Giuseppe **Petracca**

SOFTWARE ENGINEER · PH.D. CANDIDATE IN COMPUTER SCIENCE AND ENGINEERING

344 Westgate Building, Dept. of Computer Science and Engineering, The Pennsylvania State University, University Park, PA, 16802 USA

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

Education

The Pennsylvania State University   *University Park, PA, U.S.A*
PH.D. IN COMPUTER SCIENCE AND ENGINEERING (GPA 3.9)   *Aug. 2012 - Present*
- Doctoral Thesis: On Limitation of Access Control Models for Privacy-Sensitive Sensors
- Research Focus: Operating Systems Security for Mobile Platforms

Sapienza University of Rome   *Rome, Italy*
M.S. IN COMPUTER SCIENCE AND ENGINEERING (GPA 3.89)   *Jan. 2009 - Oct. 2011*
- Master Thesis: Management of Self-Protected Content in Cloud Computing

Sapienza University of Rome   *Rome, Italy*
B.S. IN COMPUTER SCIENCE AND ENGINEERING (GPA 3.95)   *Sept. 2003 - Dec. 2008*

Industry Experience

Google Inc. (Mobile Malware Team)   *Mountain View, CA, U.S.A.*
SOFTWARE ENGINEER & SECURITY RESEARCHER   *Jun. 2017 - Sept. 2017*
- Designed and implemented extensions to the dynamic analyzer tool for the detection of Ad-Fraud and unwanted apps

Samsung Research America (Knox Security Team)   *Mountain View, CA, U.S.A.*
SOFTWARE ENGINEER & SECURITY RESEARCHER   *May 2016 - Aug. 2016*
- Designed and implemented an automated tool (Bridges) for the analysis of SELinux policies in Android-powered devices

Intel Labs (Privacy and Intelligence Lab)   *Hillsboro, OR, U.S.A.*
GRADUATE TECHNICAL ENGINEER   *May 2014 - Aug. 2014*
- Researched prevention techniques of Return-Oriented Programming (ROP) attacks with shadow stack and return address checksum

Intel Corporation (Intel Micro Runtime Team)   *Hillsboro, OR, U.S.A.*
GRADUATE TECHNICAL ENGINEER   *May 2013 - Aug. 2013*
- Designed and implemented a network communication module between the Intel Micro Runtime and the Software Guard Extension

Skills

Software Design and Development: Android AOSP and SDK, Eclipse IDE, and Java 2 Platform Security
Programming Languages: Java (preferred), C, Python, and C++
Operating Systems: Android, Linux, Mac, and Windows
Computer Networks: ISO/OSI Network Protocols, Mobile Networks, Snort, Wireshark, and Emulab
Cloud Computing: OpenStack, Amazon Web Services, Hadoop, and Map Reduce
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
Project Management: Constructive Cost Model (COCOMO II), ARANEUS Data Model, andPert/Gantt Charts
Other Tools and Languages: LaTeX, OpenGL, Prolog, Scheme, SML, and Matlab
Languages Proficiency: English (Full Prof. 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 betweeen 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)

Academic Experience

The Pennsylvania State University   *University Park, PA, U.S.A.*
GRADUATE RESEARCH ASSISTANT
    Department of Computer Science and Engineering,
    Conducting research in systems security for mobile and cloud computing   *Aug. 2012 - Present*
    Collaboration with Hewlett-Packard Labs,
    Designed and implemented an network intrusion detection system (ReasOnNets)   *Aug. 2011 - Jul. 2012*
    College of Information Sciences and Technology,
    Conducted research on social media platforms and security in cloud computing   *Feb. 2011 - Jul. 2011*
GRADUATE TEACHING ASSISTANT
    CSE 543: Computer and Network Security, lead by Dr. T. Jaeger   *Fall 2016*
    CMPSC 461: Programming Language Concepts, lead by Dr. D. Heller   *Fall 2013*
    CMPEN/EE 362: Computer Networks, lead by Dr. T. La Porta   *Spring 2013*
    CMPEN/EE 362: Computer Networks, lead by Dr. J. Metzner   *Fall 2012*

Conference Publications

AWare: Preventing Abuse of Privacy-Sensitive Sensors via Operation Bindings   *Vancouver, BC, Canada*
Giuseppe Petracca, Ahmad-Atamli Reineh, Yuqiong Sun, Jens Grossklags, and Trent Jaeger   *2017*

Proceedings of the 26th USENIX Security Symposium, USENIX Security 2017

On Risk in Access Control Enforcement   *Indianapolis, IN, U.S.A.*
Giuseppe Petracca, Frank Capobianco, Christian Skalka and Trent Jaeger   *2017*

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.*
Giuseppe Petracca, Lisa M. Marvel, Ananthram Swami, and Trent Jaeger   *2016*

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.*
Yuqiong Sun, Giuseppe Petracca, Xinyang Ge and Trent Jaeger   *2016*

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.*
Giuseppe Petracca, Yuqiong Sun, Ahmad Atamli, and Trent Jaeger   *2015*

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.*
Yuqiong Sun, Giuseppe Petracca, Vijayakumar Hayawardh, Joshua Schiffman, and Trent Jaeger   *2015*

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.*
Yuqiong Sun, Giuseppe Petracca, and Trent Jaeger   *2014*

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.*
Anna Cinzia Squicciarini, Giuseppe Petracca, William Horne, and Aurnob Nath   *2014*

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.*
Anna Cinzia Squicciarini, Giuseppe Petracca, and Elisa Bertino   *2013*

Proceedings of the 3rd 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.*
Giuseppe Petracca, Anna Squicciarini, William Horne, and Marco Casassa Mont   *2012*

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.*
Anna Cinzia Squicciarini, Giuseppe Petracca, and Elisa Bertino   *2012*

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.*
Anna Cinzia Squicciarini, William McGill, Giuseppe Petracca, and Shuo Huang   *2012*

Proceedings of the 2012 IEEE International Symposium on Policies for Distributed Systems and Networks, POLICY 2012

References

Dr. Trent Jeager, Professor at the Dept. of Computer Science and Engineering at Penn State   *[tjaeger@cse.psu.edu]*
Dr. Anna C. Squicciarini, Professor at the College of Information Sciences and Technology at Penn State   *[acs20@psu.edu]*
Dr. Tiziana Catarci, Professor at the Dept. of Computer Science and Engineering at Sapienza   *[catarci@diag.uniroma1.it]*