Aldo Cassola

Web: http://www.aldocassola.com
Email: aldocassola@gmail.com

Career Summary

Computer Scientist with over 15 years of experience in industry and higher education. Highly proficient in C, C++, Java, Python, network and application security, cryptography, privacy, systems administration, research, and teaching. I am passionate about building secure and efficient services that protect assets, preserve privacy and scale to millions of users.

Education

Northeastern University, Boston, MA

Ph.D. in Computer Science — May 2015
Advisor: Prof. Guevara Noubir

Master of Science in Computer Science– 3.83/4.0 GPA — May 2008

Universidad San Francisco de Quito, Quito, Ecuador

Bachelor of Science in Computer Science– 3.47/4.0 GPA — June 2001

Industry Experience

D2Hawkeye, Waltham, Ma

Assistant Service Architect – Internship — May 2008 – July 2008

- Pioneered the company's new custom software services department through the design of a new small-business financial management system
- Improved the quality and integration of the company's health services management application

Universidad San Francisco de Quito, Quito, Ecuador

Computer Systems Administrator — August 2002 – June 2006

- Slashed spam email reaching user inboxes by 95% through the reengineering of the university's email infrastructure in Exim/Linux
- Achieved full online asset administration for the University through deployment of local and fault-tolerant DNS, email, and web infrastructure

ITABSA (Phillip Morris Intl), Quito, Ecuador

Intern developer, user support specialist — September 2001 – July 2002

- Improved employee satisfaction with enterprise systems by as much as 15% through the implementation of new financial and payroll management systems
- Modernized raw material processing software through a PLC reimplementation and Visual Basic front-end

Métodos Avanzados de Sistemas, Quito, Ecuador

Technical support intern — July 2000 – December 2000

- Performed upgrade and implementation of security software for headquarters' network, and user support

Higher Education Experience

Universidad San Francisco de Quito

Computer Science Department Chair — May 2016 – December 2017

- Improved instructor/student ratio in the department by 50% by restructuring hiring processes
- Readied department for local and international accreditation through reimplementation of existing tutoring, alumni relations, and industry contacts

- Achieved consistent growth rate of 6% per semester during difficult economic period by increasing faculty involvement in promotional events at high-schools and open houses
- Improved graduation rate to 53% through work with Student Counseling and effective class offerings

Universidad San Francisco de Quito, Ecuador

Full Professor of Computer Science August 2015 – December 2017

- Improved the quality for the Network Security course through restructuring of the curriculum and building a new fully-managed virtual lab from the ground up
- Increased student satisfaction from 68% to over 80% through teaching of 15 undergraduate computer science courses including Network Security, C++ programming, Data Mining, Computer Organization and Architecture, C# project development.
- Served as advisor to seven student capstone projects whose contribution range from an increase of over 100% in library energy efficiency to a reimplementation of university IT services with OpenStack virtual machines.

Northeastern University, Boston, MA

Teaching Assistant September 2008 – May 2015

- Offloaded 100% of computing and monitoring requirements for the network security laboratory through an infrastructure reimplementation that combined student virtual machines and streamlined the hosted server components
- Redesigned the Network Security course for distance learning at Northeastern's satellite campuses, reviewing, updating, and creating recordings of class material
- Spearheaded the use of small mote devices for the teaching of wireless networks in the department through the integration of small mote projects into the coursework

Universidad San Francisco de Quito, Ecuador

Instructor August 2002 – June 2006

- Instructed over 200 students in Ecuador's first and largest Linux, UNIX System Administration, and Java Training Program

San Francisco de Quito Community College, Quito, Ecuador

- Teaching of basic Computer Science programming courses in Java and Visual Basic

Projects

- **Dissertation on Privacy-Aware Residential Network Systems:** My thesis work is focused on designing secure and privacy-protecting services and authentication systems in the context of residential networks. This work focuses on three aspects: the feasibility and impact of home-based privacy services, the state of current Wi-Fi solutions illustrated by our previous work, and the proposal of the new *SafEdge Gate* system. *SafEdge* is an anonymous authentication scheme for Wi-Fi that allows an Access Point (AP) operator to authenticate authorized users while providing demonstrable anonymity guarantees to them. In practice, a client connecting to a SafEdge AP either knows a) the AP operator cannot distinguish the client's identity from the set of authorized AP users or b) the provider is cheating.
- **OpenInfrastructure**: OpenInfrastructure is a research platform running on residential Wi-Fi routers, for which I am a major contributor, and designer. Our deployment of 30 home Access Points over Boston, Houston, and San Francisco urban areas has served as basis to characterize residential network properties and as hotbed for research on wireless service provisioning and privacy. We have collected over 115 million network usage records since February 2011, and 1.3TB of home broadband traffic over the first six months, and hosted several research projects within our group.
- **WPA-Enterprise Security**: Despite being a trusted mechanism for Wi-Fi access control and authentication, the way its components operate and flaws in implementation and UI design allow for a multi-layer and stealthy attack that results in AP impersonation and credential hijacking. As a lead of this project we identified, implemented, and empirically evaluated effectiveness of the attack. Our

prototype using off-the-shelf hardware can attack nodes up to 1200ft away, and our experiments show it is virtually undetectable by administrators and users.

- **SNEAP:** The Social Network Enabled Authentication Method project is a Wi-Fi access method that allows secure traffic and authentication to occur against Online Social Network (OSN) credentials. SNEAP is conceived as an alternative to Open Wi-Fi hotspots, but can also be deployed in home environments and enterprise settings. We implemented SNEAP for Linux and Windows running over FreeRADIUS, using Facebook as the OSN backend. This implementation precedes the existence of the more recent Facebook Wi-Fi project, and allows clients to have WPA-grade protection for their traffic over our SNEAP-enabled hotspots.
- **TREKS:** Time-Reversed Extraction and Key Scheduling is a novel technique to transmit Spread Spectrum secrets between nodes, and in addition it provides protection against jammers. This mechanism resolves a fundamental problem in the wireless transmission realm, in which a secret is required to protect communication against jamming, but such protection is not available for the secret. Improved, implemented, and evaluated novel jamming-resistant Direct-Sequence Spread Spectrum scheme without pre-shared keys on GPU hardware. Our scheme is four orders of magnitude faster than previous solutions to the problem, and allows for real-time data communication at rates of Megabits per second. In addition, it provides jamming protection comparable to that of Direct Sequence Spread Spectrum.
- **GSM Search and Rescue:** Researched effectiveness of Portable Base Stations for GSM networks for Search and Rescue missions. Our prototype uses an adjustable mechanical dynamic antenna array to deduce the location of potential targets.

Publications

- **Authenticating Privately Over Public Wi-Fi Hotspots**, Aldo Cassola, Erik-Oliver Blass, Guevara Noubir, (submitted) *ACM Conference on Computer and Communications Security 2015*
- **A practical, targeted, and stealthy attack against WPA-Enterprise authentication,** Aldo Cassola, William Robertson, Engin Kirda, and Guevara Noubir, in *Proceedings of NDSS, vol. 2013*
- **Efficient Spread Spectrum Communications without Pre-Shared Secrets.** Aldo Cassola, Tao Jin, Guevara Noubir, Bishal Thapa, in *IEEE Transactions on Mobile Computing,* TMC, 2012
- **Spread spectrum communication without any pre-shared secret,** Aldo Cassola, Tao Jin, Guevara Noubir, Bishal Thapa (*technical report*)
- **SNEAP: A Social Network-Enabled EAP Method: No More Open Hotspots,** Aldo Cassola, Tao Jin, Harsh Kumar, Guevara Noubir, and Kamal Sharma, in *Proceedings of NSDI Demo*, Boston, 2011
- **Search and Rescue Mission using Cell Phones and Mobile Base Stations,** Aldo Cassola, Bishal Thapa, in Northeastern Annual Research Expo, Boston, MA. April 2010

Service

- Reviewer for ACM TISSEC
- Reviewer for ACM Transactions on Networking
- Reviewer for IEEE Transactions on Wireless
- Reviewer for IEEE Transactions on Mobile Computing
- Reviewer for IEEE/ACM Transactions on Privacy and Security
- Reviewer for the *Avances en Ciencas e Ingenierías* journal al USFQ
- Reviewer for *Revista Politécnica de la Escuela Politécnica Nacional* journal at EPN
- Member of the Committee to Redesign the Computer Science program at USFQ
- Reviewer for SECON, INFOCOM
- Student representative to the Ph.D. committee at the College of Computer Science at Northeastern University during spring '09 semester. Evaluated applications of over 200 applicants to the Ph.D. program.

Technical Skills

- Protocol evaluation, cryptography, networking
- Linux System Administration, networking tools (LDAP, DNS, DHCP), Apache, Mail Transfer Agents (sendmail, postfix, exim), Intrusion Detection and prevention tools (nmap, nessus, Snort)
- MS Windows Domains (NT-style and Active Directory), MS Exchange, IIS, and administration tools
- C, C++, C#, Java, Go, ASP, Perl, Python, Scheme, Racket, Standard ML, Visual Basic, PHP, Matlab, R
- SQLServer, MySQL, Postgres, SQLite databases
- Virtualization using Xen, VirtualBox, and VMware
- Development on embedded systems with MSP430
- Software Defined Radio in Ettus SDR hardware and GNURadio

Honors and Awards

- William J. Fulbright Scholarship, Quito, Ecuador 2006