Valencia, 3 de febrer de 2012

Investigadors de la UPV col·laboren amb el Naval Research Laboratory de Washington en el desenvolupament de tecnologies avançades per millorar la seguretat de les comunicacions

- Junt amb la Universitat d'Illinois a Urbana-Champaign, han desenvolupat l'eina de verificació Maude-NPA, la més competitiva per a l'anàlisi de protocols de comunicacions que utilitzen propietats criptogràfiques avançades
- El grup Extensions de la Programació Lògica de la UPV col·labora també amb el National Institute of Aerospace (NIA) de la NASA

Contribuir a garantir la màxima seguretat de les comunicacions: aquest és l'objectiu de la col·laboració que des de fa ja set anys manté un equip d'investigadors del grup ELP de la Universitat Politècnica de València amb el Naval Research Laboratory de Washington i la Universitat d'Illinois a Urbana-Champaign.

Com a resultat d'aquesta col·laboració, l'equip de treball ha desenvolupat recentment la versió 2.0 –l'any 2009 en va desenvolupar la primera versió– de l'eina de verificació Maude-NPA, la més innovadora actualment per a l'anàlisi de protocols de comunicacions que utilitzen propietats criptogràfiques avançades. Aquesta eina ajuda a trobar fallades de seguretat o verificar que un protocol està lliure d'atacs.

"Gràcies a aquesta eina podem representar el model més realista possible d'un protocol de comunicació, la qual cosa permet avaluar-ne la seguretat i detectar-hi vulnerabilitats", assenyala María Alpuente, directora del grup ELP de la Universitat Politècnica de València.

Santiago Escobar, coordinador de l'equip de treball sobre seguretat del grup ELP de la UPV, explica que fins i tot assumint que les tècniques d'encriptació de missatges siguen perfectes, poden donar-se problemes en el disseny d'un protocol a causa d'un mal ús de la informació per part dels participants que afecte la seguretat de les comunicacions.

"L'autenticitat dels participants i la confidencialitat d'alguns missatges són les propietats clau en els protocols de comunicacions. Encara que els missatges enviats per un canal insegur estiguen encriptats i les claus d'encriptació no estiguen compromeses, és a dir, no es coneguen, un protocol pot acabar alliberant algun secret o permetre a un intrús fer-se passar per un dels participants", explica el professor Escobar.

"Amb aquesta eina tenim la certesa que si hi ha un problema en el protocol, l'eina serà capaç de trobar-lo si disposa de prou recursos de còmput, i si el protocol és segur, podria certificar-ho", afig Sonia Santiago, la tesi doctoral de la qual, que va començar amb una estada a SRI International, a Califòrnia, l'any 2010, versa sobre la millora de les capacitats de Maude-NPA.

Les investigacions sobre Maude-NPA sorgeixen de la cooperació iniciada el 2003 amb la Universitat d'Illinois a Urbana-Champaign en l'àrea dels mètodes formals industrials, i s'han publicat en congressos i revistes internacionals: *Theoretical Computer Science, Foundations of Security Analysis and Design* (FOSAD 2007-2009), *European Symposium on Research in Computer Security - ESORICS 2010 (15th European Symposium on Research in Computer Security)*, i *Security and Trust Management* (2011) (tots els títols publicats per Springer).

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

Després del desenvolupament de Maude-NPA, els investigadors de la UPV treballen en estreta col·laboració amb altres universitats americanes i europees en el maneig de protocols de comunicacions amb propietats criptogràfiques molt més avançades, en l'estudi de la composició seqüencial de protocols i en l'anàlisi de protocols de grup.

Col·laboració amb la NASA

El Grup ELP de la Universitat Politècnica de València manté també una col·laboració amb el National Institute of Aerospace (NIA) de la NASA ubicat a Hampton, Virgínia. En concret, ha participat en el desenvolupament d'eines de suport per a la verificació de propietats de seguretat en diversos sistemes, incloent un protocol de sincronització amb rellotges distribuïts.

“Quan en un entorn distribuït es comuniquen dos dispositius amb rellotges no sincronitzats, pot produir-se un accés inoportú a memòria o l'ús indegut de recursos crítics, la qual cosa comprometria la seguretat del sistema. La solució a aquest problema més utilitzada en Internet és fer ús de protocols de sincronització que no requereixen un rellotge global i proporcionen alts nivells de seguretat, com ara el Network Time Protocol (NTP), però que poden presentar vulnerabilitats en alguns escenaris, vulnerabilitats que detecten les eines de verificació”, 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: