Giuseppe **Petracca**

Software Engineer and Security Researcher · Ph.D. Candidate in Computer Science and Engineering · **Seeking Full-Time Position (July 2018)**

W362 Westgate Building, Dept. of Computer Science and Engineering, Penn State University, University Park, PA, 16802, U.S.A.

+1 (203) 751-0625 | gxp18@cse.psu.edu | http://sites.psu.edu/petracca/ | gxp18 | giuseppe-petracca

Education

Penn State University, Ph.D. in Computer Science and Engineering (GPA 3.9) — *University Park, PA, U.S.A.*

Research Focus: Systems Security - Reference Monitoring of Programs' Access to Privacy-Sensitive Sensors — *Aug. 2012 - Present*

Advised by Dr. Trent Jaeger (tjaeger@cse.psu.edu) - Published 10 Conference Papers available on Google Scholar

Penn State University, Visiting Scholar in Information Sciences and Technology — *University Park, PA, U.S.A.*

Research Topic: Distributed Systems and Cloud Computing Security - Sponsor: Hewlett-Packard Labs — *Dec. 2011 - Jul. 2012*

Advised by Dr. Anna C. Squicciarini (acs20@psu.edu) - Published 5 Conference Papers available on Google Scholar

Sapienza University of Rome, M.S. in Computer Science and Engineering (GPA 3.89) — *Rome, Italy*

Master Thesis: Management of Self-Protected Content in Cloud Computing and Distributed Systems — *Jan. 2009 - Oct. 2011*

Advised by Dr. Tiziana Catarci (catarci@diag.uniroma1.it)

Sapienza University of Rome, B.S. in Computer Science and Engineering (GPA 3.95) — *Rome, Italy*

Relevant Coursework: Software Engineering, Computer Networks, Distributed Systems, Data Structures and Algorithms, Computer Security, Computer Architectures, Signal Processing, and Databases Design — *Sept. 2003 - Dec. 2008*

Industry Experience

Google Inc. (Mobile Malware Team) - Software Engineer Intern (Security) — *Mountain View, CA, U.S.A.*

Extended a dynamic analyzer tool for automatic detection of Ad-Fraud apps published on Google Play — *Jun. 2017 - Sept. 2017*

Samsung Research America (Knox Security Team) - Software Engineer Intern (Security) — *Mountain View, CA, U.S.A.*

Built an automated tool for static and dynamic analysis of SEAndroid policies for Samsung Devices — *May 2016 - Aug. 2016*

Intel Labs (Privacy and Intelligence Lab) - Graduate Technical Engineer Intern — *Hillsboro, OR, U.S.A.*

Designed defense mechanisms for Return-Oriented Programming (ROP) attacks in Intel 64-bit Architectures — *May 2014 - Aug. 2014*

Intel Corporation (Intel Micro Runtime Team) - Graduate Technical Engineer Intern — *Hillsboro, OR, U.S.A.*

Built a communication module between the Intel Micro Runtime and the Software Guard Extension (SGX) — *May 2013 - Aug. 2013*

Skills

Software Design and Development:	Android AOSP and SDK, Eclipse IDE, and Java 2 Platform Security
Programming Languages:	Java, C, and Python (preferred)
Operating Systems:	Android, Unix (Linux and MacOS), Microsoft Windows, SELinux and SEAndroid
Computer Networks:	ISO/OSI Network Protocols, Mobile Networks, Snort, Wireshark, and Emulab
Cloud Computing:	OpenStack, and Amazon Web Services
Database Design:	SQL and MySQL Workbench
Web Design:	HTML, XML, JavaScript, Joomla CMS, Servlet/JSP, and Web Server Apache Tomcat
Object-Oriented Design:	Unified Modeling Language (UML)
Software Testing:	JUnit, White-Box, and Black-Box testing
Other Tools and Languages:	Git/SVN Source Control, LaTeX, OpenGL, Prolog, Scheme, SML, and Matlab
Languages Proficiency:	English (Full Professional Proficiency - ILR Level 4), Italian (Native), and Spanish (Basic)

Academic Projects

Operating Systems Design - Designed and implemented using the C language: ● A serializer construct for processes synchronization ● A parallel file system for applications file sharing ● A pipe-based module for communication between threads and processes

System and Network Security - Designed and implemented using the C language: ● A Linux kernel module (Linux 2.3.26) to prevent link traversal attacks ● A man-in-the-middle attack for the Secure Socket Layer using libopenSSL ● A reference monitor for Linux system calls using strace ● A format-string vulnerability attack to obtain root control by exploiting the Global Offset Table (GOT)

Open Source Projects

Code Available on GitHub (https://github.com/gxp18): ● **AuDroid**: Reference monitor to control flows of sensitive data via audio channels [C and Java] ● **AWare**: Authorization mechanism to control access to privacy-sensitive sensors [C and Java] ● **Bridges**: Automatic analysis of SELinux policy to identify attack vectors [Python] ● **PolyScope**: Static and runtime analysis of SELinux and DAC policies to identify risky configurations [Python] ● **Android-Sting**: Runtime analysis of name resolution vulnerabilities in Android OS [C]

Activities

Coding Competitions: ● HackPSU 2017 - Face Recognition Challenge using Betaface API ● HackPSU 2016 - Capital One Reimagine Banking Challenge using Nessie API

Cyber Security Meetings: ● Cyber Security Collaborative Research Alliance Bootcamp, June 2017, UC Davis, CA ● BlackHat USA 2016, Las Vegas, NV ● DIMACS 2014 Workshop on Secure Cloud Computing, Rutgers University, New Brunswick, NJ

Research Meetings: ● PhD Intern Research Conference (PIRC) at Google Inc., July 2017, Mountain View, CA ● Facebook PhD Summer Itern Open House at Facebook HQ, July 2017, Menlo Park, CA

Academic Publications

EnTrust: Authorizing Cooperating Programs Access to Mobile System Sensors — *Baltimore, MD, U.S.A.* — *2018*
Giuseppe Petracca, Ahmad-Atamli Reineh, Jens Grossklags, and Trent Jaeger
Under Peer Review *for the Proceedings of the 27th USENIX Security Symposium, USENIX Security 2018*

A Survey on Sensor-based Threats to Internet-of-Things (IoT) Devices and Applications — *2018*
Amit Kumar Sikder, Giuseppe Petracca, Hidayet Aksu, Trent Jaeger, and A. Selcuk Uluagac
Under Peer Review *for the IEEE Internet of Things Journal*

AWare: Preventing Abuse of Privacy-Sensitive Sensors via Operation Bindings — *Vancouver, BC, Canada* — *2017*
Giuseppe Petracca, Ahmad-Atamli Reineh, Yuqiong Sun, Jens Grossklags, and Trent Jaeger
Proceedings of the 26th USENIX Security Symposium, USENIX Security 2017

On Risk in Access Control Enforcement — *Indianapolis, IN, U.S.A.* — *2017*
Giuseppe Petracca, Frank Capobianco, Christian Skalka, and Trent Jaeger
Proceedings of the 22nd ACM Symposium on Access Control Models and Technologies, SACMAT 2017

Agility Maneuvers to Mitigate Inference Attacks on Sensed Location Data — *Baltimore, MD, U.S.A.* — *2016*
Giuseppe Petracca, Lisa M. Marvel, Ananthram Swami, and Trent Jaeger
Proceedings of the 35th Premier International Conference for Military Communications, MILCOM 2016

Pileus: Protecting User Resources from Vulnerable Cloud Services — *Los Angeles, CA, U.S.A.* — *2016*
Yuqiong Sun, Giuseppe Petracca, Xinyang Ge, and Trent Jaeger
Proceedings of the 2016 Annual Computer Security Applications Conference, ACSAC 2016

AuDroid: Preventing Attacks on Audio Channels in Mobile Devices — *Los Angeles, CA, U.S.A.* — *2015*
Giuseppe Petracca, Yuqiong Sun, Ahmad Atamli, and Trent Jaeger
Proceedings of the 31th Annual Computer Security Applications Conference, ACSAC 2015

CloudArmor: Protecting Cloud Commands from Compromised Cloud Services — *New York, NY, U.S.A.* — *2015*
Yuqiong Sun, Giuseppe Petracca, Vijayakumar Hayawardh, Joshua Schiffman, and Trent Jaeger
Proceedings of the 8th IEEE International Conference on Cloud Computing, CLOUD 2015

Inevitable Failure: The Flawed Trust Assumption in the Cloud — *Scottsdale, Arizona, U.S.A.* — *2014*
Yuqiong Sun, Giuseppe Petracca, and Trent Jaeger
Proceedings of the 21st ACM Conference on Computer and Communications Security, ACM CCSW 2014

Situational Awareness through Reasoning on Network Incidents in Controlled Networks — *San Antonio, TX, U.S.A.* — *2014*
Anna Cinzia Squicciarini, Giuseppe Petracca, William Horne, and Aurnob Nath
Proceedings of the 4th ACM Conference on Data and Application Security and Privacy, ACM CODASPY 2014

Adaptive data protection in distributed systems — *San Antonio, TX, U.S.A.* — *2013*
Anna Cinzia Squicciarini, Giuseppe Petracca, and Elisa Bertino
Proceedings of the 3th ACM Conference on Data and Application Security and Privacy, ACM CODASPY 2013

ReasONets: a fuzzy-based approach for reasoning on network incidents — *Raleigh, NC, U.S.A.* — *2012*
Giuseppe Petracca, Anna Squicciarini, William Horne, and Marco Casassa Mont
Proceedings of the 19th ACM Conference on Computer and Communications Security, CCS 2012

Adaptive data management for self-protecting objects in cloud computing systems — *Las Vegas, NV, U.S.A.* — *2012*
Anna Cinzia Squicciarini, Giuseppe Petracca, and Elisa Bertino
Proceedings of the 8th International Conference on Network and Service Management, 2012, ACM CNSM 2012

Early Detection of Policies Violations in a Social Media Site: A Bayesian Belief Network Approach — *Chapel Hill, NC, U.S.A.* — *2012*
Anna Cinzia Squicciarini, William McGill, Giuseppe Petracca, and Shuo Huang
Proceedings of the 2012 IEEE International Symposium on Policies for Distributed Systems and Networks, POLICY 2012

Press Coverage

Your phone is like a spy in your pocket — *Science News* — *Feb. 2018*
Article by Maria Temming referencing our AWare Paper (USENIX Security 2017)
https://www.sciencenews.org/article/smartphones-data-collection-security-privacy

AuDroid security system prevents audio attacks at the device level — *The Stack* — *Apr. 2016*
Article by Alice MacGregor referencing our AuDroid Paper (ACSAC 2015)
https://thestack.com/security/2016/04/05/audroid-security-system-prevents-audio-attacks-at-the-device-level/