Hugo Gascón, PhD

Contact Information

Talstr. 5
13189 Berlin
GERMANY

Birthdate: 02/25/82
Mobile: +49-176-304-798-75
e-mail: hgascon@gmail.com
Site: https://hugogascon.com

Professional Experience

DCSO Deutsche Cyber-Sicherheitsorganisation GmbH Berlin, GERMANY

Senior Data Scientist **April 2019 to present**

- Machine learning R&D and product owner for platform engineering.

ICAI School of Engineering Madrid, SPAIN

Associate Professor **January 2020 to present**

- Artificial Intelligence applied to Cybersecurity (M.Sc. in Cybersecurity)

Institute For System Security
Technical University of Braunschweig, Braunschweig, GERMANY

Research Associate **April 2016 to July 2018**

- Research on machine learning techniques and its applications for the detection, analysis and response to targeted attacks.

Computer Security Group
University of Göttingen, Göttingen, GERMANY

Research Associate **August 2012 to March 2016**

- Research on machine learning techniques for structured data applied to identification of characteristic malware behavior, detection and analysis of targeted threats and mining of threat intelligence.

Center for Advanced Machine Learning
Symantec, Mountain View (CA), USA

Research Intern **October 2015 to December 2015**

- Research on deep learning methods for classification of code graph representations to infer behavioral patterns in malicious code.

Google Summer of Code - The Honeynet Project

Mentor **Summer 2013, 2014 and 2015**

- Droidbot: Artificial user interaction for dynamic analysis of Android malware (2015)
- Malcom: Malware Communication Analyzer (2014)
- HpfeedsHoneyGraph: Visualization of malicious intention transmission from honeypot logs (2013)

Developer Student **June 2012 to August 2012**

- Development of Acapulco, a tool to find and display clusters of meta-events built from different types of *hpfeeds* events within a parallel graph. It allows to represent multidimensional security data in a single visualization and extract significative trends of attacker behavior from honeypot traces.

Machine Learning Group
Berlin Institute of Technology, Berlin, GERMANY

Research Associate **August 2011 to August 2012**

- Research on high dimensional structured data and machine learning techniques applied to automatic reverse engineering of network protocols and modeling of malware behavior.

Robota, Madrid, SPAIN

Information Security Consultant **October 2009 to July 2011**

- Specialized in providing consulting work in all facets of information security management aspects.
- Design of network security architectures. Deployment of several vendors perimeter security solutions and Linux based systems.
- Enterprise risks assessment and network auditing projects by means of penetration testing.

Gunnebo Spain, Madrid, SPAIN

R&D Intern for Network Security Infrastructure **June 2009 to August 2009**

- Research in electronic security systems.
- Design of IP solutions, network topology, network electronics,
NAS, SAN, ISCSI systems.

Department of Telematic Engineering
Carlos III University of Madrid, Madrid, SPAIN

R&D Intern for Network Infrastructure **October 2004 to July 2005**

- Intern at *Telefónica Chair* and researcher for the European project IST Muse (Multi Service Access Everywhere).
- Research on multi-service access networks. Secure connectivity between end-user terminals and edge nodes in a multi-provider environment.

Education

Technical University of Braunschweig, Braunschweig, GERMANY

Ph.D. in Computer Science, March 2019

- Thesis Topic: *Defending Against Targeted Attacks with Pattern Recognition*
- Advisor: Prof. Dr. Konrad Rieck
- Areas of Study: Computer Security, Machine Learning

Carlos III University of Madrid, Leganés, Madrid SPAIN

M.Sc. in Telecommunication Engineering, February 2010

- Thesis Topic: *Analysis of an open source Intrusion Detection System and its response against vulnerability assessment and exploitation tools.* (Graded with Highest Honors).
- Advisor: Professor Agustín Orfila Díaz-Pabón
- Area of Study: Network Security

Universität Stuttgart, Stuttgart GERMANY

M.Sc. in Telecommunication Engineering, September 2006 to September 2007

- Socrates/Erasmus european program scolarship at Stuttgart University.
- Advisor: Prof. em. Dr.-Ing. Dr. h.c. mult. Paul J. Kühn

Selected Publications

Reading Between The Lines: Content-Agnostic Detection of Spear-Phishing Emails H. Gascon, S. Ulrich, B. Stritter and K. Rieck 21st International Symposium on Research in Attacks, Intrusions and Defenses (RAID) September 2018

Mining Attributed Graphs for Threat Intelligence H. Gascon, B. Grobauer, T. Schreck, L. Rist, D. Arp and Konrad Rieck ACM Conference on Data and Applications Security and Privacy (CODASPY) March 2017

Automatic Inference of Search Patterns for Taint-Style Vulnerabilities F. Yamaguchi, A. Maier, H. Gascon and K. Rieck. 36th IEEE Symposium on Security and Privacy (S&P) May 2015

Drebin: Efficient and Explainable Detection of Android Malware in Your Pocket. D. Arp, M. Spreitzenbarth, M. Hübner, H. Gascon and K. Rieck. Network and Distributed System Security Symposium (NDSS) February 2014.

Structural Detection of Android Malware using Embedded Call Graphs. H. Gascon, F. Yamaguchi, D. Arp and K. Rieck. *ACM Workshop on Security and Artificial Intelligence (AISEC)*, November 2013.

Chucky: Exposing Missing Checks in Source Code for Vulnerability Discovery. F. Yamaguchi, C. Wressnegger, H. Gascon and K. Rieck. *ACM Conference on Computer and Communications Security (CCS)*, November 2013

Learning Stateful Models for Network Honeypots. T. Krueger, H. Gascon, N. Krämer and K. Rieck. *ACM Workshop on Security and Artificial Intelligence (AISEC)*, October 2012.

Analysis of update delays in Signature-based Network Intrusion Detection systems. H. Gascon, A. Orfila, and J. Blasco. *Computers & Security.* 2011.

Technical Skills

Software Engineering

Over 10 years of programming experience in Python and ample knowledge of Java and C, as well as of other scripting and application specific languages such as BASH, SQL and x86 ASM. Vast experience with software engineering best practices (source version control, CI/CD, testing and reviewing) as well as agile methodologies (Scrum) and project management tools (Jira, Clubhouse).

Machine Learning Engineering

Expert knowledge of algorithms for pattern recognition (e.g. clustering and optimization algorithms, neural networks, graph theory, Fourier analysis, statistical modeling, evolutionary computation and visualization) and extensive experience with multiple techniques and toolboxes for building predictive analytic pipelines, including: SQL and NoSQL databases (PostgreSQL, Cassandra), distributed data analysis engines (Spark, RabbitMQ), general scientific programming libraries (Numpy, Scipy, Pandas, Matplotlib, iPython/Jupyter notebooks), standard machine and deep learning frameworks (Scikit-learn, Keras, PyTorch, Tensorflow) and tools for deployment, orchestration and monitoring (Docker, Apache Airflow, Prometheus/Grafana).

Security Engineering and Threat Analysis

Advanced knowledge of distributed security architectures for intrusion detection and response and threat analysis at scale, including: threat intelligence standards (STIX, ATT&CK), tools (MISP, OpenCTI, Splunk) and CSIRT processes. Practical reverse engineering experience with disassemblers for x86 and Dalvik (radare, IDA Pro, Androguard), debuggers (OllyDbg, GDB), and sandboxing/virtualisation technologies (Cuckoo, VMWare, VirtualBox).

Systems and Networking

Extensive experience with Unix-based systems and network architecture design, including network programming and building a good understanding of networking and routing protocols (UDP, advanced TCP, ARP, DNS, Dynamic routing, OSPF, BGP).

Foreign Languages

ENGLISH Full professional spoken and written proficiency.
Cambridge First Certificate in English (FCE).

GERMAN Full professional spoken and written proficiency.
Goethe-Institute Zertifikat Deutsch (ZD).

FRENCH Basic spoken and written proficiency.

SPANISH Native proficiency.

References Available for Contact

Prof. Dr. Konrad Rieck (k.rieck@tu-bs.de)

- Professor, Institute for System Security, Technical University of Braunschweig

Prof. Dr. Klaus-Robert Müller (klaus-robert.mueller@tu-berlin.de)

- Professor, Machine Learning Group, Berlin Institute of Technology

Andrew Gardner, PhD (Andrew_Gardner@symantec.com)

- Global Head of AI/ML at NortonLifeLock (Symantec)