



ROMÁN MEDINA-HEIGL HERNÁNDEZ

E-Mail: roman@rs-labs.com

PERSONAL INFO

Current Home:

28022 – Madrid - **Spain**

Nationality: Spanish

Military Service: Exempt

Marital Status: Married

Birth year: 1975

KNOWLEDGE

- *Programming:* C, Asm (68k, x86), Shell (Bash), HTML, JavaScript, PHP, Perl, SQL, Basic.
- *Systems:* Linux (Debian, SuSE, RedHat, Fedora, Ubuntu), Solaris, Tru64, Cisco IOS, MS-{DOS, Windows 9x / NT / 2k / XP / 2k3}, Amiga OS.
- *Databases:* Oracle, MySQL, PostgreSQL, Microsoft SQL Server, SQLite.
- *Networks:* Thorough knowledge of TCP/IP-based networks and protocols, Unix Programming; QoS, Ethernet, Wireless. Routers ADSL and RDSI ; Switches, Hubs. PoP. VPN. LDAP architecture. Proxies. *Experienced in Internet since 1994.*
- *Security:* Cryptography, Firewalls, Reverse proxies, Pen-Testing – Ethical hacking, Vulnerability Analysis and Exploit Development, Hardening, Forensics, IDS / IPS, Identity Management (IM), WiFi, High Availability and Load Balancing. Content filtering. Antispam. *Demonstrable experience: 15 years.*
- *Applications:* Office 97/2000/XP/2003, Spice, Matlab, VMware. Web design.
- *Languages:* Spanish (native). English (high level in technical, read and written). Basics of German.

EDUCATION AND TRAINING

- Grade (BSc + MSc equivalent) in *Telecommunication Engineering*, speciality in *Telematics*. University of Seville, Spain.
- Graduation final project entitled “Security analysis, optimization and enhancement of a PHP-MySQL based web portal” (orig.: “Análisis de seguridad, optimización y mejora de un portal web basado en PHP y MySQL”), obtaining an A grade. It covers aspects of software engineering and computer security.
- CISSP (Certified Information Systems Security Professional). (ISC)². December 2006.
- Course "Sun ONE Directory Proxy Server". Sun Microsystems. April 2004.
- Course "IPv6". Eurocomercial I&C. June 2004.
- Course: “Oracle Administration I”. AFI S.L. November 2004.
- Check Point Certification: “CPCS – Pointsec 6.1” (End-point security). June 2008.
- Course: “Project Management: Computer Projects” (PMAseores, 28 PDU’s). October 2010.
- Skybox Certified Assurance Engineer (SCAE). Skybox Security. December 2010.
- Skybox Certified Risk Management Engineer (SCRE). Skybox Security. December 2010.
- Certification: “ITIL v3 Foundation”. APMG-International. July 2011.

WORK EXPERIENCE

- Sep/2010 – Current Repsol YPF, S.A.
 INFORMATION SECURITY ENGINEER.
- In the Security Engineering area new projects are forged, cutting edge products are tested and secure architectures are designed. Tasks:
 - Innovation. Proposing projects and ideas which constitute a substantial improvement in security.
 - Managing security projects and associated resources.
 - Technical support as a security specialist.
 - Manager of Antivirus & Vulnerabilities group.

- Jun/2007 – Aug/2010 IECISA (Informática El Corte Inglés, S.A.)
SECURITY ARCHITECT / CONSULTANT.
- In the “CEX (Expert Center) of Telecommunications, Security and C4I Engineering”, taking active part in different projects:
 - Security Auditing / Assessment and Penetration-Testing in public & private sector (eg: Ministerio de Defensa [DoD alike], Unión Fenosa [utility], etc).
 - Consultancy services and Design of Security Architecture of Low-voltage Tele-control system for Endesa [utility].
 - End-point security: Authentication / encryption of USB devices, hard disks, etc. Technologies: Pointsec (Check Point) and Zitralia.
 - Solutions for Digital Signature, Data Protection and Digital Identity. Public Key Infrastructure (PKI). Technologies: Safelayer.
 - Vulnerability analysis in web applications, secure web proxies as well as other projects in Security Engineering group at Repsol.
- Mar/2010 – Current UOC (Universitat Oberta de Catalunya)
CONSULTING TEACHER IN COMPUTER SECURITY MSC.
- Teaching “Operating Systems Security” subject.
- Feb/2004 – May/2007 Telefónica Móviles España (employed by AFI, S.L.)
PROJECT MANAGER / SECURITY ENGINEER.
- Performing R&D, Consulting and Project Management tasks at “Gerencia de Seguridad de Redes y Servicios” of Telefónica Móviles. Related projects:
 - Development, implementation and operation of “Threat analysis and communication Area” (Operational Security Management)
 - Design and implementation of an advanced reverse proxy (published in SourceForge with GNU license).
 - Authentication (TACACS+, Radius, LDAP, LDAP Proxy, etc.) and Identity Management platform.
 - Software High availability (VRRP on Linux, Heartbeat / Mon on Solaris).
 - Proxy SNMP design and implementation (Linux / Netfilter / Iptables).
 - Analysis of pen-testing tools and security hardware.
 - Users management (Metadirectory / Novell DirXML).
 - Evaluation, modification and installation of a Linux “open-source” FTP Proxy (jftpgw).
 - Evaluation and debugging of a LDAP Proxy (SunONE).
- May/2003 – Feb/2004 Optenet, S.A.
HEAD OF SYSTEMS AREA / SYSTEMS ENGINEER.
- In charge of Systems area. Deployments scheduling.
 - Integration of content filtering technologies developed by Optenet over different architectures (Solaris, Linux, AIX, Novell and Windows systems; appliances such as NetApp NetCache, BlueCoat and Cisco PIX) in several environments: end user, server and ISP.
 - Handling of proxies: Squid, MS Proxy, ISA Server, Novell Border Manager.
 - Participation in Cisco’s official beta-testing program performing tests on ICAP protocol over the future version 5.1 of “Application and Content Networking System Software (ACNS)” for Cisco Content Engine.
 - Technical Support / Help desk (level 2 & 3).
- Sep/2002 – Dec/2002 Ubeda Virtual, S.L.
SECURITY AND NEW TECHNOLOGIES CONSULTANT.
- Custom-designed services and infrastructure improvement plans related to networks, security and Internet.
- Oct/2000 – Jul/2002 Batmap, S.A.
CHIEF SECURITY OFFICER / SECURITY SYSTEMS ADMINISTRATOR.

- Security officer. Development of security policies, configuration of firewalls, VPN, Antivirus, etc.
- Manager of technical support department.
- Network administrator. Configuration of routers, switches (VLAN, trunking, etc.), load balancers (Radware WSD).
- Design, deployment, configuration and support of Madrid PoP (Point of Presence), composed by an HA-based and load balanced architecture.
- Deployment and configuration of heterogeneous Unix / Windows systems. Unix services: Web (Apache), DNS (Bind), Mail (Sendmail / Qpopper), FTP (Proftpd, BSD ftpd), Proxy (Squid), Apps (Tomcat, Cocoon), Database (MySQL), E-Commerce (Apache + SSL + PHP), Archive repository SMB (Samba), IRC (Ircu), IDS (Snort). Windows services: IIS, Serv-U.

PUBLICATIONS

Articles in “@rroba” spanish magazine:

- “Caso real y práctico de hacking”, September 2002, n. 60, pp. 84-87.
- “Izhal: una comunidad dedicada al hacking”, October 2002, n. 61, pp. 16-19.
- “Hack21: diario de un participante”, May 2003, n. 68, pp. 16-19.
- “El regreso de los Boinas Negras. Solución al II reto de hacking web”, November 2003, n. 74, pp. 22-26.

Articles in digital format [<http://www.rs-labs.com/papers/>]:

- “Tácticas de guerra en el IRC”, September 1999.
- “Boinas Negras: una solución al concurso”, February 2003.
- “Solución al reto de análisis forense de RedIRIS”, December 2003.
- “Solución al III Reto Hacking - El lado del mal”, May 2007.
- “Blind LDAP Injection: Solución al Reto Hacking #4 - El lado del mal”, September 2007
- “Solución al Reto Hacking #5 - El lado del mal”, January 2008.
- “Solución al problema #15 - Codegate 2009 (Prequals)”, March 2009.
- “Solución a la prueba #3 del Reto Panda”, April 2009.
- “Solución al Reto Hacking #10 - El lado del mal”, September, 2009.
- “La historia de Rooted CON”, May, 2010.
- “SbD Wargame 2011 write-up”, February, 2011.

Conferences:

- Microsoft TechNet. “Cómo realizar un test de intrusión a una aplicación web”. 4/Oct/2007. Getafe (Madrid).

Proyectos:

- [RewritingProxyTME](#) –HTTP Reverse Proxy. March 2005.

ACTIVITIES

- **Organizer** of security contest: ”Web challenges from RootedCON'2010 CTF” (international) [September 2010].
- **Founding Member** of “Rooted CON” Security Congress (<http://www.rootedcon.es/>) and co-organizer of CTF contest [March 2010].
- **Winner** in Computer Security contests: “Swiss Cyber Storm 3 - CarGame Challenge” (team “int3pids”, international) [May 2011], “SbD Wargame 2011” (team “int3pids”, international) [January 2011], “CTF Pre-Ekoparty (5th edition)” [August 2009] (international), “Panda challenge” [May 2009] (national) and “Commemorative Challenge for 10th Anniversary of “una-día” by Hispasec Sistemas” [November 2008] (national). Third position in “CTF-prequals” in “Codegate 2010” (the second most prestigious international competition in the world) [March 2010].
- **Taken part** in numerous challenges, wargames and contests related to computer security. Successfully passed: Hackerslab, NGSEC’s Game #1 & #2, Boinas Negras #1 & #2, Mod-X, Izhal, Arcanum, Cyberarmy, Hack21 #2, Yoire, Blindsec #1 and all challenges from Informatica64. Participation in forensics challenge organized by RedIRIS.

- **Exploit** coding (eg: “IIS 5.0 WebDAV -ntdll.dll-“, “Linux Kernel 2.6.x PRCTL Core Dump Handling”, “ISC DHCPd 2.x DoS”, “Postfix local root”). Discovery and research of new **vulnerabilities** (eg: “SquirrelMail” [BID 10439 / CAN-2004-0520]). Web applications **hacking** and defense (ModSecurity). Tasks automation (**scripting**). Design, implementation and management of a secure ISP (Hosting & Remote Backup Services). Graphic intros/demos programming in Asm-68k for the Amiga-scene. Knowledge of **reverse engineering** (cracking). Deep understanding of IRC protocol. Development of a management application for agricultural analysis laboratories (in production since 10+ years ago).

OTHER INTERESTING DATA

Driving licence. Own vehicle. Analysis and documentation skills. Autodidact. My own R&D Site:
<http://www.rs-labs.com>.