Hossein Rezaei

Blockchain Researcher

14+ years of experience in cryptography and cybersecurity. Worked as programmer, designer, researcher, senior software engineer and Chief Technology Officer in public key infrastructure, smart card, blockchain and cryptocurrency.

hossein.rezaei.ghaleh@gmail.com | 407-848-7751 | Linkedin.com/in/hosseinpro | GitHub.com/hosseinpro

SKILLS

Blockchain | Cryptocurrency | Smart Card | Public Key Infrastructure | IoT | Cryptography | Java Script | Java | C++ | Node.js | React.js | React Native | VSCode | GitHub | JIRA | Product Management | Scrum | Leadership | Teamwork

WORK EXPERIENCE

Security Researcher (remote)

Nuesoft Technologies — *May 2016 – Oct 2018, Atlanta, US*

- Researched and designed a cloud-based PKI-as-service with smart card
- Consulted for implementing two-factor authentication for network access

Chief Technology Officer

PKI Co. — *Nov 2010 – Aug 2016, Iran*

- Co-founder of the company
- Researched and developed Public Key Appliance product
- Researched and developed Card Issuing System product
- Researched and developed a general cryptography middleware for browsers
- Researched and developed an identification card based of public key cryptography
- Designed architecture of cryptography systems for banks and financial institutes

Senior Software Engineer

Matiran Co. — *Feb 2010 – Sep 2012, Iran*

- Designed architecture of smart card management systems
- Consulted for public key infrastructure
- Evaluated FAT (Functional Acceptance Test) and SAT (Site Acceptance Test) of smart card issuing and mailing machineries

Senior Software Developer

SG Co. — *Jun 2005 – Feb 2010, Iran*

- Developed programs to control smart card issuing process in industrial printers
- Developed a framework for cryptography and smart card programming
- Designed and developed an IDE for smart card programming with a script language
- Programming with security devices such as crypto token, smart card, fingerprint scanner and card reader
- Cryptography programming with Hardware Security Module (HSM)

EDUCATION

PhD in Computer Science

University of Central Florida — *Aug 2016 – Expected Jan 2020, Orlando, US*

- Thesis: Improving Security of Crypto Wallets in Blockchain Technologies

MSc in Computer Science

University of Central Florida — *Aug 2016 – Dec 2017, Orlando, US*

MSc in Software Engineering

QIAU — *Sep 2005 – Mar 2008, Iran*

- Thesis: PC Secure Bootstrapping

BSc in Hardware Engineering

QIAU — *Sep 2001 – Sep 2005, Iran*

- Thesis: Efficient Implementation of RSA Cryptography Engine and PKCS#1

PUBLICATIONS

New Secure Approach to Backup Cryptocurrency Wallets
H. Rezaeighaleh, C. Zou, The 2019 Global Communications Conference (GLOBECOM-2019), IEEE, 2019 — *Dec 2019, Hawaii, US*

Deterministic Sub-Wallet for Cryptocurrencies
H. Rezaeighaleh, C. Zou, the 2019 IEEE International Conference on Blockchain (Blockchain-2019), IEEE, 2019 — *Jul 2019, Atlanta, US*

Using Disposable Domain Names to Detect Online Card Transaction Fraud
R. Laurens, H. Rezaeighaleh, C. Zou, J. Jusak, IEEE International Conference on Communications (ICC 2019) - Communication and Information Systems Security Symposium (CISS) — *May 2019, Shanghai, China*

Secure Smart Card Signing with Time-based Digital Signature
H. Rezaeighaleh, Roy Laurens, Cliff Zou, The 2018 International Conference on Computing, Networking and Communications (CNC 2018), IEEE, 2018 — *Mar 2018, Hawaii, US*

A New High-Performance Approach for Offline Replacement Attack Prevention in Trusted Clients
H. Rezaei Ghaleh, S. Khorsandi, The 2009 IEEE International Symposium on Trust, Security and Privacy for Pervasive Applications (TSP-09) — *Oct 2009, Macau SAR, China*

Improving Client Security using a Smart Card and Trusted Server
H. Rezaei Ghaleh, M.A. Doustari, International Conference on Security and Management (SAM 2009), WROLDCOMP'09 — *Jul 2009, Las Vegas, US*

A New Approach to Protect the OS from Off-line Attacks Using a Smart Card
H. Rezaei Ghaleh, S. Norouzi, The Third International Conference on Emerging Security Information, Systems and Technologies (Securware 2009) — *Jun 2009, Athens, Greece*

A New Approach for a Secure and Portable OS
H. Rezaei Ghaleh, M.A. Doustari, The Second International Conference on Emerging Security Information, Systems and Technologies (Securware 2008) — *Aug 2008, Cap Esterel, France*

HONORS AND AWARDS

Awarded US Extraordinary Ability Immigration (EB1) — *Jul 2017, US*

Awarded Membership in Iran National Elites Foundation (INEF) — *Sep 2015, Iran*

Winner of 11th Sheikh Bahaei Startups National Competition — *May 2015, Iran*

Winner of 5th Chamran Award in Innovation Competition — *Jun 2014, Iran*

Winner of 10th Sheikh Bahaei Startups National Competition — *May 2014, Iran*

Admission to Science and Technology Park of Tehran University — *Jun 2012, Iran*

Funding Award for MSc Thesis in Trusted Computing — *Feb 2007, Iran*

Admission to National Organization for Development of Exceptional Talents (NODET) — *Jun 1997, Iran*

PATENT

Public Key Appliance (PKA)
Iran Patent, Turn-Key Solution for Public Key Infrastructure — *Jun 2013, Iran*

PERSONAL PROJECTS

BitaWallet
A new secure crypto wallet that supports cryptographic backup, super-wallet/sub-wallet model and secure inquiry.
https://github.com/hosseinpro/bitaWallet (Private Repository)

smartcardPage
A java script library to use smart card in web including an online tool, a local bridge and a java card simulator template.
https://github.com/hosseinpro/smartcardPage

TspSign
Java card implementation for secure smart card signing with time-based digital Signature.
https://github.com/hosseinpro/TspSign