

# Alec Yasinsac, Ph. D.

Florida State University  
262 James Jay Love Building  
Tallahassee, Florida 32306-4530  
yasinsac@cs.fsu.edu  
850.644.6407 (voice)  
850.644.0058 (fax)

Citizenship: US

Highest Clearance Achieved: Top Secret (1999)

**Research.** The following paragraphs summarize research efforts in four areas with selected publication title and venues included. Other interest areas include computer forensics and intrusion detection. Complete bibliography entries are included in the publications section beginning on the second page.

**Wireless and Mobile Security.** Mobility brings many security challenges to distributed applications. This work focuses on cryptographic approaches suitable to resource constrained environments. We also introduce a new obfuscation paradigm called "Program Encryption".

"Limitations of Simulation for MANET Research", accepted to *IEEE Computer*

"Taxonomy for Defining Mobile Agent Security", accepted to *ACM Computing Surveys*

"Protocols for a Dynamic Key Exchange System for Ad Hoc Networks", *LNCS 3364*

"Weathering the Storm: Managing Redundancy and Security in Ad hoc Networks ", *LNCS 3158*

"Of Unicorns and Random Programs", *CCN 2005*

**Security Protocols.** The foundation of my research is security protocols. The primary emphases are formal verification and proper application of cryptography.

"Formal Analysis of Modern Security Protocols", *Information Sciences*

"An Environment for Security Protocol Intrusion Detection", *Journal of Computer Security*

**Privacy.** Fundamental societal rights, such as that of ownership, depend on our ability to keep certain information confidential. Conversely, privacy and anonymity tools are often misused to cover criminal activity or circumvent deterrence. We investigate issues of using privacy responsibly.

"Security or Privacy, Must We Choose?" *Symposium on Critical Infrastructure Protection & the Law*

"Accountable Privacy", *Twelfth International Workshop on Security Protocols*

**Security Education.** With the introduction of many information security workforce development funding programs, fundamental technical and pedagogical issues are investigated and introduced.

"Centers of Academic Excellence: A Case Study", *IEEE Security and Privacy Magazine*

"Security-Aware Coding", 39th Annual Hawaii International Conference On System Sciences

"Computer Forensics Education", *IEEE Security and Privacy*

## Background, Degrees, and Credentials

- |                           |   |
|---------------------------|---|
| Academic degrees:         | <ul style="list-style-type: none"><li>▪ Doctor of Philosophy, Computer Science, University of Virginia, 1996</li><li>▪ Master of Science, Computer Science, Naval Postgraduate School, 1986</li><li>▪ Bachelor of Science, Mathematics, Appalachian State University, 1979</li></ul>  |
| Professional positions:   | <ul style="list-style-type: none"><li>▪ Associate Professor of Computer Science, FSU, August 2005 to the present</li><li>▪ Assistant Professor of Computer Science, FSU, August 1999 to July 2005</li><li>▪ Visiting Professor, Harris Corporation, Melbourne Florida, June 2002</li><li>▪ Assistant Professor of Naval Science, University of Virginia, Jul 90-Oct 93</li><li>▪ Officer, United States Marine Corps, May 1979- July 1999</li></ul> |
| Professional Memberships: | <ul style="list-style-type: none"><li>▪ Senior Member, IEEE</li><li>▪ Member, IEEE Computer Society and ACM</li></ul>   |

## **Funding** (Total: \$4.2 million between May 2000- August 2005)

- Department of Defense, "Information Assurance Scholarship Program", 07/05, \$221,275, Co-PI
- Department of Defense, "Information Assurance Scholarship Program", 07/05, \$45,000, Co-PI
- Army Research Office, "Mobile Agent Security", 07/04-06/06, \$320,000, PI
- Department of Defense, "Information Assurance Scholarship Program", 07/04, \$172,000, Co-PI
- National Institute of Justice, "The Design and Development of the Predator and Prey Alert (PAPA) System", 07/04-06/05, \$280,998, Co-PI
- Army Research Office, "Workshop on Mobile Agent Security", 07/04, PI, \$11,000
- National Science Foundation, PI, "Collaborative Project: Expanding Information Assurance Education", 09/03-08/05, \$185,405, PI
- DoD, "Information Assurance Scholarships Program", 09/03-08/05, \$258,000, Co-PI
- Army Research Office, "Secure Tactical Mobile Intelligent Agents", 07/02-06/03, \$198,240

## **Publications**

### (a) Journal Articles

- (1) Todd R. Andel, Alec Yasinsac, "On the Credibility of Manet Simulations," *Computer*, vol. 39, no. 7, pp. 48-54, July 2006
- (2) Mike Burmester, Tri Le Van, and Alec Yasinsac, "Adaptive gossip protocols: Managing Redundancy and Security in Ad hoc Networks", *Journal of AdHoc Networks*, Elsevier, 4(3), pp. 504-515, 2006
- (3) Alec Yasinsac and Mike Burmester, "Centers of Academic Excellence: A Case Study", *IEEE Security and Privacy*, Volume 3, Issue 1, 2005, pp. 32-35
- (4) Alec Yasinsac and Justin Childs, "Formal Analysis of Modern Security Protocols", *Information Sciences*, (Elsevier), Volume 171/1-3, pp. 189-211, 2005
- (5) Tysen Leckie and Alec Yasinsac, "Metadata for Anomaly Based Security Protocol Attack Detection", *IEEE Transactions on Knowledge and Data Engineering*, Volume 16, Number 9, September 2004, pp. 1157-68
- (6) Mike Burmester and Alec Yasinsac, "Trust Infrastructures for Wireless, Mobile Networks", *WSEAS Transactions on Telecommunications*, Volume 3, #1, January 2004, pp. 377-81
- (7) Alec Yasinsac, Robert Earbacher, Donald G. Marks, Mark Pollitt, Peter M. Sommer, "Computer Forensics Education", *IEEE Security and Privacy*, July-Aug 2003, Vol. 1, No. 4, pp. 15-23
- (8) Alec Yasinsac, "An Environment for Security Protocol Intrusion Detection", *Journal of Computer Security*, Volume 10, Number 1-2, 2002, pp. 177-88
- (9) Alec Yasinsac, "Information Security Curricula in Computer Science Departments: Theory and Practice," *The George Washington University Journal of Information Security*, Volume 1, Number 2, 2002
- (10) Alec Yasinsac and Wm. A. Wulf, "A Framework for A Cryptographic Protocol Evaluation Workbench", *The International Journal of Reliability, Quality and Safety Engineering (IJRQSE)*, Volume 8, Number 4, December 01, 2001, pp 373-89

### (b) Symposium, Conference, and Workshop Publications

- (1) J. Todd McDonald and Alec Yasinsac, "Applications for Provably Secure Intent Protection with Bounded Input-Size Programs", accepted to The Second International Conference on Availability, Reliability and Security, April 10-13, 2007

- (2) J. Todd McDonald and Alec Yasinsac, "Program Intent Protection Using Circuit Encryption", 8th International Symposium on System and Information Security, Sao Jose dos Campos, Sao Paulo, Brazil, November 8-10, 2006
- (3) Alec Yasinsac and J. Todd McDonald, "Security-Aware Coding", *39th Annual Hawaii International Conference On System Sciences, Mini-track on Information Security Education and Foundational Research*, January 4-7, 2006
- (4) Alec Yasinsac, "Non-Boolean Authentication", 2nd International Semantic Web Policy Workshop, Athens, Georgia, USA, Nov 6-9, 2006
- (5) Todd Andel and Alec Yasinsac, "Wireless Protocol Security; to Simulate or not Simulate", Symposium on Simulation Software and Security, affiliated with the 2006 Spring Simulation Multi-conference (SpringSim06), Von Braun Center, Huntsville, Alabama, April 2-6, 2006
- (6) Tina Suen and Alec Yasinsac, "Peer Identification in Wireless Sensor Networks Using Signal Properties", *2005 IEEE Workshop on Wireless and Sensor Network Security*, November 7-10, 2005, Washington DC
- (7) Alec Yasinsac and J. Todd McDonald, "Of Unicorns and Random Programs", *The Third IASTED International Conference on Communications and Computer Networks*, (CCN 2005), October 24-26, 2005, Marina del Rey, California, USA
- (8) J. Todd McDonald and Alec Yasinsac, "Application Security Models for Mobile Agent Systems", *Proceedings of the 1st International Workshop on Security and Trust Management*, Electronic Notes in Theoretical Computer Science, September 15, 2005
- (9) Mike Burmester, Breno DeMederios, and Alec Yasinsac, "Community-centric vanilla-rollback access, or: How I stopped worrying and learned to love my computer", *13th International Workshop on Security Protocols*, April 20-22, 2005, to appear LNCS
- (10) Willard Thompson, Alec Yasinsac, and Todd McDonald, "Semantic Encryption Transformation Scheme", *Proceedings of the 2004 International Workshop on Security in Parallel and Distributed Systems*, San Francisco, CA, Sept. 15-17, 2004, pp. 516-21
- (11) Todd McDonald, Alec Yasinsac, and Willard Thompson, "Mobile Agent Data Integrity Using Multi-agent Architecture", *Proceedings of the 2004 International Workshop on Security in Parallel and Distributed Systems*, San Francisco, CA, September 15-17, 2004, pp. 536-42
- (12) Mike Burmester, Tri Le Van, and Alec Yasinsac, "Weathering the Storm: Managing Redundancy and Security in Ad hoc Networks ", *3rd International Conference on AD-HOC Networks & Wireless*, July 20-22, 2004, LNCS 3158, Springer, pp. 96-107
- (13) Prabha Ramachandran and Alec Yasinsac, " Limitations of On Demand Secure Routing Protocols", *IEEE Information Assurance Workshop 2004*, June 10-11, 2004, pp. 52-59
- (14) D. J. Scott and Alec Yasinsac, "Dynamic Probabilistic Rebroadcast in Ad hoc Networks", *Proceedings of the International Conference on Wireless Networks*, June 21-4, 2004, pp. 158-64
- (15) Mike Burmester and Alec Yasinsac, "Modeling Trust in Ad hoc Networks", *6th WSEAS International Conference on Telecommunications and Informatics*, May 12-15, 2004
- (16) Michael Burmester, Yvo Desmedt, Rebecca Wright, and Alec Yasinsac, "Accountable Privacy" *Twelfth International Workshop on Security Protocols*, April 26-28, 2004, pp. 22-33, LNCS
- (17) Yanet Manzano and Alec Yasinsac, "Honeytraps, a Valuable Tool To Provide Effective Countermeasures for Crime Against Computer and Network Systems", *Proceedings of the 7th World Multi-conference on Systemics, Cybernetics and Informatics (SCI)*, July 30, 2003
- (18) Alec Yasinsac, "Rate of Change in Ad Hoc Networks", *Proceedings of the Information Resources Management Association International Conference*, pp. 698-701, May 18-21, 2003, Philadelphia, PA

- (19) John Marshall, Vikram Thakur, and Alec Yasinsac, "Identifying Flaws in the Secure Routing Protocol", *Proceedings of The 22nd International Performance, Computing, and Communications Conference (IPCCC 2003)* April 9-11, 2003, pp. 167-174
- (20) Mike Burmester and Alec Yasinsac, "Protocols for a Dynamic Key Exchange System for Ad Hoc Networks", *Eleventh International Workshop on Security Protocols*, Cambridge, UK, Apr. 2-4, 2003, Springer, LNCS 3364, pp. 274-87
- (21) Stephen Carter and Alec Yasinsac, "Secure Position Aided Ad hoc Routing Protocol", *Proceedings of the IASTED International Conference on Communications and Computer Networks (CCN02)*, pp. 329-334, Nov. 4-6, 2002.
- (22) Alec Yasinsac, Vikram Thakur, Stephen Carter, and Ilkay Cubukcu, "A Family of Protocols for Group Key Generation in Ad Hoc Networks," *Proceedings of the IASTED International Conference on Communications and Computer Networks (CCN02)*, pp. 183-187, Nov.4-6, 2002
- (23) Michael Burmester, Yvo Desmedt, Rebecca Wright, and Alec Yasinsac, "Security or Privacy, Must We Choose?" *Symposium on Critical Infrastructure Protection and the Law*, Computer Science and Telecommunication Board, October, 2002
- (24) Alec Yasinsac and Yanet Manzano, "Honeytraps, A Network Forensic Tool", *Proceedings of the 6th World Multi-conference on Systemics, Cybernetics, and Informatics (SCI 02)*, July 15-19, 2002, pp. 600-05
- (25) Alec Yasinsac and James A. Davis, "Modeling Protocols for Secure Group Communication in AdHoc Networks", 10th International Workshop, Cambridge, UK, April 17-19, 2002, Revised Papers Series: LNCS 2845, Christianson, B.; Crispo, B.; Malcolm, J.A.; Roe, M. (Eds.), 2004, VIII, 243, pp. 189-202, ISBN: 3-540-20830-5
- (26) Ladislav Kohout, Alec Yasinsac, and Ernest McDuffie, "Activity Profiles for Intrusion Detection", *North American Fuzzy Information Processing Society-Fuzzy Logic and the Internet (NAFIPS-FLINT 2002)*, New Orleans, LA, pp. 463-468, June 27-29, 2002
- (27) Alec Yasinsac, Marion Bogdonav, and Jennifer Frazier, "Building An Information Security Laboratory", *6th IEEE National Colloquium for Information Systems Security Education, Government, Industry, and Academia*, June 4, 2002, 8 pages
- (28) Justin Childs and Alec Yasinsac, "Analyzing Internet Security Protocols", *The Sixth IEEE International Symposium on High Assurance Systems Engineering*, pp 149-59, Boca Raton, Florida, Oct 24-26, 2001
- (29) Yanet Manzano and Alec Yasinsac, "Policies to Enhance Computer and Network Forensics", *The 2nd Annual IEEE Systems, Man, and Cybernetics Information Assurance Workshop*, United States Military Academy, June 2001, pp. 289-95
- (30) Alec Yasinsac, "Detecting Intrusions in Security Protocols", *ACM Workshop on Intrusion Detection*, 7th ACM Conference on Computer and Communication Security, Nov 2000
- (31) Alec Yasinsac, "Dynamic Analysis of Security Protocols", *Proceedings of the New Security Paradigms 2000 Workshop*, Sept 18-21, Ballycotton, Ireland, pp. 77-87
- (32) Alec Yasinsac and Wm. A. Wulf, "A Framework for A Cryptographic Protocol Evaluation Workbench", *Proceedings of the Fourth IEEE International High Assurance Systems Engineering Symposium (HASE99)*, Washington D.C., November 1999, pp. 197-205
- (33) Alec Yasinsac and Wm. A. Wulf, "Evaluating Cryptographic Protocols", *4th Cambridge International Workshop on Cryptographic Protocols*, March 1996
- (34) Wm. A. Wulf, Alec Yasinsac, Katie S. Oliver, and Ramesh Peri, "A Technique for Remote Authentication ", *Proceedings of the Internet Society Symposium on Network and Distributed System Security*, February 2-4, 1994, San Diego, California, pp. 159-164.

(c) Book Chapters

- (1) M. Burmester and A. Yasinsac (Editors), MADNES 2005, LNCS 4074, Springer-Verlag Berlin Heidelberg, 2006
- (2) Alec Yasinsac, "Rate of Change in Ad Hoc Networks", in Commerce and M-Commerce Technologies, Chapter # 8, pp. 166-183 , edited by Dr. Candace Deans, July 2004, Idea Group Inc. Publishers, ISBN 1-59140-566-1

(d) Theses

- (1) Alec Yasinsac, "A Formal Semantics for Evaluating Cryptographic Protocols", Ph.D. Dissertation, University of Virginia, January 1996
- (2) Alec Yasinsac and Robert Hartman, "JANUS/ADA Implementation of a Star Cluster Network of Personal Computers with Interface to an Ethernet LAN Allowing Access to DDN Resources", Master's Thesis, Naval Postgraduate School, Monterey, California, June 1986

(e) Invited talks

- (1) "Security Aware Software", Tallahassee Technology Alliance, Tallahassee Florida, Sept 30, 2005, <http://www.taltech.org>
- (2) Keynote Address, "The Changing Face of Information Security", The Northwest Regional Data Center Conference 2003, Tallahassee, FL., October 9, 2003
- (3) "Wireless Network Security", Summer School on Information Security, SAIT Laboratory, Florida State University, May 23, 2003

## Teaching and Training

(a) Courses

- (1) Spring 2006, CIS 5370, Computer Security
- (2) Spring 2006, CEN 5035, Software Engineering
- (3) Fall 2005, CIS 4930, Wireless Security
- (4) Fall 2005, CIS 6935, Mobile Agent Security
- (5) Spring 2005, CEN 5035, Software Engineering
- (6) Fall 2004, CIS 6930, Secure Wireless Networks
- (7) Spring 2004, CIS 4362, Network Security and Cryptography
- (8) Fall 2003, CIS 5357, Network Security, Active and Passive Defense
- (9) Fall 2003, CIS 4930, Applied Security
- (10) Spring 2003, CEN 5452, Network Security, Active and Passive Defense
- (11) Spring 2003, CEN 4452, Network Security and Cryptography

(b) Dissertations Directed

- (1) Todd MacDonald (present)
- (2) Todd Andel (present)
- (3) Sarah Diesburg (present)

(c) Masters Committee Chair

- (1) D.J. Scott (present)
- (2) Ilkay Cubuku, May 2005, FSU CS Technical Report #050730
- (3) Khandys Polite, May 2004, FSU CS Technical Report #040502
- (4) Anna Suen, May 2003, FSU CS Technical Report #030402
- (5) Kristin Burke, May 2003, FSU CS Technical Report #030403
- (6) John Marshall, May 2003, FSU CS Technical Report #030502

- (7) Stephen Carter, December 2002, FSU CS Technical Report #021202
- (8) Tysen Leckie, December 2002, FSU CS Technical Report #021203
- (9) Jenny Frazier, April 2002, FSU CS Technical Report #020403
- (10) Shanmuga Ramaswamy, April 2002, FSU CS Technical Report #020602
- (11) Nikhil Patel, Graduated December 2001, FSU CS Technical Report #011203
- (12) Marion Bogdanov, December 2001, FSU CS Technical Report #011202
- (13) Edwin Melendez, July 2001, FSU CS Technical Report #010701
- (14) Sachin Goregoaker, July 2001, FSU CS Technical Report #010703
- (15) Mike Runy, May 2001, FSU CS Technical Report #010601
- (16) Justin Childs, July 2000, FSU CS Technical Report #000703

(d) Undergraduate Project Directorships.

- (1) Jon Nilson, Spring 2006
- (2) Tina Suen, Spring 2005
- (3) Don Scott, Fall 2003
- (4) Yanet Manzano, Spring 2001, FSU CS Technical Report #000902
- (5) Precious Jones, Spring 2001

**National and International Service Since 2004**

(a) Conference and Program Committees.

- (1) Program Committee, 2006 ACM Conference on Computer and Communication Security (CCS), Alexandria, VA, USA, October 30 - November 3, 2006.
- (2) Program Committee, International Conference on Security and Cryptography, Setubal, Portugal, August 7-10, 2006
- (3) Program Committee, Second Wireless Security and Privacy (WiSPr '06), Columbus, OH, from Aug. 14 to 18, 2006
- (4) Program Committee, The First International Conference on Availability, Reliability and Security (AREs), Vienna, AUSTRIA, April 20-22, 2006 (IEEE)
- (5) Program Committee, International Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing (SecPerU2006), Lyon, France, June 29, 2006
- (6) Program Committee, 7th Annual IEEE Information Assurance Workshop, United States Military Academy, West Point, NY, 21-23 June 2006
- (7) Program Committee, 1st International Conference on Information Systems Security (ICISS 2005), December, 2005
- (8) Program Committee, IASTED International Conference on Communication, Network and Information Security (CNIS 2005), November, 2005
- (9) Session Chair, Information Security, The Third IASTED International Conference on Communications and Computer Networks, (CCN 2005), October 24-26, 2005, Marina del Rey, CA, USA
- (10) Program Committee, *2005 Information Resources Management Association (IRMA) International Conference*, October 2005
- (11) Program Committee, European Symposium on Research in Computer Security (ESORICS-05), September 2005
- (12) Program Committee, *Eighth International Symposium on Recent Advances in Intrusion Detection (RAID 2005)*, September 7-9, 2005

- (13) Program Co-Chair, *Secure Mobile Ad-hoc Networks and Sensors*, proceedings in Springer-Verlag, September, 2005
  - (14) Program Committee, International Conference on Pervasive Systems and Computing (PSC-05), June 2005
  - (15) Program Committee, *6th IEEE Information Assurance Workshop (IAW 2005)*, 15-17 June 2005
  - (16) Program Committee, *2nd International Conference on E-Business and Telecommunication Networks*, (ICETE 2005), Oct. 3-7, 2005
  - (17) Program Committee, *IEEE GLOBECOM Workshop on Wireless Ad hoc and Sensor Networks*, Nov. 29- Dec 1, 2004
  - (18) Program Committee, *2005 Information Resources Management Association (IRMA) International Conference*, October 2005
  - (19) Program Committee, *International Workshop on Security in Parallel and Distributed Systems*, San Francisco, CA, September 15-17, 2004
  - (20) Program Committee, *Conference on E-business and Telecommunication Networks*, 24-25 August, 2004, Setubal, Portugal
  - (21) Program Committee, *International Workshop on VoIP Security* , 24-25 August, 2004, Setubal, Portugal
  - (22) Program Committee, *International Conference on E-business and Telecommunication Networks" (ICETE 2004)*, August 2004
  - (23) Program Committee, *1st. International Symposium on Risk Management and Cyber-Informatics (RMCI '04)*, Orlando, Florida, USA on July, 18-21, 2004
  - (24) Program Committee, *The 2004 International Conference on Wireless Networks (ICWN 2004)*, June 21-24, Las Vegas, Nevada
  - (25) Program Committee, *5th Annual IEEE Information Assurance Workshop (IAW 2004)*, 10-11 June, 2004, U.S. Military Academy, WestPoint, NY
  - (26) Co-Organizer, *FSU Summer School on Information Security*, May 3-7, 2004
  - (27) Program Committee, *The 23rd International Performance, Computing and Communications Conference*, April 14-17, 2004, Co-sponsored by the IEEE Computer Society
- (b) Boards and Councils
- (1) The Florida IT Executive Council (member), August 2005 - present
  - (2) Tallahassee Community College, Computer Programming Advisory Committee, November 2002-present