Arthur Gervais

I am motivated by revolutionizing how society trades and interacts. Bitcoin and the security properties of its blockchain provide technical means to catalyze societal evolution. My research therefore focuses on the security, privacy and performance of blockchain technology. Because this technology is still in its infancy, I largely focus on understanding and quantifying the tension points and tradeoffs in terms of security, privacy and performance, with the goal to build a mainstream, scalable, open, and decentralized blockchain. Part of my research is e.g., the design of novel consensus mechanisms, connecting the real world with blockchain, and the development of practical and competitive blockchain applications. My research is inherently multidisciplinary and I frequently collaborate with colleagues worldwide in various fields (e.g., machine learning).

Kornhausstrasse 19
8037 Zürich
Switzerland

Website
http://arthur.gervais.cc

Email
arthur@gervais.cc

Mobile
+41 78 203 26 82

Educational background

12/2012 - 12/2016 (exp.) **Research Assistant and PhD Candidate, Advisor: Srdjan Capkun, ETH Zurich**
Zurich, Switzerland

- Research fields: Security and privacy of digital currencies (e.g., Bitcoin), web privacy
- Collaboration with Armasuisse (Thun, Switzerland) and NEC Laboratories (Heidelberg, Germany)
- Supervision of 6 Master thesis, 1 Bachelor thesis and 5 Semester thesis
- 7 peer-reviewed publications, 3 years consecutively in tier 1 conference (ACM CCS)

09/2010 - 09/2012 **Double Master of Science in Security and Mobile Computing**, Erasmus Mundus NordSecMob
Royal Institute of Technology (KTH), Advisor: Peter Sjödin, Sweden (1 year)
Aalto University, Advisor: Tuomas Aura, Finland (6 months)
Relevant coursework: Advanced Networks, Routing Protocols, Internet Security and Privacy, Cryptographic Protocols, Software Security, Mobile Application Development

09/2008 - 09/2012 **Master of Science in Computer Engineering**
National Institute of Applied Sciences (INSA) Lyon, Advisor: Youakim Badr, France
Relevant coursework: C/C++ Programming, Java, Operating Systems, Project Management, Computer Architecture, Data Modeling, Reverse Engineering, Database Management Systems.

08/2006 - 06/2008 **Classes préparatoires**
National Institute of Applied Sciences (INSA) Lyon, France
2 year undergraduate scientific foundation course in Engineering Sciences in a department with emphasis on foreign exchanges and international scientific connections in Europe

06/2006 **High School Diploma**
Gymnasium Starnberg, Germany
Focus on Mathematics and Physics

Professional experience

08/2015 - 11/2015 **Research Intern, Supervisor: Mic Bowman, Intel Labs**
Portland, United States of America

- Quantifying incentives for participation in blockchain based systems
- Received Letter of Intent from Intel consisting of a job offer upon PhD graduation

07/2011 - 12/2014 **CEO and Founder, Consulting and Management, Hatforce**
Leverkusen, Germany

- First startup to develop a bug bounty platform (like hackerone.com)
- Winner of the SSES (Stockholm School of Entrepreneurship) Venture Challenge, January 2012
- Semi-finalist of the Venture Challenge Competition, San Diego State University, USA, March 2012

12/2011 - 06/2012 **Junior Security Consultant, Nixu Ltd.**
Helsinki, Finland
- Master Thesis about SCADA/ICS security, elaborated security testing guidelines for ICS
- Detected important vulnerabilities in widespread Industrial Control Systems hardware

05/2010 - 08/2010 **Intern, IPv6 Networking, German Federal Office for Information Security (BSI)**
Bonn, Germany
- Deep analysis of the IPv6 protocol and its inherent protocol weaknesses
- Conducting various IPv6 related network attacks and analysis of possible defenses

06/2009 - 09/2009 **Intern, Programming, EADS Secure Networks Oy**
Jyväskylä, Finland
- Planned and programmed reliable tracing software in C++ and Java for the TETRA network

05/2005 - 01/2006 **Intern, Programming, Timmann GmbH & Co**
Tutzing, Germany
- Optimization of the AES reference implementation for use in FPGA's

Invited Talks

Scaling Bitcoin **On the Security and Performance of Proof of Work Blockchains**
Milan, Italy, October 2016

Tampering with the Delivery of Blocks and Transactions in Bitcoin
Hong Kong, China, December 2015

Google **Quantifying Web-Search Privacy**
Zürich, Switzerland, May 2015

S4 **New Modicon PLC Vulns, SCAPY and ModbusSec**
SCADA Security Scientific Symposium (S4)
Miami, United States, January 2013

Cambridge University **Security Analysis of Industrial Control Systems**
University of Cambridge Computer Laboratory, Security seminar series
Cambridge, United Kingdom, July 2012

Nuit du Hack **SCADA System Attacks**
Paris, France, June 2012

BSI **IPv6 attacks and defenses in local area networks**
German IT-Security Conference "12. IT-Sicherheitskongress des BSI"
Won the „Best Student Award 2011" from the German Federal Office for Information Security
Bonn, Germany, May 2011

Awards / Honors

2016 Heidelberg Laureate Forum invitation
Acquired funding for Blockchain Summerschool ETH Zurich
Scholarship for Scaling Bitcoin

2015 Letter of Intent after internship completion at Intel Labs
Scholarship for Scaling Bitcoin

2012 Winner of SSES (Stockholm School of Entrepreneurship) Venture Challenge

2011 Best Student Award from the German Federal Office for Information Security

2010 Erasmus Mundus NordSecMob Master Double Degree scholarship, 2010 – 2012

Academic Publications

2016 On the Security and Performance of Proof of Work Blockchains
Arthur Gervais, Ghassan Karame, Karl Wüst, Vasileios Glykantzis, Hubert Ritzdorf, Srdjan Capkun
in Proceedings of the ACM Conference on Computer and Communication Security (CCS), 2016

Quantifying Web Adblocker Privacy
Arthur Gervais, Alexandros Filios, Vincent Lenders, Srdjan Capkun
On ePrint Archive 2016/900 (under submission), 2016

Quantifying Location Privacy Leakage from Transaction Prices
Arthur Gervais, Hubert Ritzdorf, Mario Lucic, Srdjan Capkun
In Proceedings of the 21th European Symposium on Research in Computer Security (ESORICS), 2016

Ethereum Eclipse Attacks
Karl Wüst and **Arthur Gervais**
Technical Report, ETH Zurich, Department of Computer Science, 2016

Bitcoin Protocol Specification
Arthur Gervais and Ghassan Karame
Bitcoin and Blockchain Security (Chapter 3), ISBN: 978-1-63081-013-9 (Invited Chapter), 2016

2015 Tampering with the Delivery of Blocks and Transactions in Bitcoin
Arthur Gervais, Hubert Ritzdorf, Ghassan Karame, Srdjan Capkun
In Proceedings of the ACM Conference on Computer and Communication Security (CCS), 2015

Misbehavior in Bitcoin: A Study of Double-Spending and Accountability
Ghassan Karame, Elli Androulaki, Marc Roeschlin, **Arthur Gervais**, Srdjan Capkun
in ACM Transactions on Information and System Security (TISSEC), 2015

2014 On the Privacy Provisions of Bloom Filters in Lightweight Bitcoin Clients
Arthur Gervais, Ghassan Karame, Damian Gruber, Srdjan Capkun
In Proceedings of the 30th Annual Computer Security Applications Conference (ACSAC), 2014

Quantifying Web-Search Privacy
Arthur Gervais, Reza Shokri, Adish Singla, Srdjan Capkun and Vincent Lenders
in Proceedings of the ACM Conference on Computer and Communication Security (CCS), 2014

Is Bitcoin a Decentralized Currency?
Arthur Gervais, Ghassan Karame, Srdjan Capkun, Vedran Capkun
IEEE Security and Privacy Magazine, 2014

2013 Double-Spending Fast Payments in Bitcoin due to Client versions 0.8.1
Arthur Gervais, Hubert Ritzdorf, Ghassan Karame
Technical Report, ETH Zürich, Department of Computer Science, 2013

2012 Security Analysis of Industrial Control Systems
Arthur Gervais
Master Thesis

Other Publications

2012

Whitepaper on Industrial Automation Security in Fieldbus and Field Device Level
Magnus Sundell, Janne Kuivalainen, Juhani Mäkelä, **Arthur Gervais**, Jouko Orava, Mikko H. Hyppönen
Vacon, supplier of variable speed AC drives

Security Analysis of Google Wallet (text in German)
http://arthur.gervais.cc/Google_wallet.pdf
Hatforce

2011

Attacks and defenses in IPv6 local area networks (text in German)
Arthur Gervais
<KES> SecuMedia, IT security magazine of the German Federal Office for Information Security (BSI)

New Penetration Testing Business Model, Crowd-sourcing for IT-Security
Arthur Gervais
PenTest Magazine

Thesis Mentoring

Master Students

Karl Wüst
Security of Proof of Work Blockchains
Master Thesis, ETH Zurich, Spring 2016
Co-author on
On the Security and Performance of PoW Blockchains

Vasileios Glykantzis
Security of Proof of Work Blockchains
Master Thesis, ETH Zurich, Spring 2016
Co-author on
On the Security and Performance of PoW Blockchains

Alexandros Filios
Web Privacy
Master Thesis, ETH Zurich, Spring 2016
Co-author on
Quantifying Web Adblocker Privacy

Fabian Schewetofski
Software assisted dry-run
Master Thesis, ETH Zurich, Spring 2016

Lorenzo Wölckner
Security and Privacy of Bitcoin
Master Thesis, ETH Zurich, Spring 2014

Mathias Wellig
Security Analysis of Digital Currencies
Master Thesis, ETH Zurich, Spring 2013

Bachelor Students

Damian Gruber
Security and Privacy of Bitcoin
Bachelor Thesis, ETH Zurich, Summer 2014
Co-author on
On the Privacy Provisions of Bloom Filters in Lightweight Bitcoin Clients

Semester Students

Guillaume Felley
Data Feeds for Blockchains
Semester Thesis, ETH Zurich, Fall 2016

Ferran Llamas
Bitmessage Security Analysis
Semester Thesis, ETH Zurich, Spring 2015

Alexandros Filios
Web Privacy
Semester Thesis, ETH Zurich, Spring 2015

Stathakopoulou Chrysoula
Web Search Personalization
Semester Thesis, ETH Zurich, Spring 2015

Jesse Badash
Web Search Privacy
Semester Project, ETH Zurich, Summer 2014

Teaching Experience

Teaching Assistant

Information Security
ETH Zurich, Spring 2016

Foundations of Computer Science
ETH Zurich, Fall 2015, 2016

Security of Wireless Networks
ETH Zurich, Fall 2013, 2014

Design of Digital Circuits
ETH Zurich, Spring 2013

Introduction to Eiffel Programming
ETH Zurich, Fall 2016

Lecturer

Blockchain and Internet of Things (BIoTs) Summerschool
ETH Zurich, Spring 2016

Primary School
Computer Science for children of the 4th and 5th grade
Vaduz, Lichtenstein, Fall 2016

Selected Skills

Languages

German:	Native speaker
French:	Bilingual
English:	Fluent
Spanish:	Intermediate

Technical

Programming:	Python, C/C++, Java, HTML, Java Script, CSS, Assembler
Network:	IPv4/v6, P2P, TCP, Routing
Security:	Bitcoin, SCADA, TLS, Web
Data Analysis:	Machine Learning basics
Operating Systems:	Linux, Mac OS, Windows

Selected Press

2016 **Interview with the Swiss National Radio and Television (SRF)**
Blockchain Security and Privacy

Interview with the Austrian Science Radio Channel (ORF)
On the Security and Privacy of Proof of Work Blockchains

Interview and article with CoinDesk
On the Security and Privacy of Proof of Work Blockchains

2011 **Forbes Article about Hatforce**
Crowdsourcing meets Vulnerability Testing

Service

Program Committee
Program Committee, BITCOIN'17
Shadow Program Committee, ASIACCS'17

Organizing Committee
Blockchain Summerschool, EPFL and ETH, 2017

Reviewer

CCS, 2013-2016
USENIX, 2013-2016
IEEE S&P (Oakland), 2013-2015
NDSS, 2013-2015
Euro S&P, 2015-2016
Mobicom, 2012, 2013, 2015
ESORICS, 2013-2014
PETS, 2014-2015
WiSec, 2013
ACSAC, 2014
ACNS, 2013
ICDCS, 2015
IJIS, 2016

Open Source Contributions

Blockchain Simulator
https://github.com/arthurgervais/Bitcoin-Simulator

Web Search Obfuscation Quantification Tool
http://arthur.gervais.cc/WebSearchPrivacy.zip

Web Adblocker Privacy Quantification Tool
http://arthur.gervais.cc/AdblockerPrivacy.zip

SCAPY Module for Modbus TCP
https://github.com/secdev/scapy/blob/master/scapy/contrib/modbus.py

References

Srdjan Capkun
Professor, ETH Zurich
Phone: +41 44 632 71 90
Fax: +41 44 632 11 72
srdjan.capkun@inf.ethz.ch

Emin Gün Sirer
Associate Professor, Cornell University
Phone: +1 607 255 7673
Fax: +1 607 255 4428
egs@systems.cs.cornell.edu

Adrian Perrig
Professor, ETH Zurich
Phone: +41 44 632 99 69
Fax: +41 44 632 99 69
adrian.perrig@inf.ethz.ch

Roger Wattenhofer
Professor, ETH Zurich
Phone: +41 44 632 6312
Fax: +41 44 632 1035
wattenhofer@ethz.ch

Additional references can be provided upon request