Vikash Kumar Jha
Finland +358(0)403690870, vikash.aalto@gmail.com

SUMMARY

Highly motivated problem solver, with thorough understanding of programming constructs, structures and algorithms, secure programming and through understanding of cryptographic algorithms and its implementation.

- 4 years of software industry experience.
- MS and BS in computer science.
- Erasmus Mundus traineeship for Master thesis
- Finalist in code4bill programming contest.
- Awarded twice the certificate of appreciation by NOKIA for the work.

TECHNICAL SUMMARY

Languages: C, C++, JAVA, Python, C#, x86 Assembler, PHP, Perl R, MATLAB
UI Frameworks :Qt, wxPython, PyQt
Operating Systems: Linux, Embedded Linux, Windows 9X / XP / NT, UNIX, z/OS.
Database: Oracle, MySQL, SQL
Mobile Development Platforms: Android, S60
Web Servers/Frameworks: Apache, Django, Vaadin
Protocols: CAN, TCP/IP, MPLS, SOAP, 802.11, Mobile IP, ad-hoc Network Routing.
Tools Familiarity: MS Visual Studio, Eclipse, Ftrace, GDB, Wireshark, VirtualBox
Technical areas: Design of Algorithms, Information security, Secure programming, Systems programming, Kernel programming, Web technologies

EDUCATION

University of Vaasa Business studies **(Results excepted on 15th May 2013)**

Aalto University School of Science and Technology, Finland, **Master of Science** in Computer Science. (Formerly Helsinki University of Technology) May 2012

Visveswaraiah Technological University, Karnataka, India, **Bachelor of Engineering** in Computer Science. July 2006

WORK EXPERIENCE

Wapice Oy, Finland Software Engineer Jun-2012- May -2013

- Worked with embedded systems and desktop applications
- Worked on embedded development for Wapice remote management device(WRM)
- Developed internal combustion engine simulator with Python
- Involved in resolution of security related issues for WRM device.
- Developed various mathematical and business critical software for large industrial systems.

Laboratory of Algorithm and Cryptology and Security Research Intern Jun-2011- Dec 2011

- Master thesis position for "Cryptanalysis of lightweight block cipher"

Helsinki Institute of Information Technology

- Design and implementation of a system to securely collect and transfer audio and video content
- Designed and implemented the security and privacy mechanism for the content of server
- Customized Ubuntu kernel to suit needs of the designed system.
- Implemented stream cipher and performed the comparative study of the various video and text encryption algorithms.
- Wrote and deployed init scripts.
- Developed a web interface to control various functionalities of the system.

NOKIA R&D (Bangalore, India) R&D Engineer Oct 2007 – Aug 2009

- Worked on SyncML protocol and FOTA (firmware over the air), developed fast algorithms for update
- Was completely responsible for FOTA application , actively involved in three market releases
- Developed a module to make the GPRS connection wait for more than transport layer timeout
- Developed phone-tracker as a part of innovation road show in the organization.
- Found a security flaw in UI notification in SyncML protocol and proposed a solution for it.
- Good understanding of Software Development Life Cycle and general Quality Processes.

IBM (Kolkata, India) Application programmer Aug 2006- Sept 2007

- Developed software for managing insurance products
- Automated many of the manual batch processes.
- Designed an application to measure disk usage and prepare a report of redundancy in storage.
- Successfully debugged many of the legacy errors.

RECOGNITIONS

- Awarded twice the certificate of appreciation by NOKIA for the work.
- Finalist in code4bill 2006 (top 2% of programmers, nationwide).
- IEEE Student Chapter C programming contest winner for 2 consecutive years
- IEEE Student Chapter Debugging contest winner
- IEEE Student Chapter 8086 assembler programming contest winner
- Second prize in C/C++ programming contest in an inter-collegiate technical fest (BROWSE, SIT, Tumkur) .
- Department level programming contest winner for 2 consecutive years

ACADEMIC PROJECTS

- Design and implementation of a distributed data repository based on Shamir's perfect secrecy. Proposed the mechanisms to make the system fault-tolerant.
- Implemented a web server to transfer pages using Differential Compression scheme, extended it for file transfer in a distributed systems and analysed the performance.
- Implemented a server and client based on remote differential compression protocol.
- Designed and implemented secure e-Voting system with the help of Blind RSA signature.
- Working on a concept to break CAPTCHA with the uses of pattern recognition technique(k-nearest neighbours algorithm (k-NN))
- Implemented wireless LAN driver based on 802.11a protocol
- Demonstration of buffer overflow attack and sandbox prevention
- Implemented a simple malware analyser in python
- Implemented Web Server Application and Kernel module, Web Proxy Server application.
- Designed and implemented a two-pass 8086 assembler.
- Designed and implemented a graphics editor.
- NAT Kernel module, Transparent Web Cache Kernel module, MPLS tunnel simulation & analysis.
- Implemented Reactor pattern, Chat server and client using basic java concurrency primitives.
- Implemented some crypto-algorithms as Cube-HASH , Trivium, RSA,DES,AES,MD5,El-Gmal and Threefish.

ACADEMIC SEMINARS

- Presented a seminar and paper on "BitLocker encryption: its vulnerabilities and alternative solution". Proposed to divide the key in memory to make the brute force attack difficult on the key.
- Presented a paper on "Mobile Peer-to-Peer", it analyzed and summarized various issues that need to be addressed to make it popular.

PUBLICATION

- Presented a poster on Survey of Mobile Phone Security in NordSec -2010