

Damiano Bolzoni

PERSONAL DETAILS

Name: Damiano Bolzoni

Date and Place of Birth: 19/01/1981 - Torino (Italy)

Address: PO Box 217 7500AE - Enschede, The Netherlands

Mobile: +31629008724

e-Mail: damiano.bolzoni@utwente.nl

PRACTICAL EXPERIENCE

- July 2005 – present: PhD student at the University of Twente, Netherlands, in the Distributed and Embedded Systems group. Topics:
 - Intrusion Detection Systems
 - Risk Management

- February 2003 - July 2004: KPMG SpA (Treviso head office), Information Risk Management division:
 - Penetration test
 - Risk assessment
 - IT Audit (COBIT and BS7799)
 - Creation, evaluation and analysis of business-level and technical policies (in particular Minimum Security Baseline)
 - Design and development of Intrusion Detection Systems
 - Hardening
 - Development of web applications on J2EE platform

- January 2002 - : consultant activity as freelancer

EDUCATION

- March 2005: MSC in Computer Science (110/110 cum laude) - Ca' Foscari University in Venice - Computer Science Department - Advisor Ch.mo Prof. Alessandro Roncato – “Intrusion Detection Systems: tecniche per la classificazione non supervisionata del traffico di rete” (Intrusion Detection Systems: unsupervised classification techniques of network traffic)

- July 2002: BSC in Computer Science (102/110) received from Ca' Foscari University in Venice - Computer Science Department - Advisor Ch.mo Prof. Francesco Dalla Libera – “Uno strumento di controllo di attacchi Denial Of Service” (A tool for controlling Denial of Service attacks)

COMPUTER SKILLS

- O.S.: Microsoft Windows 98/ME/2000/XP/2003, Sun Solaris, GNU/Linux Mandrake/RedHat/Debian
- Networking: TCP/IP, HTTP/FTP/SMTP/POP/SSL/SNMP
- Perimetric systems: CISCO router, IpTables firewall, IDS (Snort and some proprietary systems)
- Hacking: Nmap, Ettercap, Nessus, Shadow Security Scan, Internet Security Scanner, Solar Winds, Essential Network Tools, Retina Vulnerability Scanner, Ethereal, TcpDump

- Programming Languages: C/C++, C#, Java (Enterprise Edition), Visual Basic
- Scripting Languages: PHP, ASP, Javascript
- DBMS: Microsoft SQL Server, MySQL, Postgres, Firebird (Interbase), Oracle 10i
- Application/Web Server: Microsoft Internet Information Server, Apache HTTP Server, Apache Tomcat
- Development: Microsoft Visual Studio .NET, Borland JBuilder, NetBeans, Sun ONE
- Kernel Linux and Windows (device driver) Programming

LIST OF PUBLICATIONS

- D. Bolzoni, B. Crispo and S. Etalle. **ATLANTIDES: An Architecture for Alert Verification in Network Intrusion Detection Systems**. In LISA '07: PROC. 21ST LARGE INSTALLATION SYSTEM ADMINISTRATION CONFERENCE. USENIX Association, 2007.
- X. Su, D. Bolzoni and P. van Eck. **Understanding and Specifying Information Security Needs to Support the Delivery of High Quality Security Services**. In SECURWARE '07: PROC. INTERNATIONAL CONFERENCE ON EMERGING SECURITY INFORMATION, SYSTEMS AND TECHNOLOGIES. IEEE Computer Society, 2007.
- E. Zambon, D. Bolzoni, S. Etalle and M. Salvato. **A model supporting Business Continuity auditing & planning in Information Systems**. In ICGD&BC '07: PROC. INTERNATIONAL CONFERENCE ON GLOBAL DEFENSE AND BUSINESS CONTINUITY. IEEE Computer Society, 2007.
- E. Zambon, D. Bolzoni, S. Etalle and M. Salvato. **Model-Based Mitigation of Availability Risks**. In BDIM '07: PROC. 2ND INTERNATIONAL WORKSHOP ON BUSINESS-DRIVEN IT MANAGEMENT (in conjunction with IM '07), pages 75-83. IEEE Computer Society, 2007.
- X. Su, D. Bolzoni and P. van Eck. **A Business Goal Driven Approach for Understanding and Specifying Information Security Requirements**. In EMMSAD '06: PROC. 11TH INTERNATIONAL WORKSHOP ON EXPLORING MODELING METHODS IN SYSTEMS ANALYSIS AND DESIGN (in conjunction with CAiSE '06), pages 465-472. Presses Universitaires de Namur, 2006.
- D. Bolzoni, E. Zambon, S. Etalle and P. Hartel. **POSEIDON: a 2-tier Anomaly-based Network Intrusion Detection System**. In IWIA '06: PROC. 4TH IEEE INTERNATIONAL WORKSHOP ON INFORMATION ASSURANCE, pages 144-156. IEEE Computer Society, 2006.

SIGNIFICANT WORKING ACTIVITIES

- Development of web applications both on J2EE (framework Jakarta Struts) and on .NET platforms, with backend on DBMSs (SQL Server, MySQL, PostgreSQL and Oracle)
- Development of monitoring software for net activities
- Development and installation of intrusion detection systems (Snort and other products) and log correlation
- Hardening of Windows 2000 and Sun Solaris systems for protection of judicial sensitive information

TALKS

- Webbit 2004:
 - Minimum Security Baseline (URL <http://www.webb.it/event/eventview/3117/>)
 - Return On Investment of Security Assessments (URL <http://www.webb.it/event/eventview/3115/>)

- BlackHat USA 2006 & BlackHat Europe 2007
 - NIDS: False Positive Reduction Through Anomaly Detection

- BlackHat USA 2007
 - Sphinx: An Anomaly-based Web Intrusion Detection System