Curriculum Vitæ—Aldo Cassola

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

Títulos

Northeastern University, Boston, MA Ph.D. en Ciencias de la Computación Advisor: Prof. Guevara Noubir	Mayo 2015
Master of Science en Ciencias de la Computación– 3.83/4.0 GPA	Mayo 2008
Universidad San Francisco de Quito, Quito, Ecuador Bachelor of Science en Ciencias de la Computación– 3.47/4.0 GPA	Junio 2001

Investigación y Proyectos Académicos

- **Disertación en sistemas residenciales que proveen servicios de Internet enfocados en privacidad:** El trabajo de mi tesis doctoral se enfoca en el diseño de sistemas seguros y dedicados a la privacidad de datos construidos en el contexto de instalaciones de internet residenciales. Este trabajo se enfocó en tres aspectos puntuales: la viabilidad de dichos sistemas incluyendo el impacto en el tráfico de las mismas residencias, el estado de la autenticación Wi-Fi ilustrado en nuestro trabajo anterior, y en la propuesta de un nuevo sistema que llamamos *SafEdge Gate* que permita a dueños de internet residencial compartir su red a clientes externos. *SafEdge Gate*, es un protocolo de autenticación anónima para Wi-Fi que permite al dueño del ruteador Wi-Fi permitir acceso a usuarios autorizados y al mismo tiempo provee garantías de anonimidad a dichos usuarios. En la práctica un usuario que se conecta a un ruteador con SafEdge tiene la garantía de solo una de las siguientes: a) el operador del ruteador Wi-Fi no puede distinguir la identidad del usuario de entre el conjunto de usuarios autorizados o b) tiene pruebas que el proveedor está intentando des-anonimizarlo.
- **OpenInfrastructure**: OpenInfrastructure es una plataforma de investigación que corre en ruteadores Wi-Fi residenciales, y del cual soy uno de sus dos contribuidores y diseñadores originales. Nuestro despliegue del sistema en 30 puntos en áreas urbanas de Boston, Houston y San Francisco ha servido como base para caracterizar propiedades de las redes residenciales actuales con datos de primera mano y como plataforma de investigación acerca de provisionamiento inalámbrico y privacidad. Hemos recolectado más de 115 millones de registros de uso del sistema desde febrero de 2011, 1.3TBytes de tráfico de red durante los primeros seis meses de implementación, y ha servido de plataforma para varios proyectos de investigación y publicaciones de nuestro grupo de investigación.
- **Seguridad de WPA-Enterprise**: A pesar de que WPA-Enterprise es un mecanismo de autenticación para Wi-Fi que goza de confianza y amplia distribución, la forma en que sus componentes internos cooperan y fallas en el diseño e implementación de la Interfaz de Usuario hacen posible un ataque multi-capa y sigiloso que permite la creación de puntos de acceso impostores y captura de credenciales de red. Como líder de este proyecto implementamos y evaluamos la efectividad del ataque empíricamente. Nuestro prototipo utiliza *hardware* disponible al público y es capaz de atacar clientes colocados hasta 400m de distancia, y nuestros experimentos muestran que es virtualmente indetectable a ojos de administradores de red, equipos de monitoreo y usuarios.
- **SNEAP:** El Proyecto del *Método de Autenticación a Través de Redes Sociales* (SNEAP por sus siglas en inglés) es un protocolo de acceso a Wi-Fi que permite control de acceso y cifrado de tráfico a través de servicios de credenciales y enlaces entre usuarios de redes sociales. SNEAP se ha concebido como una alternative a Hotspots de Wi-Fi abiertos sin autenticación, pero que también puede instalarse en ambientes residenciales y empresariales. Implementamos SNEAP para GNU/Linux and Windows sobre FreeRADIUS, utilizando Facebook como la plataforma de red social. Esta implementación es anterior al proyecto Facebook Wi-Fi, y permite a los clientes tener protección de datos al nivel de WPA para sus

conexiones a hotspots.

- **TREKS:** La *Extracción y programación de llaves en Tiempo Reverso* es una técnica novedosa para transmitir secretos para Espectro Repartido entre nodos inalámbricos, que además provee protección contra inhibidores. Este mecanismo resuelve un problema fundamental en el campo de la transmisión inalámbrica, en el que es necesario transmitir un secreto para proteger transmisiones contra inhibición, pero dicha protección no está disponible para la transmisión del secreto. Mejoramos, implementamos y y evaluamos este nuevo esquema de Espectro Repartido de Secuencia Directa sin secretos pre-compartidos utilizando Unidades de Procesamiento Gráfico (GPUs) como *hardware*. Nuestro esquema tiene eficiencia cuatro órdenes de magnitud mayor a soluciones existentes al problema y permite comunicación en tiempo real a tasas de Megabits por segundo. Además, provee protección contra inhibición comparable al Espectro Repartido de Secuencia Directa puro.
- **Búsqueda y Rescate GSM:** Investigamos la efectividad de Estaciones Base GSM para misiones de búsqueda y rescate. Nuestro prototipo usa un arreglo de antenas dinámicas ajustable mecánicamente que flexibiliza la creación de lóbulos de influencia de recepción y transmisión para una mejor deducción de la posición de los objetivos de búsqueda.

Publicaciones

- **TracEdge, A New Model for Anonymous Wi-Fi Authentication,** Aldo Cassola, Erik-Oliver Blass, Guevara Noubir, *IEEE Transactions on Mobile Computing,* TMC; (en revisión)
- **Authenticating Privately Over Public Wi-Fi Hotspots**, Aldo Cassola, Erik-Oliver Blass, Guevara Noubir, *Proceedings of the 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 Session*, 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

Experiencia Administrativa

Universidad San Francisco de Quito

Coordinador de Carrera, Ciencias de la Computación — Mayo 2016-hoy

- Coordiné contratación de nuevos instructores a tiempo parcial y profesores a tiempo completo
- Administré proceso de acredicaión con el gobierno ecuatoriano y acreditaciones internacionales
- Coordiné relaciones del departamento con industria
- Dirigí actividades promocionales del departamento, como charlas, casas abiertas y ferias

Experiencia Docente

Universidad San Francisco de Quito — Agosto 2015–hoy

Profesor a tiempo completo

- Impartí el cursos *core* de Programación básica y media , minería de datos, seguridad en redes, organización de computadoras, C# intermedio para el Colegio Politécnico con alrededor de 20 estudiantes por semestre, incluidas calificación, y horas de oficina para estudiantes.
- Dirigí y serví de consejero para cuatro proyectos de titulación
- Rediseñé, actualicé, traduje e impartí contenidos del curso de Seguridad de Redes a nivel de último año con 10 estudiantes promedio por semestre, incluyendo el rediseño de la plataforma virtual de

laboratorio, su implementación en la infraestructura local.
- Dirigí el curso avanzado de Tópicos Especiales dirigido a *Data Mining* para estudiantes de últimos años de carrera

Northeastern University, Boston, MA Septiembre 2008–Mayo 2015

Asistente de Cátedra

- Me desempeñé como asistente para la clase de Seguridad en Redes a nivel de Maestría con 40 estudiantes en promedio por semestre, incluyendo calificación, y horas de oficina para estudiantes. Revisé, actualicé, e implementé ejercicios de laboratorio para la clase utilizando plataformas virtuales VMWare y VirtualBox. Lideré sesiones de ayuda y laboratorio para estudiantes e impartí contenidos en reemplazo del instructor principal. Evalué proyectos finales del curso necesarios para su aprobación y el desempeño de la competencia antagónica de los sistemas desarrollados por los estudiantes.
- Revisé y examine el contenido del curso de Seguridad en Redes y el diseño de las prácticas de laboratorio para la versión a distancia en línea.
- Desempeñé como asistente del curso de Redes Inalámbricas a nivel de Maestría incluyendo calificación y horas de oficina. Actualicé y examiné prácticas de laboratorio de *Motes* sensores programables Crossbow.

Universidad San Francisco de Quito, Quito, Ecuador Agosto 2002–Junio 2006

Instructor de Academia Cisco de Redes y Sistemas

- Instruí más de 200 estudiantes en el primer y más grande programa de administración de sistemas Linux en el Ecuador en la Academia de Redes y Sistemas Operativos.
- Fui instructor del curso de Administración de Sistemas e Introducción a Java.

Colegio de la Comunidad San Francisco de Quito, Quito, Ecuador

Instructor del Colegio

- Instruí cursos de Introducción a la Programación en Visual Basic y Java.

Servicio Académico

- Revisor de publicaciones para la revista *ACM Transactions on Privacy and Security (prev. ACM Transaction on Information and System Security), SciMago Q1*
- Revisor de Publicaciones para la Revista *IEEE/ACM Transactions on Networking, SciMago Q1*
- Revisor de Publicaciones para la Revista *Avances en Ciencias e Ingenierías* del Politécnico USFQ
- Revisor de Publicaciones para la *Revista Politécnica de la Escuela Politécnica Nacional*
- Colaborador para el rediseño de carrera aprobado por el Consejo de Educación Superior del Ecuador para USFQ, Mayo 2016
- Revisor de publicaciones para las conferencias SECON e INFOCOM
- Representante de estudiantes ante el comité del programa de Ph.D. del *College of Computer Science* de *Northeastern University* durante el año 2008-2009. Evalué las aplicaciones de más de 200 aplicantes al programa de Ph.D.

Experiencia Laboral

D2Hawkeye, Waltham, MA Mayo 2008–Julio 2008

Arquitecto Asistente de Servicios - Pasantía

- Diseñé servicios de pagos en línea para pequeños comerciantes a nombre de importantes clientes de la empresa.
- Diseñé una aplicación completa de gestión en línea de servicios de salud para empleadores que incluye monitoreo de objetivos de salud de los miembros del plan de salud e integración con servicios existentes.

Universidad San Francisco de Quito, Quito, Ecuador Agosto 2002–Junio 2006

Administrador de Sistemas de Computación, Soporte a Usuarios

- Lideré, diseñé e implementé varios proyectos que permitieron un uso más eficiente de la red de la institución en un ambiente altamente heterogéneo (800 workstations, Mac, Windows, and Linux) incluyendo la implementación de varios servicios necesarios en Linux para la infraestructura de la red interna, lo que resultó en una reducción del correo no deseado a menos del 5% y en el control total de la presencia de la institución en línea, incluyendo la infraestructura de DNS, página web y correo electrónico como primer paso a mejoras futuras del sistema.
- Reorganicé la estructura de DNS y correo electrónico de la Universidad para permitir la tolerancia a fallos e independencia de los proveedores de internet locales.

ITABSA (Phillip Morris Intl), Quito, Ecuador — Septiembre 2001–Julio 2002

Desarrollador, especialista en soporte a usuarios–Pasantía

- Trabajé con un equipo de desarrolladores *in-house* y tercerizados para implementar y mejorar sistemas financieros, rol de pagos y de procesamiento de materia prima en fábricas sobre Visual Basic.
- Implementé varios servicios web sobre ASP y SQL Server para reportes semanales de empleados.

Métodos Avanzados de Sistemas, Quito, Ecuador — July 2000–December 2000

Especialista en soporte técnico—Pasantía

Implementé y mejoré el software de seguridad en red y correo electrónico para la red de la agencia principal y di soporte a los usuarios.

Habilidades Técnicas

- Administración de Sistemas Linux, servicios de red (LDAP, DNS, DHCP), Apache, Agentes de Transferencia de Email (sendmail, postfix, exim), herramientas de prevención y detección de intrusos (nmap, nessus, Snort)
- Administración de Dominios MS Windows (NT y Active Directory), MS Exchange, IIS
- Visual Basic, C, C++, Java, PHP, ASP, Perl, .NET, Python, Scheme, Bracket, Standard ML
- Bases de datos SQL Server, Oracle 9i and later, MySQL, PostgreSQL
- Virtualización bajo Xen, VirtualBox and VMware
- Desarrollo de sistemas embebidos con chips MSP430 y compatibles
- Desarrollo de aplicaciones de procesamiento paralelo de alto rendimiento en GPU
- Desarrollo de protocolos seguros de red
- Radio Definida en Software (SDR) en *hardware* de Ettus y GNURadio

Honores y Becas

- William J. Fulbright Scholarship para el desarrollo de docentes, Quito, Ecuador 2006

Referencias

- Prof. Guevara Noubir, Tutor Académico, College of Computer and Information Science, Northeastern University, noubir@ccs.neu.edu
- Prof. Agnes Chan, Decana del Programa de Postgrado, College of Computer and Information Science, Northeastern University, ahchan@ccs.neu.edu
- Tao Jin, estudiante Ph.D. y coautor, hoy Ingeniero Senior, Qualcomm, jintao.pku@gmail.com
- Bishal Thapa, estudiante Ph.D. y coautor, hoy Investigador Raytheon BBN Technologies bthapa@bbn.com
- Fausto Pasmay, profesor USFQ, colaborador, fpasmay@usfq.edu.ec
- Himal Karmacharya, Supervisor de Desarrollo de Servicios, D2Hawkeye, hoy en LeapFrog Technology hkarmacharya@lftechnology.com
- Susana Cabeza de Vaca, Directora Comisión Fulbright Ecuador, director@fulbright.org.ec