Resumen

El área de análisis formal de protocolos criptográficos ha experimentado una gran actividad desde mediados de los 80. El objetivo es verificar protocolos que utilizan un mecanismo de cifrado para garantizar la confidencialidad y la autenticación de los datos. Los métodos formales han sido utilizados en el análisis de protocolos para proporcionar pruebas formales de seguridad y para descubrir errores y flujos de seguridad que en algunos casos han permanecido ocultos durante mucho tiempo después de la publicación del protocolo original, como es el caso del conocido protocolo Needham-Schroeder Public Key (NSPK). En esta tesis abordamos problemas relacionados con los tres pilares principales de la verificación de protocolos: capacidades de modelado, propiedades verificables y eficiencia.

Esta tesis está dedicada a investigar características avanzadas del análisis de protocolos criptográficos, centrándose en la herramienta Maude-NPA. Esta herramienta es un comprobador de modelos (model-checker) para el análisis de protocolos criptográficos que permite la incorporación de distintas teorías ecuacionales y que opera en el modelo de número ilimitado de sesiones, sin realizar ningún tipo de abstracción de datos o de control.

Una contribución importante de esta tesis está relacionada con aspectos teóricos de verificación de protocolos en Maude-NPA. En primer lugar, definimos una semántica operacional hacia adelante, usando la lógica de reescritura como marco teórico y el lenguaje de programación Maude como herramienta de soporte. Esta es la primera vez que se define una semántica operacional hacia adelante basada en reescritura para Maude-NPA. En segundo lugar, estudiamos el problema que surge en el análisis de protocolos criptográficos cuando es necesario garantizar que determinados términos generados durante la exploración de estados están

en forma normal con respecto a la teoría ecuacional del protocolo.

También estudiamos técnicas para extender las capacidades de Maude-NPA para que se pueda verificar un abanico más amplio de protocolos y de propiedades de seguridad. En primer lugar, presentamos un marco para especificar y verificar composiciones secuenciales de protocolos en las que uno o más protocolos "hijo" hacen uso de información obtenida después de ejecutar un protocolo "padre". En segundo lugar, presentamos un marco teórico para especificar y verificar indistinguibilidad de protocolos en Maude-NPA. El objetivo de este tipo de propiedades es verificar que un atacante no puede distinguir dos versiones diferentes de un protocolo: por ejemplo, una en la que se utiliza un secreto y otra en la que se utiliza un secreto diferente, como ocurre en los protocolos de voto electrónico.

Por último, esta tesis contribuye a mejorar la eficiencia de la verificación de protocolos en Maude-NPA. Definimos varias técnicas que reducen drásticamente el espacio de búsqueda generado en el análisis de un protocolo, y que, a menudo, permite obtener un espacio de búsqueda finito de tal modo que se puede decidir automáticamente si la propiedad de seguridad deseada se satisface o no, a pesar de que tales problemas sean generalmente indecidibles.