Ehsan Toreini

PhD Student in Cryptography and Security,
Newcastle upon Tyne,
+447456524018,
e.toreini@ncl.ac.uk
LinkedIn | **Home Page** | **Git**

Summary

I am an award-winning (the Economist) security expert with more than 3 years of experience as Web Developer (JavaScript, HTML 5, and Node.js), .Net Framework (C# and VB.Net), Python and Database Administration (MS SQL Server 2005, 2008, MongoDb). My main field of research is web security and authentication protocols. I am always ready to face new challenges, especially if it involves new technologies and ideas.

Education

PHD Doctorate, Computing Science, Newcastle University 2013 - Now

- Thesis Title: "New Advances in Tamper Evident Technologies",
- Conducted a series of research on the importance of inherited properties in authentication protocols. I did my research in two levels:
  - Physical: Proposed a new fast, easy, and reliable method to detect unique texture patterns of a Paper Sheet, also known as Paper Fingerprints, to ensure its authenticity.
  - Cyber: Proposed an authentication protocol in JavaScript and Node.js to ensure integrity and authenticity of a parsed web page source code to the server against any possible forgery especially by Malicious Browser Extensions. I developed the system in vanilla JavaScript, Node.js and Python.
- Led two separate teams to deliver above projects. Both resulted into decent academic papers within planned schedules.

Master's Degree, Software Engineering, Azad University, Mashhad Branch 2007 - 2010

GPA -- 17.30 (out of 20), 3.63 (out of 4.0)
Thesis Title: "A New Approach in Data Clustering using PSO Algorithm"

Bachelor's Degree, Software Engineering, Ferdowsi University of Mashhad 2002 – 2007

GPA -- 15.11 (out of 20), 3.04 (out of 4.0)
Thesis Title: "Mobile Robot Navigation with Genetic Algorithm"

Experience

Project Technician, Newcastle University 2013 - 2016

- Created Responsive web page graphical interface using bootstrap and JavaScript.
- Maintained a PowerPoint plug-in for E-Voting Project which involved basic browsing functionality with Microsoft C# and Office Development Tools.
- Designed and rendered relevant icons in the front-end webpage as well as adjustments in redesigning some HTML elements such as checkboxes and Radio Buttons.

Summer Research Scholarship, School of Computing Science, Newcastle University 2015

- Developed a PowerPoint plug-in in C# to tightly integrate the PowerPoint slides with the back-end e-voting web server for rendering and interacting with Verifiable Classroom Voting System in Newcastle University.

Summer Vocation Studentship, School of Computing Science, Newcastle University 2014

- Project Title: "Security Analysis of Browser Extensions" for £2,000
- Investigated the security impact of browser extensions on web applications.

Skills

Physical Protection

Interested Topics: Physical unclonable Functions in non-electrical objects

Blockchain

E-Voting over Block Chain

Web Security

Browser Security, Integrity Assurance, Protection against Browser Vulnerabilities

Authentication

Interested Topics: Biometric Authentication, E2E Integrity, Designing Authentication Protocols, Identity Protection

Web Programming

Expertise: PHP, Vanilla JavaScript, JQUERY, Node.js, JavaScript OOP, Developing Secure Frameworks, WebCrypto API, WebSockets API, DOM mutation behavior on Client Side

C#

Expertise: OOP Design in .Net Framework, Data-Centric Application Development, Office Development Kit, Xamarin Mobile Development for Android

Python

Expertise: Vanilla Python,

Selenium Browser Automation

Database

Expertise: T-SQL, MS SQL Server Administrator, MySQL Server Administration, No-SQL DB Systems, MongoDB

Machine Learning

Interested Topics: Classification, Neural Networks, Evolutionary Algorithms, Optimization

Signal Processing

Interested Topics: Voice Recognition, Image Processing, Texture Recognition

- Analyzed and implemented an array of attacks to mainstream financial websites by browser Extensions in both Firefox (XUL) and Chrome (WebExtensions).

Analysis of Privacy Leakage in Browsers in Private Mode 2014

Visiting Researcher, Newcastle University Jan 2013 - 2014

- Designed an acoustic attack on historic Enigma by the noises produced while typing.
- Utilized voice recognition techniques to generate an identifier for each keypress, then used machine learning algorithms to identify the pressed key. The results were impressively accurate.

Software Analyst, Mashhad Municipality, Iran 2011 – Nov 2012

- ERP and BPMS Selection Analyst,
- ASMX Web Service development with C#
- Database Administration, Designing and Implementing Stored Procedures in MS SQL Server 2008, Designing the Security Layers

Co-Founder and Developer, Amir Kabir Inc., Iran 2010 - 2012

- Co-Founded a startup company
- Member of a development team to implement and support software for a local chain supermarket in VB.Net and MS SQL Server 2008. I managed to experience PDA development to record the product flow as part of the software package while performing common supermarket supply chain processes. The system implemented successfully for more than a year.

Lecturer in various universities, Iran 2007 - 2012

- Mainly Taught: Web Programming, Technical English and Operating Systems Fundamentals

Founder and Executive chief of "Scientific Translation Committee", Ferdowsi University of Mashhad, Iran 2006

Awards and Key Accomplishments

Featured in the Economist and Wall Street Journal for Paper Fingerprinting Project during my PhD Studies 2017

Cyber Security Case Study Competition, The Economist 2016

- Ranked 3rd in The Kaspersky Lab Cyber Security Case Study Competition Hosted By The Economist Which MBA?

Our Paper: "TouchSignatures: Identification of user touch actions and PINs based on mobile sensor data via JavaScript" got several successes in the past two years: 2015 - Now

- Implemented an attack by using Accelerometer and Gyroscope access of JavaScript and storing in a MongoDB server. Then, we used Neural Networks to recognize victim's PINs and actions.
- **Runner Up in the Best Paper Award**, SRS Group, Newcastle University
- **Acknowledged by Apple, Mozilla, and Chrome**: discovered some critical bugs in mainstream browsers for JavaScript Mobile Sensor Permissions. Firefox and Safari fixed the vulnerability in their latest releases in iOS 9.3 and Firefox 46.
- **Cited by W3C standard draft for deviceorientation API**: Our research paper was cited in W3C sensor standards. They added a security section based on our contributions.
- **Media featured our work including the Guardian, BBC, etc.**

Ranked Less than Top 1% in: 2002 - 2007

- Out of 400,000: National University Entrance Exam, Iran, 2002
- Out of 2000: Azad University Entrance Exam, Iran, 2002
- Out of 10,000: National University MSc Entrance Exam, Iran, 2007
- Out of 500: Azad University MSc Entrance Exam, Iran, 2007

Elected as the Guild Council Member, Engineering Faculty, Ferdowsi University, Iran 2005

- Supervised improvements and general affairs of the public services in the faculty.

CDP

- **Attended Several Workshops during my PhD studies in Newcastle University regarding self-development and professional behavior, 2014 – Now**
- **Member of EPSRC CryptoForma Network, 2013 – 2015:** A network in computer science and mathematics to support the development of formal notations, methods and techniques for modeling and analyzing modern cryptographic protocols.
- **School on Foundations of Security Analysis and Design, 2015**
- **School on Foundations of Security Analysis and Design, 2013**
- **Managing business meetings and presentations on Selection of BPMS system in Mashhad Municipality, Iran, 2011 – 2012**
- **APA workshop on Buffer Overflow Attacks, 2008**
- **Rational Unified Process (RUP) Design with Rational Rose, 2007**
- **Attended Microsoft MCITP SQL Server 2005 Implementation and Maintenance (70-431) Course, 2006**