

CURRICULUM VITAE

Sergio Pastrana Portillo

Research Associate
Department of Computer Science and Technology
University of Cambridge

Contact information

e-mail: sp849@cam.ac.uk
WWW: <https://www.cl.cam.ac.uk/~sp849/>
Address: Computer Laboratory
15 JJ Thomson Avenue
Cambridge CB3 0FD
United Kingdom

Education

PhD: Universidad Carlos III de Madrid, June 2014 (Cum Laude)
Thesis Title: “*Attacks Against Intrusion Detection Networks: Evasion, Reverse Engineering and Optimal Countermeasures*”
Distinction Award by Universidad Carlos III de Madrid
MS: Master in Computer Science and Engineering, Universidad Carlos III de Madrid, June 2009
Thesis Title: “*Design of Quantum Algorithms*” (in Spanish)
BCS: Bachelor in Computer Science, Universidad Carlos III de Madrid, September 2008
Project Title: “*Genetic Algorithms applied to the RISK game*” (in Spanish)

Academic experience

09/08 – 01/10: Research Assistant at Computer Science and Engineering Department, Universidad Carlos III de Madrid (COSEC research group)
08/12 – 11/12 Pre-doctoral Internship at Norwegian Information Security Lab, Gjøvik, Norway (supervised by professor Slobodan Pètrovic)
01/10 – 09/15: Teaching Assistant at Computer Science and Engineering Department, Universidad Carlos III de Madrid (COSEC research group)
09/15 – 09/16: Assistant Professor at Computer Science and Engineering Department, Universidad Carlos III de Madrid (COSEC research group)
10/16 – present Research Associate at Computer Laboratory, University of Cambridge

Publications

Conference Proceedings

1. Sergio Pastrana, Daniel R. Thomas, Alice Hutchings, and Richard Clayton "CrimeBB: Enabling Cybercrime Research on Underground Forums at Scale", ACM The Web Conference 2018 (WWW), Lyon, France, April 2018.

2. Daniel R. Thomas, Sergio Pastrana, Alice Hutchings, Richard Clayton, and Alastair R. Beresford "Ethical issues of research using datasets of illicit origin". ACM Internet Measurement Conference (IMC), London, UK, November 2017.
3. Roberto Garrido-Pelaz, Lorena González-Manzano, and Sergio Pastrana. "Shall we collaborate?: A model to analyse the benefits of information sharing." Proceedings of the 2016 ACM CCS Workshop on Information Sharing and Collaborative Security. 2016.
4. Sergio Pastrana, Juan E. Tapiador, Guillermo Suarez-Tangil, Pedro Peris-Lopez, "AVRAND: A Software Based Defense Against Code Reuse Attacks in AVR Architectures", 13th Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA), San Sebastian, Spain, July 2016,
5. Sergio Pastrana; Carlos Alberca; Guillermo Suarez-Tangil; Paolo Palmieri, "Security Analysis and Exploitation of Arduino Devices in the Internet of Things", Workshop on Malicious Software and Hardware in Internet of Things (MAL-IOT), ACM Digital Library, Como, Italy, May 2016
6. Carlos Alario, Carlos Delgado, Iria Estevez, Carmen Fernandez, Jorge Blasco, Sergio Pastrana, Guillermo Suarez, and Julio Villena. "Interactive activities: the key to learning programming with MOOCs." Proceedings of the European Stakeholder Summit on experiences and best practices in and around MOOCs (EMOOCs), 2016.
7. Sergio Pastrana; Carmen Torrano-Giménez; Hai Than Nguyen; Agustín Orfila, "Anomalous Web Payload Detection: Evaluating the Resilience of 1-gram Based Classifiers", 8th International Symposium on Intelligent Distributed Computing - IDC'2014, (570) , 195-201SPRINGER , Madrid, 2014.
8. Sergio Pastrana; Agustín Orfila; Arturo Ribagorda , "A Functional Framework to Evade Network IDS", Proceedings of the 44th Hawaii International Conference on System Sciences (HICSS 2011), 1-10, Hawai (USA), 2011.
9. Sergio Pastrana; Arturo Ribagorda ; Agustín Orfila, "Modeling NIDS Evasion using Genetic Programming", Proceedings of the The 2010 World Congress in Computer Science, Computer Engineering and Applied Computing, Las Vegas, NE. (USA), 2010.

Journal papers

1. Lorena Gonzalez-Manzano, José María de Fuentes, Sergio Pastrana, Pedro Peris-Lopez, Luis Hernandez, 2016 "PAGIoT: Privacy-preserving Aggregation protocol for Internet of Things". Journal of Network and Computer Applications (Q1). 71. 59-71
2. José María de Fuentes; Pedro Peris-Lopez; Juan E. Tapiador; Sergio Pastrana, 2015, Probabilistic yoking proofs for large scale IoT systems, Ad Hoc Networks (Q2), 32, 43-52, 1570-8705.
3. Sergio Pastrana; Juan E. Tapiador; Agustín Orfila ; Pedro Peris-Lopez, 2015, DEFIDNET: A framework for optimal allocation of cyberdefenses in Intrusion Detection Networks, Computer networks (Q2), 80, 66- 88, 1389-1286.
4. Guillermo Suarez-Tangil; Juan E. Tapiador; Pedro Peris-Lopez; Sergio Pastrana, 2015, Power-aware anomaly detection in smartphones: An analysis of on-platform versus

- externalized operation, Pervasive and Mobile Computing (Q1), 18, 137- 151, 1574-1192.
5. Sergio Pastrana; Agustín Orfila ; Juan E. Tapiador; Pedro Peris-Lopez, 2014, Randomized Anagram Revisited, Journal of Network and Computer Applications (Q1), 41, 182- 196, 1084-8045.
 6. Sergio Pastrana; Aikaterini Mitrokotsa; Agustín Orfila; Pedro Peris-Lopez, 2012, Evaluation of classification algorithms for intrusion detection in MANETs, Knowledge-Based Systems (Q1), 36, 217- 225, 0950-7051.

Book chapters

1. Sergio Pastrana; Jose Montero; Agustín Orfila, 2013, Evading IDSs and Firewalls as Fundamental Sources of Information in SIEMs, 157- 180, NOVA SCIENCE PUBLISHERS INC, 978-1-624-17204-5.

Research Activities

Reviewer of the following journals

Knowledge Based Systems
Future Generation Computer Systems
Information Sciences
KSII Transactions on Internet and Information Systems
Ad Hoc Networks

PC Member or conference sub-reviewer:

IV Jornadas Nacionales de Investigación en Ciberseguridad (JNIC) 2018
International Conference on Networks & Communications 2016
13th International Conference on Security and Cryptography (SECRYPT) 2016
12th International Conference on Security and Cryptography (SECRYPT) 2015
IEEE International Conference on Trust, Security and Privacy 2015
International Conference on Information Security Practice and Experience 2015

Others

Project reviewer at Spanish Association for Standardisation and Certification
Project reviewer at Israeli Ministry of Science, Technology and Space

Participation in projects and research funding

- DS/SDS/1718/4. Data Science Approaches to Understanding Key Actors on Online Hacking Forums. ALAN TURING INSTITUTE, Paula Buttery/Alice Hutchings 01/10/17 – 31/03/18. £72.444
- S2013/ICE-3095, CIBERDINE-CM. Ciberseguridad: Datos, información, riesgos, CAM-CONSEJERIA EDUCACION DIR. GRAL. UNIVERSIDADES E INVESTIGACION, , Arturo Ribagorda , 01/10/2014- 30/09/2016, 128.685€.

- TIN2013-46469-R, Security and Privacy in the Internet of You, MINISTERIO DE ECONOMIA Y COMPETITIVIDAD, Juan Manuel Estevez Tapiador, 01/01/2014-31/12/2016, 86.381,90€.
- IPT-2011-1593-390000, Simulador avanzado para la Ciberdefensa Organizada (SACO), MINISTERIO DE CIENCIA E INNOVACION, Arturo Ribagorda , 02/09/2011-31/03/2015, 145.991.
- CCG10-UC3M/TIC-5570, Metodología para la generación de evasiones en sistemas de Detección de Intrusiones de Red, COMUNIDAD DE MADRID-UC3M, Agustín Orfila , 01/01/2011- 31/12/2011, 1.645€.
- TSI-020100-2010-1032, IMAE - Identidad Móvil para la Administración Electrónica, MINISTERIO DE INDUSTRIA, ENERGIA Y TURISMO, Agustín Orfila , 06/05/2010- 31/12/2011, 29.957,08€.

Teaching experience

| | |
|--------------|--|
| 2008 - 2009: | Security in Distributed Systems, BS in Computer Science, 30 hours (Spanish) Information Security and Protection, BS in Computer Science, 30 hours (Spanish) |
| 2009-2010: | Programming in Fortran, BS in Electronics, Mechanics and Electricity, 63 hours (English) Security in Distributed Systems, BS in Computer Science, 30 hours (Spanish) |
| 2010-2011: | Programming in Fortran, BS in Electronics, Mechanics and Electricity, 56 hours (English) |
| 2011-2012: | Programming in Fortran, BS in Electronics, Mechanics and Electricity, 84 hours (English) Security Engineering, BS in Computer Science, 21 hours (Spanish) Prepared new material |
| 2012-2013: | Security Engineering, BS in Computer Science, 53 hours (English) Vulnerabilities, Threats and Protocols, BS in Security Engineering, 6 hours (Spanish) |
| 2013 – 2014: | Programming in Fortran, BS in Electronics, Mechanics and Electricity, 34 hours (English) |
| 2014 – 2015: | Cyberdefense Systems, MS in Cybersecurity, 18 hours (English). Prepared new material / Course director Persistent Threats and Information Leakage, MS in Cybersecurity, 6 hours (English) Introduction to Programming in Java, Part I (Online, English) EdX MOOC |
| 2015 – 2016: | Cyberdefense Systems, MS in Cybersecurity, 18 hours (English) Prepared new material / Course director Malware Analysis and Engineering, MS in Cybersecurity, 18 hours (English) Prepared new material / Course director |

Advising

BSc Students

- Joel Barra Muñoz, 2012, Topic: Linux security

- Antonio Parra Truyol, 2013, Topic: Malware analysis
- Javier Alvarez Izquierdo, 2014, Topic: Bio-engineering
- Ricardo Ramirez de Antón, 2014, Topic: Security Legislation
- Marta Canes López, 2014. Topic: Intrusion Detection Networks
- Carlos Alberca Pozo, 2014. Topic: Security in RFID
- Antonio Requena, 2016. Topic: Android Security

MS Students

- Christian Lopez Hormiga, 2015, Topic: SIEM systems
- Carlos Alberca López, 2015. Topic: Security in IoT
(Published at Mal-IoT16 Workshop)
- José Ramón Rapallo, 2015. Topic: Military Cyber-ranges
- Victor Sánchez, 2015. Topic: SIEM systems
- Eric Mendillo, 2015. Topic: Cybersecurity simulator
- Roberto Garrido, 2016. Topic: Cooperative Cyberdefense
- Fernando Vañó, (expected 2016). Topic: IoT Honeypot
- Luis Nuñez, (expected 2016). Topic: Malware analysis
- Jaime Morales, (expected 2016). Topic: Information Sharing
- Iñigo Serrano, (expected 2016). Topic: Stego-malware
- José María Alonso (expected 2016). Topic: Security in SCADA