Erik M. Ferragut

Applied Research Mathematician
Cyber Security Research Scientist
Oak Ridge National Laboratory
http://erikferragut.me
ferragutem@ornl.gov

Research Interests

My research focus is in improving the security and dependability of network, computer, and cyber-physical systems through the development and application of data analytics and machine learning. My main areas of recent research are (1) anomaly detection for network intrusion defense and (2) resilience analysis for cyber-physical defense. I am also interested in other areas of security, such as analyzing network sensor data and measuring the advantage information provides in an adversarial setting.

Publications

Classified Papers

Authored 16 peer-reviewed classified papers in cryptology and related fields (1994–2005, 2007–2009). Received several Crypto-Mathematics Institute and KRYPTOS competitive paper awards.

Refereed Journal Papers

[1] Bogdan Denny Czejdo, **Ferragut, Erik M**, John R Goodall, and Jason Laska. Data warehouse for event streams violating rules. *Foundations of Computing and Decision Sciences*, 38(2):87–96, 2013.

[2] Bogdan Denny Czejdo, **Ferragut, Erik M**, John R Goodall, and Jason Laska. Network intrusion detection and visualization using aggregations in a cyber security data warehouse. *Int'l J. of Communications, Network and System Sciences*, 5(29):593–602, 2012.

Refereed Conference Papers

[1] Alexander M Melin, **Ferragut, Erik M**, Jason A Laska, David L Fugate, and Roger Kisner. A mathematical framework for the analysis of cyber-resilient control systems. In *6th International Symposium on Resilient Control Systems (ISRCS), 2013*, pages 13–18. IEEE, 2013.

[2] **Ferragut, Erik M**, Jason A Laska, Bogdan D Czejdo, and Alexander M Melin. Addressing the challenges of anomaly detection for cyber physical energy grid systems. In *Proceedings of the Eighth Annual Workshop on Cyber Security and Information Intelligence Research*, 2012.

[3] **Ferragut, Erik M**, Jason Laska, and Robert A Bridges. A new, principled approach to anomaly detection. In *11th International Conference on Machine Learning and Applications (ICMLA), 2012*, volume 2, pages 210–215. IEEE, 2012.

[4] **Ferragut, Erik M** and Jason Laska. Randomized sampling for large data applications of SVM. In *11th International Conference on Machine Learning and Applications (ICMLA), 2012*, volume 1, pages 350–355. IEEE, 2012.

[5] Lane Harrison, Jason Laska, Riley Spahn, Mike Iannacone, Evan Downing, **Ferragut, Erik M**, and John R Goodall. situ: Situational understanding and discovery for cyber attacks. In *IEEE Conference on Visual Analytics Science and Technology (VAST), 2012*, pages 307–308. IEEE, 2012.

[6] Bogdan Czejdo and **Ferragut, Erik M**. Time analysis for probabilistic workflows. In *International Conference on Future Communication and Computer Technology (ICFCCT)*, pages 62–66, 2012.

[7] Robert K Abercrombie, **Ferragut, Erik M**, and Shane Boone. Hidden markov modeling for weigh-in-motion estimation. In *6th International Conference on Weigh-In-Motion (ICWIM6)*, 2012.

[8] Robert K Abercrombie, **Ferragut, Erik M**, Frederick T Sheldon, and Michael R Grimaila. Addressing the need for independence in the CSE model. In *IEEE Symposium on Computational Intelligence in Cyber Security (CICS), 2011*, pages 68–75. IEEE, April 2011.

[9] **Ferragut, Erik M**, David M Darmon, Craig A Shue, and Stephen Kelley. Automatic construction of anomaly detectors from graphical models. In *IEEE Symposium on Computational Intelligence in Cyber Security (CICS), 2011*, pages 9–16. IEEE, April 2011.

[10] Anita N Zakrzewska and **Ferragut, Erik M**. Modeling cyber conflicts using an extended Petri net formalism. In *IEEE Symposium on Computational Intelligence in Cyber Security (CICS), 2011*, pages 60–67. IEEE, April 2011.

[11] **Ferragut, Erik M** and E Nicole Braden. System log summarization via semi-Markov models of inter-arrival times. In *Proceedings of the Seventh Annual Workshop on Cyber Security and Information Intelligence Research*, page 44. ACM, 2011.

[12] Craig A Shue and **Ferragut, Erik M**. Dead Phish: An examination of deactivated phishing sites. In *Collaboration, Electronic Messaging, Anti-Abuse an Spam Conference (CEAS)*, July 2010.

[13] **Ferragut, Erik M**. A dynamic erasure code for multicasting live data. In *Proceedings of the 5th Annual Workshop on Cyber Security and Information Intelligence Research*. ACM, April 2009.

Works in Progress

[1] Seddik M Djouadi, Alexander M Melin, **Ferragut, Erik M**, Jason A Laska, and Jin Dong. Finite energy and bounded attacks on control system sensor signals, 2013. Preprint.

[2] **Ferragut, Erik M**. Meta-Rarity: Operationally relevant anomaly detection, 2013. Preprint.

[3] **Ferragut, Erik M**, Jason A Laska, Seddik M Djouadi, and Alexander M Melin. Quantitative cyber-physical resilience: Metric and algorithm, 2013. Preprint.

[4] **Ferragut, Erik M** and Jason A Laska. Nonparametric Bayesian modeling for automated database schema matching, 2013. Preprint.

Presentations

[1] **Ferragut, Erik M**. Probabilistic schema matching. The Center for Intelligent Systems and Machine Learning (CISML), University of Tennessee, Knoxville *(Scheduled)*, January 31, 2014.

[2] **Ferragut, Erik M**. Graph-based analysis of cyber-physical system resiliency. American Mathematical Society Southeastern Sectional Meeting (AMS-SE), Louisville, Kentucky, October 4, 2013.

[3] **Ferragut, Erik M**. A principled approach to anomaly detection. The Center for Intelligent Systems and Machine Learning (CISML), University of Tennessee, Knoxville, November 14, 2012.

Patents

[1] **Ferragut, Erik M**, John R Goodall, Michael D Iannacone, Jason A Laska, and Lane T Harrison. Real-time detection and classification of anomolous events in streaming data, October 14 2013. US Patent Pending.

[2] **Ferragut, Erik M**, Jason A Laska, and Robert A Bridges. Model independent probability distribution based anomaly detection method, 2013. ORNL Invention Disclosure ID 3010.0.

[3] Robert K Abercrombie, Frederick T Sheldon, and **Ferragut, Erik M**. Cyberspace security system, September 13 2012. US Patent 20,120,232,679.

[4] Robert K Abercrombie, **Ferragut, Erik M**, and Lee M Hively. Weight and piece-wise analysis for weigh-in-motion, May 3 2012. US Patent Pending.

[5] Robert K Abercrombie and **Ferragut, Erik M**. Weigh-in-motion estimation via probabilistic hidden variable modeling, May 2 2012. US Patent Pending.

Education

December 2003	Ph.D. in Mathematics University of Michigan, Ann Arbor Dissertation: "*Detection of Epistatic Effects in Genetic Data*" Advisor: Phil Hanlon
August 1999	M.S. in Mathematics University of Michigan, Ann Arbor
May 1997	B.S. in Mathematics, *Summa Cum Laude* Highest honors in Mathematics, Physics, and Philosophy Ursinus College, Collegeville, PA

Research Experience

6/2009 – Present

Cyber Security Research Scientist
Oak Ridge National Laboratory
Oak Ridge, Tennessee

Research scientist and principal investigator for cyber security, anomaly and intrusion detection, situation awareness, probabilistic modeling, and machine learning. Key contributor to research in visual analytics, adversarial control theory, quantum computing, compressive sensing, and formal methods. Leading research/operations integration for the deployment of research-developed tools in ORNL's cyber infrastructure.

8/2007 – 6/2009

Applied Research Mathematician
Institute for Defense Analyses
Princeton, New Jersey

Applied multiple areas of mathematics (group theory, representation theory, coding theory, combinatorial commutative algebra, probability theory, combinatorics, and topology) to research problems for national security.

8/2006 – 8/2007 *Cyber Security Research Scientist*
Oak Ridge National Laboratory
Oak Ridge, Tennessee

Research staff contributing to distributed anomaly detection algorithms for cyber security. Supported projects in weigh-in-motion and communications.

10/2005 – 8/2006 *Applied Research Mathematician*
Johns Hopkins University, Applied Physics Laboratory
Laurel, Maryland

Improved methods for systematizing and validating large-scale risk assessments. Co-discovered and reported a cyber vulnerability on a high-value system together with an effective exploit.

8/1993 – 10/2005 *Applied Research Mathematician*
National Security Agency
Fort George G. Meade, Maryland

Participant of Stokes Fellowship Co-operative program (1993–1997), Director's Summer Program (1995), and Applied Mathematics Program (1997–2002). Research staff member in Cryptographic Research. Applied multiple areas of mathematics (group theory, representation theory, combinatorial commutative algebra, probability theory, combinatorics, and topology) to research problems for national security.

9/1997 – 12/1999 *Graduate Research Assistant*
University of Michigan
Ann Arbor, Michigan

Instructor for two sessions of pre-calculus.

Mentoring

- John P. Collins, Post-Masters Researcher, 2013–2014.
- Robert Bridges, Post-Doctoral Researcher, 2012–2013.
- Riley Spahn, Post-Baccalaureate Researcher, Fall 2012 to Spring 2013, and Auburn University Undergraduate Student, Summer 2011
- Jason Laska, Intelligence Community Post-Doctoral Researcher, 2011–2012.
- E. Nicole Braden, University of the Cumberlands Undergraduate Student, Summer 2011.
- Scott Mancuso, Brigham Young University Undergraduate Student, Summer 2011.
- Stephen Kelley, Intelligence Community Post-Doctoral Researcher, Summer 2010 to Spring 2012.
- Alicia Marino, Quinnipiac University Undergraduate Student, Spring 2011.
- David Darmon, Ursinus College Undergraduate Student, Summer 2010.
- Anita Zakrzewska, Brandeis University Undergraduate Student, Summer 2010.
- Aimee Cothran, High School Mathematics Teacher in the Greater Memphis Area, Summer 2010.

Teaching Experience

Spring 2011 – Fall 2012 *Online Adjunct Instructor (4 Classes Taught)*
University of Maryland University College
Adelphi, Maryland

Instructor (online) for core courses leading to a Master's Degree in Cybersecurity. CSEC 610 Cyberspace and Cybersecurity (2 sessions). CSEC 630 Prevention and Protection Strategies in Cybersecurity (2 sessions).

Spring 1998 – Fall 1999 *Graduate Teaching Assistant*
University of Michigan
Ann Arbor, Michigan

Instructor for precalculus mathematics course (2 sessions).

PI Experience and Funds Awarded

- Oak Ridge National Laboratory, PI for Laboratory Directed Research and Development **$790K** research project "Situation Awareness in Complex Networks". October 2013 to September 2015.
- Center for Medicare and Medicaid Services (CMS), Affordable Care Act data solutions task. On the basis of success of a schema matching tool, PI for **$1M** automated data quality assessment task. October 2013 to September 2014.
- Intelligence Community Post-Doctoral Research Program, PI (Mentor) for **$240K** research project "Deception Detection". October 2011 to September 2010.
- Johnson C. Smith University (HBCU), PI for a **$60K** Cyber Security Curriculum Development and Training. October 2010 to September 2011.

Awards and Fellowships

- Supplemental Employee Performance Merit Award, Oak Ridge National Laboratory, October 2013.
- Crypto-Mathematics Institute (NSA's oldest learned society), Theoretical Category Honorable Mention, Paper Award, 2009
- KRYPTOS (NSA cryptanalysis society), Best Paper Award, 2003
- Crypto-Mathematics Institute, Theoretical Category Best Paper Award, 2003
- Crypto-Mathematics Institute, Theoretical Category Honorable Mention Paper Award, 2003
- The University of Michigan, Rackham Merit Fellowship, Rackham School of Graduate Studies, 1997
- National Science Foundation Minority Graduate Fellowship, Mathematics, 1997

Professional Membership and Service

Memberships

- Member, American Mathematical Society (AMS)
- Member, Society for Industrial and Applied Mathematics (SIAM)
- Member, Latinos in Science and Engineering (MAES)

Service

- Organizer, Machine Learning Challenges in Cyber Security Applications, Special Session for the International Conference on Machine Learning Applications (ICMLA) 2013
- Reviewer for Cyber Security and Information Intelligence Research Workshop (CSIIRW) 2010–2012, IEEE Networks Magazine 2012, ACM Transactions on Modeling and Computer Simulation Journal (ACM TOMACS) 2010, Hawaii International Conference on System Sciences (HICSS) 2010

Skills and Clearances

- Fluent in English and Spanish
- Programming preferences: Python, C/C++, Matlab/Octave, Sage
- Citizenship: USA
- Clearances: Q and TS//SI