

Ali Demiröz

Site 59, Üsküdar
34700 Istanbul, Turkey
☎ +90 5366091696
✉ demirozali@gmail.com



Info

Born December 30th, 1985 at Antalya (Turkey) Citizenship Turkish
Blog <http://demirozali.com> Driving B License

Objective

Working in a challenging environment that I can contribute with the best of technical and personal abilities and while doing that, improving myself to overcome further challenges.

Summary of Qualifications

- Possess expertise in OOD&OOP, Java development and Android application development(Developer of Criticker for Android)
- Solid experience in requirement analysis, design, implementation, testing and documentation
- Strong understanding of security concepts including: authentication, authorization, access control, integrity, confidentiality, non-repudiation, auditing, single sign-on, identity management, key management and symmetric/asymmetric cryptography
- Known for problem solving skills those are gained with the help of desire to learn every part of the project, that I work on, top to bottom.
- Able to reverse engineer and comprehend any kind of process no matter which environment it lies in.

Technical Skills

Concepts OOA/OOD(UML, Design Patterns, Refactoring), Test Driven Development, Concurrent Programming, Obfuscation, Reverse Engineering, Socket Programming, Multithreading, Profiling, Mobile Programming

Languages JAVA, C, C++, Python

APIs& Frameworks BouncyCastle, JCA, JAAS, JSSE, Java CertPath, Java PKCS#11, Java OCSP, JavaMail, Log4j, J2EE, Java NIO, Java Concurrency, JNI, Apache MINA, Trove High Performance Collections, Boost C++ Libraries, OpenSSL, QT

Platforms Linux(Ubuntu, CentOS, Redhat), DB MySQL, Derby, Berkeley DB
Windows, Android

Tools Eclipse IDE, IntelliJ IDEA, VS2010, Git, SVN, Jenkins, Sonar, Maven, ClearCase, Wireshark, WinDbg, OllyDbg, IDA(Interactive Disassembler)

Professional Experience

2010-Present **Software Developer & Researcher**, *TUBITAK BILGEM UEKAE*, Kocaeli, Turkey.

The National Research Institute of Electronics and Cryptology (UEKAE), an affiliate of the Scientific and Technological Research Council of Turkey (TUBITAK), produces and applies scientific and technological solutions in the areas of information security, communications and advanced electronics.

Military Message Handling System (MMHS) (Java)

- Developing cross-cutting security modules of the X.500 Directory, LDAP, X.400 Messaging System, SMTP, IMAP, GUI, Management Interfaces and all other MMHS related components
- Implementing required security concepts of the MMHS like simple & strong authentication (PKI), authorization (PMI), access control for the directory, messages and all system resources, signing & encrypting operations, security policy enforcement, audition and alarm system, TLS/SSL, SASL, message security (proof and non-repudiation services, counter-signature etc.), transporting S/MIME objects in X.400, securing X.400 content with S/MIME etc.
- Also working closely with smartcard manufacturers to identify and report anomalies on their PKCS#11 API implementations.
- Current phase: Integration & Testing (in an iterative way)

2009-2010 **Software Developer & System Engineer**, *Labris Networks*, ODTU, Turkey.

Labris produces network solutions like LBRUTM, LBRLOG DDoS Mitigator which provide firewall/VPN, web security, email security, lawful interception and availability protection.

Wireless Guest Authentication (WAUTH) (Python, Django, Bash Scripting)

- Developed authentication mechanism based on IPTables which allows administrator to limit and control their internet service on public networks such as university campus, hotel, cafe...
- Implemented admin and user sides individually with Django framework to provide options like multiple authentications and mobile-payment

Labris UTM Web Security (Java, C++, Bash Scripting)

- Worked on implementing features and resolving bugs on services such as firewall, webfilter, antivirus... These modules are implemented by C++ and bash scripting on server side and JAVA on administration side.

Certification

- Offensive Security Certified Professional-2013

Trainings

- Developing Enterprise Applications with JavaEE, Murat Karakas, Eteration, Gebze - 2013
- Penetration Testing, Dr. Emin Islam Tatli, Daimler TSS, Gebze - 2013
- Concurrent Programming, Talip Ozturk, Hazelcast, Gebze - 2012
- Test Driven Development, Cenk Civici, Prime Technology, Gebze - 2011

Education

2005-2009 **Bachelor's Degree in Computer Engineering**, *Dokuz Eylul University*, Izmir, Turkey.

GPA: 3.11/4.0

Languages

Self-assessment European level CEFR (C2 maximum evaluation)

		Comprehension		Speaking	Writing	
		Listening	Reading	Interaction	Production	
Turkish	Native Language	<i>C2</i>	<i>C2</i>	<i>C2</i>	<i>C2</i>	<i>C2</i>
English	Advanced	<i>C1</i>	<i>C2</i>	<i>B2</i>	<i>B2</i>	<i>B2</i>

Interests and Hobbies

- I like spending time on stackoverflow and learning while trying to answer questions.
- I love doing extreme-sports such as snowboarding and scuba diving. I am holder of PADI-Open Water Diver certificate.
- I enjoy reading fantasy novels.

Extra

Here listed some of my projects, done in my spare times:

- **google-play-crawler:** This project uses Google Android protobuf-wrapped mobile api to list&download&retrieve information from Google Play. This API is not a publicly documented so all protobuf structures are generated by reverse engineering google mobile applications. This project has also a feature to simulate Google's GCM protocol and act as a receiver client for web-initiated download request.
I developed this project to help my friend with his PhD project about android application permissions.
- **Criticker for Android:** Android client for Criticker, a movie recommendation web-site based on user's previous rankings. This mobile application has all capabilities of the site.
- **mitmsocks4j:** Standalone SOCKS proxy with the ability to dump traffic.