Valencia, 3 de febrero de 2012

Investigadores de la UPV colaboran con el Naval Research Laboratory de Washington en el desarrollo de avanzadas tecnologías para mejorar la seguridad de las comunicaciones

- Junto con la Universidad de Illinois en Urbana-Champaign, han desarrollado la herramienta de verificación Maude-NPA, la más competitiva para el análisis de protocolos de comunicaciones que utilicen propiedades criptográficas avanzadas
- El Grupo de Extensiones de la Programación Lógica de la UPV colabora también con el National Institute of Aerospace (NIA) de la NASA

Contribuir a garantizar la máxima seguridad de las comunicaciones. Este es el objetivo de la colaboración que desde hace ya siete años mantiene un equipo de investigadores del Grupo ELP de la Universitat Politècnica de València con el Naval Research Laboratory de Washington y la Universidad de Illinois en Urbana-Champaign.

Como resultado de esta colaboración, el equipo de trabajo ha desarrollado recientemente la versión 2.0 –en 2009 desarrollaron la primera versión– de la herramienta de verificación Maude-NPA, la más innovadora actualmente para el análisis de protocolos de comunicaciones que utilicen propiedades criptográficas avanzadas. Esta herramienta ayuda a encontrar fallos de seguridad o verificar que un protocolo está libre de ataques.

“Gracias a esta herramienta podemos representar el modelo más realista posible de un protocolo de comunicación, lo que permite evaluar su seguridad y detectar vulnerabilidades”, señala María Alpuente, directora del Grupo ELP de la Universitat Politècnica de València.

Santiago Escobar, coordinador del equipo de trabajo sobre seguridad del Grupo ELP de la UPV, explica que aún asumiendo que las técnicas de encriptación de mensajes sean perfectas, pueden darse problemas en el diseño de un protocolo debido a un mal uso de la información de los participantes que afecte a la seguridad de las comunicaciones. “La autenticidad de los participantes y la confidencialidad de algunos mensajes son las propiedades clave en los protocolos de comunicaciones. Aunque los mensajes enviados por un canal inseguro estén encriptados y las claves de encriptación no estén comprometidas, es decir, no se conozcan, un protocolo puede acabar liberando algún secreto o permitir a un intruso hacerse pasar por uno de los participantes”, explica el profesor Escobar.

“Con esta herramienta “tenemos la certeza de que si existe un problema en el protocolo, será capaz de encontrarlo si dispone de suficientes recursos de cómputo, y si el protocolo es seguro, la herramienta podría certificarlo”, añade Sonia Santiago, cuya tesis doctoral -que comenzó con una estancia en SRI International en California en 2010- versa sobre la mejora de las capacidades de Maude-NPA.

Las investigaciones sobre Maude-NPA surgen de la cooperación iniciada en 2003 con la Universidad de Urbana-Champaign en el área de los métodos formales industriales, y se han publicado en congresos y revistas internacionales como Theoretical Computer Science, Foundations of Security Analysis and Design (FOSAD 2007-2009), European Symposium on Research in Computer Security (ESORICS 2010), y Security and Trust Management, Springer 2011.

Área de Comunicación
Edificio Nexus (6G), Camino de Vera, s/n - 46022 VALENCIA

Tras el desarrollo de Maude-NPA, los investigadores de la UPV trabajan en estrecha colaboración con otras universidades americanas y europeas en el manejo de protocolos de comunicaciones con propiedades criptográficas mucho más avanzadas, en el estudio de la composición secuencial de protocolos y en el análisis de protocolos de grupo.

Colaboración con la NASA

El Grupo ELP de la Universitat Politècnica de València mantiene también una colaboración con el National Institute of Aerospace (NIA) de la NASA en Hampton, Virginia. En concreto, ha participado en el desarrollo de herramientas de soporte para la verificación de propiedades de seguridad en diferentes sistemas, incluyendo un protocolo de sincronización con relojes distribuidos.

“Cuando en un entorno distribuido se comunican dos dispositivos con relojes no sincronizados, puede producirse un acceso inoportuno a memoria o el uso indebido de recursos críticos, comprometiendo así la seguridad del sistema. La solución más utilizada a este problema en internet es el uso de protocolos de sincronización que no requieren un reloj global y proporcionan altos niveles de seguridad, como el Network Time Protocol (NTP), pero que pueden exhibir vulnerabilidades en algunos escenarios que detectan las herramientas de verificación”, explica María Alpuente.

Datos de contacto: Luis Zurano Conches
Unidad de Comunicación Científica e Innovación (UCC+i)
actualidadi+d@ctt.upv.es
647 422 347

Anexos: