

Ali Abbasi

Room 4126, Zilverling Building,
University of Twente, Enschede, Netherlands
Email: a.abbasi@utwente.nl



EDUCATION

- **Ruhr University Bochum** Bochum, Germany
Visiting Research Scholar, SYSSEC Group 2016
 - Visiting researcher at Chair of Systems Security of Ruhr-University Bochum under supervision of Professor Thorsten Holz. I was working there for designing mitigation techniques for code-reuse attacks in Programmable Logic Controllers.
- **University of Twente** Enschede, Netherlands
PhD. Candidate in Computer Security Nov 2013- Present
 - PhD student at Distributed and Embedded System Security Group, working on security of embedded systems that are used for Industrial Control Systems.
- **Tsinghua University** Beijing, China
M.Sc. in Computer Science (GPA: 83/100) 2011- 2013
 - Thesis: Critical Infrastructures Vulnerability Assessment and Protection from Protocol Layer to Hardware Layer.
- **Mazandaran University of Science and Technology** Babol, Iran
B.Sc. in Industrial Engineering (GPA: 14.3) 2005-2009

RESEARCH INTERESTS

- Industrial Control Systems Security & Embedded Systems Security, Real-time Operating Systems Security, Software Testing, Fuzzing, Vulnerability Analysis, APT detection

PROFESSIONAL EXPERIENCE

- **Intel Corporation** Beijing, China
Security Researcher Aug 2012-Jan 2013
 - I was involved in Intel research program called "Security Vulnerability Analysis Based on Cloud Platform" at Beijing, China.
- **CCERT Computer Emergency Response Team of China (CN-CERT)** Beijing, China
Security Researcher October 2011-October 2012
 - CCERT is the Computer Emergency Response Team for CERNET(Chinese Education and Research Network), which is the first CSIRT team in mainland China. I was Researching in HTML5 Security Countermeasures in CCERT.
- **National Computer Emergency Response Team of Iran (IR-CERT)** Tehran, Iran
Head of Vulnerability Analysis and Penetration Testing Group 2008-2011

- I was working as Head of a Vulnerability Analysis and Penetration Testing Group at Iran's National CERT.

TEACHING EXPERIENCE

- TA in Advanced Exploit Development on ARM Platform (ROP), Operating Systems Course, University of Twente (2014)
- Instructor of Penetration Testing for students at Network and Information Security lab of Tsinghua University (2011)
- TA of Computer Security Course at Tsinghua University (2011-2012)
- TA of Internet Security Explorer Course at Tsinghua University (2011-2012)
- Instructor of Certified Ethical Hackers (CEH) Course for MSc and PHD Students at Sharif University of Technology (2009)
- Instructor of Computer Security Course, Iranian School Network (2003)

PUBLICATIONS, PRESENTATIONS AND WHITE PAPERS

- Stealth Low-Level Manipulation of Programmable Logic Controllers I/O by Pin Control Exploitation. In 11th International Conference on Critical Information Infrastructures Security, October 2016.
- Ghost in the PLC: Designing an Undetectable Programmable Logic Controller Rootkit, Ali Abbasi, Majid Hashemi, Black Hat Europe, November 2016, London, United Kingdom.
- APTs Way, Evading your EBNIDS, Ali Abbasi, Jos Wetzels, Black Hat Europe, October 2014, Amsterdam, The Netherlands.
- On Emulation-Based Network Intrusion Detection Systems, Ali Abbasi, Jos Wetzels, Wouter Bokslag, Emmanuele Zambon, and Sandro Etalle, Proceedings of the 17th International Symposium on Research in Attacks, Intrusions and Defences (RAID), September 17-19, 2014, Gothenburg, Sweden
- Project IRUS: A Multifaceted Approach to Attacking and Defending ICS, Ali Abbasi, Dillon Beresford, Digital Bond's SCADA Security Scientific Symposium (S4), Miami, USA(2013)
- Ghost Domain Names in Iran, Introduction to 0day attack against DNS servers, Ali Abbasi, Haixin Duan, Alireza Danesh, Sharif University Capture The Flag Conference, Tehran, Iran (2012)
- "The HTML5 Attacks, CNCC 2012, CCF China National Computer Congress 2012 (CNCC201200118)"
- A Gray-Box DPDA-Based Intrusion Detection Technique Using System-Call Monitoring, Jafar Hadi Jafarian, Ali Abbasi, Siavash Safaei, CEAS 2011, The 8th Annual Collaboration, Electronic messaging, Anti-Abuse and Spam Conference, Perth, WA, Australia. Sep 2011 "

HONORS

- I am member of FluxFingers CTF team.
- I was member of Blue-Lotus CTF team until December 2012. We ranked 19 in DefCon 20.
- The Award of Most Creative Student at Mazandaran University of Science And Technology Between 5000 student (2009).
- The Award of Best Researcher at Mazandaran University of Science and Technology for two consecutive years (2008 and 2009)
- 1st Place In Penetration Testing and Hacking Contest Between All Universities In Iran at International Conference of Information Security and Cryptography 2009 Isfahan, Iran.