Curriculum Vitae

author:
Pavol Lupták

Personal information

Name:	Pavol Lupták
Address:	Štefana Moyzesa 1571/47, Ružomberok, 034 01, Slovak Republic
Mobil Phone (SK):	+421 905 400542
Mobil Phone (CZ):	+421 910 800955
Email:	pavol dot luptak at nethemba dot com
Date of birth:	May 15th 1979
Place of birth:	Ružomberok, Slovak Republic
Driving license:	Full

Education

- 1997-2001

  Faculty of Electrical Engineering and Information Technology, The Slovak University of Technology, Bratislava, Bachelor's degree of Software Engineering - BSc. thesis: "Input-output characteristics of impulse neurons" (in Slovak language)

- 2001-2004

  Faculty of Electrical Engineering, Czech Technical University in Prague, MSc degree in Computer Science - MSc. thesis: "Generating security description of applications for security frameworks.", short presentation

Security Certification

- April 2006

  Certified Information Systems Security Professional (CISSP) certification, Frankfurt/Germany

- May 2007

  Certified Ethical Hacker (CEH) certification

- 2008

  Preparing for Computer Hacking Forensic Investigator (CHFI) certification

- May 2008

  I became OWASP (Open Web Application Security Project) Leader for Slovakia

I am willing and able to gain any other security-related certification (CISA, GCIA, GSEC, ..)

Languages

- English

  Fluent both writing and speaking (TOEFL certificate).

- Spanish

  Very good (practical experiences from Mexico, Peru, Chile and Spain).

- Slovak

  The mother language.

Work Experience

- 1999 - 2000 S&T, Bratislava

  Contract work for Slovak Telecom, the distributed shut-downing UPS system for HP-UX development (in C/perl).

- 2000 - August 2001 UI42 s.r.o, Bratislava

  Securing and administration of the most visited job portal in Slovakia www.profesia.sk , the intranet & internet company www.ui42.com, a lot of client's servers (www.pcrevue.sk, www.limba.sk, ..), experience in creating security audits and consulting.

- September 2001 - December 2001 LMC, Prague

  Development and maintenance of the complex monitoring system based on Netsaint for www.jobs.cz

- January 2002 - January 2008 ICZ, Prague

  Security Consultant focused on securing and administration of central servers of The University of Economics, Prague, Czech National Radio, Czech post services, network & server security, creating large penetration tests and security audits for Czech government institutions, almost all Czech mobile operators, American corporations and other international customers.

- February 2008 Nethemba s.r.o, Bratislava

  Owner, CTO and Lead Security Consultant of the security-based company Nethemba s.r.o. focused on comprehensive penetration tests and security audits, proposing ultra secure solutions, VOIP solutions, clusters, consulting & training in security areas.

Consultancy Experience

- A lot of large penetration tests for international online-casinos, Czech banks, Slovak insurance companies, American corporations, etc.
- Design and implementation of the load balanced and high availability cluster (11 servers) for the biggest job portal in Slovakia for Profesia s.r.o. (owned by Daily Mail and General Trust plc - DMGT).
- Design and implementation of the load balanced and high availability cluster (6 servers) for the biggest "reservation of accommodation" portal in Slovakia for Limba s.r.o.
- Design and implementation of the load balanced and high availability cluster (4 servers) for the biggest economic & business portal in Slovakia
- Design and implementation of the antispam and antivirus mail clusters for UI42 s.r.o., Profesia s.r.o, Faculty of Philosophy - Comenius University in Bratislava

Academical Experience

- 2000 - 2002 Kmit, Bratislava

  Securing and administration of the large collegiate network on the college dormitory ŠD-Mladosť for students of FEI-STU.

- 2001 - Strahov Network

Administration of the central SMTP/DNS/DHCP server on Sillicon Hill, the college dormitory of Czech Technical University.

- 2001 - Together with Michal Medvecký and Antonín Král we founded an international security conference OpenWeekend

Lecturing and papers

I have 8 years of experience in lecturing at various security conferences

- Prielom (blackhat magazine), February 2000

  Paper (in Slovak language) about HEAP & BSS overflows

- Prielom (blackhat magazine), September 2000

  Paper (in Slovak language) about Exploiting binaries through PLT (procedure linkage table) and GOT (global offset table)

- Security of data in information systems seminar in Kongresove centrum, Prague, 24-25.4.2001

  Common vulnerabilities and practical hacking demonstration

- Openweekend security conference, Prague, September 2001

  Practical hacking demonstration, presentation about Linux advanced packet filtering

- Hysteria blackhat session, Bratislava, July 2003

  Attacks and defence on physical/link layer of 802.11 (in Slovak language)

- Hysteria blackhat session, Bratislava, April 2004

  Presentation about NSA SELinux and my proposed Security Description of Applications for Security Framework

- Openweekend security conference, Prague, October 2004

  NSA Security-enhanced Linux

- Openweekend security conference, Prague, October 2005

  802.11 Wireless Attacks

- CVTSS (Czech organization for telecommunication networks), Prague, November, 2005

  802.11 Wireless Attacks & Detection/Defense

- Network Security Congress, Prague, April, 2007

  New web applications attacks & protection

Security auditing & penetration testing skills

I have 9 years of experience in creating security audits and penetration tests.

- Deep knowledge of OSSTMM - Open Source Security Testing Methodology Manual, OWASP testing guide, ISO 17799 and ISO 27001
- Knowledge of many security scanners and exploiting frameworks
- 10 years of experience in manual seeking of buffer/heap overflows, race conditions, web application vulnerabilities (SQL injection, XSS, CSRF, directory traversal, ..) and other serious vulnerabilities
- Network / local auditing of all operating systems
- Wireless network auditing
- Web application testing (deep knowledge of Burpsuite, WebScarab, Paros, SpikeProxy,

CAL9000) according to the OWASP Testing Guide

- Auditing of mobile phones & PDAs
- Source code audit (PHP, perl, C, dot net, java)
- Experience with social engineering (simulating of phishing attacks)

Programming languages

I have 13 years of experience and knowledge in (user-space, application, server, network) programming in various languages (including low-level assembler programming), bug-tracing and code auditing.

- **ASM (x86, Alpha, 6502)** - writing shell codes, reverse engineering, own 3D engine
- **C** - my second native language, the most large projects (e.g.TTT talker) I wrote in pure C, also have experience with security source code audit
- **C++** - my bachelor thesis was written in C++, experience with QT graphics library
- **XML/XSLT** - my master thesis was written in XSLT language
- **Perl** - I coded the distributed shut-downing UPS system for Slovak Telecom
- **PHP, Javascript, Java** - security source code audit
- **PL/SQL, Lisp, Prolog, Visual Basic, Pascal** - many academical projects I wrote in these languages
- **Script languages (bash, awk, sed, ..)** - daily usage

Technologies

I have 11 years experience in Unix systems (Linux, all BSD systems, Solaris, HP/UX, AIX, ..), detailed knowledge of TCP/IP networking, load balancing, fail-over clusters, web servers and various other technologies

- **Ultra secure OS (NSA SELinux, RSBAC, Medusa DS9, GRSecurity** - I have a deep knowledge of NSA SELinux (I used it in my master thesis as the main security framework)
- **Firewalling** - iptables, ipfw, ipf, Cisco/PIX IOS, Apache mod_security, kernun application firewall, Zorp Apllication Gateway
- **VPNs** - OpenVPN, CiscoVPN, various IPSEC implementations
- **PKIs** - OpenCA, NewPKI, PyCA, SimpleCA, IDX-PKI
- **IDS** - snort, prelude
- **Honeypots** - honey pot project, sebek, also I wrote own patches to SSH to monitor the attackers
- **LVS HA clusters** - lvs, ldirectord, heartbeat, keepalived - I implemented many production clusters
- **Various databases (MySQL, PostgreSQL, Oracle)** - experience with MySQL cluster
- **LDAP** - I use OpenLDAP as a main backend for large-scale mail clusters
- **Antispam/antivirus mail clusters** - postfix, amavisd-new, clamav, spamassassin, pyzor, razor, dccproc - I designed and implemented many big mail clusters (up to 20000 users)
- **IP Telephony** - I wrote my own patches to Asterisk SVN trunk and proposed large call centers
- **Virtual machine technologies** - I have experience with KVM, XEN and VMWare
- **Latex, XML DocBook** - I wrote my bachelor thesis in Latex and my master thesis in XML