
Ismael Briones Vilar

Personal/Contact Information

- **Phone:** +0034 654 751 182
- **Email:** ismak@inkatel.com
ismak@uninet.edu
ismael.briones@gmail.com
- **Web:** <http://www.inkatel.com>
- **Birth Date:** April 12, 1977

Education

Technical Engineer of Telecommunications (Electronic Systems)
University of Valencia (Spain)

Languages

Spanish: Native

English: Medium-High level

Professional Experience

- **Panda Security** (Bilbao-Spain)

November 2003 - Present

As a Malware Researcher I'm involved in vulnerability analysis, Windows/Unix security and malware research.

Malware dissassembling is one of my daily works and I'm involved with HoneyPot research, development and research of new proactive techniques to fight and detect malware, automatization for malware analysis, research of new Rootkits techniques and anti-rootkits technologies.

I daily work with tools like SoftIce, OllyDBG, IdaPro, Hiew and WinDBG and the following programming languages: C, C++, Perl, Python

Actually I'm involved in automatic malware classification. I'm developing several system, using graph and entropy theory, to automatically classify malware and clusterize malware.

My daily work involves:

- Malware analysis and reverse engineering (WinDBG, SoftIce, IdaPro)
- Protocols and network security analysis: TCP/IP, DHCP, DNS, SMTP, SNMP, IPsec, SSL, VLAN, VPN, Sniffers. Security topologies. IDS/IPS. Firewalls
- Vulnerability assessment
- HoneyPots development
- Operating System security: Unix/Linux and Windows

I'm particularly interested in security, malware research and Unix/Linux system administration:

- Reverse engineering
- Vulnerability assessment

- Packers
- Fuzzers
- Always interested in system administration, as well as close interaction with disassembling and debugging techniques for malware research
- **El Mundo** (Madrid-Spain)
September 2000 - November 2003

I was involved in maintenance the systems and network infrastructure of the Internet site of this spanish journal.

The high availability was one of our first goal so we deployed and manage a farm of about 25 linux systems

I was involved in the following tasks:

- Unix/Linux administration (load balancing and high availability), system backups, monitoring systems, web servers (apache), SMTP (qmail), SNMP, DHCP
- Network Security: IDS (Snort), Firewall, VPN's
- Perl, Python, PHP and bash scripting development
- Routers Cisco (3660, 7206 VXR)
- Alteon AceDirector switches / WebOS (AD3 y AD4)
- SAN Network Storage (NetApp F710 y F810)
- **Amutis Telecomunications, S.A.** (Valencia)
January 2000 - September 2000
I was a Network and System Administrator of Linux (Red Hat, Debian), Solaris 7 and OpenBSD systems
Perl, C/C++, PHP, Python, bash
Security Consultancy: ISO 17799 Security Standard

Security Consultant at:

- Telefonica Spain
- Oncology Research Center of Valencia
- **AIMPLAS (Technological Institute of Plastics (Valencia))**
October 1999 - January 2000
6 months research fellowship
ISO 17799 (Security Policies)
Network and System Administrator (Linux: Red Hat, Debian, Solaris 7 e Irix)
Perl, C/C++, PHP, Python, bash

Personal Projects

Personal projects are for me a way to improve my skills in Perl/Python and web development, Unix/Linux administration, malware research, vulnerability analysis and master new tools/technologies before applying them to work projects.

- **WildBoar:** Free Online Network Traffic Scan
<http://wildboar.inkatel.com>

Skills

- **Vulnerabilities Research**

- **Skype File URI Security Bypass Code Execution Vulnerability**
[Idefense Advisory](http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=711): <http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=711>
[Skype advisory](http://www.skype.com/security/skype-sb-2008-003.html): <http://www.skype.com/security/skype-sb-2008-003.html>
- **Trend Micro SSAPI Long Path Buffer Overflow Vulnerability**
[Idefense Advisory](http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=586): <http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=586>
[Technical advisory](http://www.inkatel.com/index.php/2007/09/16/trend-micro-ssapi-long-path-buffer-overflow-vulnerability/): <http://www.inkatel.com/index.php/2007/09/16/trend-micro-ssapi-long-path-buffer-overflow-vulnerability/>
- **NOD32 Antivirus Long Path Name Stack Overflow Vulnerabilities**
[Bugtraq Advisory](http://www.securityfocus.com/archive/1/469300): <http://www.securityfocus.com/archive/1/469300>
[Advisory](http://www.inkatel.com/wp-content/uploads/2007/05/Advisory.txt): <http://www.inkatel.com/wp-content/uploads/2007/05/Advisory.txt>
- **Oracle 8.1.5 CHOWN Path Environment Variable Vulnerability**
[Bugtraq Advisory](http://www.securityfocus.com/bid/3129): <http://www.securityfocus.com/bid/3129>
 Oracle Official Advisories
http://otn.oracle.com/deploy/security/pdf/dbsmp_alert.pdf
- **Vulnerability in 3Com® OfficeConnect® Remote 812 ADSL Router**
[Bugtraq Advisory](http://www.securityfocus.com/bid/4841): <http://www.securityfocus.com/bid/4841>
- **Intrusion test in an International Bank environment (BBVA)**
 Danger SQL Injection vulnerability detected
- **Intrusion test in an International Bank environment (La Caixa)**
 Danger Web access to Database Customer Information

- **Technical Knowledge**

- Unix (Solaris, Linux, OpenBSD)
- Windows 2003, XP, 2000, NT
- C, C++
- Perl, PHP, Python, Ruby, shellsript
- MySQL, PostgreSQL, Oracle
- DNS(Bind 8,9), Apache Web Server, Mail servers (qmail, postfix)
- Firewalls (CheckPoint FireWall-1, Iptables)
- Policy Routing
- TCP/IP, QoS, Ipsec, IPv6, DNS, DHCP, SNMP, SNTTP
- Snort IDS (Intrusion Detection System)
- Load balance and High disponibility systems (24/7/365). Alteon AceDirector switches
- Cisco Routers (3660, 7206 VXR)
- SAN Network Storage

Certifications

- **SANS Institute**

- **SANS GIAC Reverse Engineering Malware (GREM)**

- SANS Mastering Packet Analysis (SSP-MPA)

Publications and meetings

- Virus Bulletin
 - Speaker at Virus Bulletin Conference 2008 (Ottawa)
Graph, entropy and grid computing: automatic comparison of malware
Paper: <http://www.inkatel.com/ismael/papers/vb/2008/IsmaelBriones-VB2008.pdf>
Slides http://www.inkatel.com/ismael/papers/vb/2008/IsmaelBrionesVB2008_slides.pdf
- UniNet
 - Member of UniNET (University network of Services IRC and Telematics)
<http://www.uninet.edu>
 - I Unix Meeting (Umeet2000) Organizing Committee member
<http://umet.uninet.edu>
 - I Unix Meeting (Umeet2000) speaker
Secure Programming (Buffer Overflows)
 - II Unix Meeting (Umeet2001) Organizing Committee member
El Mundo, Spanish Journal
 - II Unix Meeting (Umeet2001) speaker
Arp Spoofing: Spying in switched networks
Doc: PDF, PS
 - III Unix Meeting (Umeet2002) Organizing Committee member
 - III Unix Meeting (Umeet2002) speaker
An Introduction to User-Mode-Linux
Doc: PDF, PS
 - I IPV6+Firewall+Encrypt+VPN Meeting (6FEVU) Organizing Committee member
<http://www.uninet.edu/6fevu/>
 - I Computer Security Meeting (InfoSec 2002) Organizing Committee member
<http://infosec.uninet.edu/>
 - II Computer Security Meeting (InfoSec 2002) Organizing Committee member and speaker
<http://infosec.uninet.edu/>
- Arroba Spanish Computer Security Journal
 - N° 44: Arp Spoofing
<http://www.inkatel.com/new/textos/Arroba/arp-spoofing.pdf>
 - N° 66: Sniffing in Network Wireless
<http://www.megamultimedia.com/arroba/bd/noticiaweb.asp?nrev=66&idnot=tema3>
 - N° 67: Hack Zones y Wargames
<http://www.megamultimedia.com/arroba/bd/noticiaweb.asp?nrev=67&idnot=tema3>
 - N° 70: Portscanning (July 2003)
<http://www.megamultimedia.com/arroba/bd/noticiaweb.asp?nrev=70&idnot=tema3>

- **Nº 71: DoS, DDOS, DRDOS (August 2003)**
<http://www.megamultimedia.com/arroba/bd/noticiaweb.asp?nrev=71&idnot=tema1>
- **Nº 72: Linux Privilege Escalation (September 2003)**
<http://www.megamultimedia.com/arroba/bd/noticiaweb.asp?nrev=72&idnot=tema3>
- **Nº 73: Network Data Interception: Sniffers (October 2003)**
<http://www.megamultimedia.com/arroba/bd/noticiaweb.asp?nrev=73&idnot=tema2>
- **El Mundo Spanish Journal**
 - Campus Magazine (El Mundo): [UniNet: Una 'médula espinal' para las universidades](#)
([UniNet: Spinal Marrow for the Universities](#))