

Francisco Corella

Pomcor
2977 Barnard Street
San Diego, CA 92110
fcorella@pomcor.com
+1.619.255.7486

Education

PhD, Computer Science

University of Cambridge, 1990

MS, Computer Engineering

Stanford University, 1982

Ingénieur Civil des Mines

Ecole N.S. des Mines de Paris, 1977

Professional Experience

Pomian & Corella, LLC

(An Oregon company, d.b.a Pomcor)

Co-founder and CTO

July 2011 to present

Identified inadequacies of TLS for use in DoD tactical networks and devised a comprehensive package of TLS optimizations to address them.

January 2011 to present (joint work with Karen Lewison)

Found a security flaw in OAuth, which was acknowledged by the IETF OAuth working group. Presented a poster on PKAuth at the NIST Symposium on Identity and Trust on the Internet. Proposed a method for meeting some of the privacy goals of the National Strategy for Trusted Identities in Cyberspace (NSTIC) via double-redirection, and presented it at the 12th Internet Identity Workshop. Made a presentation on NSTIC, privacy and social login at the W3C workshop on Identity in the Browser. Participated in the two workshops organized by NSTIC. Proposed a high-privacy architecture for the NSTIC ecosystem. Responded to the NSTIC Notice of Inquiry; later, the head of the NSTIC National Program Office called a session at the 13th Internet Identity workshop to discuss the issues raised in the response. Responded to the call for comments on the Cybersecurity Green Paper. Published a series of blog posts on privacy-enhancing technologies that led to an invitation to participate in the panel on Privacy in the Identification Domain at the forthcoming NIST workshop on Privacy-Enhancing Cryptography. Led a session on deployment and usability of cryptographic credentials at the 13th Internet Identity workshop.

July 2010 to December 2010

Led an NSF SBIR Phase I research project, Collaborative Information Retrieval from Multiple Real-Time Sources, as principal investigator. In joint work with Karen Lewison: invented a method for browsing real-time search results ranked by a balanced combination of recency and relevance, and filed a patent application; conceived PKAuth, a secure alternative to OAuth that does not require prior registration of the relying party with the identity provider.

August 2008 to June 2010

Created Noflail Search, a multisearch engine available at <http://noflail.com/> that features a cross-engine search history that lets the user browse multiple result sets at once, and cooperative responses to queries that produce zero results. Filed patent applications on those features.

January 2003 to August 2008

Developed a Web application with multi-user instances administered by end users for collaborative file sharing. Filed two patent applications on methods to improve password security in a user-administered Web application multi-user instance. Filed a patent application on a method for protecting a Web application against attacks through browser-rendered shared files.

Pomian and Corella, Inc

(A Pennsylvania corporation)

Co-founder and CEO

January 2001 to December 2003

Conceived and developed a Web application for teleradiology.

HP

Engineer, then Engineer-Scientist

December 1997 to December 2000: Cryptography and Internet security.

Proposed a means of providing client-certificate identity protection in TLS by reordering the handshake messages. Discovered a security flaw in the implementation of IPsec on HP-UX servers. Improved the implementation of the HP-UX IPsec stack, doubling performance on the wire for DES encryption. Successfully championed the creation of a hardware cryptographic accelerator for HP-UX servers. Filed 5 patent applications related to cryptography, all now granted. Taught a course on cryptography and Internet security at CSU Sacramento as part of a HP community outreach and recruitment initiative.

June 1995 to December 1997: Hardware architecture and formal methods.

Made contributions to the I2O specification as HP representative in I2O SIG working groups. Contributed to the PCI-X specification. Identified an ordering problem in the PCI 2.1 specification and proposed a solution that was used in HP-UX platforms. Invented a method for maintaining ordering of DMA reads with respect to PIO writes without sacrificing performance that was used in HP-UX platforms, and was co-inventor of a related patent application, now granted. Found and corrected an IO ordering problem in the joint HP-Intel IA64 architecture. Developed a methodology for verifying liveness by formal proof in the early stages of the design of a computer system, and used it to find deadlock scenarios in an HP-UX platform.

Led the specification of the memory ordering model of PA-RISC 2.0 (included as Appendix G in G. Kane, *PA-RISC 2.0 Architecture*, Prentice Hall, 1996.)

IBM

Research staff member, T. J. Watson Research Center

December 1987 to June 1995

Invented the concept of an Expertsheet, a spreadsheet paradigm for implementing decision support systems, and applied for a patent related to it, now granted.

Developed a formal memory model for the PowerPC architecture. Pioneered the use of abstract types and uninterpreted function symbols in automated hardware verification, to allow verification of RTL designs in time and space independent of the width of the data path. In collaboration with the University of Montreal, invented the concept of a Multiway Decision Graph (MDG), a generalization of a Binary Decision Diagram that incorporates abstract types and uninterpreted functions symbols, and initiated the development of the MDG package. Conceived and implemented a general purpose interactive theorem prover based on ZF/HOL, and used it to prove the correctness of an asynchronous sequential circuit using an axiomatization of time as a continuum.

Schlumberger

Member of Technical Staff, Palo Alto Research Center

May 1984 to November 1987

Conceived the formal system ZF/HOL to address difficulties presented by ZF set theory for mechanical theorem proving, and proved that it is a conservative extension of ZF. Pioneered the study of context-sensitive substitution as a derived rule of inference. Implemented a proof-checker for HOL and used it to verify the correctness of digital circuits. Built a prototype information retrieval system that pioneered intensional responses.

Symantec

Program Manager, Database Management Systems

March 1982 to May 1984

Conceived an object-oriented data model and innovative data structures for disk storage. Led the design and development of a memory-based DBMS and a disk-based DBMS, both supporting a natural language interface.

Stanford University

Research and Teaching Assistant

June 1981 to March 1982

Pioneered the study of cooperative answering for Boolean queries and implemented a cooperative answering algorithm on the bibliographic database of the Research Libraries Group. Assisted Prof. Gio Wiederhold in teaching the course *File and Database Systems*.

CEFISA

(A Spanish company) Electrical Engineer

January 1978 to September 1980

Designed industrial automation algorithms for the Moroccan Office Chérifien des Phosphates. Supervised the installation of the electrical infrastructure of a cement storage plant in the port of Lagos, Nigeria.

US Patents Granted

8,046,827 Access control of interaction context of application

7,975,292 Secure password reset for application

7,340,600 Authorization infrastructure based on public key cryptography (assigned to HP)

7,269,726 Lightweight public key infrastructure employing unsigned certificates (assigned to HP)

7,010,683 Public key validation service (assigned to HP)

6,802,002 Method and apparatus for providing field confidentiality in digital certificates (assigned to HP)

6,763,459 Lightweight public key infrastructure employing disposable certificates (assigned to HP)

6,157,977 Bus bridge and method for ordering read and write operations in a write posting system (assigned to HP)

5,835,683 System and method for authoring an expert system (assigned to IBM)

US Patents Pending

Provisional: Browsing Real Time Search Results

20100100836 Facilitating Browsing of Result Sets

20100100563 Method of Computing a Cooperative Answer to a Zero-Result Query through a High Latency API

20090313261 Protecting a Web Application Against Attacks through Shared Files

Publications and Presentations

Panel participant: *Privacy in the Identification Domain*. At the forthcoming NIST workshop on Privacy-Enhancing Cryptography, December 8-9, 2011.

F. Corella, K. P. Lewison. Deployment and Usability of Cryptographic Credentials. Presentation at the 13th Internet Identity Workshop, Mountain View, October 2011.

F. Corella, K. P. Lewison. NSTIC, Privacy and Social Login. Presentation at the World Wide Web Consortium's workshop on Identity in the Browser, Mountain View, May 2011.

F. Corella, K. P. Lewison. Meeting the Privacy Goals of NSTIC in the Short Term. Presentation at the 12th Internet Identity Workshop, Mountain View, May 2011.

F. Corella, K. P. Lewison. PKAuth: A Social Login Protocol for Unregistered Applications. Poster presentation at the 10th NIST Symposium on Identity and Trust on the Internet. April 2011.

F. Corella, K. P. Lewison. *Searching the Web More Effectively with Multiple Simultaneous Queries*. Presentation at the 2009 Search Engine Meeting, Boston, MA.

F. Corella, K. P. Lewison, M. Talukder. *A teleradiology architecture featuring security and high performance*. Journal of Digital Imaging 2002; 15: 214-215.

F. Corella: *A Fast Implementation of DES and Triple-DES on PA-RISC 2.0*. In Proceedings of the Usenix Workshop on Industrial Experiences with System Software (WIESS) 2000: 83-84.

F. Corella. *Structured certificates and their applications to distributed systems security*. Presented at RSA Conference 2000 (San Jose, Calif., Jan. 16-20).

Y. Xu, E. Cerny, X. Song, F. Corella, O. A. Mohamed. *Model Checking for First-Order Temporal Logic using Multiway Decision Graphs*. In A. Hu and M. Vardi (eds.), Computer Aided Verification, LNCS 1427, Springer Verlag, 1998, pp. 219--231.

E. Cerny, F. Corella, M. Langevin, X. Song, S. Tahar, Z. Zhou. *Verification with Abstract State Machines Using MDGs*. Formal Hardware Verification 1997, pp. 79-113.

F. Corella, R. Shaw, C. Zhang. *A formal proof of absence of deadlock for any acyclic network of PCI buses*. In Computer Hardware Description Languages (CHDL) 1997, pp. 134--156.

F. Corella. *The World of I/O: A Rich Application Area for Formal Methods*. Invited presentation at Computer Hardware Description Languages (CHDL) 1997, Toledo, Spain.

F. Corella. *A proof of absence of deadlock for the Stretch CEC*. in Proceedings of the (employees-only) 1997 Hewlett-Packard Design Technology Conference.

F. Corella, Z. Zhou, X. Song, M. Langevin, E. Cerny. *Multiway decision graphs for automated hardware verification*. Formal Methods in System Design: An International Journal, 10(1):7--46, Feb. 1997.

Panel Chair: *Is there a Crisis in Hardware Verification?* At the IFIP Conference on Correct Hardware Design and Verification Methods (CHARME) 1997, Montreal.

Z. Zhou, X. Song, S. Tahar, E. Cerny, F. Corella, M. Langevin. *Formal Verification of the Island Tunnel Controller using Multiway Decision Graphs*. In Formal Methods in Computer-Aided Design, LNCS 1166, Springer Verlag, 1996, pp. 233--246.

K. D. Anon, N. Boulterice, E. Cerny, F. Corella, M. Langevin, X. Song, S. Tahar, Y. Xu, Z. Zhou. *MDG Tools for the Verification of RTL Designs*. In Proceedings of Computer Aided Verification, CAV 1996, pp. 433-436.

Francisco Corella and Michelle Kim. *Expertsheets: A Spreadsheet Paradigm for Authoring Expert Systems*. In Proceedings of Software Engineering and Knowledge Engineering (SEKE) 1996, pp. 25-31.

F. Corella and R. Odineal. *A strategy for verifying coherence and ordering of memory systems with multiple Merced buses*. Confidential paper in Proceedings of the (employees-only) 1996 Hewlett-Packard Design Technology Conference.

F. Corella, M. Langevin, E. Cerny, Z. Zhou, X. Song. *State enumeration with abstract descriptions of state machines*. In Proceedings of the IFIP Conference on Correct Hardware Design and Verification Methods (CHARME) 1995, pp. 146-160.

Z. Zhou, X. Song, F. Corella, E. Cerny, M. Langevin: *Partitioning transition relations efficiently and automatically*. Great Lakes Symposium on VLSI 1995, pp. 106-111.

F. Corella, *Automated Verification of Behavioral Equivalence for Microprocessors*, IEEE Transactions on Computers, v.43 n.1, p.115-117, January 1994.

F. Corella. *Formal Verification of Digital Circuits*. White paper and invited presentation at the NIST Workshop on Dependable and Renewable Industrial Systems, Palo Alto, August 1994.

F. Corella. *Automated High-level Verification Against Clocked Algorithmic Specifications*. In Proceedings of Computer Hardware Description Languages (CHDL) 1993: 147-154.

F. Corella: *What Holds in a Context?* J. Autom. Reasoning 10(1): 79-93 (1993).

F. Corella. *Semantic Retrieval and Levels of Abstraction*. In Proceedings of Expert Database Workshop 1984, pp. 91-114.

F. Corella, S. J. Kaplan, G. Wiederhold, L. Yesil: *Cooperative Responses to Boolean Queries*. In Proceedings of the First International Conference on Data Engineering (ICDE) 1984, pp. 77-85.

Panel participant: *The impact of natural language on database design and implementation*, S. J. Kaplan, chair. At the First Conference on Applied Natural Language Processing, Santa Monica, California, 1983.

C. Gaudeau, M. Boiron, J. Thouvenot, F. Corella. *Squelettisation et anamorphose dans l'étude de la déformation des structures; application à l'étude de la motricité*

gastrique. In Proceedings of Reconnaissance des Formes et Intelligence Artificielle, Toulouse, France, 1979.

Professional Activities

Member of the *Association for Computing Machinery* (ACM).

Member of the IFIP Working Group 10.5, *Design and Engineering of Electronic Systems*, active from 1993 to 1997.

Member of the program committee of *Formal Methods in Computer-Aided Design* (FMCAD) 1998.

Member of the program committee of *Correct Hardware Design and Verification Methods* (CHARME) 1997.

Member of the program committee of *Computer Hardware Description Languages* (CHDL) 1997 and 1995.

Languages

Trilingual English-French-Spanish. Knowledge of Italian and German.