Hugo Gascón

Contact Information

Eberswalder Strasse 16
10437 Berlin
GERMANY

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

Research Interests

Development of new learning methods for high dimentional structured data to analyse and reverse engineer malicious code and build system behavioral models (software and human) that facilitate the early identification of targeted attacks (a.k.a. APTs)

Professional Experience

Computer Security Group
University of Göttingen, Göttingen, GERMANY

Research Associate - Ph.D. Candidate **August 2012 to present**

- 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 classifcation of code graph representations to infer behavioral patterns in malicious code.

Google Summer of Code - The Honeynet Project

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.

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)

Machine Learning Group
Berlin Institute of Technology, Berlin, GERMANY

Research Associate - Ph.D. Candidate **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 architecture. 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 network. Secure connectivity between end-user terminals and edge nodes in a multi-provider environment.

Education

Carlos III University of Madrid, Leganés, Madrid SPAIN

M.Sc. 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).
- Adviser: Professor Agustín Orfila Díaz-Pabón
- Area of Study: Network Security

Universität Stuttgart, Stuttgart GERMANY

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

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

Selected Publications

Fingerprinting Mobile Devices Using Personalized Configurations A. Kurtz, H. Gascon, T. Becker, K. Rieck and F. Freiling. 16th Privacy Enhancing Technologies Symposium (PETS) to appear July 2016.

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.

Technical Skills

Reverse Engineering and Code Analysis
Disassemblers for x86, Dalvik, etc (radare, IDA Pro, Androguard), debuggers (OllyDbg, GDB), virtualization technologies (VMWare, VirtualBox).

Programming
Python, Java, C, Bash, JavaScript, D3, CSS, ASM, SQL.

Networking
Extensive knowledge of protocols (UDP, advanced TCP, ARP, DNS, Dynamic routing, OSPF, BGP), services (Apache, SQL, POP, IMAP, SMTP, application-specific daemon design) and network programming.

Machine Learning
Specific toolboxes (Numpy, Scipy, scikit-learn, Theano, Pandas) and skills for pattern recognition (clustering and optimization algorithms, graph theory, fourier analysis, statistical modeling, evolutionary computation and visualization).

Organizations

Association for Computing Machinery (ACM)
Student Member

Society of Spanish Researchers in Germany (CERFA/SFBD)
Member

The Honeynet Project
Norway Chapter Leader, Contributor

Foreign Languages

ENGLISH Advanced spoken and written level.
Cambridge First Certificate in English (FCE).

GERMAN Intermediate spoken and written level.
Goethe-Institute Zertifikat Deutsch (ZD).

FRENCH Basic spoken and written level.

SPANISH Mother tongue.

References Available for Contact

Prof. Dr. Konrad Rieck (konrad.rieck@uni-goettingen.de)
- Professor, Computer Security Group, University of Göttingen
- *Prof. Rieck is currently my Ph.D. supervisor.*

Prof. Dr. Klaus-Robert Müller (klaus-robert.mueller@tu-berlin.de)
- Professor, Machine Learning Group, Berlin Institute of Technology
- *Prof. Müller is currently my Ph.D. co-supervisor.*

Andrew Gardner, PhD (Andrew_Gardner@symantec.com)
- Sr Technical Director, Machine Learning at Symantec