MARK STAMP

mark.stamp@sjsu.edu
Department of Computer Science
San Jose State University
One Washington Square
San Jose, California 95192

Education

PhD	Mathematics	Texas Tech University Lubbock, Texas	1/89–5/92
MS	Mathematics	Texas Tech University Lubbock, Texas	8/86–8/88
BS	Computer Science	Morningside College Sioux City, Iowa	8/79–5/83
	High School	Harlan Community High School Harlan, Iowa	8/75–5/79

Employment

- **Professor** (8/02–present)
  Department of Computer Science
  San Jose State University
  San Jose, California

  Responsibilities
  - Teach undergraduate classes
    - Information Security (CS 166)
    - Computer Networks (CS 158A)
    - Network Management (CS 158B)
    - Introduction to Programming in Java (CS 46A)
    - Introduction to Data Structures (CS 46B)

- Teach graduate classes
  - Cryptography and Computer Security (CS 265)
  - Software Reverse Engineering (CS 286)
  - Distributed Computing (CS 249)
  - Applied Network Security (CS 286)
- Research and publication in information security and related fields
- Direct Master's and undergraduate student research projects

- **Lecturer** (Winter Quarter 2003)
  Department of Computer Science
  University of California, Santa Cruz
  Santa Cruz, California

  Responsibilities
  - Taught graduate Combinatorial Algorithms (CMPS 211)

- **Chief Cryptologic Scientist** (12/00–4/02)
  MediaSnap, Inc.
  San Jose, California

  Responsibilities
  - Design, analyze, implement, and test security features of digital rights management (DRM) system, including proprietary scrambling, key management, and software uniqueness algorithms
  - Cryptographic, statistical, and mathematical analysis in support of digital watermarking, software encryption, and anti-debugging techniques
  - Implement and verify correct usage of encryption algorithms including AES and RSA
  - Software development in Microsoft Windows Visual C++
  - Analyze competing DRM systems, including patent reviews
  - Supervise junior software engineers
  - Produce written documentation including patent disclosures, detailed system specifications, and user documentation

- **Cryptologic Mathematician** (5/93–12/00)
  National Security Agency
  Fort George G. Meade, Maryland

  Responsibilities

- Classified research and development in the fields of cryptography, algorithms, and networks in support of signals intelligence (SIGINT)
- Classified speech research and development in support of SIGINT
- Applied supercomputing and distributed computing
- Software development using C in a UNIX environment on DEC/Compaq, Sun, and HP workstations
- Project supervisor

- **Visiting Assistant Professor** (8/92–5/93)
  Mathematical Sciences
  Worcester Polytechnic Institute
  Worcester, Massachusetts

  Responsibilities
  - Academic research and publication in cryptography, combinatorics, epidemiology, simulation, numerical analysis, and control theory
  - Taught undergraduate Calculus I, Calculus III, and Graph Theory

- **Teaching/Research Assistant** (1/86–8/92)
  Department of Mathematics
  Texas Tech University
  Lubbock, Texas

  Responsibilities
  - Research in cryptography, control theory, epidemiology, and numerical analysis in support of research grants
  - Taught undergraduate Business Mathematics and College Algebra

- **Part-time Instructor** (5/85–8/85)
  Private language schools
  Taiwan

  Responsibilities
  - Taught English conversation

- **Instructor** (1/85–5/85)
  Nebraska Indian Community College

Winnebago, Nebraska

Responsibilities
- Taught Introduction to Computers

Personal Data

- Citizenship: United States
- Highest security clearance held: TS//SI

Selected Academic Referee Experience

- Frontiers of Information Technology & Electronic Engineering
- *Computer Networks*
- *International Journal of Information Security*
- *Proceedings of the IEEE*
- *Information Sciences*
- *Security and Communication Networks*
- *ACM Transactions on Information and System Security*
- *The Ramanujan Journal*
- *Journal of Cryptographic Engineering*
- *Designs, Codes and Cryptography*
- *Theoretical Computer Science*

- *IEEE Transactions on Information Forensics and Security*
- *Engineering Applications of Artificial Intelligence*
- *IEEE Transactions on Computers*
- *Computers & Security*
- *Information Processing Letters*
- *Journal of Computer Virology and Hacking Techniques*
- *Computer Communications*
- *IEEE Transactions on Image Processing*
- *IEEE Computer*
- *Journal of Systems and Software*
- *IEEE Transactions on Information Theory*

Recent Conferences

- 3rd International Workshop on Security and Privacy Analytics 2017 (IWSPA 2017), co-located with ACM CODASPY 2017, March 24, 2017, Scottsdale, Arizona. Technical program committee.
- Second International Workshop on Malware Analysis (WMA 2017), co-located with ARES Conference 2017, August 29–September 1, 2017, Reggio Calabria, Italy. Workshop co-chair.
- Malware Conference 2017, Puerto Rico, dates TBD, Technical program committee.
- Malware Conference 2016 (MALCON 2016), Fajardo, Puerto Rico, October 18–21, 2016. Technical program committee.
- 12th International Conference on Information Systems Security (ICISS 2016), December 16–20, 2016, Jaipur, India. Technical program committee.

- First International Workshop on Malware Analysis (WMA 2016), co-located with ARES Conference 2016, August 31–September 2, 2016, Salzburg, Austria. Workshop co-chair.

- 2nd International Workshop on Security and Privacy Analytics 2016 (IWSPA 2016), co-located with ACM CODASPY 2016, March 11, 2016, New Orleans. Technical program committee.

- 10th International Conference on Malicious and Unwanted Software (MALCON 2015), Fajardo, Puerto Rico, USA, October 20–22, 2015. Technical program committee.

- 9th International Conference on Malicious and Unwanted Software (MALCON 2014), Fajardo, Puerto Rico, October 28–30, 2014. Technical program committee.

- 8th International Conference on Malicious and Unwanted Software "The Americas" (MALWARE 2013 The Americas), Fajardo, Puerto Rico, October 21–25, 2013. Technical program committee.

- 21st EICAR Annual Conference (EICAR2012), Lisbon, Portugal, May 7–8, 2012. Program committee.

- 20th USENIX Security Symposium (USENIX Security '11), San Francisco, California, August 8–12, 2011. Poster presentation: Robust watermarking using hidden Markov models, M. Mungale (student).

- USENIX Workshop on Cyber Security Experimentation and Test (CSET '10), Washington, DC, August 9, 2010. Program committee.

- 20th EICAR Annual Conference (EICAR2011), Krems, Austria, May 9–10, 2010. Program committee.

- USENIX Workshop on Cyber Security Experimentation and Test (CSET '09), Montreal, Canada, August 10, 2009. Program committee.

- 2008 International Workshop on Multimedia Security in Communication (MUSIC '08), Hangzhou, China, August 25–28, 2008. Technical program committee

- USENIX Workshop on Cyber Security Experimentation and Test (CSET '08), San Jose, California, July 28, 2008. Program committee.

- 2008 International Conference on Security and Cryptography (SECRYPT 2008), Porto, Portugal, July 26–29, 2008. Program committee.

Publications

1. A survey of machine learning algorithms and their application in information security, to appear in *Guide to Vulnerability Analysis for Computer Networks and Systems — An Artificial Intelligence Approach*, S. Parkinson, A. Crampton, and R. Hill, editors, Springer 2018.

2. Function call graphs versus machine learning for malware detection, with D. Rajeswaran (student), F. Di Troia, and T. H. Austin, to appear in *Guide to Vulnerability Analysis for Computer Networks and Systems — An Artificial Intelligence Approach*, S. Parkinson, A. Crampton, and R. Hill, editors, Springer 2018.

3. Detecting encrypted and polymorphic malware using hidden Markov models, with D. Dhanasekar (student), F. Di Troia, and K. Potika, to appear in *Guide to Vulnerability Analysis for Computer Networks and Systems — An Artificial Intelligence Approach*, S. Parkinson, A. Crampton, and R. Hill, editors, Springer 2018.

4. Masquerade detection on mobile devices, with S. N. K. Manikoth (student) and F. Di Troia, to appear in *Guide to Vulnerability Analysis for Computer Networks and Systems — An Artificial Intelligence Approach*, S. Parkinson, A. Crampton, and R. Hill, editors, Springer 2018.

5. On the effectiveness of generic malware models, with N. Bagga (student) and F. Di Troia, submitted.

6. Hidden Markov models for Vigenère cryptanalysis, with F. Di Troia, M. Stamp (student), and J. Huang (student), International Conference on Historical Cryptology (HistoCrypt 2018), Uppsala, Sweden, June 18–20, 2018.

7. A comparison of machine learning classifiers for acoustic gait analysis, with F. Di Troia and J. Huang (student), submitted.

8. Bootbandit: A macOS bootloader attack, with A. Boursalian (student), submitted.

9. Acoustic gait analysis using support vector machines, with J. Huang (student), and F. Di Troia, 2nd International Workshop on Formal Methods for Security Engineering (ForSE 2018), Funchal, Madeira, Portugal, January 22–24, 2018.

10. Black box analysis of Android malware detectors, with G. Nellaivadivelu (student), and F. Di Troia, submitted.

11. Deep learning versus gist descriptors for image-based malware classification, with S. Yajamanam (student), V. R. S. Selvin (student), and F. Di Troia, 2nd International Workshop on Formal Methods for Security Engineering (ForSE 2018), Funchal, Madeira, Portugal, January 22–24, 2018.

12. Autocorrelation analysis of financial botnet traffic, with P. Nagarajan (student), F. Di Troia, and T. H. Austin, 2nd International Workshop on Formal Methods for Security Engineering (ForSE 2018), Funchal, Madeira, Portugal, January 22–24, 2018.

13. Improved image spam detection, with A. Chavda (student), K. Potika, and F. Di Troia, submitted.

14. *Introduction to Machine Learning with Applications in Information Security*, Chapman and Hall/CRC, August 2017.

15. Virtual values for taint and information flow analysis, with P. Kannan, T. H. Austin, T. Disney, and C. Flanagan, Workshop on Meta-Programming Techniques and Reflection (META 2016), co-located with ACM SPLASH 2016, October 30–November 4, 2016, Amsterdam.

16. Static and dynamic analysis of Android malware, with A. Kapratwar (student) and F. Di Troia, 1st International Workshop on Formal Methods for Security Engineering (ForSE 2017), Porto, Portugal, February 19–21, 2017, in *Proceedings of the 3rd International Conference on Information Systems Security and Privacy*.

17. Image spam analysis and detection, with A. Annadatha (student), *Journal of Computer Virology and Hacking Techniques*, online first.

18. Vigenère scores for malware detection, with S. Deshmukh (student) and F. Di Troia, *Journal of Computer Virology and Hacking Techniques*, online first.

19. Advanced Transcriptase for JavaScript malware, with F. Di Troia, C. A. Visaggio, and T. H. Austin, MALCON 2016, Fajardo, Puerto Rico, October 18–21, 2016.

20. A completely covert audio channel in Android, with S. Thakur (student), *Journal of Computer Virology and Hacking Techniques*, 13(3):141–152, August 2017.

21. A comparison of static, dynamic, and hybrid analysis for malware detection, with A. Damodaran (student), F. Di Troia, C. A. Visaggio, and T. H. Austin, *Journal of Computer Virology and Hacking Techniques*, 13(1):1–12, February 2017.

22. Support vector machines and malware detection, with T. Singh (student), F. Di Troia, C. A. Visaggio, and T. H. Austin, *Journal of Computer Virology and Hacking Techniques*, 12(4):203–212, November 2016.

23. Malware detection using dynamic birthmarks, with S. Vemparala (student), F. Di Troia, C. A. Visaggio, and T. H. Austin, 2nd International Workshop on Security & Privacy Analytics (IWSPA 2016), co-located with ACM CODASPY 2016, March 9–11, 2016.

24. Clustering versus SVM for malware detection, with U. Narra (student), F. Di Troia, C. A. Visaggio, and T. H. Austin, *Journal of Computer Virology and Hacking Techniques*, 12(4):213–224, November 2016.

25. Clustering for malware classification, with S. Pai (student), F. Di Troia, C. A. Visaggio, and T. H. Austin, *Journal of Computer Virology and Hacking Techniques*, 13(4):95–107, May 2017.

26. Static analysis of malicious Java applets, N. Ganesh (student), F. Di Troia, C. A. Visaggio, and T. H. Austin, 2nd International Workshop on Security & Privacy Analytics (IWSPA 2016), co-located with ACM CODASPY 2016, March 9–11, 2016.

27. SocioBot: A Twitter-based botnet, with I. Kaur Makkar (student), F. Di Troia, C. A. Visaggio, and T. H. Austin, *International Journal of Security and Networks*, 12(1):1–12, 2017.

28. Classic cryptanalysis using hidden Markov models, with R. Vobbilisetty (student), F. Di Troia, R. M. Low, and C. A. Visaggio, *Cryptologia*, 41(1):1–28, 2017.

29. Dueling hidden Markov models for virus analysis, with A. Kalbhor (student), T. H. Austin, E. Filiol, and S. Josse, *Journal of Computer Virology and Hacking Techniques*, 11(2):103–118, May 2015.

30. Automating NFC message sending for good and evil, with N. B. Brandt (student), *Journal of Computer Virology and Hacking Techniques*, 10(4):273–297, November 2014.

31. Hunting for metamorphic JavaScript malware, with M. Musale (student) and T. H. Austin, *Journal of Computer Virology and Hacking Techniques*, 11(2):89–102, May 2015.

32. Hunting for pirated software using metamorphic analysis, with H. Rana (student), *Information Security Journal: A Global Perspective*, 23(3):68–85, November 2014.

33. Metamorphic detection using function call graph analysis, with P. Deshpande (student), *MIS Review: An International Journal*, 21(1/2):15–34, September 2015/March 2016.

34. Singular value decomposition and metamorphic detection, with R. K. Jidigam (student) and T. H. Austin, *Journal of Computer Virology and Hacking Techniques*, 11(4):203–216, 2015.

35. Compression-based analysis of metamorphic malware, with J. Lee (student) and T. H. Austin, *International Journal of Security and Networks*, 10(2):124–136, 2015.

36. Hidden Markov models for malware classification, with C. Annachhatre (student) and T. H. Austin, *Journal of Computer Virology and Hacking Techniques*, 11(2):59–73, May 2015.

37. Deriving common malware behavior through graph clustering, with Y. Park and D. S. Reeves, *Computers & Security*, 39(B):419–430, November 2013.

38. Masquerade detection for GUI-based Windows systems, with A. Agrawal (student), *International Journal of Security and Networks*, 10(1):32–41, 2015

39. Kullback-Leibler divergence for masquerade detection, with G. R. Viswanathan (student) and R. M. Low, *Journal of Network and Information Security*, 1(1):44–53, June 2013.

40. Metamorphic code from LLVM bytecode, with T. Tamboli (student) and T. H. Austin, *Journal of Computer Virology and Hacking Techniques*, 10(3):177–187, August 2014.

41. HTTP attack detection using *n*-gram analysis, with A. Oza (student), R. M. Low, et al., *Computers & Security*, 45:242–254, September 2014.

42. Eigenvalue analysis for metamorphic detection, with S. Deshpande (student) and Y. Park, *Journal of Computer Virology and Hacking Techniques*, 10(1):53–65, February 2014.

43. Simple substitution distance and metamorphic detection, with G. Shanmugam (student) and R. M. Low, *Journal of Computer Virology and Hacking Techniques*, 9(3):159–170, August 2013.

44. Structural entropy and metamorphic malware, with D. Baysa (student) and R. M. Low, *Journal of Computer Virology and Hacking Techniques*, 9(4):179–192, November 2013.

45. Social networking for botnet command and control, with A. Singh (student), A. H. Toderici (student), et al., *International Journal of Computer Network and Information Security*, 5(6):11–17, May 2013.

46. Java design pattern obfuscation, with P. K. Gone (student), *Proceedings of the 2013 International Conference on Security & Management* (SAM'13), July 22–25, 2013.

47. Chi-squared distance and metamorphic virus detection, with A. H. Toderici (student), *Journal of Computer Virology and Hacking Techniques*, 9(1):1–14, February 2013.

48. Cryptanalysis of Typex, with K. Chang (student) and R. M. Low, *Cryptologia*, 38(2):116–132, 2014.

49. Metamorphic worm that carries its own morphing engine, with S. M. Sridhara (student), *Journal of Computer Virology and Hacking Techniques*, 9(2):49–58, May 2013.

50. Hidden Markov models for software piracy detection, with S. Kazi (student), *Information Security Journal: A Global Perspective*, 22(3):140–149, 2013.

51. Exploring hidden Markov models for virus analysis: A semantic approach, with T. H. Austin, E. Filiol, and S. Josse, *Proceedings of 46th Hawaii International Conference on System Sciences* (HICSS 46), January 7–10, 2013.

52. Efficient cryptanalysis of homophonic substitution ciphers, with A. Dhavare (student) and R. M. Low, *Cryptologia*, 37(3):250–281, 2013.

53. Opcode graph similarity and metamorphic detection, with N. Runwal (student) and R. M. Low, *Journal in Computer Virology*, 8(1-2):37–52, May 2012.

54. Software similarity and metamorphic detection, with M. Mungale (student), in *Proceedings of 2012 International Conference on Security & Management* (SAM '12).

55. Masquerade detection using profile hidden Markov models, with L. Huang (student), *Computers & Security*, 30(8):732–747, November 2011.

56. *Information Security: Principles and Practice*, 2nd edition, Wiley, May 2011, ISBN: 978-0-470-62639-9.

57. Improved software activation using multithreading, with J. Zhang (student), *International Journal of Computer Network and Information Security*, 4(12):1–17, November 2012.

58. Hunting for undetectable metamorphic viruses, with D. Lin (student), *Journal in Computer Virology*, 7(3):201–214, August 2011.

59. Detecting undetectable metamorphic viruses, with S. Venkatachalam (student), *Proceedings of 2011 International Conference on Security & Management* (SAM '11), pp. 340–345.

60. A highly metamorphic virus generator, with P. Desai (student), *International Journal of*

Multimedia Intelligence and Security, 1(4):402–427, 2010.

61. iPhone security analysis, with V. Pandya (student), *Journal of Information Security*, 1(2):73–86, October 2010.

62. *Handbook of Information and Communication Security*, editor, with P. Stavroulakis, Springer, March 2010, ISBN: 978-3-642-04116-7.

63. An introduction to software reverse engineering, with T. Cipresso (student), in *Handbook of Information and Communication Security*, Springer, March 2010.

64. QuickPay online payment protocol, with J. Dai (student), *Proceedings of SEKE '08*.

65. Profile hidden Markov models and metamorphic virus detection, with S. Attaluri (student) and S. McGhee (student), *Journal in Computer Virology*, 5(2):151–169, May 2009.

66. Digital rights management for streaming media, with D. Brahmbhatt (student), *Handbook of Research on Secure Multimedia Distribution*, IGI Global, March 2009, ISBN: 978-1-60566-262-6.

67. Digital rights management for untrusted peer-to-peer networks, with P. Priyadarshini (student), *Handbook of Research on Secure Multimedia Distribution*, IGI Global, March 2009, ISBN: 978-1-60566-262-6.

68. An agent-based privacy enhancing model, with H.-H. Lee (student), *Information Management & Computer Security*, 16(3):305–319, 2008.

69. P2PTunes: A peer-to-peer digital rights management system, with R. Venkataramu (student), *Handbook of Research on Secure Multimedia Distribution*, IGI Global, March 2009, ISBN: 978-1-60566-262-6.

70. SIGABA: Cryptanalysis of the full keyspace, with W. O. Chan (student), *Cryptologia*, 31(3):201–222, July 2007.

71. P3P privacy enhancing agent, with H.-H. Lee (student), *Proceedings of the 3rd ACM Workshop on Secure Web Services* (SWS'06), Alexandria, Virginia, November 3, 2006, pp. 109–110.

72. Hunting for metamorphic engines, with W. Wong (student), *Journal in Computer Virology*, 2(3):211–229, December 2006.

73. *Applied Cryptanalysis: Breaking Ciphers in the Real World*, with R. M. Low, Wiley-IEEE Press,

April 2007, ISBN: 978-0-470-11486-5.

74. King and rook vs. king on a quarter-infinite board, with R. M. Low, *Integers: The Electronic Journal of Combinatorial Number Theory*, 6:Article G3, 2006.

75. Information theory, with D. Blockus, invited book chapter, *The Handbook of Computer Networks*, H. Bidgoli, editor, John Wiley & Sons, Inc., November 2007, ISBN: 978-0-471-64833-8.

76. Role based access control and the JXTA peer-to-peer framework, with A. Mathur (student) and S. Kim, *Proceedings of 2006 International Conference on Security & Management* (SAM '06), Las Vegas, Nevada, June 26–29, 2006.

77. Metamorphic software for buffer overflow mitigation, with X. Gao (student), *Proceedings of 3rd Conference on Computer Science and its Applications*, P. P. Dey and M. N. Amin, editors, San Diego, California, June 28–30, 2005.

78. On using mouse movements as a biometric, with S. Hashia (student) and C. Pollett, *Proceedings of 3rd Conference on Computer Science and its Applications*, P. P. Dey and M. N. Amin, editors, San Diego, California, June 28–30, 2005.

79. Stealthy ciphertext, with M. Simova (student) and C. Pollett, *Proceedings of 3rd International Conference on Internet Computing* (ICOMP '05), Las Vegas, Nevada, June 27–30, 2005.

80. Unpredictable binary strings, with R. M. Low, R. Craigen, and G. Faucher, *Congressus Numerantium* 177, 2005, pp. 65–75, **MR2198651**.

81. *Information Security: Principles and Practice*, Wiley Interscience, September 2005, ISBN: 0-471-73848-4.

82. Software watermarking via assembly code transformations, with S. Thaker (student), *Proceedings of 2nd Conference on Computer Science and its Applications*, P. P. Dey, M. N. Amin, and T. M. Gatton, editors, San Diego, California, June 2004, pp. 205–209.

83. Hamptonese and hidden Markov models, with E. Le (student), Lecture Notes in Control and Information Sciences, Vol. 321, *New Directions and Applications in Control Theory*, Springer 2005, W. P. Dayawansa, A. Lindquist, and Y. Zhou, editors, pp. 367–378.

84. Enterprise digital rights management: Ready for primetime?, with E. J. Sebes, *Business Communications Review*, March 2004, pp. 52–55.

85. Risks of monoculture, Inside Risks 165, *Communications of the ACM*, 47(3):120, March 2004.

86. Multilevel security models, with A. Hushyar (student), invited chapter, *The Handbook of Information Security*, H. Bidgoli, editor, John Wiley & Sons, Inc., January 2006, ISBN: 0-471-64833-7.

87. A characterization of a class of discrete nonlinear feedback systems, with D. I. Wallace, and C. F. Martin, *Communications in Information and Systems*, 5(3):305–310, 2005.

88. Solvable problems in enterprise digital rights management, with E. J. Sebes, *Information Management & Computer Security*, 15(1):33–45, 2007.

89. Secure streaming media and digital rights management, with D. Holankar (student), *Proceedings of the 2004 Hawaii International Conference on Computer Science*, Honolulu, Hawaii, January 2004, pp. 85–97.

90. Digital rights management: For better or for worse?, *ExtremeTech*, May 20, 2003. Also appeared on *eWEEK*, May 1, 2003.

91. The MediaSnap® digital rights management system, with P. Sabadra (student), *Proceedings of Conference on Computer Science and its Applications*, P. P. Dey, M. N. Amin, and T. M. Gatton, editors, San Diego, California, July 2003.

92. Software uniqueness: How and why, with P. Mishra (student), *Proceedings of Conference on Computer Science and its Applications*, P. P. Dey, M. N. Amin, and T. M. Gatton, editors, San Diego, California, July 2003.

93. Pokémon® cards and the shortest common superstring, with A. E Stamp, *Graph Theory Notes of New York*, XLVII:19–24, 2004, **MR2134214**.

94. Risks of digital rights management, Inside Risks 147, *Communications of the ACM*, 45(9):120, September 2002.

95. Digital rights management: The technology behind the hype, *Journal of Electronic Commerce Research*, 4(3):102–112, 2003.

96. NSA paper, A stroll through WOK THROUGH, status unknown.

97. Rush Hour® and Dijkstra's algorithm, with B. Engel (student), M. Ewell (student), and V. Morrow (student), *Graph Theory Notes of New York* XL:23–30, 2001, **MR1823243**. Expanded tables of results.

98. NSA paper, Let me count the ways..., status unknown.

99. NSA paper, Hitchhiker's guide to dynamic programming, status unknown.

100. NSA paper, STA PUF is no marshmallow, status unknown.

101. Random walks on wheels, with M. Lee (student), *Graph Theory Notes of New York* XXXIII, 1997, pp. 24–25.

102. NSA paper R51/TECH/038/93, S-243,676, November 1996: Title and subject classified.

103. NSA paper Z52 TSR-007-95, August 1995: Title and subject classified.

104. NSA paper Z21 TSR-21-94, December 1994: Title and subject classified.

105. NSA paper Z52 ITN-004-94, February 1994: Title and subject classified.

106. A model for the optimal control of a measles epidemic, with C. F. Martin, L. Allen, M. Jones, and R. Carpio, *Computation and Control III: Proceedings of the Third Bozeman Conference*, Progress in Systems and Control Theory, Vol. 15, K. Bowers and J. Lund, editors, Boston: Birkhäuser, 1993, **MR1247482**.

107. Urn model simulations of a sexually transmitted disease epidemic, with C. F. Martin, and L. J. S. Allen, *Applied Mathematics and Computation*, 71:179–199, 1995.

108. Pseudo-random sequences in secret key cryptography, with C. F. Martin, *Proceedings of the 1992 International Computer Symposium*, Vol. 1, Feng Chia University, Taichung, Taiwan, 1992, pp. 166–173.

109. Stochastic analysis of vaccination strategies, with L. Allen, T. Lewis, C. Martin, R. Carpio, M. Jones, G. Mundel, and A. Way, *Stochastic Theory and Adaptive Control*, Proceedings of a workshop held in Lawrence, Kansas, September 26–28, 1991, Lecture Notes in Control and Information Sciences 184, T. E. Duncan and B. Pasik-Duncan, editors, Springer-Verlag, 1992, pp. 1–11.

110. An analysis of the transmission of *Chlamydia* in a closed population, with C. F. Martin and L. J. S. Allen, *Journal of Difference Equations and Applications*, 2(1):1–29, 1996, **MR1375593**.

111. An algorithm for the k-error linear complexity of binary sequences with period 2^n, with C. F. Martin, *IEEE Transactions on Information Theory*, 39(4):1398–1401, July 1993,

MR1267161.

112. Gaussian quadrature and linear systems, with C. F. Martin, *Computation and Control II: Proceedings of the Second Bozeman Conference*, Progress in Systems and Control Theory, Vol. 11, K. Bowers and J. Lund, editors, Boston: Birkhäuser, 1991, pp. 263–277, **MR1140027**.

113. Analysis of a measles epidemic, with L. J. S. Allen, T. Lewis, C. F. Martin, G. Mundel, A. B. Way, C. K. Lo, and M. A. Jones, *Statistics in Medicine*, 12:229–239, 1993.

114. A note on the error in Gaussian quadrature, with C. F. Martin, *Applied Mathematics and Computation*, 47:25–35, 1992, **MR1137059**.

115. A generalized linear complexity, Ph.D. dissertation, Department of Mathematics, Texas Tech University, May 1992.

116. Analysis of infinite dimensional dynamic systems with nonlinear observation over a finite field, with C. F. Martin, *Modeling, Estimation and Control of Systems with Uncertainty*, Progress in Systems and Control Theory, Vol. 10, G. B. DiMasi, A. Gombani, and A. B. Kurzhansky, editors, Boston: Birkhäuser, 1991, pp. 301–323, **MR1133379**.

117. Discrete observability and numerical quadrature, with C. F. Martin and X. Wang, *IEEE Transacations on Automatic Control*, 36(11):1337–1340, November 1991, **MR1130511**.

118. Mathematical analyses and simulations of a measles epidemic, with L. Allen, T. Lewis, C. Martin, M. Jones, C. Lo, G. Mundel, and A. Way *Proceedings of the American Statistical Association Biometric Society-Eastern North American Region (ENAR) Spring Meeting*, March 24–27, 1991, Houston, Texas.

119. A mathematical analysis and simulation of a localized measles epidemic, with L. J. S. Allen, T. Lewis, and C. F. Martin, *Applied Mathematics and Computation*, 39:61–77, 1990.

120. Classification and realization of pseudo-random number generators, with C. F. Martin, *Systems and Control Letters*, 14:169–175, 1990, **MR1044323**.

121. Constructing polynomials over finite fields, with C. F. Martin, *Computation and Control: Proceedings of the Bozeman Conference*, Progress in Systems and Control Theory, Vol. 1, K. Bowers and J. Lund, editors, Boston: Birkhäuser, 1989, pp. 233–252, **MR1046854**.

122. Constructing polynomials over finite fields, Master's thesis, Department of Mathematics, Texas Tech University, December 1988.

Cryptanalysis Challenge Problems

1. Typex — Part 1 (known plaintext, recover key), with K. Chang and R. M. Low. Level II challenge at MysteryTwister C3: The Crypto Challenge Contest.

2. Typex — Part 2 (known plaintext, recover rotor wirings), with K. Chang and R. M. Low, submitted.

3. Substitution Cipher with Non-Prefix Codes (ciphertext only), with R. Muralidhar. Level III challenge at MysteryTwister C3: The Crypto Challenge Contest.

4. Zodiac Cipher (homophonic substitution). Level I challenge at MysteryTwister C3: The Crypto Challenge Contest.

5. CMEA 1 (known plaintext). Level II challenge at MysteryTwister C3: The Crypto Challenge Contest.

6. CMEA 2 (known plaintext with limited data). Level III challenge at MysteryTwister C3: The Crypto Challenge Contest.

7. Akelarre Part 1 (known plaintext). Level II challenge at MysteryTwister C3: The Crypto Challenge Contest.

8. Purple 1 (ciphertext only). Level II challenge at MysteryTwister C3: The Crypto Challenge Contest.

9. ORYX Stream Cipher Part I (known keystream). Level II challenge at MysteryTwister C3: The Crypto Challenge Contest.

10. ORYX Stream Cipher Part II (known keystream with non-standard "L" table). Level II challenge at MysteryTwister C3: The Crypto Challenge Contest.

11. ORYX Stream Cipher Part III (known keystream with unknown "L" table), submitted.

12. Enigma Part 1 (ciphertext only, determine rotor settings). Level II challenge at MysteryTwister C3: The Crypto Challenge Contest.

13. Enigma Part 2 (ciphertext only, determine stecker). Level II challenge at MysteryTwister C3:

The Crypto Challenge Contest.

14. Sigaba Part 1 (known plaintext, restricted keyspace). Level II challenge at MysteryTwister C3: The Crypto Challenge Contest.

15. Sigaba Part 2 (known plaintext). Level III challenge at MysteryTwister C3: The Crypto Challenge Contest.

Unpublished Writings

1. Efficient cryptanalysis of homophonic substitution ciphers, 2011.

2. A revealing introduction to hidden Markov models, 2004.

3. Once upon a time-memory tradeoff, 2003.

4. Pokémon® trading card sequences, with A. E Stamp, 2002.

Students

- **Master's**

    1. S. Basole, Big data analysis of generic malware models, in progress.

    2. P. Sundaravaradhan, An attack on smartphone gesture based authentication, in progress.

    3. A. Sinha, Emulation vs instrumentation for Android malware detection, in progress.

    4. T. Sharmin, Improved image spam scores, in progress.

    5. S. Suresh, Machine learning for adware detection, in progress.

    6. A. Raghavan, Hidden Markov models: Boosting versus random restarts, in progress.

    7. A. S. Shekhawat, Malicious SSL traffic detection, in progress.

8. W. C. Huang, Robust hashing for malware detection, in progress.
9. I. Shinde, Malware detection based on image analysis techniques, in progress.
10. D. Dhanasekar, Detecting encrypted malware using hidden Markov models, Fall 2017.
11. N. Bagga, Measuring the effectiveness of generic malware models, Fall 2017.
12. S. Kim, PE headers for malware classification, in progress.
13. V. R. S. Selvin, Malware scores from image-based features, Spring 2017.
14. S. N. K. Manikoth, Masquerade detection in mobile devices, Spring 2017.
15. R. Gonsalves, Stealthy ciphertext generation, in progress.
16. P. Nagarajan, Analysis of periodicity in botnets, Spring 2017.
17. G. Nellaivadivelu, Black box analysis of Android malware detectors, Spring 2017.
18. A. Chavda, Image spam detection, Spring 2017.
19. A. Boursalian, Bootbandit: A macOS bootloader attack, Fall 2017.
20. G. Zhong, Cryptanalysis of homophonic substitution ciphers using hidden Markov models, Fall 2016.
21. A. Kapratwar, Static and dynamic analysis for Android malware detection, Spring 2016.
22. S. Deshmukh Vigenère scores for malware detection, Spring 2016.
23. S. Sridharan, Defeating *n*-gram scores for HTTP attack detection, Spring 2016.
24. A. Annadatha, Image spam analysis, Spring 2016.
25. B. Gurnani, Malware detection using the index of coincidence, Fall 2016.
26. S. Thakur, A completely covert audio channel in Android, Fall 2015.
27. D. Rajeswaran, Function call graph score for malware detection, Fall 2015.

28. P. Ponnambalam, Measuring malware evolution, Fall 2015.

29. S. Srinivasan, SSCT score for malware detection, Fall 2015.

30. R. Vobbilisetty, Cryptanalysis of classic ciphers using hidden Markov models, Spring 2015.

31. S. Vemparala, Malware detection using dynamic analysis, Spring 2015.

32. T. Singh, Support vector machines and metamorphic malware detection, Spring 2015.

33. G. Kasliwal, Cheating detection in online examinations, Spring 2015.

34. N. Ganesh, Static analysis of malicious Java applets, Spring 2015.

35. U. Narra, Clustering versus SVM for malware detection, Spring 2015.

36. A. Damodaran, Combining dynamic and static analysis for malware detection, Spring 2015.

37. I. Kaur, SocioBot: Twitter for command and control of a botnet, Spring 2015.

38. S. Pai, A comparison of \ clustering techniques for malware analysis, Spring 2015.

39. M. Crawford, Metamorphic code generation using LLVM, Fall 2017.

40. N. Brandt, Automating NFC message sending for good and evil, Spring 2014.

41. H. Rana, Hunting for pirated software using metamorphic analysis, Spring 2014.

42. J. Yi, Cryptanalysis of a homophonic substitution-transposition cipher, Spring 2014.

43. M. Musale, Hunting for metamorphic JavaScript malware, Spring 2014.

44. R. Jidigam, Metamorphic detection using Singular Value Decomposition, Fall 2013.

45. C. Annachhatre, Hidden Markov models for malware classification, Fall 2013.

46. P. Deshpande, Functional call graph analysis for metamorphic detection, Fall 2013.

47. G. R. Viswanathan, Analysis of Kullback-Leibler divergence for masquerade detection, Spring 2013.

48. A. Oza, HTTP attack detection using *N*-gram analysis, Spring 2013.

49. T. Tamboli, Metamorphic code generation from LLVM IR bytecode, Spring 2013.

50. Y. Liu, Analysis of parallel Montgomery multiplication in CUDA, Spring 2013.

51. G. Shanmugam, Simple substitution distance and metamorphic detection, Fall 2012.

52. D. Baysa, Structural entropy and metamorphic malware, Fall 2012.

53. A. Agrawal, User profiling in GUI based windows systems for intrusion detection, Spring 2013.

54. A. Mahajan, Masquerade detection based on UNIX commands, Fall 2012.

55. S. Deshpande, Eigenvalue analysis for metamorphic detection, Fall 2012.

56. J. Patil, Secure media streaming for Android, Fall 2012.

57. A. Kothari, Defeating masquerade detection, Spring 2012.

58. C. Wong, Analysis of DPA and DEMA attacks, Fall 2012.

59. S. Kazi, Hidden Markov models for software piracy detection, Spring 2012.

60. K. Chang, Cryptanalysis of Typex, Spring 2012.

61. S. M. Sridhara, Metamorphic worm that carries its own morphing engine, Spring 2012.

62. S. Kumar, Online monitoring using Kismet, Spring 2012.

63. P. K. Gone, Java design pattern obfuscation, Spring 2012.

64. M. Ai, CryptSim: Simulators for classic rotor ciphers, Spring 2012.

65. A. Dhavare, Efficient attacks on homophonic substitution ciphers, Fall 2011. A technical report based on this project can be found here.

66. N. Runwal, Graph technique for metamorphic virus detection, Fall 2011.

67. A. Singh, Social networks for botnet command and control, Spring 2012.

68. S. Anandan, Online application monitoring tool, Fall 2010.

69. A. H. Toderici, Chi-squared distance and metamorphic virus detection, Spring 2012.

70. M. Patel, Similarity tests for metamorphic virus detection, Spring 2011.

71. R. Muralidhar, Substitution cipher with non-prefix codes, Spring 2011.

72. S. Priyadarshi, Metamorphic detection via emulation, Spring 2011.

73. N. Buddhadev, User monitor and feedback mechanism for social scientific study on laptop energy reduction, Spring 2011.

74. M. Mungale, Robust watermarking using hidden Markov models, Spring 2011.

75. A. Patel, Decompiler for pseudo-code generation, Spring 2011.

76. N. Samant, Automated penetration testing, Spring 2011.

77. A. Sharma, Dynamic code checksum generator, Spring 2011.

78. A. Suvatne, Improved worm simulator and simulations, Fall 2010.

79. X. Zhang, ActiBot: A botnet to evade active detection, Fall 2011.

80. A. Shah, Approximate disassembly using dynamic programming, Fall 2010.

81. D. Mulani, How smart is your Android smartphone?, Spring 2010.

82. D. Kundu, JShield: A Java anti-reversing tool, Spring 2011.

83. F. Yang, Automatic execution path finding tool, Fall 2010.

84. L. Huang, A study on masquerade detection, Fall 2010.

85. J. Zhang, Improved software activation using multithreading, Spring 2010.

86. S. Venkatachalam, Detecting undetectable computer viruses, Spring 2010.

87. V. Luong, Intrusion detection and prevention system: SQL-injection attacks, Fall 2010.

88. R. Shah, Metatamorphic viruses with built-in buffer overflow, Spring 2010.

89. D. Radhakrishnan, Approximate disassembly, Spring 2010.

90. D. Lin, Hunting for undetectable metamorphic viruses, Spring 2010.

91. T. Aulakh, Intrusion detection and prevention system—CGI attacks, Fall 2009.

92. T. Cipresso, Software reverse engineering education, Spring 2009. See also online resources at Software Reverse Engineering (SRE).

93. S. Samptur, Scalable end-to-end available bandwidth inference based on node-centric clusters, Spring 2009.

94. E. Benjamin, UNDO: A system for neutralizing nuisance attacks, Spring 2010.

95. J. Krishnaswamy, Wormulator: Simulator for rapidly spreading malware, Fall 2009.

96. G. Gokhale, WiSeNetor: A scalable wireless sensor network simulator, Spring 2010.

97. S. Govindaraj, Practical detection of metamorphic computer viruses, Fall 2008.

98. A. Panicker, Botnets and distributed denial of service attacks, Fall 2008.

99. P. Desai, Towards an undetectable computer virus, Fall 2008.

100. P. Basavaraju, Heuristic-search cryptanalysis of the Zodiac 340 cipher, Fall 2009.

101. V. Pandya, iPhone security analysis, Spring 2008.

102. H. Kwong, Cryptanalysis of the Sigaba cipher, Fall 2008.

103. A. Venkatesan, Code obfuscation and virus detection, Spring 2008.

104. E. Patil, Analysis of rxbot, Spring 2009.

105. J. Morparia, Peer-to-peer botnets: Analysis and detection, Fall 2008.

106. T. Dao, Analysis of the Zodiac 340-cipher, Fall 2007.

107. Y. Zhang, Single sign-on web portal based on Kerberos, Spring 2008.

108. S. McGhee, Pairwise alignment of metamorphic computer viruses, Fall 2007.

109. S. Attaluri, Profile hidden Markov models for metamorphic virus analysis, Fall 2007.

110. R. Philip, Securing wireless networks from ARP cache poisoning, Spring 2007.

111. K. V. Nguyen, A hierarchical trusted third-party system for secure peer-to-peer transactions, Spring 2007.

112. R. Venkataramu, Analysis and enhancement of Apple's Fairplay digital rights management, Spring 2007.

113. W. O. Chan, Cryptanalysis of SIGABA, Spring 2007.

114. S. S. Kim, Geometry-based detection of flash worms, Fall 2006.

115. P. Priyadarshini, P2PRM: A peer-to-peer rights management system, Fall 2006.

116. H.-H. Lee, P3P privacy enhancing agent, Fall 2006.

117. C. S. Lee, Bluetooth security protocol analysis and improvements, Spring 2006.

118. W. Wong, Analysis and detection of metamorphic computer viruses, Spring 2006.

119. J. Dai, QuickPay: an online payment protocol, Spring 2006.

120. M. Simova, Stealthy ciphertext, Spring 2005.

121. A. Mathur, Incorporating RBAC into the JXTA peer-to-peer infrastructure, Spring 2005.

122. J. Yang, APTPFS: Anonymous peer-to-peer file sharing, Spring 2005.

123. X. Gao, Metamorphic software for buffer overflow mitigation, Spring 2005.

124. A. Hushyar, Network traffic clustering and visualization, Fall 2009.

125. N. D. Kashyap, A meaningful MD5 hash collision attack, Fall 2006.
126. T. T. Tsai, Hidden Markov model for text analysis, Fall 2004.
127. S. Thaker, Software watermarking via assembly code transformations, Spring 2004.
128. T. Tran, Document builder, Spring 2010.
129. S. Manwani, ARP cache poisoning detection and prevention, Fall 2003.
130. S. Parihar, Fraud tolerant distributed computing, Fall 2003.
131. D. Holankar, Streaming media security using digital rights management, Spring 2004.
132. K. Skachkov, Tamper-resistant software: design and implementation, Fall 2003.
133. P. Mishra, A taxonomy of software uniqueness transformations, Fall 2003.

- **Undergraduate**

1. S. Yajamanam, Deep learning for malware detection based on image features, Fall 2017.
2. T. Braginets, Cryptanalysis of the Zodiac 340 cipher, Spring 2012.
3. T. Y. D. Li, TwitterBot: A social media botnet, Spring 2011.
4. P. Towyenis, SRE exercises based on an online game, 2009–2010.
5. E. Bongso, A. Khera, F. Negandhi, and S. Quintero, Flash worm detection, 2007–2008.
6. T. Stehle, Analysis of viruses that carry their metamorphic engine, Spring 2007.
7. Y. Li, Anomaly based detection of flash worms, Fall 2005.
8. T. Dao, Purple cipher: Simulation and improved hill climb attack, Fall 2005.
9. T. Nikl, Flash worm simulation and detection, Spring 2005.
10. J. Olsen, Spyware detection for Mac OS X, Spring 2005.
11. E. Le, A linguistic analysis of Hamptonese, Spring 2005.

12. H. Ghorbani-Moghaddam, DNA sequence alignment, Fall 2003.

13. E. Le, A hidden Markov model analysis of Hamptonese, Summer 2003.

Other

- Citations according to Google Scholar and Researchgate.
- A discussion of Information security journals: The good, the bad, and the ugly.
- Cracking the Code of James Hampton's Private Language, by Casey N. Cep, discusses some of our work.
- Robert Slade's review of *Information Security: Principles and Practice* (first edition)
- Mark's biography on the SJSU website.