# UPV researchers are working with the Naval Research Laboratory in Washington in the development of advanced technologies to improve the security of communication

- Together with the University of Illinois at Urbana-Champaign, they have developed Maude-NPA, the most competitive verification tool for the analysis of communications protocols that use advanced cryptographic features
- The UPV's Extensions of Logic Programming (ELP) group also collaborates with the NASA's National Institute of Aerospace (NIA)

To help ensure maximum security of communications: such is the aim of the collaborative project that a team of researchers from the Universitat Politècnica de València's ELP group, the Naval Research Laboratory in Washington and the University of Illinois at Urbana-Champaign have been pursuing for seven years.

As a result of this collaboration, the team has recently developed the 2.0 version –they developed the first version in 2009– of the verification tool Maude-NPA, which is currently the most innovative tool for the analysis of communications protocols that use advanced cryptographic features. This tool helps users find security flaws or verify that a protocol is free from attacks.

"With this tool we can represent the most realistic model of a communications protocol, which allows us to evaluate its safety and identify its vulnerabilities," says María Alpuente, who is the director of the ELP group at the Universitat Politècnica de València.

Santiago Escobar, who is the coordinator of the UPV's ELP group's team working on security, explains that even assuming that message encryption techniques are perfect, problems may arise in the design of a protocol due to improper use of information by participants affecting the security of communications.

"The authenticity of the participants and the confidentiality of some messages are the key properties in communication protocols. Whenever messages are sent by an insecure channel, even if they are encrypted and the encryption keys are not compromised, i.e. are not known, a protocol may release some secrets or may allow an attacker to pose as one of the participants", explains Professor Escobar.

"With this tool we are certain that in case there is a problem in the protocol, the tool will be able to find it if it has enough computing resources, and if the protocol is secure, it can certify its security", says Sonia Santiago, whose doctoral thesis, which began with a stay at SRI International, in California, in 2010, is about improving the capabilities of Maude-NPA.

The research leading to Maude-NPA arises from the UPV's cooperative project with the University of Illinois at Urbana-Champaign in the area of industrial formal methods, which started in 2003, and has been published in international conferences and journals: *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)*, and *Security and Trust Management* (2011) (all titles published by Springer).

After developing Maude-NPA, UPV researchers are working closely with other American and European universities in handling communications protocols with much more advanced cryptographic properties, in the study of the sequential composition of protocols, and in the analysis of group protocols.

**Collaboration with NASA**

The Universitat Politècnica de València's ELP group also pursues a collaboration with the NASA's National Institute of Aerospace (NIA) in Hampton, Virginia. Specifically, the group has participated in developing support tools for verifying security properties in various systems, including a distributed clock synchronization protocol.

"When in a distributed environment two devices using non-synchronized clocks communicate with each other, an inappropriate access to memory or a case of undue use of critical resources may happen, which would compromise the security of the system. The most common solution to this problem on the Internet is using synchronization protocols that do not require a global clock and provide high levels of security, such as Network Time Protocol (NTP), but these may have vulnerabilities in some scenarios, vulnerabilities that are detected by verification tools ", says 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:**