Roberto Perdisci

CONTACT INFORMATION

Georgia Institute of Technology
College of Computing
KACB, Room 3111
266 Ferst Drive, Atlanta, GA 30332, USA

Phone: 1-404-824-7476
E-mail: perdisci@gtisc.gatech.edu
Web: http://roberto.perdisci.com

RESEARCH INTERESTS

My current research focuses on network security, with an emphasis on *botnet* detection. I am broadly interested in all aspects of computer and network security, networked systems, and machine learning techniques for efficient mining and modeling of massive sets of network and system information.

EDUCATION

GEORGIA INSTITUTE OF TECHNOLOGY, Atlanta, GA, USA

Post-Doctoral Fellow (Aug. 2009 - *Present*)
Advisor: Prof. Wenke Lee

Research Scholar at *Georgia Tech Information Security Center* (Jul. 2005 - Feb. 2007)
Advisor: Prof. Wenke Lee

UNIVERSITY OF CAGLIARI, ITALY

PhD in Computer Engineering (Mar. 2007)
Thesis: Pattern Recognition Techniques for Intrusion Detection in Computer Networks, Challenges and Solutions.
Highest Ranked PhD Thesis in Computer Engineering, 2007
Grade: *Excellent*
Thesis work mostly prepared during visiting period at *Georgia Tech Information Security Center*, from Jul. 2005 to Feb. 2007.
Advisors: Prof. Giorgio Giacinto, Prof. Wenke Lee, and Prof. Fabio Roli

M.Sc. in Electronic Engineering (Dec. 2003)
Thesis: Alarm Clustering for Intrusion Detection Systems in Computer Networks
Grade: 110/110 *Summa cum Laude*
Advisor: Prof. Giorgio Giacinto

REFEREED JOURNALS AND CONFERENCE PUBLICATIONS

1. **Roberto Perdisci**, Wenke Lee, Nick Feamster. Behavioral Clustering of HTTP-based Malware and Signature Generation using Malicious Network Traces. *USENIX Symposium on Networked Systems Design and Implementation* (NSDI) 2010. (to appear)
2. **Roberto Perdisci**, Igino Corona, David Dagon, Wenke Lee. Detecting Malicious Flux Service Networks through Passive Analysis of Recursive DNS Traces. In *Annual Computer Security Applications Conference* (ACSAC) 2009. (acceptance rate 19.6%)
3. **Roberto Perdisci**, Manos Antonakakis, Xiapu Luo, Wenke Lee. WSEC DNS: Protecting Recursive DNS Resolvers from Poisoning Attacks. In *IEEE/IFIP International Conference on Dependable Systems and Networks* (DSN-DCCS) 2009. (acceptance rate 21%)
4. **Roberto Perdisci**, Davide Ariu, Prahlad Fogla, Giorgio Giacinto, and Wenke Lee. McPAD : A Multiple-Classifier System for Accurate Payload-based Anomaly Detection. In *Computer Networks Journal*, 5(6), 2009, pp. 864—881, Elsevier.

5. **Roberto Perdisci**, Andrea Lanzi, Wenke Lee. McBoost: Boosting Scalability in Malware Collection and Analysis using Statistical Classification of Executables. In *Annual Computer Security Applications Conference* (ACSAC) 2008. (acceptance rate 24.3%)
6. Guofei Gu, **Roberto Perdisci**, Junjie Zhang, Wenke Lee. BotMiner: Clustering Analysis of Network Traffic for Protocol- and Structure-Independent Botnet Detection. In *USENIX Security Symposium* 2008. (acceptance rate 15.9%)
7. **Roberto Perdisci**, Andrea Lanzi, Wenke Lee. Classification of Packed Executables for Accurate Computer Virus Detection. In *Pattern Recognition Letters Journal*, 29(14), 2008, pp. 1941—1946, Elsevier.
8. Giorgio Giacinto, **Roberto Perdisci**, Mauro Del Rio, Fabio Roli. Intrusion Detection in Computer Networks by a Modular Ensemble of One-Class Classifiers. In *Journal of Information Fusion*, 9(1), 2008, pp. 69—82, Elsevier.
9. Davide Ariu, Giorgio Giacinto, **Roberto Perdisci**. Sensing Attacks in Computers Networks with Hidden Markov Models. In *International Conference on Machine Learning and Data Mining in Pattern recognition* (MLDM) 2007.
10. **Roberto Perdisci**, Guofei Gu, Wenke Lee. Using an Ensemble of One-Class SVM Classifiers to Harden Payload-based Anomaly Detection Systems. In *IEEE International Conference on Data Mining* (ICDM) 2006. (regular papers acceptance rate 9.4%)
11. Prahlad Fogla, Monirul Sharif, **Roberto Perdisci**, Oleg Kolesnikov, Wenke Lee. Polymorphic Blending Attacks. In *USENIX Security Symposium* 2006. (acceptance rate 12.3%)
12. **Roberto Perdisci**, David Dagon, Wenke Lee, Prahlad Fogla, Monirul Sharif. Misleading Worm Signature Generators Using Deliberate Noise Injection. In *IEEE Symposium on Security and Privacy* 2006. (regular papers acceptance rate 9.2%)
13. **Roberto Perdisci**, Giorgio Giacinto, Fabio Roli. Alarm Clustering for Intrusion Detection Systems in Computer Networks. In *Engineering Applications of Artificial Intelligence Journal*, 19(4), 2006, pp. 429—438, Elsevier.
14. Giorgio Giacinto, **Roberto Perdisci**, Fabio Roli. Network Intrusion Detection by Combining One-class Classifiers. In *International Conference on Image Analysis and Processing* (ICIAP) 2005, *Special Session on Intrusion Detection.*
15. Giorgio Giacinto, **Roberto Perdisci**, and Fabio Roli. Alarm Clustering for Intrusion Detection Systems in Computer Networks. In *International Conference on Machine Learning and Data Mining in Pattern recognition* (MLDM) 2005.

WORK IN PROGRESS

1. Xiapu Luo, Junjie Zhang, **Roberto Perdisci**, Wenke Lee. Countering Time-based Traffic Watermarking. *In submission*.
2. Junjie Zhang, Xiapy Luo, **Roberto Perdisci**, Guofei Gu, Wenke Lee. Boosting the Scalability of Botnet Detection using Adaptive Traffic Sampling. *Under Review*.

WORKSHOPS AND TECH REPORTS

1. **Roberto Perdisci**, Guofei Gu, Wenke Lee. Combining Multiple One-Class Classifiers for Hardening Payload-based Anomaly Detection Systems. In Neural Information Processing Systems (NIPS) 2007, Workshop on Machine Learning in Adversarial Environments for Computer Security.
2. Davide Ariu, Igino Corona, Giorgio Giacinto, **Roberto Perdisci**, Fabio Roli,

Intrusion Detection Systems based on Anomaly Detection Techniques. In Italian Workshop on Privacy and Security (PRISE), 2007.

PATENTS

1. **Roberto Perdisci**, Wenke Lee. Method and System for Detecting Malicious and/or Botnet-Related Domain Names. (Patent Pending)

TALKS

- *Detecting Malicious Flux Service Networks through Passive Analysis of Recursive DNS Traces.*
  Annual Computer Security Applications Conference, Honolulu, Hawaii, Dec. 2009.
- *WSEC DNS: Protecting Recursive DNS Resolvers from Poisoning Attacks.*
  IEEE International Conference on Dependable Systems and Networks, Estoril, Portugal, June 2009.
- *McBoost: Boosting Scalability in Malware Collection and Analysis using Statistical Classification of Executables.*
  Annual Computer Security Applications Conference, Anhaim, CA, Dec. 2008.
- *Using an Ensemble of One-Class SVM Classifiers to Harden Payload-based Anomaly Detection Systems*.
  IEEE International Conference on Data Mining, ICDM 2006, Hong Kong, Dec. 2006.
- *Misleading Worm Signature Generators Using Deliberate Noise Injection.*
  IEEE Symposium on Security and Privacy 2006. Oakland, CA, USA, May 2006.
- *The Role of Machine Learning in Network Intrusion Detection.* (Invited Talk)
  Georgia Institute of Technology, College of Computing, Computational Science and Engineering division. Atlanta, GA, USA , October 6, 2006.

PROFESSIONAL ACTIVITIES

Reviewer for Journal Publications

- Pattern Recognition – Elsevier
- ACM Transactions on Information and System Security
- Information Fusion – Elsevier
- IEEE Transactions on Dependable and Secure Computing
- IEEE Transactions on Computers
- ACM Transactions on Knowledge Discovery in Data

External Reviewer for Conferences

- IEEE Symposium on Security & Privacy (2007, 2008, 2009)
- USENIX Security Symposium (2007, 2009)
- ACM Conference on Computer and Communications Security (2007, 2009)
- Network & Distributed System Security Symposium (2008, 2009)
- Annual Computer Security Applications Conference (2007, 2009)

Teaching

- Teaching Assistant/Lecturer for *Operating Systems* (70/495), University of Cagliari. Course instructor: Prof. Giorgio Giacinto.
  - *14 hours of lectures on system programming in Linux*
  - *Graded students*
- Teaching Assistant/Lecturer for *Data Bases* (70/28), University of Cagliari. Course Instructor: Prof. Giorgio Giacinto.
  - *4 hours of lectures on ER diagrams and design of relational databses*

- *Graded students*

Mentoring

- *"Special problems" project advisor* (CS-8903)
  Graduate Student: Preetam Joshi, Georgia Institute of Technology, 2009
  Project focused on *detecting malicious executable code in packed PE files*
- *Intern advisor* - Damballa, Inc., Summer 2009
  Graduate Student: Junjie Zhang, Georgia Institute of Technology
  Project focused on *root cause analysis for drive-by malware downloads*
- *Intern advisor* - Damballa, Inc., Summer 2009
  Graduate Student: Manos Antonakakis, Georgia Institute of Technology
  Project focused on *botnet detection through passive analysis of DNS traffic*
- *Master's thesis co-advisor*
  Graduate Student: Davide Ariu, University of Cagliari, 2006
  Thesis focused on *detecting remote FTP attacks using Hidden Markov Models*
- *Master's thesis co-advisor*
  Graduate Student: Mauro Del Rio, University of Cagliari, 2006
  Thesis focused on *one-class classifier systems for network intrusion detection*

Grant Proposals

- Co-author of ONR grant proposal titled "*On the robustness and secrecy of traffic watermarks*". PI: Prof. Wenke Lee

Departmental Services

- Organizer of the *Security Reading Group* at Georgia Tech Information Security Center, Fall 2009

INDUSTRY EXPERIENCE

Principal Scientist at Damballa, Inc. (www.damballa.com), Atlanta, GA, USA, a **Spin-off of Georgia Tech** that focuses on commercial botnet detection solutions (Mar. 2007 – Jul. 2009)

- Research and development of botnet detection systems
- DNS traffic analysis and classification
- Machine learning-based technologies for malware/botnet classification

Internship with **LAN Security Group** at TISCALI, S.p.a. (www.tiscali.com), European Internet Service Provider. (February 2004 – June 2005)

- Evaluation of commercial IDS products
- Research and development of alarm clustering algorithms

REFERENCES

Prof. Wenke Lee
Georgia Institute of Technology, College of Computing
Klaus Advanced Computing Building, Room 3142
266 Ferst Drive, Atlanta, GA 30332-0765
Phone: +1-404-385-2879
Email: wenke@cc.gatech.edu

Prof. Nick Feamster
Georgia Institute of Technology, College of Computing
Klaus Advanced Computing Building, Room 3348
266 Ferst Drive, Atlanta, GA 30332-0765
Phone: +1-404-385-1944
Email: feamster@cc.gatech.edu

Prof. Guofei Gu
Texas A&M University, Department of Computer Science
301 Harvey R. Bright Building, Room 502C
College Station, TX 77843
Phone: +1-979-845-2475
Email: guofei@cs.tamu.edu

Prof. Giorgio Giacinto
University of Cagliari
Department of Electrical and Electronic Engineering
Piazza d'Armi, 09123 Cagliari, Italy
Phone: +39-070-675-5752
Email: giacinto@diee.unica.it

Prof. Fabio Roli
University of Cagliari
Department of Electrical and Electronic Engineering
Piazza d'Armi, 09123 Cagliari, Italy
Phone: +39-070-675-5779
Email: roli@diee.unica.it