

## CURRICULUM VITAE

---

Francesco Bergadano

born in Turin on 12/8/1963

**Office address:**

Dept. Of Computer Science, University of Turin, Corso Svizzera 185, 10149 Turin, Italy  
Tel. (39) 011 6706743 Fax (39) 011 751603 email: Francesco.Bergadano@di.unito.it

---

### STUDIES

1991: **Ph.D., Computer Science**, (Universities of Turin and Milan)  
1986: **Degree ("Laurea"), Computer Science** (University of Turin)

### UNIVERSITY POSITIONS

1995-pres: **Full Professor**, University of Turin  
1992-1995: **Associate Professor**, Universities of Catania and Messina  
1990-1992: **Researcher**, University of Turin  
1989: **Visiting Professor**, George Mason University (USA)  
1984-1985: **System Manager**, Polytechnic University of Torino

### CONSULTING AND RESEARCH PROJECTS

**2003-2005: Research contract with Telecom Italia S.p.a.: anonymous and auditable system administration protocol, group signatures**  
**2000-pres: ICT and Organization Consulting for a number of Italian public administrations**  
**2002-2005: IT Security Consulting with Webegg S.p.a. (now NTT data)**  
**2001: Security Consulting & Education for the Italian Military Police (Carabinieri - Piemonte)**  
**2000: PKI system (Municipality of Biella)**  
**1996-1999: PM for the the Italian partner (EU - IV Framework)**  
**1992-1995: PM for the the Italian partner (ESPRIT III) - BRA 6020**  
**1992-1995: PM for the the Italian partner (ESPRIT III) - BRA 6156**  
**1998-2003: PM, Certification Authority (University of Turin)**  
**1998-pres: Teaching for the Officers of the Italian Army (Security)**  
**1988-1989: IT Consulting (Sogesta/ENI, Urbino)**  
**1986-1987: IT Consulting (SIA, Turin)**

## ORGANIZATION AND MANAGEMENT

Francesco Bergadano has worked with technical, research and development, sales and management professionals of different nationalities, in different contexts, both in academia and in the private sector. His relevant experiences include:

**Management of the Security Research Group** of the Dept. Of Computer Science (Univ. Turin) 1995-present:

organization of the activities of a group of seven researchers and a variable number of short term collaborators and Ph.D. Students: definition of objectives, lines of research, projects, grants, expenses and investments;

**Organization of the Master Program in Web Technology and Security** (School of Management, University of Turin) 2000-2002, 2004, 2005: project, economic plan, choice of teachers, relation with the sponsors);

**Organization of the Master Program in Cloud Computing** (Faculty of Science, University of Turin) 2009-present: project, economic plan, choice of teachers);

**Founder of the first spin-off company of the University of Turin (Certimter srl), founded in 2003.**

**President of the Computer Science Degree Board '95-'98 and '09-present:** teaching organization for about 50 professors;

**Member of the Evaluation Commission** for selecting teachers, researchers and technical staff in Italy, France and the USA;

**Organization and Chairing of Conferences:** ECML 1994 (Catania), Wtforum 2001, 2002, 2003, 2004 (Turin), with an average of 200 participants each.

## TECHNICAL COMPETENCE

Security and Privacy; Digital Signatures and PKI, Electronic Commerce; Reliability, Security and Analysis of Web-based Systems; Computer Networks; Multicast Security; Computer forensics, Log Analytics; Data Analysis and Mining.

## COMMUNICATION SKILLS

Francesco Bergadano has developed excellent communication and public speaking abilities in the context of IT projects and presentations:

- more than 90 scientific publications, 2 books, 2 italian patents, 1 US patent and 4 patent applications;
- more than 30 university courses since 1989 - since 1995 mainly in computer networks and security;
- presentations and tutorials in more than 60 international conferences and in a number of IT presentations and workshops for the private sector;
- presentations in the context of IT and security consulting.

He knows well English and French, and has taught courses and made technical presentations in both languages.

### RECENT PUBLICATIONS (JOURNALS)

R. Anderson, F. Bergadano, B. Crispo, J. Lee, C. Manifavas and R. Needham. "A New Family of Authentication Protocols", *Operating Systems Review*, 32(4):9-20, October 1998.

F. Bergadano, B. Crispo and G. Ruffo.  
"High dictionary compression with proactive password checking", *ACM Transactions on Information and System Security (TISSEC)*, pages 3-25, November 1998.

A. Beimel, F. Bergadano, N.H. Bshouty, E. Kushilevitz, and S. Varricchio.  
*Learning Functions Represented as Multiplicity Automata*, *Journal of the ACM*, 47(3):506-530, May 2000.

F. Bergadano, D. Gunetti and C. Picardi.  
*User Authentication through Keystroke Dynamics*.  
*ACM Transactions on Information and System Security (ACM TISSEC)*, 5(4), 2002

F. Bergadano, B. Crispo, D. Cavagnino.  
*Individual Authentication in Multiparty Communications*.  
*Computer & Security Journal*, Elsevier Science, vol. 21 n. 8, November 2002, pp.719-735.

F. Bergadano, D. Gunetti and C. Picardi.  
*Identity Verification through Dynamic Keystroke Analysis*.  
*Journal of Intelligent Data Analysis*, Volume 7(5), IOS press, 2003.

F. Bergadano and D. Cavagnino  
*Dealing with packet loss in the Interactive Chained Stream Authentication protocol*, *Computers and Security (Elsevier)*.  
Volume/Issue 24/2, pages 139-146, 2005

P. Dal Checco, F. Bergadano, D. Cavagnino, A. Nesta, M. Miraglia, P. Zaccone  
*Secure Logging for Irrefutable Administration*  
*Int. Journal of Network Security*, Vol. 4, No. 3, pp. 340-347, may 2007.

A. Basso, F. Bergadano, D. Cavagnino, V. Pomponiu and A. Vernone  
*A Novel Block-based Watermarking Scheme Using SVD Transform*  
*MDPI Algorithms 2009*, Volume 2(1), Page 46-75.

### RECENT PUBLICATIONS (CONFERENCES and CHAPTERS IN BOOKS)

F. Bergadano, B. Crispo, M. Eccettuato.  
"Secure WWW Transactions using standard HTTP and Java applets",  
*Third USENIX Workshop on Electronic Commerce*, pages 109-120,  
Boston, Massachusetts, August 1998.

F. Bergadano, D. Cavagnino, B. Crispo.  
"Issues in Multicast Security",

Cambridge Int. Workshop on Security Protocols, Cambridge, UK, 1999,  
Lecture Notes in Computer Science, LNCS 1796 pp 121-144 (Springer).

F. Bergadano, D. Cavagnino, B. Crispo.  
"Individual Single Source Authentication on the MBONE",  
IEEE Int. Conf. on Multimedia and Expo,  
pages 541-544, New York, July 2000.

F. Bergadano, D. Cavagnino, B. Crispo.  
"Chained Stream Authentication",  
Proc. of Selected Areas in Cryptography 2000,  
D. R. Stinson, S. Tavares Eds., LNCS 2012,  
pages 144-157, 14-15 August, Waterloo, Ontario, Canada.

F. Bergadano, D. Cavagnino, P. A. Nesta,  
Certification of Web Access Statistics.  
Pubblicato in "E-work and E-commerce", Vol.1, pp. 326-332,  
IOS Press (2001).

F. Bergadano, D. Cavagnino, L. Egidi,  
Partially sighted signatures on large documents, pp 373-380,  
INC 2002 Conference, Plymouth, UK, July 2002.

F. Bergadano, D. Cavagnino, P. A. Nesta,  
"Server-based Access Verification",  
International Workshop on Electronic Government and Commerce: Design,  
Modeling, Analysis and Security  
(EGCDMAS 2004), Setúbal, Portugal, August 2004.

A. Basso, F. Bergadano, I. Coradazzi, P. Dal Checco,  
"Lightweight Security for Internet Polls",  
International Workshop on Electronic Government and Commerce: Design,  
Modeling, Analysis and Security  
(EGCDMAS 2004), Setúbal, Portugal, August 2004.

G. Ruffo and F. Bergadano, "EnFilter: a Password Enforcement and Filter  
Tool based on Pattern Recognition Techniques", in Proc. ICIAP 2005 -  
Special Session in "Pattern Recognition in Computer Security",  
LNCS 3617, Springer Verlag, pp.75--82.

F. Bergadano, D. Cavagnino, P. Dal Checco, G. Falzetta, M. V. Garzelli,  
"A Partial Brute Force Attack on AES using GRID computing resources",  
Proceedings of the International Conference on Advances in the  
Internet, Processing, Systems, and Interdisciplinary research,  
VIPSI-2006 Bled, Slovenia, ISBN: 86-7466-117-3

Beimel, Bergadano, Bshouty,  
Kushilevitz, Varricchio: "Learning automata"  
in Encyclopedia of Algorithms, Kao, Ming Yang (Ed.)  
2008, ISBN: 978-0-387-30770-1

A. Basso, F. Bergadano.  
"Anti-bot strategies based on human interactive proofs".  
Handbook of Information and Communication Security,  
P. Stavroulakis and M. Stamp (Eds.), pp 273-291, Springer 2010.

R. Accornero, D. Rispoli, F. Bergadano,  
"Privacy-enhanced Identity via Browser Extensions and Linking Services"  
Proc. 5th Int. Conf. on Network and System Security  
Milan, Italy, September 2011

### PATENTS

Metodo e Apparecchio per la Verifica dell'Identita` Dichiarata da un  
Utilizzatore di una Risorsa Controllata, Mediante Digitazione su una  
Tastiera Alfanumerica. Italian Patent 1.311.278 of 12 mar 2002

Method and Apparatus for the Verification of Server Access Logs and  
Statistics, [US Patent 6,574,627](#) del 3 giugno 2003.

Sistema e Metodo per la verifica delle richieste HTTP  
Italian Patent 1320716 of 10/12/2003.

Appareillage et Methode pour l'Autentification du Trafic sur le Web,  
French Patent Application 0002347 of 24.02.2000 (allowed August 2004).