

Aldo Cassola

Web: <http://www.ccs.neu.edu/home/acassola>

Email: aldocassola@gmail.com
acassola@ccs.neu.edu

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

Project Experience

- **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 is able to 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

Teaching Experience

Northeastern University, Boston, MA

September 2008 – Present

Teaching Assistant

- Assisted Network Security Master's Level Class with grading and student office hours. Revised, updated, and implemented laboratory exercises over VMware and VirtualBox virtual machine platforms. Led laboratory and help sessions for students and lectures in lieu of principal instructor. Evaluated final projects and final competition of systems designed by students
- Reviewed and tested Network Security course content, and laboratory design for online version
- Assisted Wireless Networks Master's Level Class with general grading and student office hours. Updated and tested lab designs that use Crossbow Programmable Wireless Sensor Motes

Universidad San Francisco de Quito, Quito, Ecuador

August 2002 – June 2006

Instructor

- Instructed over 200 students in Ecuador's first and largest Linux System Administration Training Program at USFQ
- Taught Basic UNIX Administration and Java Programming Courses

San Francisco de Quito Community College, Quito, Ecuador

- Taught basic Computer Science programming courses in Java and Visual Basic

Service

- 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.

Work Experience

D2Hawkeye, Waltham, MA

May 2008 – July 2008

Assistant Services Architect - Internship

- Designed small-merchant online payment services for important company clients
- Designed a complete online employer health services management application and integration with

existing services

Universidad San Francisco de Quito, Quito, Ecuador

August 2002 – June 2006

Computer Systems Administrator, User support, Cisco Networking Academy Instructor

- Led, designed, and implemented several projects which allowed for a more efficient use of the network in a highly heterogeneous (800 workstations, Mac, Windows, and Linux) environment, by implementing several needed network services in Linux in the internal network infrastructure, resulting in reduction of spam-related traffic to less than 5%.
- Reorganized the E-mail and DNS infrastructure of the University, to allow for fault tolerance, and independence from the local ISPs

ITABSA (Phillip Morris Intl), Quito, Ecuador

September 2001 – July 2002

Intern developer, user support specialist

- Worked on a team of in-house and outsourced developers to implement and improve on financial, payroll, and raw material processing systems in Visual Basic
- Implemented several small Web Applications using ASP and SQL Server for weekly task reports of employees

Métodos Avanzados de Sistemas, Quito, Ecuador

July 2000 – December 2000

Technical support intern

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

Technical Skills

- 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
- Visual Basic, C, C++, Java, PHP, ASP, Perl, .NET, Python, Scheme, Bracket, Standard ML
- SQLServer, Oracle 9i and later, MySQL, PostgreSQL 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

References

- Prof. Guevara Noubir, Academic Advisor, College of Computer and Information Science, Northeastern University, noubir@ccs.neu.edu
- Prof. Agnes Chan, Dean of the Graduate School, College of Computer and Information Science, Northeastern University, ahchan@ccs.neu.edu
- Tao Jin, Ph.D. student and coauthor, Senior Engineer, Qualcomm, jintao.pku@gmail.com
- Bishal Thapa, Ph.D. student and coauthor, Researcher at Raytheon BBN Technologies bthapa@bbn.com
- Prof. Fernando Sánchez, alumnus USFQ, collaborator, USFQ Faculty fsanchez@usfq.edu.ec
- Himal Karmacharya, Service Development Supervisor, D2Hawkeye, LeapFrog Technology hkarmacharya@lfttechnology.com
- Susana Cabeza de Vaca, Fulbright Ecuador Director, director@fulbright.org.ec