CLCERT investigación en criptografía aplicada y seguridad computacional

Mapa de ataques computacionales.

Alejandro Hevia
Profesor Asistente, DCC, U. de Chile. Ph.D. Computer Science, University of California, San Diego (2006); Ingeniero Civil en Computación, Universidad de Chile (1998). Director CLCERT.
ahevia@dcc.uchile.cl

El CLCERT es un grupo de investigación de la Facultad de Ciencias Físicas y Matemáticas (FCFM) de la Universidad de Chile, dirigido por el profesor Alejandro Hevia. Sus áreas de trabajo son Criptografía Aplicada y Seguridad Computacional. En la primera, el Grupo busca investigar nuevos protocolos computacionales, técnicas y herramientas matemáticas para construir sistemas computacionales que funcionen correctamente incluso ante la presencia de ataques. Ejemplos de estos son los sistemas de votación y comunicación anónima. Su segundo objetivo es el estudio y monitoreo de la seguridad computacional de las redes, mediante el análisis y la anticipación a las amenazas y la reducción, en particular, de la cantidad de incidentes de seguridad perpetrados desde y hacia los sistemas computacionales en Chile. En este sentido, el grupo busca desarrollar herramientas computacionales y recursos humanos apropiados para mejorar la seguridad de nuestras redes. Es en esta última área donde se enmarca la labor de difusión del CLCERT, el cual se constituye como un punto nacional de encuentro, contacto y coordinación entre instituciones y personas relacionadas del medio local.

Integrantes de CLCERT, de izq. a der.: Sergio Miranda, Alejandro Hevia, Marcos Kiwi.

INTEGRANTES DEL GRUPO

Actualmente el CLCERT está integrado por miembros de la FCFM en los siguientes cargos: director, profesor Alejandro Hevia (Ph.D.), del Departamento de Ciencias de la Computación (DCC); director Alterno, profesor Marcos Kiwi (Ph.D.), del Departamento de Ingeniería Matemática; y director de Tecnología, el ingeniero Sergio Miranda. A ellos se suman los asistentes de investigación Philippe Camacho, Julio Quinteros, Cristian Rojas y los estudiantes Francisca Moreno, Alonso González, Renata Faccilongo, Rodrigo Porras, Felipe Troncoso, Fernando Krell, Patricio Seguel y Gastón L'Huillier.

ÁREAS DE INVESTIGACIÓN

La Criptografía históricamente ha buscado estudiar las técnicas, modelos y herramientas matemáticas necesarias para resolver problemas relacionados con la privacidad, integridad y disponibilidad de la información. Ejemplos clásicos de estos problemas son la encriptación y firmas digitales. Recientemente, las herramientas criptográficas han mostrado ser fundamentales para implementar sistemas distribuidos seguros, como sistemas de votación electrónica verificable, sistemas de manejo de identidad online y/o móvil y sistemas de reportes y denuncias de crímenes en forma anónima.

En el CLCERT no sólo se investigan dichas herramientas y técnicas matemáticas, sino también los conceptos y nociones de seguridad apropiadas para los problemas (¿qué significa que un sistema de votación electrónica sea seguro?, ¿hasta qué punto puede un sistema de comunicación anónima ser reversible en caso de que se detecten abusos?).

En la práctica, un buen sistema computacional debe satisfacer todos los requerimientos funcionales y de seguridad. Este último no sólo se logra usando las herramientas adecuadas, sino que entregando evidencia matemática de seguridad. Esto es, demostraciones formales y rigurosas que ataques al sistema no son posibles si resolver ciertos problemas matemáticos es computacionalmente difícil. Es en este círculo formado por el desarrollo de herramientas matemáticas, el diseño de protocolos criptográficos, la definición de nociones y demostraciones de seguridad, donde los criptógrafos del CLCERT realizan su trabajo.

El área de la seguridad computacional representa un aspecto aplicado de los problemas anteriores. La interconexión de nuestros sistemas a escala internacional ha permitido niveles de acceso e intercambio de la información sin precedentes, con claros beneficios económicos y sociales. Sistemas de acceso bancario en forma remota han permitido manejar nuestras finanzas online desde cualquier parte y a cualquier hora. Sin embargo, la interconexión de sistemas con información valiosa, usando tecnologías esencialmente sin buenos mecanismos de autentificación (como TCP/IP), ha creado una poco deseable consecuencia: los ataques computacionales como un negocio rentable. Hoy en día, nuestras redes computacionales son continuamente atacadas desde distintas partes del mundo, en forma totalmente automatizada (vía programas maliciosos como gusanos y troyanos) a fin de robar esta información valiosa. Los miembros del CLCERT buscan estudiar dichos ataques en las redes, alcances y métodos, a fin de proponer mecanismos para prevenirlos, detectarlos y en efecto disminuirlos.

Las principales áreas de investigación en Criptografía y Seguridad Computacional en

Interfaz de sistema de votación electrónica.

las cuales miembros del CLCERT trabajan son:

- Votación Electrónica Verificable.
- Sistemas de Comunicación Anónima Robustos.
- Acumuladores Criptográficos.
- Sistemas de Monitoreo y Análisis de Malware.

PROYECTOS DE INVESTIGACIÓN

Los proyectos de investigación del CLCERT usualmente se canalizan a través de las tesis de memoria, magíster y doctorado de sus participantes. A continuación se mencionan algunos ejemplos.

Votación Electrónica Verificable

Un sistema de votación electrónica es verificable si permite garantizar matemáticamente la exactitud del cómputo del resultado final a votantes y observadores externos. En particular, debe permitir convencer a cada votante que su voto, y el de todos los votantes, ha sido contado exactamente una sola vez y, al mismo tiempo, preservar la privacidad del voto. Más aún, el sistema debe garantizar que no existe un único punto de falla. Esto es, el conteo debe ser llevado a cabo por un conjunto de servidores distribuidos que garanticen un cálculo correcto, incluso aunque una minoría de los servidores sea comprometido (hacheado) para alterar la elección o violar la privacidad de los votos. Garantías tan fuertes sólo pueden obtenerse usando mecanismos criptográficos, objeto del estudio de varias memorias en el CLCERT. De hecho, un prototipo funcional de sistema de votación electrónica verificable ya ha sido utilizado durante las elecciones tanto de Director del Departamento de Ciencias de la Computación (diciembre 2008) como de la directiva del Centro de Alumnos del DCC (2008 y 2009). Actualmente el sistema está siendo mejorado a fin de facilitar su uso en un mayor espectro de elecciones. Otras líneas de investigación relacionadas incluyen el desarrollo de sistemas *lightweight* para plataformas móviles.

Sistemas Robustos de Comunicación Anónima

Existen escenarios donde poder comunicar mensajes en forma anónima es imprescindible, por ejemplo, en un sistema de reporte de tips (o denuncias) contra el narcotráfico, organizaciones criminales o corrupción. O bien, en un sistema de consulta online sobre temas "sensibles" médicos como tratamientos contra el SIDA o políticamente comprometedores. El éxito de tales sistemas depende de su capacidad de garantizar el anonimato, aún ante la corrupción o curiosidad de los "administradores" del sistema. En reciente proyecto en el CLCERT, el estudiante Patricio Seguel, usando técnicas criptográficas, diseñó uno de tales sistemas: un canal de comunicación anónima robusta. Asimismo, el estudiante de doctorado Julio Quinteros actualmente investiga maneras de proveer comunicación anónima eficiente, pero con altas garantías de seguridad y nueva funcionalidad, como mecanismos de revocación del anonimato a fin de evitar abusos al sistema.

Acumuladores Criptográficos

Una importante línea de investigación en el CLCERT es el estudio e implementación de acumuladores criptográficos. Estos objetos consisten en protocolos distribuidos que permiten, entre otros, implementar mecanismos de estampas de tiempo confiables y credenciales anónimas de autentificación. Liderada por el estudiante de doctorado Philippe Camacho, el estudio incluye el desarrollo de versiones que toleren administradores maliciosos y/o provean nuevas funcionalidades, así como la precisión de sus posibles limitaciones teóricas.

Sistemas de Monitoreo y Análisis de Malware

Fruto de las tesis de los estudiantes Felipe Troncoso y Francisco Echeverría, el CLCERT ha desarrollado varios sistemas de monitoreo de redes a fin de detectar y caracterizar el *malware* (programa malicioso) que actualmente circula por las redes. Este proyecto ha permitido finalmente desarrollar un Laboratorio de Malware, mediante el

cual se captura, clasifica y estudia instancias de programas maliciosos. Además, Sergio Miranda recientemente ha obtenido financiamiento por parte de LACNIC (proyecto Amparo) para implementar la primera *"Darknet"* chilena: un sistema automático diseñado para monitorear un amplio espectro de actividad maliciosa en la Red y así proveer de información oportuna y precisa a los profesionales de seguridad de nuestra comunidad local.

Cooperación Internacional

En 2009 el CLCERT organizó el FIRST Technical Colloquium por primera vez en Chile. Este evento es una instancia de discusión e intercambio de información respecto a incidentes, vulnerabilidades, herramientas y varios otros que afectan la operación de grupos de respuesta a incidentes de seguridad de FIRST (Forum of Incident Response Teams, www.first.org). El evento fue realizado el 22 y 23 de octubre de 2009 y precedido por el CLCERT/FIRST Security Workshop; un evento de seguridad computacional abierto a la comunidad local, el cual contó con la participación de más de 120 profesionales del área. La actividad fue patrocinada por el gobierno de Chile y financiado en parte por el Centro de Modelamiento Matemático de la Universidad de Chile, NIC Chile, Microsoft-Chile, Intel y Sinapsis.

En términos de investigación, el CLCERT mantiene lazos de colaboración con investigadores internacionales. Ejemplos de proyectos realizados en conjunto recientemente incluyen:

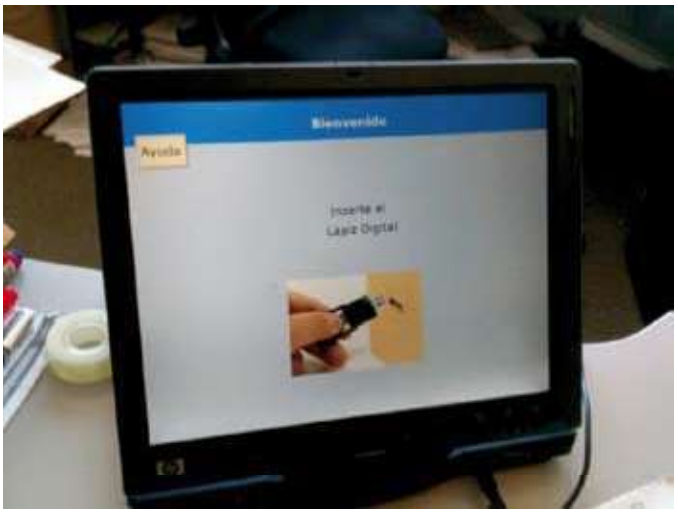
- Estudio de sistemas de Anonimatos Robustos: Dr. Tamara Rezk, INRIA Sophia, Antipolis, Francia; Dr. Gilles Barthe, IMDEA, España; Dr. Bogdan Warinschi, Universidad de Bristol, UK.
- Estudio de la Eficiencia de Comunicación Anónima vía DC nets: Dr. Alfredo Viola, Universidad de la República, Uruguay.
- FACTOIDS: Modelos y Herramientas para el Análisis e Intercambio Seguro de Datos Colectados por Sensores: Carlos Martínez-Cagnazzo (ANTEL, Uruguay) y Dr. Gustavo Betarte, Universidad de la República, Uruguay.

Interacción con el Medio Local

Aparte de la realización de eventos de seguridad como los mencionados anteriormente, el CLCERT realiza desde 2005 actividades de difusión y distribución de información de seguridad. En particular, distribuye alertas de seguridad en forma periódica las cuales son recibidas por miembros de la comunidad local de esta área, incluido el gobierno de Chile. En particular, 236 alertas fueron enviadas durante el año 2009.

Asimismo, el CLCERT realiza diversas actividades de capacitación y generación de recurso humano especializado. Entre ellas se incluye un Diploma de Postítulo en Seguridad Computacional (impartido por el DCC), el cual ya tiene su sexta versión. El CLCERT también ofrece diversos cursos de capacitación en temas como derecho informático para ingenieros, biometría, administración de parches de seguridad y 'segurización' de plataformas específicas tales como Microsoft Windows y Linux. Estos cursos son dictados a través de una red de colaboradores del CLCERT formada por profesionales y expertos del área como Luis Montenegro, Isabel de la Barra, Marco Antonio Zúñiga y Paula Jervis, Rosina Ordoqui y Pablo Rojo, entre otros.

Recientemente miembros del CLCERT han colaborado con ingenieros de NIC Labs (NIC Chile), entre ellos Tomás Barros y Víctor Ramiro, en la implementación de nuevos mecanismos de seguridad para el desarrollo de DNSSEC. En particular, en este proyecto se busca implementar un sistema de firma electrónica distribuida robusta, el cual pueda sostener el sistema de generación de firmas requerido por DNSSEC de manera altamente resistente a fallas. BITS



Sistema de votación electrónica en una Tablet PC.

CONTACTO

www.clcert.cl
Profesor Alejandro Hevia,
ahevia@dcc.uchile.cl