

Daniele Antonioli

✉ antonioli.daniele@gmail.com • 🌐 <https://francozappa.github.io/>

🐙 francozappa • 🐦 francozappa • in antoniolidaniele

Google scholar: RkX4eFsAAAAJ, Last CV update: December 10, 2019

Summary

- Main research interests:
 - *Cyber-Physical systems*: simulation/emulation [1], attacks [2], defenses [3, 4], and gamification [5]
 - *Wireless systems*: Wi-Fi [6], Bluetooth [7, 8], and hybrid physical layers [9].
 - *Embedded systems and applied cryptography*: authentication [10] and RNG [11]

Education

PhD in CS at Singapore University of Technology and Design (SUTD) <i>Thesis: Secure Cyber-Physical and Wireless Systems [12], Adv: N.O. Tippenhauer</i>	Sep 2015 - Aug 2019 <i>GPA: 4.90/5.00</i>
MS in Electronics and Telecom Engineering at University of Bologna <i>Thesis: Design and Testing of RNG [13], Adv: R. Rovatti, W. Bursleson</i>	Sep 2010 - Mar 2013 <i>Grade: 110/110</i>
BS in Electronics and Telecom Engineering at University of Bologna <i>Thesis: Principles and Evolution of Radio Imaging, Adv: C. Lamberti</i>	Sep 2006 - Mar 2010 <i>Grade: 91/110</i>
High School Diploma at Liceo Scientifico G. Marconi, Italy <i>Science specialisation</i>	Sep 2000 - Jul 2006 <i>Grade: 98/100</i>

Selected Projects

- KNOB: the Key Negotiation Of Bluetooth (KNOB) attack.
- REarby: toolkit to reverse engineer and attack Google's Nearby Connections.
- MiniCPS: a framework for Cyber-Physical Systems real-time simulation built on top of Mininet
- S3: SWaT Security Showdown is a novel CTF for Industrial Control Systems (2015, 2016, 2017)

Awards

- Singaporean Presidential Graduate Fellowship (PFG), 2015 - 2019
- Research excellence award by ST Engineering (see [3]), 2017
- Foundations of Security Analysis and Design (FOSAD) Summer School Scholarship, 2016
- UniBO Overseas Master Thesis Scholarship (research in the USA), 2012

Service

- Reviewer for IEEE Transactions on Information Forensics and Security (TIFS), since 2017
- Reviewer for IEEE Transactions on Wireless Communications (TWC), since 2019

Skills

Programming: object-oriented, procedural, trait-oriented, test-driven	Langs: Pythons, C, Rust, SQL, bash, C++, Java, Octave/MATLAB, Mathematica, VHDL, spice
Architectures: x86, amd64, ARM	Pentest: SQLi, Fuzzing, MitM, BOF, ROP
Tools: unix, vim, git, tmux, make, inkscape, ghidra	Markup: md, \LaTeX , rst, toml

Research Experience

- RA for Helmholtz Center for Information Security (CISPA), DE** Aug 2018 - Jun 2019
Wireless Systems Security, Adv: N.O. Tippenhauer
◦ Wireless systems security, protocol analysis, RE, and applied cryptography [7, 8]
- RA for Dept of Computer Science University of Oxford, UK** Jan 2018 - Jul 2018
Protocols and Systems Security, Adv: K.B. Rasmussen
◦ Wireless systems security, protocol analysis, RE, and applied cryptography [9, 7]
- RA for iTrust Research Centre at SUTD, Singapore** Feb 2015 - Sep 2015
Cyber-Physical Systems Security, Adv: N.O. Tippenhauer
◦ Design, and implementation of MiniCPS [1]. Pentesting on the SWaT testbed.
- RA for VLSI Circuits and Systems Group at UMass, Amherst** Oct 2012 - Dec 2012
Hardware Testing and Security, Adv: W. Burleson, V. Suresh
◦ Work on Master thesis and related e-book [13].
◦ Publish lightweight on-chip implementation of reduced NIST randomness test suite [11]

Teaching Experience

- TA for Security Principles (SPR) at University of Oxford, UK** Summer 2018
Instructor: Prof. K.B. Rasmussen
◦ Responsible for the exercises and presentation of Scyther
◦ Topics: CIA, Authentication, Cryptography, RSA, Protocols
- TA for 50.012 Networks at SUTD, Singapore** Fall 2017
Instructor: Prof. N.O. Tippenhauer
◦ Manage weekly lab session, grading of homeworks, office hours for 30 students.
◦ Topics: Internet, TCP/IP, UDP, BGP, SDN, HTTP, REST API, TLS, tunnels, NAT, embedded networks
- TA for 50.020 Security at SUTD, Singapore** Spring 2017
Instructor: Prof. N.O. Tippenhauer
◦ Manage weekly lab session, grading of homeworks, office hours for 30 students.
◦ Topics: sym/asym crypto, BOF, TLS, CTF, hashing, XSS, input validation, code injection, MitM.
- Private Teacher, Italy** Jan 2013 - Jan 2015
Audience: Grad, Undergrad, and High school students
◦ Grad/undergrad: linear algebra, calculus, programming (C, Pascal).
◦ High school: math, physics, programming (C++).
- CS External Commissioner Prof for High School Final Exams, Italy** Jun 2013 - Jul 2013
Institutes: ITIS Urbino, ITI Don Orione
◦ Grade written exams prepared by MIUR, oral interviews and grade assignment for 40 students.
◦ Topics: LAMP stack, SQL, design and implementation of relational DB, MVC paradigm, HTTP(S).

Industry Experience

- Chief of Transportation and Logistics for FIG World Cup, Italy** Apr 2013
Adv: Colombo F, Porfiri P
◦ Plan and manage transportation services for 43 International Delegations and Press.
◦ Coordinate a senior team of drivers, MGMT of facilities, cash fund, lost property and meals plan.
- Intern Clinical Engineer at Infermi Hospital Rimini, Italy** Apr 2010 - Jul 2010
Adv: Camillini R.
◦ Study and measurement about the safety of optical radiations [14].
◦ Lab activity, Logistics, Electrical Checks and inspections in various departments of the hospital.

Selected Self Learning

Unix tools by University of Cambridge <i>Instructor: Kuhn M. Topics</i>	2017
Learning How to Learn by UCSD (Coursera) <i>Instructors: Sejnowsky T., Oakley B. Topics</i>	2014
Hardware/Software Interface by Washington University (Coursera) <i>Instructors: Borriello G., Ceze L. Certificate with Distinction</i>	2014
Entrepreneurship 101: Who is your customer? by MITx (edX) <i>Instructor: Aulet B.,</i>	2014
Cryptography Part 1 by Stanford University (Coursera) <i>Instructor: Boneh D. Topics Certificate with Distinction</i>	2013
Algorithms Part 1 by Princeton University (Coursera) <i>Instructors: Wayne K., Sedgewick R Topics</i>	2013
Quantum Mechanics and Quantum Computation by BerkleyX (edx) <i>Instructor: Vazirani U. Topics Certificate Notes</i>	2013

Languages

Italian: Native	English: Professional proficiency: TOEFL iBT: 94 (2013). B-2 CEFR (2012)
Spanish: Intermediate proficiency	

Events and Talks

Invited talk by Prof Conti's SPRITZ group at the University of Padova <i>Towards high-interaction virtual honeypots in-a-box and MiniCPS.</i>	Summer 2017
SMART MIT/ETH/NUS/SUTD Workshop at NUS CREATE Tower (Singapore) <i>Mentoring six grad students for the track of cyber-security policies. ADAPT research paper.</i>	2017
SGCSC Cybersecurity Camp at NUS (Singapore) <i>Instructors: Liang Z., Roychoudhury A. Directed fuzzing LibPNG with peach and Binutils with afl</i>	2017
SCy-Phy Systems Week at SUTD (iTrust, Singapore) <i>SWaT Security Showdown (S3) CTF and testbed experiments. Technical talks.</i>	2015, 2016, 2017
FOSAD International Summer School at Bertinoro (Italy) <i>Foundations of Security Analysis and Design. Selected with scholarship.</i>	Summer 2016

Misc

Sports: Soccer, Swimming, Basketball	Hobbies: Dog owner, Traveling, Nature, Food
Events: Concerts, Museums, Art, Sport	Music: R&R, Amateur guitar player, Vinyl collector

Publications

- [1] Daniele Antonioli and Nils Ole Tippenhauer. Minicps: A toolkit for security research on CPS networks. In *Proceedings of the First ACM Workshop on Cyber-Physical Systems-Security and/or Privacy (co-located with CCS)*, pages 91–100. ACM, 2015. <https://arxiv.org/pdf/1507.04860>, Repo: <https://github.com/scy-phy/minicps>.
- [2] Daniele Antonioli, Giuseppe Bernieri, and Nils Ole Tippenhauer. Taking control: Design and implementation of botnets for cyber-physical attacks with cpsbot. *arXiv preprint arXiv:1802.00152*, 2018.

- [3] Daniele Antonioli, Anand Agrawal, and Nils Ole Tippenhauer. Towards high-interaction virtual ICS honeypots-in-a-box. In *Proceedings of the 2nd ACM Workshop on Cyber-Physical Systems Security and Privacy (co-located with CCS)*, pages 13–22. ACM, 2016. <https://dl.acm.org/citation.cfm?id=2994493> **Research excellence award by ST Engineering at FIRST workshop 2017.**
- [4] Hamid Reza Ghaeini, Daniele Antonioli, Ferdinand Brasser, Ahmad-Reza Sadeghi, and Nils Ole Tippenhauer. State-Aware Anomaly Detection for Industrial Control Systems. In *Proceedings of Symposium on Applied Computing(SAC)*, 2018.
- [5] Daniele Antonioli, Hamid Reza Ghaeini, Sridhar Adepu, Martín Ochoa, and Nils Ole Tippenhauer. Gamifying ICS Security Training and Research: Design, Implementation, and Results of S3. In *Proceedings of Workshop on Cyber-Physical Systems Security & Privacy (co-located with CCS)*, November 2017.
- [6] Daniele Antonioli, Sandra Siby, and Nils Ole Tippenhauer. Practical evaluation of passive COTS eavesdropping in 802.11b/n/ac WLAN. In *Proceedings of Conference on Cryptology And Network Security (CANS)*, November 2017.
- [7] Daniele Antonioli, Nils Ole Tippenhauer, and Kasper Rasmussen. The KNOB is Broken: Exploiting Low Entropy in the Encryption Key Negotiation of Bluetooth BR/EDR. In *Proceedings of the USENIX Security Symposium (USEC)*, August 2019.
- [8] Daniele Antonioli, Nils Ole Tippenhauer, and Kasper Rasmussen. Low entropy key negotiation attacks on bluetooth and bluetooth low energy. 2019.
- [9] Daniele Antonioli, Nils Ole Tippenhauer, and Kasper Rasmussen. Nearby Threats: Reversing, Analyzing, and Attacking Google’s “Nearby Connections” on Android. In *Network and Distributed System Security Symposium (NDSS)*, February 2019.
- [10] John Henry Castellanos, Daniele Antonioli, Nils Ole Tippenhauer, and Martín Ochoa. Legacy-Compliant Data Authentication for Industrial Control System Traffic. In *Proceedings of the Conference on Applied Cryptography and Network Security (ACNS)*, July 2017.
- [11] Vikram B Suresh, Daniele Antonioli, and Wayne P Burleson. On-chip lightweight implementation of reduced NIST randomness test suite. In *IEEE International Symposium on Hardware-Oriented Security and Trust (HOST)*, pages 93–98. IEEE, 2013. <http://sharps.org/wp-content/uploads/SURESH-HOST13.pdf>.
- [12] Daniele Antonioli. *Design, Implementation, and Evaluation of Secure Cyber-Physical and Wireless Systems*. PhD thesis, Singapore University of Technology and Design, 2019.
- [13] Daniele Antonioli. Design and testing of RNG. Master’s thesis, University of Bologna and University of Massachusetts Amherst, 2013. <http://www.lulu.com/shop/daniele-antonioli/design-and-testing-of-rng/ebook/product-20965725.html>.
- [14] Daniele Antonioli. Artificial Optical Radiation Management, Risk and Safety in the Hospital Environment. *Tecnica Ospedaliera (Italian Technical Magazine)*, 2010.