Gergely Revay

Personal Data

Place and Date of Birth:	place | date
Address:	address
Phone:	phone
Email:	email
Blog	http://aetherlab.net
Trainings	http://hackademy.aetherlab.net
Youtube	https://youtube.com/aetherlabnet
Github	https://github.com/gergelyrevay
Twitter	@geri_revay

Work Experience

Present – **Oct 2017**

Senior Key Expert Penetration Tester at Siemens Corporation, Princeton, NJ, USA

As a delegate in the USA I continue with my previous responsibilities as a penetration tester. Besides that I lead a research project related to Concolic Execution in cooperation with NYU and EURECOM. As the research lead of the team I designed the offsec research agenda, which focused on OT/ICS security assessment.

Sept 2017 – **Oct 2013**

Penetration Tester at Siemens AG, Munich, Germany

As part of the CERT Security Assessment team, I was responsible to lead and execute various penetration tests. Testing Siemens products gives me the opportunity to work with various exotic systems in healthcare, transportation, energy, building technologies, intelligent cities etc... Apart from that, we regularly test third party systems, which are going to be deployed at Siemens. It is a great place to work with very different technologies, such as web, client-server architecture, embedded devices, mobile technologies etc

Sept 2013 – **Dec 2011**

Penetration Tester at OPTIMAbit GmbH, Munich, Germany

I worked as a external consultant for various companies from multinational insurance, banking and telecommunication companies through government agencies to industry leader technology companies. I executed 32 penetration tests, from that 2 Client-Server applications, 4 network assessment and 26 web application tests. This gave me the opportunity to get to know various networks, systems and application frameworks. I deal with customers on a day to day basis.

Oct 2011 – **Jan 2008**

Senior Quality Assurance Engineer at Balabit IT Security, Budapest, Hungary

My job changed a lot during the years, but the one thing that was always there is the low level black- and white-box testing manually and by writing automated test scripts as well. I worked on all products of the company, which gave me deep understanding of firewalls, logging architectures and high availability appliances mostly in linux environment. I gathered deep knowledge from the PHP web interface through the shell script and C background process to the underlying OS internals. I was also a team leader of 3 testers until the company embraced the SCRUM methodology, which made me a SCRUM master. I also worked in the development of our internal systems especially our automated test system, which was written in Python.

Jul-Dec 2007

Call Centre Advisor at British Telecommunications Plc., Glasgow, UK

I went to Glasgow to improve my English, which I did, thanks to my job in the call centre. It was related to my profession since I was selling telephone and Internet services and helped people to solve there issues with their services. Besides this the more important was that it gave a huge boost to my communication and soft skills.

Spring 2007

Developer Trainee at Telenor Hungary, Budaörs, Hungary

As a trainee I worked mostly on internal projects at one of the 3 mobile service providers of Hungary. I wrote an address and phone book for the whole company with WEB and WAP interface in *PHP*. I worked with an open source MMSC implementation, which was written in C.

Automn 2006	**Assistance in teaching Project Management** at Budapest University of Technology and Economics, Budapest, Hungary I was responsible for keeping touch with the students, help them with their homeworks and give them feedback on their progress. This work and the professor gave me deep understanding of the waterfall project management and the PMBOK methodology.

Education

June 2009	**M.Sc. in Computer Engineering** specialized on Security of Information and Communication Systems at Budapest University of Technology and Economics, Hungary http://english.www.bme.hu/ Thesis: "Automatic security testing of web content"
Spring 2006	**European Project Semester** at Oslo University College, Oslo, Norway Project: "Collaborative photo taking with mobile phones"

Trainings and Certificates

Feb 2019	**SANS FOR 508: Advanced Incident Response, Threat Hunting, and Digital Forensics** Incident investigation, memory analysis, filesystem analysis, lateral movement, timeline analysis. For more information visit: https://www.sans.org/course/advanced-incident-response-threat-hunting-training
April 2018	**SANS ICS 410: ICS/SCADA Security Essentials** Bootcamp for ICS environments and their security. For more information visit: https://www.sans.org/course/ics-scada-cyber-security-essentials
Jan 2018	**Hardware Hacking Workshop, Tactical Network Solutions** This workshop focuses on low level hardware attacks. For more information visit: https://www.tacnetsol.com/p/registration
March 2017	**SANS FOR 610: Reverse Engineering Malware (GREM Certified)** This training focuses on malware reverse engineering from binary to JavaScript. For more information visit: https://www.sans.org/course/reverse-engineering-malware-malware-analysis-tools-techniques
June 2016	**The ARM Exploit Laboratory by Saumil Shah, 0xA RECON** The class covers everything from an introduction to ARM assembly all the way to Return Oriented Programming (ROP) on ARM architectures. For more information visit: https://recon.cx/2016/training/trainingexploitlab.html.
April 2015	**SANS SEC 575: Mobile Device Security and Ethical Hacking (GMOB Certified)** Hands-on course on the security of mobile devices, particularly on IOS and Android. For more information visit: http://www.sans.org/course/mobile-device-security-ethical-hacking
July 2014	**SANS SEC 760: Advanced Exploit Development for Penetration Testers** It teaches the skills required to reverse-engineer 32-bit and 64-bit applications, perform remote user application and kernel debugging, analyze patches for 1-day exploits, and write complex exploit, such as use-after-free attacks against modern software and operating systems.For more information visit: http://www.sans.org/course/advance-exploit-development-pentetration-testers
May 2013	**Offensive Security Certified Professional (OSCP Certified)** In-depth technical training course which covers the techniques and the whole process of penetration testing from the initial information gathering through exploitation and post exploitation techniques to writing a penetration testing report. For more information download the syllabus from http://www.offensive-security.com/documentation/penetration-testing-with-backtrack.pdf

May 2009	**One week training on writing scientific papers at Telecom ParisTech, Paris, France** http://www.telecom-paristech.fr The training went through the research work in general, how to choose a topic, how a research process should go and how to write different scientific papers.
Nov 2008	**One week training on international team management** http://www.telecom-paristech.fr The training dealt with the communication and management of multinational teams.
June 2003	**Computer Administrator qualification (OKJ 52464103) at Iron- and Electrical Industrial Technical High School, Sopron, Hungary** As the end of the IT studies in high school we took this exam which includes network and desktop administration and deep understanding of the Office programs.

Languages

Hungarian:	Mother tongue
English:	Fluent
German:	Fluent

Conference Presentations

From Hardware to Exploit
2 days workshop on hardware hacking created and presented by Georg Kremsner, Anton Ebertzeder, Gergely Revay, Michael Messner
Presented at:
2016 | Siemens PSS Conference, Munich, Germany
2017 | Siemens Campus, Munich, Germany
2018 | Siemens Campus, Munich, Germany

Security Implication of the Cross-Origin Resource Sharing
https://www.youtube.com/watch?v=8HMSH-uES9M
Presented at:
2014 | OWASP APPSec, Cambridge, UK
2014 | CONFidence, Cracow, Poland
2013 | Hacktivity, Budapest, Hungary

Hello Burp Suite
Introductory workshop to the Burp Suite.
Presented at:
2014 | Hacktivity, Budapest, Hungary

Hello Radare2
Introductory workshop to Radare2.
Presented at:
2016 | Hacktivity, Budapest, Hungary

Publications

Learn Burp Suite, the Nr. 1 Web Hacking Tool
https://hackademy.aetherlab.net/p/burp-suite

Web Hacking: Become a Web Pentester
https://hackademy.aetherlab.net/p/web-hacking

Reverse Engineering with Radare2
https://hackademy.aetherlab.net/p/radare2

Practical Windows Penetration Testing
https://www.packtpub.com/networking-and-servers/practical-windows-penetration-testing-video