Wireless Device Pairing Using Hyphen-Delimited Numeric Comparison. In International Symposium on Emerging Ubiquitous and Pervasive Systems (EUPS), 273-278, August 2009.

70. N. Saxena and Md. B. Uddin. Secure Pairing of "Interface-Constrained" Devices Resistant Against Rushing User Behavior. Applied Cryptography and Network Security (ACNS), 34-52, June 2009. [acceptance rate = **21%** (32/150)]

71. A. Kumar, N. Saxena, G. Tsudik and E. Uzun. Caveat Emptor: A Comparative Study of Secure Device Pairing Methods. International Conference on Pervasive Computing and Communications (PerCom), 1-10, March 2009. [acceptance rate = **13%** (26/199)]

72. N. Saxena and Md. B. Uddin. Automated Device Pairing for Asymmetric Pairing Scenarios. In International Conference on Information and Communications Security (ICICS), 311-327, October 2008. [acceptance rate = **21%** (27/125)]

73. N. Saxena, Md. B. Uddin and J. Voris. Universal Device Pairing using an Auxiliary Device. In Symposium On Usable Privacy and Security (SOUPS), 56-67, July 2008. [acceptance rate = **27%** (12/43)]

74. R. Prasad and N. Saxena. Efficient Device Pairing using Synchronized "Human-Comparable" Audiovisual Patterns. Applied Cryptography and Network Security (ACNS), 328-345, June 2008. [acceptance rate = **22%** (30/131)]

75. N. Saxena and J. Voris. Pairing Devices with Good Quality Output Interfaces. International Workshop on Wireless Security and Privacy (WISP) (co-located with ICDCS), 382-387, June 2008.

76. N. Saxena and Md. Borhan Uddin**.** Device Pairing using Unidirectional Physical Channels. The Mobile and Wireless Networks Security Workshop (MWNS 2008) (co-located with IFIP Networking), May 2008.

77. P. Dhungel, X. Hei, K. W. Ross, and N. Saxena. The Pollution Attack in P2P Live Video Streaming: Measurement Results and Defenses. In Peer-to-Peer Streaming and IP-TV Workshop (P2P-TV) (co-located with SIGCOMM), 323-328, August 2007.

78. N. Saxena. Public Key Cryptography sans Certificates in Ad Hoc Networks. In Applied Cryptography and Network Security (ACNS), 375-389, June 2006 (**Best Student Paper Award**). [acceptance rate = **15%** (33/218)]

79. N. Saxena, J. Ekberg, K. Kostiainen, and N. Asokan. Secure Device Pairing based on Visual Channel. In IEEE Symposium on Security and Privacy (S&P), Oakland, extended abstract, 306-313, May 2006. [acceptance rate = **12%** (32/251)]

80. N. Saxena. Securing Communication in Various Ad Hoc Network Settings. In IEEE Infocom Student Workshop, April 2006.

81. N. Saxena, G. Tsudik, and J. H. Yi. Efficient Node Admission for Short-lived Mobile Ad Hoc Networks. In International Conference on Networking Protocols (ICNP), 269-278, November 2005. [acceptance rate = **17%** (36/212)]

82. C. Castelluccia, N. Saxena, and J. H. Yi. Self-configurable key pre-distribution in mobile ad hoc networks. In IFIP Networking, 1083-1095, May 2005. [acceptance rate = **24%** (106/430)]

83. S. Jarecki and N. Saxena. Further Simplifications in Proactive RSA Signatures. In Theory of Cryptography Conference (TCC), 510-528, February 2005.

84. S. Jarecki, N. Saxena, and J. H. Yi. An Attack on the Proactive RSA Signature Scheme in the URSA Ad Hoc Network Access Control Protocol. In ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN), 1-9, October 2004. [acceptance rate = **20%**]

85. N. Saxena, G. Tsudik, and J. H. Yi. Identity-based Access Control for Ad Hoc Groups. In International Conference on Information Security and Cryptology (ICISC), 362-379, December 2004. [acceptance rate = **17%** (34/194)]

86. N. Saxena, G. Tsudik, and J. H. Yi. Access Control in Ad Hoc Groups. In International Workshop on Hot Topics in Peer-to-Peer Systems (HOT-P2P), 2-7, October 2004.

87. N. Saxena, G. Tsudik, and J. H. Yi. Experimenting with Admission Control in P2P. In International Workshop on Advanced Developments in Software and Systems Security (WADIS), December 2003.

88. N. Saxena, G. Tsudik, and J. H. Yi. Admission Control in Peer-to-Peer: Design and Performance Evaluation. In ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN), 104-113, October 2003. [acceptance rate = **20%**]

4.3 Book Chapters

89. D. Ma and N. Saxena. Towards sensing-enabled RFID security and privacy. In Security and Trends in Wireless Identification and Sensing Platform Tags: Advancements in RFID. IGI Global, August, 2012.

90. A. G. Konheim and N. Saxena. Chapter 6.11: Lorenz Schlusselzusatz. In Computer Security and Cryptography, (ISBN: 978-0-471-94783-7), Wiley, 2007.

91. N. Saxena, G. Tsudik, and J. H. Yi. Chapter 5: Experimenting with Admission Control in P2P Networks. In Computer Security in the 21st Century (ISBN: 0-387-24005-5), Springer, 2005.

4.4 Invited Talks

1. Topic TBD, University of Alabama at Birmingham, Mathematics Colloquium, March 2015.
2. Secure Pairing of Constrained Wireless Devices: Challenges and Pitfalls, University of Alabama (Tuscaloosa), Computer Science Colloquium, October 2014. This was a featured talk of the Alabama IEEE Computer Society for the month of October, 2014.
3. SPIES: Security and Privacy in Emerging Computing and Networking Systems, AT&T Standing Meeting (electronic; host Amy Zwarico), July 2013.
4. NFC: A Convenient Mobile Payment Platform, or Fraudster's Playground, TechMixer University & Expo, Birmingham, Organized by the TechBirmingham group, October, 2012.
5. User-Aided Device Authentication: The Case of Constrained Wireless Devices, Computer Science Colloquium, **Carleton University**, August 2012.
6. Acoustic Eavesdropping Attacks on Constrained Wireless Device Pairing, Computer Science Colloquium, **Brown University**, January 2012.
7. Tree-based HB Protocols for Privacy-Preserving Authentication of RFID Tags, American Mathematical Society, Special Session on Mathematics for Cyber-Security, **Cornell University**, September 2011.
8. SPIES: Security and Privacy in Emerging Computing and Networking Systems, Oregon State University, April 2011.
9. SPIES: Security and Privacy in Emerging Computing and Networking Systems, Naval Postgraduate School, March 2011.
10. SPIES: Security and Privacy in Emerging Computing and Networking Systems, University of Alabama at Birmingham, February 2011.
11. On the Usability of Secure Device Pairing Methods, Hofstra University, October 2010.
12. On the Usability of Secure Device Pairing Methods, Security and Privacy Day, NYU-Poly, December 2009.
13. User-Aided Secure Association of Wireless Devices**,** CS Seminar, **State University of New York, Stony Brook**, June 2009.
14. User-Aided Secure Association of Wireless Devices**,** ECE Seminar, New Jersey Institute of Technology, October 2008.
15. User-Assisted Secure Association of Wireless Devices**,** Security and Privacy Day, Pitney Bowes, July 2008.

16. Threshold Cryptography in MANETs. Security and Privacy Day, **Columbia University**, June 2007.
17. Secure Device Pairing and Privacy on the Internet. Seminar Talk, CIS, Polytechnic University, January 2007.
18. WICAT Research Review, Polytechnic University, May 2008
19. RFID Security and Privacy, a one-hour invited crash course delivered (telephonically) in the "October Meeting of the AT&T IP Services Security Council".
20. Providing Robust and Secure Decentralized Services. Invited Talk at computer science seminar, **Institute for Infocomm Research**, Singapore, Jun 2006.
21. Providing Robust and Secure Decentralized Services. Invited Talk at computer science seminar, University of Rome La Sapienza, May 2006.
22. Providing Robust and Secure Decentralized Services. Invited Talk at computer science seminar, University of Trento, May 2006.
23. On the Role of Threshold Cryptography Towards Securing Ad Hoc Networks. Invited Talk at theoretical computer science seminar, **Helsinki University of Technology**, Sep 2005.

4.5 Patents

- Detecting Physical Gestures for Mobile Device Security, Nitesh Saxena and Babins Shrestha, Pending Patent Application, filed on April 12, 2014.
- Efficient Device Pairing using Synchronized Audiovisual Patterns, Ramnath Prasad and Nitesh Saxena, CATT, Poly patent. Filed, August 2007.
- Method and System of Improved Security in Wireless Environments Using Out-of-Band Channel Communication. Pending patent application (no. PCT/IB05/003107) filed at Nokia Research Center, Helsinki, October 2005.

4.6 Selected Media Coverage

- Voice Hackers Can Record Your Voice Then Use Morpher To Trick Authentication Systems, Linkedin, Oct 18, 2015
- UAB Research Finds Automated Voice Imitation Can Fool Humans and Machines, ACM TechNews, Sep 30, 2015
- Experts warn of morphing threat to voice biometrics, Planet Biometric, Sep 28, 2015
- New mobile-malware detection technique uses gestures, COPMUTERWORLD, Mar 27, 2015
- New mobile-malware detection technique uses gestures, PCWorld, Mar 27, 2015
- New mobile-malware detection technique uses gestures, CIO, Mar 27, 2015
- Cisco funds university research into VoIP security, Networked World, Nov 12, 2014
- Mobile VoIP Security Vulnerable to Mimicry Attacks, CACM News, Nov 6, 2014

- Research Unveils Improved Method To Let Computers Know You Are Human , Slashdot, Aug 19, 2014
- New Research Presents an Improved Method to Let Computers Know You Are Human , ACM TechNews, Aug 20, 2014
- Game-Like CAPTCHA Lets Computers Know You Are Human, Communications of the ACM, Aug 26, 2014
- Better than CAPTCHA: Improved method to let computers know you are human, ScienceDaily, Aug 25, 2014
- UAB researchers work on next-gen security methods, Alabama's 13, June 3, 2014
- Passwords no more? Researchers develop mechanisms that enable users to log in securely without passwords, Phys.org, June 4, 2014
- Passwords No More? UAB Researchers Develop Mechanisms That Enable Users to Log in Securely Without Passwords, Newswise, June 4, 2014
- Passwords No More? Mechanisms Enables Users to Log in Securely Without Passwords, Science Daily, June 4, 2014
- UAB researchers could kill the password as we know it, Birmingham Business Journal, June 5, 2014
- New mechanism allows users to log in to their terminals without inputting a password, Electronic Products, June 5, 2014
- Indian-origin scientist working on a system to end passwords, The Times of India, June 5, 2014
- Passwords No More? Communications of the ACM, June 5, 2014
- UAB researching technological alternative to online passwords, Myfoxal, June 6, 2014
- UAB researchers seek easy, hacker-proof way for users to open their cars, computers, other gadgets, Alabama Local News, June 10, 2014
- Interview With Dr. Nitesh Saxena, Beyond The Computer Password, Crush Plate, June 10, 2014
- Passwords? Soon You May Log In Securely Without Them, ACM TechNews, June 11, 2014
- Our brains work hard to spot phishing scams, but still often fail, NakedSecurity, March 4, 2014
- Most People Can't Tell the Difference Between a Real Website and a Scam, Motherboard, March 5, 2014
- Users' brains scanned in bid to fix infosec, CSO, March 15, 2014
- Neue Studie zu Phishing: Opfer kennen die Warnsignale nicht (German), Gulli, March 6, 2014
- Brain research tracks internet safety performance, dispels assumptions, identifies traits of those at-risk, Science Daily, February 28, 2014
- Study suggests users pay more attention to Internet safety than previously assumed, Phys.org, February 28, 2014
- Strengthening Two-Factor Authentication, Industrial Safety and Security Source, March 5, 2014
- Ease and security of password protections improved, Science Daily, February 28, 2014

- New methods for password protection proposed, The Economic Times, March 3, 2014
- Password protection: Scientists propose new methods, The Times of India, March 3, 2014
- Future credit cards could thwart Target hackers, Yahoo! Finance, December 23, 2013.
- How secure is Skype? UAB gets $150K to improve VoIP security. Birmingham Business Journal, July 19, 2013
- Music, lighting can let hackers onto your phone. MSN News, May 29, 2013
- Cafe, Mall Music Could Trigger Malware. Discovery News, May 31, 2013
- Music playing 55 feet away could covertly activate Android mobile malware. Computer World, May 29, 2013
- Music is a Turn-On for Malware. Symantec, May 29, 2013
- Security boffins say music could trigger mobile malware. The Register, May 28, 2013
- Music, lighting or vibration could trigger mobile malware. Yahoo News, May 27, 2013
- Music and Movies Could Trigger Mobile Malware. Slashdot, May 20, 2013
- UAB Research Finds New Channels to Trigger Mobile Malware. ACM TechNews, May 16, 2013
- Beware, that music at Starbucks can be malware. The Times of India, May 27, 2013.
- Lights, Music Could Trigger Smartphone Malware. NBC News, May 20, 2013
- UAB develops malware defense for smartphones. Birmingham Business Journal, Mar 1, 2013
- On Your Side: New UAB app defends against malware. Fox 6, Mar 14, 2013
- UAB Develops a Simple Defense for Complex Smartphone Malware. ACM TechNews, Feb 28, 2013
- 13 INVESTIGATES: Wi-fi thieves. NBC 12, Feb 25, 2013
- System Improves Mobile Payment Security, Protects Personal Info. Communications of the ACM, Sep 12, 2012.
- Mobile Payments: A New Frontier for Criminals. Bloomberg BusinessWeek, Oct 4, 2012.
- Audio samples used to secure NFC authentication. ZDNet, Sep 19, 2012.
- UAB creates system to bolster mobile payment security, personal info. NFC News, Sep 13, 2012.

4.7 Dissertations

- Decentralized Security Services, Ph.D. Dissertation, University of California, Irvine, Aug 2006. Primary Advisor: Gene Tsudik
- Cryptanalysis of the Schlusselzusatz, M.S. Dissertation, University of California, Santa Barbara, Mar 2002. Primary Advisor: Alan Konheim

5 RESEARCH GRANTS

[*Include:* ***5 active NSF grants, 2 Google faculty research awards, 1 Cisco grant, 1 Comcast award****; Funding as PI:* ***about $1.8M****; Total Funding:* ***about $5.2M***]

1. **NSF** Secure and Trustworthy Cyberspace Program Grant, "*Spoof-Resistant Smartphone Authentication using Cooperating Wearables*", **$207,965**, Sep 2015 – Aug 2018, **PI**. Total award: **$507,963**. Other participant: Syracuse University.

   This project is investigating how to design smartphone authentication mechanisms (biometrics) based on multiple wearable devices and on-board sensors on these devices.

2. **NSF** Cybersecurity Innovation for Cyberinfrastructure Program Grant, "*Improving the Security and Usability of Two-Factor Authentication for Cyberinfrastructure,*", **$ $249,719.00**, Jan 2016 – Dec 2018, **PI**. Total award: **$500,00**. Other participant: UC Irvine University.

   This project is investigating how to improve the security and usability of two-factor authentication. A pilot deployment within university IT systems is also planned.

3. **Comcast** Tech Research and Development Award, "Secure and Usable Game CAPTCHAs", **$75,000**, unrestricted gift awarded Aug 2014, **PI**. Other Co-PI: Chengcui Zhang (UAB, CIS)

   This project explores next generation CAPTCHAs based on the notion of computer games, which will be user-friendly and fun as well as secure against both automated attacks and human-solver relay attacks.

4. **Google** Faculty Research Award, "*Contextual Security: Balancing Security and Usability via Context Inference*", **$50,000**, unrestricted gift awarded Aug 2013, **PI**. Other PI: N. Asokan (Aalto University, Finland)

   This project explores the notion of contextual security, which utilizes a wealth of contextual information available to computing devices about the device and the user to make informed security and privacy decisions.

   This is a well-established and very competitive grant. Only 105 proposals were awarded out of a total of 550 proposals (acceptance rate of 19%) from 50 countries.

5. **Cisco Systems** Research Contract, "*Establishing Peer-to-Peer Secure VoIP Connections*", **$150,000**, contract, June 2013 to May 2015. **PI**. Co-PI: Purushotham Bangalore (UAB CIS).

   This project explores the establishment of secure end-to-end connections for voice over IP communications based on out-of-band voice channels. This way future voice over IP communications can be protected from eavesdropping and man-in-the-middle attacks without relying upon any trusted infrastructure.

6. **NSF** Early-Concept Grants for Exploratory Research Grant (Secure and Trustworthy Cyberspace Program), "*Establishing Secure Wireless Connections via Playful User Engagement*", **$91,016** (including an REU supplement), Oct 2012 – Sep 2014, **Sole PI**.

   This project is investigating the use of playful mechanisms using which users can bootstrap secure connections among their wireless devices in a fun and an enjoyable way, improving both security and usability of the connection establishment process.

   The EAGER awards are given to "*potentially transformative*" and "*high-risk/high-payoff*" research projects.

7. **NSF** Trustworthy Computing Grant, "*Mobile Phone Password Managers: An Evaluation and a Re-Design Based on Human Perceptible Communication*", **$453,433**, Sep 2011 – Aug 2014, **Sole PI**.

   This project is investigating how to strengthen the security of password-based authentication while improving its usability. It is developing novel password management approaches using mobile devices (e.g., mobile phones), whose ubiquity make them an appealing authentication aid.

8. **NSF** Early-Concept Grants for Exploratory Research Grant (Trustworthy Computing Program), "*Towards Context-Aware Security and Privacy for RFID Systems*", **$90,000**, Oct 2011 – Sept 2013, **PI**. Total award: **$200,000**. Other participant: University of Michigan-Dearborn.

   This project is investigating novel context-aware approaches to protect RFID and other related devices. The idea is to attach low-cost, low-power sensors to these tags (or just use these sensors when already available, such as on NFC phones), and utilize the data acquired by these sensors to make informed security decisions.

   The EAGER awards are given to "*potentially transformative*" and "*high-risk/high-payoff*" research projects. As a result of this grant, we have already published a number of papers at top conferences, such as at Percom, WiSec and ESORICS and at a top journal TDSC.

9. **NSF** Cybertrust Grant, "*User-Aided Secure Association of Wireless Devices*," **$225,000**, Oct 2008 – Sep 2013, **Lead PI**. Total award: **$475,000**. Other participant: UC Irvine.

   This project, in its concluding phases, investigates a fundamental problem in security – that of bootstrapping secure communication between two or more wireless devices. To this end, it leverages user-aided out-of-band (audio, visual, tactile) channels. It covers: cryptographic protocol design, secure association mechanism design and usability studies.

As a result of this grant, we have published numerous papers, several at top-tier venues, including CCS, Ubicomp, CHI and Percom. We have also graduated 2 PhD students, 4 MS students, and 2 undergraduate students. Currently, we are transitioning our research into possible commercial products, working together with our industry partners, such as Nokia Research.

10. **Google** Faculty Research Award, "*Towards Playful Security: A First Look at Secure Device Pairing*", **$50,000**, unrestricted gift awarded Mar 2011, **Sole PI**.

    This project explores a new paradigm for user-centered security, called "Playful Security" -- the use of intuitive games or game-like constructs, and game elements to make security tasks fun, entertaining and engaging for the users.

    This is a well-established and very competitive grant.

11. **Research in Motion** Research Award in the form of 30 Blackberry Bold 9000 smartphones, worth **$14, 970**, January 2010, **Sole PI**.

12. **NYU/Poly** Seed Grant (externally reviewed), "*Fault-Tolerant User-Centric Security Services Exploiting Social Networks*," **$21,817**, Mar 2009 – Dec 2010, **PI**. Total award: **$44,878**. Other participant: NYU.

    This project involves the design of distributed user-centric security and cryptographic services that are resistant to faults (malicious or otherwise). It led to a top conference paper at CCS'11 on *password-protected secret sharing.* It also formed a central component of our proposal to the **NIST** National Strategy for Trusted Identities in Cyberspace (**NSTIC**) Pilot Grant Program. This proposal was one of the only 27 finalists selected out of a total of 186 submissions in the first round of competition; an acceptance rate of **14.5%**.

    This was a competitive grant with an external review process.

13. **NSF** IGERT Grant, "*INSPIRE: Information Security and Privacy: An Interdisciplinary, Research and Education Program*", **$2.85 million**, Jul 2010 – June 2015, **Senior Person**. Project led by NYU-Poly. Other participant: NYU. Provided **full support for 1 of my PhD students for one full year 2011-2012**.

6 AWARDS

- Distinguished Paper Award at NDSS 2014, the Network and Distributed System Security Symposium
- Comcast Tech Research and Development Award, 2014
- Google Faculty Research Award, 2013

- The Kevin and Jo Ann Reilly Endowed Award (UAB, CIS), 2012
  The award recognizes an outstanding member of the faculty in the department
  (award description: http://www.uab.edu/development/winter-2011-contents/awarding-faculty)
- Google Faculty Research Award, 2011
- NYU-Poly Sole Nominee for the Microsoft New Faculty Fellowship Program, 2009
- UC Irvine Sole Nominee for the ACM Dissertation Award, Aug 2006
- Best Student Paper Award, Applied Cryptography and Network Security Conference (ACNS), 2006
- Dissertation Fellowship, UC Irvine, Summer 2006

7 TEACHING AND EDUCATIONAL ACTIVITIES

[***Leadership*** *of UAB's* ***Computer Forensics and Security Management M.S. program,*** *and NYU-Poly's* ***Cyber-Security M.S. program****; instruction* ***of more than a dozen core CS courses*** *(some newly developed); supervision of numerous graduate (PhD and MS) and undergraduate students as well as few high school students.* ***1st PhD student graduated*** *in 2011 -- now an Assistant Professor NYIT;* ***2nd PhD student graduated*** *in the summer of 2012 – now a post-doc at NYU-Poly;* **3rd PhD student graduated** *in the Fall of 2015 – now a Software Engineer at Google*]

7.1 Educational Program Development and Leadership

1. *Co-Director* for UAB's **M.S. program in Computer Forensics and Security Management**, starting January 2013
   (Program Web: http://www.cis.uab.edu/Computer_Forensics_and_Security_Management)

   Program Synopsis: The Master of Science in Computer Forensics and Security Management is an interdisciplinary professional/practice graduate program involving faculty from the Departments of Computer & Information Sciences, Justice Sciences, Management, Information Systems, and Quantitative Methods, and Accounting & Finance. The program is designed to prepare graduate students with backgrounds in criminal justice, computer and information sciences, information systems, information technology, and forensic accounting to practice in the fields of computer forensics and security management including information security and forensic accounting. Further, the program is intended to develop skills, including familiarity with industry practices, innovative methods, critical thinking, and problem solving crucial for competitiveness and success in entry- and (depending on experience), advanced-level positions in the areas of computer forensics, information security management, and forensic accounting. Further, the program is intended to increase the pipeline of prospective, high-quality, entry- and advanced level employees involved with protecting physical and virtual systems, vital to the U.S., whose incapacitation or destruction would have a debilitating effect on national security, the nation's economic system. The program also seeks to provide to current employees in the public and private sectors an opportunity to obtain advanced-level, high-quality training in the core areas of computer forensics, information security management, and forensic accounting, to facilitate career advancement.

2. *The Principal Architect, and a Co-Director* for the new **M.S. program in Cyber-Security**, at NYU-Poly, from Fall 2009 to Spring 2011
   (Program Web: http://www.poly.edu/academics/programs/cybersecurity-ms)

   Program Synopsis: The demand for skilled computer security professionals has been continuously growing as businesses and government continue to invest heavily in "cyber-security," the science of protecting vital computer networks and electronic infrastructures from attacks. To help fulfill this demand, Computer Science and Engineering department at NYU-Poly launched the new M.S. program in Cyber-Security. This MS program offers strong, well-rounded and specialized education covering both theory and hands-on practice, producing graduates ready to meet the real-world and unforeseen cyber-security challenges.

7.2 New Curriculum Development

@UAB

- **CS 336/536:** Network Security, first offering Fall 2013
  This *undergraduate/graduate* level course has been completely re-designed as one of the core courses in the Security area

- **CS 436/636/736:** Computer Security, first offering Spring 2012
  This *undergraduate/graduate* level course has been completely re-designed as one of the core courses in the Security area

@NYU-Poly

- **CS6903** (previously CS996): Modern Cryptography
  One of the core *graduate* courses in the “Theory” Area
  One of the mandatory courses for the M.S. program in Cyber-Security

7.3 Course Instruction

@UAB

1. **CS 336/536:** Network Security

(course web page: http://www.cis.uab.edu/saxena/teaching/cs336-f14/)

2. **CS 250**: Discrete Structures, Fall 2013
   (course web page: http://www.cis.uab.edu/saxena/teaching/cs250-f14/)
3. **CS 436/636/736:** Computer Security, Spring 2014
   (course web page: http://www.cis.uab.edu/saxena/teaching/csx36-s14/)
4. **CS 336/536:** Network Security
   (course web page: http://www.cis.uab.edu/saxena/teaching/cs336-f13/)
5. **CS 250**: Discrete Structures, Fall 2013
   (course web page: http://www.cis.uab.edu/saxena/teaching/cs250-f13/)
6. **CS 436/636/736:** Computer Security, Spring 2013
   (course web page: http://www.cis.uab.edu/saxena/teaching/csx36-s13/)
7. **CS 250**: Discrete Structures, Fall 2012
   (course web page: http://www.cis.uab.edu/saxena/teaching/cs250-f12/)
8. **CS 436/636/736:** Computer Security, Spring 2012
   (course web page: http://www.cis.uab.edu/saxena/teaching/csx36-s12/)
9. **CS 250**: Discrete Structures, Fall 2011
   (course web page: http://www.cis.uab.edu/saxena/teaching/cs250-f11/)

@NYU-Poly

10. **CS6903**: Modern Cryptography, Spring 2011
    (course web-page: http://isis.poly.edu/courses/cs6903-s11/)
11. **CS392/6813**: Computer Security, Fall 2010
    (course web-page: http://isis.poly.edu/courses/cs392-f2010/)
12. **CS6903**: Modern Cryptography, Spring 2010
    (course web-page: http://isis.poly.edu/courses/cs6903-s10/)
13. **CS392/6813**: Computer Security, Fall 2009
    (course web-page: http://isis.poly.edu/courses/cs392-f2009/)
14. **CS6903**: Modern Cryptography, Spring 2009
    (course web-page: http://isis.poly.edu/courses/cs6903-s09/)
15. **CS392/6813**: Computer Security, Fall 2008
    (course web-page: http://isis.poly.edu/courses/cs392-f2008/)
16. **CS6903**: Modern Cryptography, Spring 2008
    (course web-page: http://isis.poly.edu/courses/cs6903/)
17. **CS392/6813**: Computer Security, Fall 2007
    (course web-page: http://isis.poly.edu/courses/cs392-f2007/)
18. **RFID Security and Privacy**, CATT One-Day Short Course, Summer 2007
19. **RFID Security and Privacy**, a one-hour crash course delivered (telephonically) in the "October Meeting of the AT&T IP Services Security Council"
    (Hosted by Cristina Serban, AT&T)
20. **CS996:** Modern Cryptography, Spring 2007
    (course web-page: http://isis.poly.edu/courses/cs996-s2007/)
21. **CS392/681**: Computer Security, Fall 2006

(course web-page: http://isis.poly.edu/courses/cs392-f2006/)

7.4 Student Supervision

@UAB

Ph.D. Students

1. Babins Shrestha (ongoing; since Spring 2012)
2. Manar Mohamed (ongoing; since Summer 2012)
3. Ajaya Neupane (ongoing; since Fall 2012; winner of the NDSS 2014 Distinguished Paper Award)
4. Maliheh Shirvanian (ongoing; since Summer 2013)
5. Dibya Mukhopadhyay (ongoing; since Fall 2013)
6. Prakash Shrestha (ongoing; since Fall 2014)
7. Abhishek Anand (ongoing; since Fall 2013; winner of CIS outstanding graduating MS student award, 2015)
8. Song Gao (**graduated** in Fall 2014; thesis title *"An Evolutionary Study of Dynamic Cognitive Game CAPTCHAs: Automated Attacks and Defenses"*; now a Software Engineer at Google; co-advised with Chengcui Zhang; winner of the College of Arts and Sciences Graduate Student Entrepreneurship Awards, 2014; winner of College of Arts and Sciences Dean's Outstanding Graduating Student Award, 2014; winner of CIS outstanding graduating PhD student award, 2014)

Visiting Ph.D. Students

- Niharika Sachdeva (Spring to Summer 2012; visiting PhD student from IIITD, India)

M.S. Students

1. Abhishek Anand (Fall 2013 to Summer 2015; winner of CIS outstanding graduating MS student award, 2015; now continuing as PhD student)
2. Md. Lutfor Rahman (Fall 2012 to Spring 2014; now a lead developer at Marvin Technology)
3. Richard Edgar Niedermeier (Summer 2012)
4. Chatchai Satienpattanakul (Spring 2012)
5. Dustin Reinhart (Spring 2012; co-advised with Dr. Ragib Hasan)

Undergraduate Students

1. Eric Leinert (ongoing; since Fall 2015)
2. Anders Borg (Summer 2013 to Summer 2014)
3. Oliver Nick Harper (ongoing; since Spring 2013)
4. Jacinta Cai (ongoing; since Spring 2013)
5. Michael Georgescu (ongoing; since Fall 2012)
6. Justin Harrison (ongoing; since Fall 2012)
7. Sam Cleveland (Spring 2012)
8. Logan Holmes (Summer 2012; Talladega College; through Ronald McNair Program)

High School Students

1. Austin Robinson (Fall 2011 and Spring 2012; Alabama School of Fine Arts; now an undergraduate student at Embry-Riddle Aeronautical University; won the **Mu Alpha Theta Award** for "*the most challenging, thorough, and creative investigation of a problem involving mathematics accessible to high school students*" at the Regional Science and Engineering Fair, 2012)
2. Casey Barnette (Summer 2012; Alabama School of Fine Arts)

@NYU-Poly

Ph.D. Students

1. Tzipora Halevi (started Spring 2009; **graduated** in Summer 2012; thesis title "*Using Audio for Security and Privacy: A Dual Perspective*"; now a post-doctoral researcher at, and the assistant director of, the NYU/NYU-Poly Center for Interdisciplinary Studies in Security and Privacy)
2. Jonathan Voris (started Fall 2007; **graduated** in August 2011; thesis title "*User-Centered Security and Privacy Primitives for Emerging Mobile Platforms*"; now an **Assistant Professor** at the School of Engineering and Computing Sciences at the *New York Institute of Technology*; received **the Deborah Rosenthal MD Award**, 2009 for an outstanding performance in the PhD Qualifying Exam)
3. Cong Tang (Spring 2009 – Fall 2010) (visiting PhD student from Peking University; co-advised with Keith Ross; **graduated** in August 2011; now a researcher at China Academy of Electronics and Information Technology, Beijing)
4. Md. Borhan Uddin (Fall 2007 – Fall 2009; **graduated** with an M.S. and now a member of technical staff at VMware)
5. Justin (Sein) Lin (Fall 2010 and Spring 2011; **graduated** with an M.S. and now a financial software engineer at Bloomberg)
6. Sai Teja Peddinti (Fall 2009 – Spring 2011; received **the Deborah Rosenthal MD Award**, 2011 for an outstanding performance in the PhD Qualifying Exam; now a researcher at Google)

M.S. Students (all graduated)

1. Avis Dsouza, Spring 2011
2. Devansh Mehta, Spring 2010
3. Vinay Prabhushankaran, Spring 2010
4. Sathesh Kiran, Spring 2010
5. Samiksha Saxena, Fall 2009
6. Alimuddin Aagwan, Spring and Summer 2009
7. Ambarish Karole, since Spring 2009
8. Arun Kumar**,** graduated with **MS Thesis** (title "*Comparative Usability Evaluation of Device Pairing Methods*"), Fall 2009
9. Seshadri, Fall 2008
10. Aaron R. Pathripala, Fall 2008
11. Mansi Tolia, Summer and Fall 2007
12. Siddharth Vangavaragu, Summer and Fall 2007
13. Abhay Nayak, Fall 2007
14. Pravin Ghate, Fall 2007
15. Ramnath Prasad, Spring and Summer 2007
16. Ragini Okhandiar, Spring 2007

Undergraduate Students (graduated)

1. Alexander Gallego (Spring 2010 – Summer 2011; now a Software Engineer at Hashable)
2. Luis E. Garcia II (Spring 2009 – Fall 2010; now a graduate student at NYU-Poly)

7.5 Professional Development in Teaching

Attended a 5-day NSF sponsored workshop on *Teaching Information Assurance through Case Studies and Hands-on Experiences*, held at the University of Tennessee at Chattanooga, from May 20 – 25, 2012. The workshop provided advanced training on incorporating practical tools for teaching security-focused courses, such as applied cryptography, network security, wireless security and cloud computing.

(workshop web page: http://teaching-ia.appspot.com/workshop)

8 COMMUNITY SERVICE

[***Reviewer** for **key security programs**; **Editor** of two top-tier journals, **TPC member** of over **50 conferences/workshops**; **Reviewer** of over **400 papers,** and many grant proposals*]

8.1 University/Internal Service

- Departmental representative on the Faculty Affairs Committee (FAC) of the College of Arts and Sciences (CAS), since August 2014.
- Faculty Search Committee Chair, Computer and Information Science, 2015-2016.
- Chair's Advisory Committee member, Computer and Information Sciences, since August 2014.
- Faculty Controller, Computer and Information Sciences Website, since August 2014.

8.2 Graduate Program Review

- Invited reviewer for Sam Houston State University's (Huntsville, TX) Information Assurance and Security graduate program, March 2014. Selected and served as an out-of-state reviewer. Reviewed the Texas Higher Education Coordinating Board self-study, performed an onsite review of the program, and provided a written report containing a response to the self-study, a summary of observations during the onsite visit and recommendations (strengths and concerns).

8.3 Panels and Grant Proposal Review

- Reviewer for a proposal submitted to the Natural Sciences and Engineering Research Council of Canada Discovery Grants Program, December 2012.
- Reviewer for NSF Panel project proposals submitted under the "Medium Projects" category for the CISE Cross-Cutting Programs: FY 2009 and FY 2010, "Trustworthy Computing", January and February, 2009.
- Ad Hoc Reviewer for NSF Panel project proposal submitted under the "Large Projects" category for the CISE Cross-Cutting Programs: FY 2009 and FY 2010, "Human-Centered Computing", March 2009.

8.4 Journal Editorial Board Membership

- IEEE Transactions on Information Forensics and Security (since July 2013)
- Springer's International Journal of Information Security (IJIS) (since May 2013)
- International Journal of Reliable Information and Assurance (IJRIA) (since January 2014)

8.5 Books Editorial Advisory Board Membership

- Security, Privacy, and Digital Forensics in the Cloud, Wiley, to be published in 2015

8.6 Conference / Workshop Leadership

- *Technical Program Co-Chair*, Protocols and Security Track, the 10th Annual International Conference on RFID (IEEE RFID), 2016: http://2016.ieee-rfid.org/

- *Steering Committee Member*, Workshop on RFID Security and Privacy (RFIDSec), since 2014.
- *Technical Program Co-Chair*, the 10th International Workshop on RFID Security and Privacy (RFIDSec), University of Oxford, UK, 2014: http://rfidsec2014.cis.uab.edu/
- *Primary organizer* for the North-East Security and Privacy Day, held at NYU-Poly in Fall 2009: http://isis.poly.edu/snp2009/

8.7 Conference / Workshop Technical Program Committees

1. International Conference on RFID: IEEE RFID 2016
2. USENIX Security Symposium: Usenix Security 2015
3. ACM Conference on Computer and Communications Security: CCS 2014
4. European Symposium on Research in Computer Security: ESORICS 2015
5. International Conference on Network and System Security: NSS 2015
6. International workshop on RFID Security: RFIDSec 2015
7. International Conference on Computer Communications and Networks (Security Track): ICCCN 2015
8. International Conference on Information Security and Cryptology: ICISC 2015
9. International Workshop on Lightweight Cryptography for Security & Privacy: LightSec 2014
10. ACM Conference on Computer and Communications Security: CCS 2014
11. International Workshop on Lightweight Cryptography for Security & Privacy: LightSec 2014
12. ASE/IEEE International Conference on Cyber Security: CyberSecurity 2014
13. International Conference on Cryptology and Network Security: CANS 2014
14. International Conference on Information Security and Cryptology: ICISC 2014
15. International Workshop on Secure Internet of Things: SIoT 2014
16. International Conference on Big Data and Smart Computing: BigComp 2014
17. International Workshop on Security and Privacy aspects of Mobile Environments: SMPE 2014 (co-located with MobiCom 2014)
18. International Conference on Information Security and Cryptology: Inscrypt 2013
19. International Conference on Information Security and Cryptology: ICISC 2013
20. IEEE International Conference on Communications: ICC 2013
21. International workshop on RFID Security: RFIDSec 2013
22. IEEE Global Communications Conference (Communication & Information System Security Track): Globecom 2013
23. International Conference on Information Security and Cryptology: ICISC 2012
24. International Workshop on Management and Security technologies for Cloud Computing (colocated with Globecom): ManSec-CC 2012
25. ASE/IEEE International Conference on Cyber Security: CyberSecurity 2012
26. Workshop on Information Security Applications: WISA 2012
27. IEEE International Conference on Information Reuse and Integration (IRI)

28. ACM Conference on Wireless Network Security: WiSec 2012
29. Network and Distributed Systems Security: NDSS 2012
30. International workshop on RFID Security: RFIDSec 2012
31. Workshop on Information Security Applications: WISA 2011
32. Network and Distributed Systems Security: NDSS 2011
33. Applied Cryptography and Network Security: ACNS 2011
34. ACM Conference on Wireless Network Security: WiSec 2011
35. International workshop on RFID Security: RFIDSec 2011
36. IEEE Global Communications Conference (Communication & Information System Security Track): Globecom 2011
37. Cryptology and Network Security: CANS 2010
38. Conference on Information Systems Security: ICISS 2010
39. Information Security Conference: ISC 2010
40. Network and System Security: NSS 2010
41. IEEE Global Communications Conference (Communication & Information System Security Track): Globecom 2010
42. Applied Cryptography and Network Security Conference: ACNS 2010
43. ACM Conference on Wireless Network Security: WiSec 2010
44. International Workshop on Security, Privacy and Trust of Computer and Cyber-Physical Networks: SecureCPN 2009
45. Network and System Security: NSS 2009
46. Asia-Pacific Signal and Information Processing Association: APSIPA 2009
47. IACR International Conference on Theory and Practice of Public-Key Cryptography: PKC 2009
48. IEEE International Workshop on Network and System Security: NeSS 2008
49. Security and Privacy in Communication Networks: SecureComm 2008
50. ACM International Conference on emerging Networking EXperiments and Technologies: CoNext 2008
51. Workshop on Cryptpgraphy for Ad Hoc Networks: WCAN 2007
52. Security and Privacy in Communication Networks: SecureComm 2007
53. International Conferences on Information Security and Cryptology: Inscrypt (formerly CISC) 2006
54. Workshop on Secure Network Protocols: NPSec 2006

8.8 Journal / Conference / Workshop Reviewing

Refereed for international journals, conferences, and workshops, including ACM conference on computer and communications security (*CCS 2003, 2004*); IEEE Symposium on Security and Privacy (*ISP 2004*); Network and Distributed System Security Symposium (*NDSS 2004*); European Workshop on Security in Ad-Hoc and Sensor Networks (*ESAS 2004*); ACM Workshop on Security of Ad Hoc and Sensor Networks (*SASN 2004*); IEEE Wireless Communications and Networking Conference (*WCNC 2004*); International Conference on Distributed Computing Systems (*ICDCS 2005*); International Conference on Applied

Cryptography and Network Security (*ACNS 2005*); ACM Symposium on Principles of Distributed Computing (*PODC 2005*); IEEE Journal on Selected Areas in Communications (*J-SAC 2005, J-SAC 2007*); Financial Cryptography and Data Security (*FC 2006*); Workshop on Secure Network Protocols (*NPSec 2006*); Conference on Computer Communications (*Infocom 2007*); International Conferences on Information Security and Cryptology (*Inscrypt 2006*); IEEE Signal Processing Magazine 2007; European Workshop on Security and Privacy in Ad hoc and Sensor Networks *(ESAS 2007)*, ACM Transactions on Information and System Security (*TISSEC 2007*); Security and Privacy in Communication Networks (*SecureComm 2007*); IACR Conference on the Theory and Applications of Cryptographic Techniques (*Eurocrypt 2008*); Workshop on Cryptpgraphy for Ad Hoc Networks (*WCAN 2007*); Security and Privacy in Communication Networks (*SecureComm 2008*); IEEE International Workshop on Network and System Security (*NeSS 2008*); ACM International Conference on emerging Networking EXperiments and Technologies (*CoNExt 2008*); IACR International Conference on Theory and Practice of Public-Key Cryptography (*PKC 2009*); Conference on Computer Communications (*Infocom 2009*); Elsevier Computer Communications Journal 2009; Asia-Pacific Signal and Information Processing Association (*APSIPA 2009*); Network and System Security (*NSS 2009*); International Workshop on Security, Privacy and Trust of Computer and Cyber-Physical Networks (*SecureCPN 2009*); Journal of Communications and Networks (*JCN*) 2009; International Conference on Information Systems Security (*ICISS 2009*) ; ACM Conference on Wireless Network Security (*WiSec 2010*); Applied Cryptography and Network Security Conference (*ACNS 2010*); IEEE Global Communications Conference (Communication & Information System Security Track, *Globecom 2010*); Network and System Security (*NSS 2010*); Information Security Conference (*ISC 2010*); Conference on Information Systems Security (*ICISS 2010*); Network and Distributed Systems Security (*NDSS 2011*); ACM Conference on Wireless Network Security (*WiSec 2011*); Applied Cryptography and Network Security Conference (*ACNS 2011*); Symposium On Usable Privacy and Security (SOUPS 2011); IEEE Transactions on Information Forensics and Security (*TIFS 2011*); International Workshop on Information Security Applications (WISA2011); RFID Security (RFIDSec 2011); Network and Distributed Systems Security (*NDSS 2012);* ACM Conference on Wireless Network Security (*WiSec 2012*); RFID Security (*RFIDSec 2012*); IEEE International Conference on Information Reuse and Integration (*IRI 2012*); Workshop on Information Security Applications (*WISA 2012*); IEEE Transactions on Information Forensics and Security (*TIFS 2012*); IEEE Transactions on Dependable and Secure Computing (*TDSC 2012*); IEEE Transactions on Mobile Computing (*TMC 2012*); IEEE Transactions on Internet Technology (*TOIT 2012*); ACM Transactions on Information and System Security (*TISSEC 2012*) – 2 papers; International Conference on Information Security and Cryptology (*Inscrypt 2013*); International Conference on Information Security and Cryptology (*ICISC 2013*); IEEE International Conference on Communications (*ICC 2013*); International workshop on RFID Security (RFIDSec 2013);IEEE Global Communications Conference (Communication & Information System Security Track) (*Globecom 2013*); ACM Conference on Computer and Communications Security (*CCS 2014);* International Workshop on Lightweight Cryptography for Security & Privacy (*LightSec 2014*); ASE/IEEE International Conference on Cyber Security (*CyberSecurity 2014*); International Conference on Cryptology and Network Security (*CANS 2014*); International

Conference on Big Data and Smart Computing (*BigComp 2014*); Usenix Security Symposium (*Usenix Security 2014*); International Conference on Information Security and Cryptology (*ICISC 2014*).