Lógicas de autenticación aplicadas al estudio de protocolos

Maya Carrillo mcarrill@lycos.com
Raúl Monroy raulm@campus.cem.itesm.mx
Centro de investigación e innovación en ingeniería y tecnología
ITESM-CEM
Atizapán, México, 52926

Resumen

El empleo de Internet como herramienta de trabajo, de comercio electrónico y la proliferación de aplicaciones distribuidas, hacen de la seguridad computacional un requerimiento prioritario. Cualquier comunicación segura se inicia generalmente con un proceso de autenticación. Un protocolo de autenticación es un conjunto de reglas mediante las cuales dos o más principales establecen su mutua identidad. Las lógicas basadas en creencias deducen conocimiento nuevo a partir de suposiciones y mensajes iniciales, para verificar si ciertas condiciones de autenticación existen y posibilitan la comunicación segura entre dos principales. Uno de los primeros esfuerzos de formalización fue hecho por Burrows, Abadi y Needham, quienes, cuando publicaron su trabajo acerca de la lógica BAN [3], despertaron el interés de otros autores, que a partir de BAN definieron otras lógicas: GNY [4], AUTLOG[5], AT[6], SVO[7], G[2]. Proponemos un sistema automático para analizar un protocolo de autenticación desde la perspectiva de diferentes lógicas de creencias. El sistema es genérico, recibe dos argumentos: la especificación de la lógica y del protocolo. Pruebas experimentales mostraron que el sistema desarrollado es útil para comparar lógicas de creencias de manera experimental y para determinar el nivel de certeza al que un protocolo de autenticación llega al ser analizado.

Palabras clave: Verificación de protocolos, seguridad computacional, autenticación, análisis automático, lógica, métodos formales.

Abstract

The use of Internet as a work tool for doing e-business or e-commerce, together with the proliferation of distributed applications, has made computer security a strong requirement. Secure communications start with an authentication process. An authentication protocol is a set of rules whereby two o more principals agree about each other's identity. Belief logics are used to formalize what a principal may deduce from both the messages she reads and a set of initial assumptions. With this, it is possible to verify whether certain authentication conditions exist allowing for secure communication between a pair of principals. The first attempt at using belief logics to verify authentication protocols was reported by Burrows, Abadi and Needham [3]. Their pioneer work, the BAN logic, quickly captured the attention of a number of researchers, giving rise to a number of logics that extend BAN in one way or other: GNY [4], AUTLOG[5], AT[6], SVO[7], G[2]. We propose an automatic system to analyze an authentication protocol from the perspective of different belief logics. The system is generic, it takes two arguments: the logic and the specification of the protocol to be analyzed. Experimental results show that the developed system is useful to compare belief logics and to determine the guarantee level that an authentication protocol reaches when it is analyzed.

Keywords: Protocol verification, computer security, authentication, automatic program verification, logic, formal methods.