Daniele Antonioli

antonioli.daniele@gmail.com • https://francozappa.github.io/
francozappa • francozappa • antoniolidaniele
Google scholar: RkX4eFsAAAAJ, Last CV update: September 7, 2020

Summary

- Currently postdoc at EPFL working with HexHive group led by Prof. Mathias Payer
- Main research interests:
  - *Cyber-Physical systems*: simulation/emulation [1], attacks [2], defenses [3, 4], and gamification [5]
  - *Wireless systems*: DP3T for COVID-19 [6], Wi-Fi [7], Bluetooth [8, 9, 10], and hybrid physical layers [11].
  - *Embedded systems* and *applied cryptography*: authentication [12] and RNG [13]

Education

PhD in CS at Singapore University of Technology and Design (SUTD) **Sep 2015 - Aug 2019**
Thesis: Secure Cyber-Physical and Wireless Systems [14], Adv: N.O. Tippenhauer *GPA: 4.90/5.00*

MS in Electronics and Telecom Engineering at University of Bologna **Sep 2010 - Mar 2013**
Thesis: Design and Testing of RNG [15], Adv: R. Rovatti, W. Burleson *Grade: 110/110*

BS in Electronics and Telecom Engineering at University of Bologna **Sep 2006 - Mar 2010**
Thesis: Principles and Evolution of Radio Imaging, Adv: C. Lamberti *Grade: 91/110*

High School Diploma at Liceo Scientifico G. Marconi, Italy **Sep 2000 - Jul 2006**
Science specialisation *Grade: 98/100*

Selected Projects

- DP3T: Decentralized Privacy-Preserving Proximity Tracing for COVID-19.
- BIAS: Bluetooth Impersonation AttackS (CVE-2020-10135).
- KNOB: Key Negotiation Of Bluetooth attack (CVE-2019-9506).
- 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

- Conferences
  - ACM ASIA Conference on Computer and Communications Security (ASIACCS)
  - International Conference on Network and System Security (NSS)
- Journals
  - IEEE Transactions on Information Forensics and Security (TIFS)
  - IEEE Transactions on Wireless Communications (TWC)
- Workshops

- IEEE Workshop on Cyber-Physical Systems Security (CPS-Sec)

Skills

Programming: object-oriented, procedural, trait-oriented, test-driven
Architectures: x86, amd64, ARM
Tools: unix, vim, git, tmux, make, inkscape, ghidra
Langs: Pythons, C, Rust, SQL, bash, C++, Java, Octave/MATLAB, Mathematica, VHDL, spice
Pentest: SQLi, Fuzzing, MitM, BOF, ROP
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 [8, 9]

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 [11, 8]

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 [15].
- Publish lightweight on-chip implementation of reduced NIST randomness test suite [13]

Teaching Experience

TA for Security Principles (SPR) at University of Oxford, UK **Summer 2018**
Instructor: Prof. K.B. Rasmussen
- Responsable 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 [16].
- Lab activity, Logistics, Electrical Checks and inspections in various departments of the hospital.

Selected Self Learning

Unix tools by University of Cambridge **2017**
Instructor: Kuhn M. Topics

Learning How to Learn by UCSD (Coursera) **2014**
Instructors: Sejnowsky T., Oakley B. Topics

Hardware/Software Interface by Washington University (Coursera) **2014**
Instructors: Borriello G., Ceze L. Certificate with Distinction

Entrepreneurship 101: Who is your customer? by MITx (edX) **2014**
Instructor: Aulet B,.

Cryptography Part 1 by Stanford University (Coursera) **2013**
Instructor: Boneh D. Topics Certificate with Distinction

Algorithms Part 1 by Princeton University (Coursera) **2013**
Instructors: Wayne K., Sedgewick R Topics

Quantum Mechanics and Quantum Computation by BerkleyX (edx) **2013**
Instructor: Vazirani U. Topics Certificate Notes

Languages

Italian: Native

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

Spanish: Intermediate proficiency

Talks

BIAS and KNOB attacks against Bluetooth BR/EDR/LE **2020**
Invited talk at Workshop on Attacks in Cryptography (WAC) co-located with CRYPTO

From the Bluetooth Standard to Standard-Compliant 0-days **2020**
Talk at Hardwear.io Virtual Conference

Bluetooth blues: KNOB Attack Explained **2019**
Invited talk at CyberWire Research Saturday with Dave Bittner

Towards high-interaction virtual honeypots in-a-box and MiniCPS. **2017**
Invited talk at Mauro Conti's SPRITZ research group University of Padova

Events

SMART MIT/ETH/NUS/SUTD Workshop at NUS CREATE Tower (Singapore) **2017**
Mentoring six grad students for the track of cyber-security policies. ADAPT research paper.

SGCSC Cybersecurity Camp at NUS (Singapore) **2017**
Instructors: Liang Z., Roychoudhury A. Directed fuzzing LibPNG with peach and Binutils with afl

SCy-Phy Systems Week at SUTD (iTrust, Singapore) **2015, 2016, 2017**
SWaT Security Showdown (S3) CTF and testbed experiments. Technical talks.

FOSAD International Summer School at Bertinoro (Italy) **Summer 2016**
Foundations of Security Analysis and Design. Selected with scholarship.

Misc

Sports: Soccer, Swimming, Basketball
Events: Concerts, Museums, Art, Sport
Hobbies: Dog owner, Traveling, Nature, Food
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] Carmela Troncoso, Mathias Payer, Jean-Pierre Hubaux, Marcel Salathé, James Larus, Edouard Bugnion, Wouter Lueks, Theresa Stadler, Apostolos Pyrgelis, Daniele Antonioli, et al. Decentralized privacy-preserving proximity tracing. *arXiv preprint arXiv:2005.12273*, 2020.

[7] 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.

[8] 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.

[9] Daniele Antonioli, Nils Ole Tippenhauer, and Kasper Rasmussen. Key negotiation downgrade attacks on bluetooth and bluetooth low energy. *ACM Trans. Priv. Secur.*, 2020.

[10] Daniele Antonioli, Nils Ole Tippenhauer, and Kasper Rasmussen. BIAS: Bluetooth Impersonation AttackS. In *Proceedings of the IEEE Symposium on Security and Privacy (S&P)*, May 2020.

[11] 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.

[12] 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.

[13] 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.

[14] Daniele Antonioli. *Design, Implementation, and Evaluation of Secure Cyber-Physical and Wireless Systems*. PhD thesis, Singapore University of Technology and Design, 2019.

[15] Daniele Antonioli. Design and testing of RNG. Master's thesis, University of Bologna and University of Massachussets Amherst, 2013. http://www.lulu.com/shop/daniele-antonioli/design-and-testing-of-rng/ebook/product-20965725.html.

[16] Daniele Antonioli. Artificial Optical Radiation Management, Risk and Safety in the Hospital Environment. *Tecnica Ospedaliera (Italian Technical Magazine)*, 2010.