

Muhammad Ali Akbar

<http://muhammadakbar.com/>
akbar@securisive.com

About Me

Experienced information security and secure software development consultant and researcher who can perform web and mobile application penetration tests, automated and manual code reviews, software debugging, security testing on cloud based environments, smartphone platforms such as iOS and Android, and develop security-aware web and mobile applications.

Fields of Interest

Software Security & Exploitation, Penetration Testing, Web, Mobile & Cloud Applications Development, Information & Communications Security

Work Experience

— **Senior Security Engineer** Apr 2016 – Present

VMware, San Francisco Bay Area CA

Job Description: VMware virtualizes computing, from the data center to the cloud to mobile devices, to help our customers be more agile, responsive, and profitable. My job functions include providing security advice and expertise to help VMware product teams with Secure Software development throughout products lifecycle, finding new vulnerabilities in VMware products, analyzing externally reported vulnerabilities, developing demonstration exploits, developing vulnerability mitigations and workarounds, act as the technical reviewer for external security communications such as VMware Security Advisories, security response engineering and tools development.

— **Senior Security Consultant** Oct 2014 – Apr 2016

IOActive Inc., Seattle WA

Job Description: IOActive is an industry leading security services firm. My essential job function is to perform security services for IOActive's Global client portfolio. These can include penetration testing, vulnerability assessments, reverse engineering, fuzzing, exploit development, and more. The focus of my work is to provide leadership on mobile penetration testing for Android and iOS platforms. Other important job functions include participation in the business development process, performing research and delivering talks at industry events.

— **Security Consultant** Apr 2013 – Sep 2014

IOActive Ltd., London UK

Job Description: The essential job functions include vulnerability assessments and analysis, penetration testing and source code review of web and mobile applications and platforms, reporting and documentation of all security findings, and travel to customer site locations as required. I have performed comprehensive security assessments of Android ROMs for major smartphone vendors. I have carried out code review and penetration testing of smartphone applications (Android, iPhone, iPad and Kindle Fire apps) and C/Java based web services for some of the Fortune top 50 companies. I have also worked in red team network penetration testing for major service providers on behalf of IOActive.

— **Research Engineer (Mobile App Development Manager)** Mar 2012 – Feb 2013

nexGIN RC, Islamabad

Job Description: Development of Secure SMS and Secure VoIP applications on Android and iPhone. The core task was to help the programmers apply the theory of information security, cryptography and secure development in real world mobile applications. I managed a team of mobile application developers to achieve these tasks. I was also responsible for completing reports and deliverables to meet requirements of the funding agency.

— **Visiting Faculty** Aug 2012 – Dec 2012

National University of Computer & Emerging Sciences, Islamabad

Courses Taught: Data Communication & Networking

— **Mobile Development, Security and Testing Intern** May 2011 – Dec 2011

Cigital, NY

Job Description: Basics of mobile (Android, Blackberry, iPhone/iPad) development. iPhone and iPad applications security. The concentration of my work was on penetration testing of a number of iPhone, iPad applications for some of the Fortune 50 companies. I also worked on image assessment, and some Linux based embedded system pen-testing.

— **Research Engineer (Team Lead)** April 2008 – August 2010

Next Generation Intelligent Networks Research Center (nexGIN RC), Islamabad

Job Description: The aim of this project was to develop an intelligent security framework for IP Multimedia System (IMS) and Next Generation All-IP Networks, to protect infrastructure nodes and subscribers against IMS framework-related vulnerabilities, SIP protocol vulnerabilities, VoIP/ video/ PoC/ Messaging/ Presence/ Conferencing application vulnerabilities; and voice spam, media plane related vulnerabilities.

Education

MS Computer Science (Security). (CGPA: 4.0). Columbia University, New York, NY. 2011.

BE Electrical Engineering. (CGPA: 3.85). National University of Sciences & Technology, Rawalpindi, Pakistan. 2008.

Relevant Courses

- Software Security & Exploitation
- Security Architecture & Engineering
- Network Security
- Intro to Cryptography

Relevant Projects

- Instruction Set Randomization of PE binaries on Windows 7 using Intel's PIN tool.
- Implementation of a secure file repository with access control and encryption. C++ on Linux.
- Implementation, Simulation and attack-based scenario testing of Secure Ad hoc On-demand Distance Vector routing (SAODV) using Network Simulator (NS-2)
- Exploitation of VideoLan Media Player v0.8.6d Stack based buffer overflow vulnerability for shellcode code execution on Windows XP
- Black box Fuzzing against commercial and open source SIP servers and Responsible Disclosure of vulnerabilities to the vendor
- Analyzing OS protections (Windows 7 and Ubuntu 10) against buffer overflows using Case Study of Mozilla Firefox
- Linux OS Kernel development for Android mobile devices
- Linear Algebra made Easy (LAME): A new C like language compiler for linear algebra with built-in support for matrices and matrix operations. Implemented using O'Caml and C++.
<http://www.cs.columbia.edu/~sedwards/classes/2010/w4115-fall/reports/lame.pdf>
- Twenty Five Across: A collaborative crossword puzzle solving game where two or more players work together to solve a crossword puzzle; each user can see the other's modifications to the board in real-time. Implemented using Java Swing and EJB 3.0. <http://code.google.com/p/twenty-five-across/>

Relevant Research Publications

Available at: <http://muhammadakbar.com/publications.php>

- Salman H. Khan and M. Ali Akbar. "*Multi-Factor Authentication on Cloud*", IEEE International Conference on Digital Image Computing: Techniques and Applications (DICTA 2015). Nov, 2015.
- **(Journal Paper)** Salman H. Khan, M. Ali Akbar, et al. "*Secure Biometric Template Generation for Multi-factor Authentication*", Pattern Recognition. Sep, 2014.
- **(Journal Paper)** M. Ali Akbar and Muddassar Farooq. "*Securing SIP based VoIP Infrastructure Against Flooding Attacks and Spam Over IP Telephony*", Knowledge and Information Systems (KAIS). Feb, 2014.
- M. Ali Akbar, Farrukh Shahzad and Muddassar Farooq. "*The Droid Knight: a silent guardian for the Android kernel, hunting for rogue smartphone malware applications*", Virus Bulletin (VB 2013), Berlin, Germany. Oct, 2013.
- M. Ali Akbar and Muddassar Farooq. "*RTP-Miner: A Real-time Security Framework for RTP Fuzzing Attacks*", 20th International Workshop on Network and Operating Systems Support for Digital Audio and Video (NOSSDAV 2010), Amsterdam, Netherlands. June 2010.

- M. Zubair Rafique, M. Ali Akbar and Muddassar Farooq. “*Evaluating DoS Attacks Against SIP-Based VoIP Systems*”, IEEE Global Communications Conference (GLOBECOM 2009), Honolulu, Hawaii USA. Nov, 2009.
- M. Ali Akbar and Muddassar Farooq. “*Application of Evolutionary Algorithms in Detection of SIP based Flooding Attacks*”, Genetic and Evolutionary Computation Conference (GECCO 2009), Montreal, Canada. July 2009.
- M. Ali Akbar, Zeeshan Tariq and Muddassar Farooq. “*A Comparative Study of Anomaly Detection Algorithms for Detection of SIP Flooding in IMS*”, International Conference on Internet Multimedia Services Architecture and Application (IMSAA 2008), Bangalore, India. Dec, 2008. (**First Best Paper Award**)
- M. Ali Akbar and M. Zulkifl Khalid. “*Fuzz-Fortuna: A fuzzified approach to generation of cryptographically secure pseudo-random numbers*”, IEEE International Multitopic Conference (INMIC 2008), Karachi, Pakistan. Dec, 2008.
- M. Ali Akbar, Hamza Bin Tila, M. Zulkifl Khalid and Asim Ajaz. “*Bit Error Rate Improvement using ESPRIT based Beamforming and RAKE receiver*”, 13th IEEE International Multitopic Conference 2009 (INMIC 2009), Islamabad, Pakistan. Dec, 2009.
- M. Zulkifl Khalid, M. Ali Akbar and others. “*Using Telemedicine as an Enabler for Antenatal Care in Pakistan*”, 2nd International Conference on E-Medical System (E-Medisys), Sfax, Tunisia. Oct, 2008.

Awards & Achievements

- Fulbright Grant for Masters in Computer Science at Columbia University NYC, NY. 2010-11.
- First Prize in Research Category at 9th All Pakistan Inter Colleges/Universities Computer Project Exhibition & Competition (COMPPEC 2010), College of E&ME, Rawalpindi, Pakistan. June, 2010.
- First Best Paper Award at International Conference on Internet Multimedia Services Architecture and Application (IMSAA 2008), Bangalore, India. Dec, 2008.
- Development of Proposal for ‘*Remote Patient Monitoring System for Rural Areas with Focus on Antenatal Care*’, Awarded a Research Grant of \$0.25 million from National ICT R&D Fund, Ministry of IT, Pakistan in 2007-08. This project was carried out at nexGIN RC, Islamabad, inline with the UNDP’s Millennium Development Goals (MDGs) to reduce Maternal Mortality Ratio (MMR) and Infant Mortality Ratio (IMR) in Pakistan. 2008.
- Various Merit based Academic Scholarships & distinction shields throughout the academic career

Technical Skills

- *Reverse Engineering*: GDB, OllyDbg, IDA Pro, Hex Workshop, Java decompilers, Mach-executables disassembly, IDA scripts
- *Mobile/Web Apps for Pen-testing*: Jailbreaking tools (absinthe, redsnow, evasion), Web traffic analysis (Charles proxy, Burp, Wireshark, libpcap), Android related tools (androguard, Android SDK tools, smali/baksmali, apktool, dex2jar, JD-GUI, JEB), Objective-C hooks and Cydia tweaks development, Keychain decryption tools, Custom bash scripts for pentest automation
- *VoIP Servers*: OpenIMScore, OpenSER, OpenSBC, MjServer
- *VoIP attack tools*: Spitter, SIPVicious, SipSAK, PROTOS, SIPp, osip SIP parsing library, Custom SIP firewall using netfilterqueue & IPTables
- *Sniffers and Pen-test Tools*: Nmap, Metasploit Framework, ZAP, BackTrack 5
- *Network Simulators*: Network Simulator (NS-2), OMNET++
- *Statistical Analysis & AI Tools*: MATLAB, Mathematica, Weka, KEEL
- *Virtualization Tools*: VMWare, Virtual Box, QEMU
- *Development Environments*: Microsoft Visual Studio, Eclipse, Netbeans
- *Programming Languages*: C, C++, Objective-C, Java, Python, Perl, PHP, O’Camel
- *Operating Systems*: Linux (Fedora, Ubuntu, CentOS), Microsoft Windows (7, XP), Mac OS