Verifikasi protokol otentitikasi horn-preneel menggunakan AVISPA (automated validation of internet security protocols and applications)

Ilham Karunia, author

Abstrak

Salah satu teknologi selular generasi ketiga adalah Universal Mobile Telephone System (UMTS). Ada kebutuhan layanan keamanan yang harus disediakan oleh UMTS, antara lain adalah otentikasi mutual antara pengguna teknologi ini dengan jaringan penyedia layanan secara anonim. G¨unther Horn dan Bart Preneel merancang sebuah protokol otentikasi untuk digunakan pada UMTS yang memenuhi kebutuhan tersebut dengan mempertimbangkan keterbatasan perangkat keras yang tersedia.

Dalam tugas akhir ini, dibuat sebuah model dari protokol otentikasi Horn- Preneel tanpa pihak ketiga dengan menggunakan alat bantu AVISPA (Automated Validation of Internet Security Protocols and Applications). Model tersebut diverifikasi secara formal menggunakan pengecek model OFMC (Onthe-Fly Model Checker) yang terintegrasi dengan AVISPA.

Hasil dari verifikasi menunjukkan bahwa protokol otentikasi Horn-Preneel tanpa pihak ketiga memiliki kelemahan yang memungkinkan terjadi denial of service dari sisi pengguna. Waktu yang digunakan untuk melakukan verifikasi hanya kurang dari 1 detik menggunakan Pentium III 1,0 GHz memori 128 MB di atas sistem operasi Ubuntu Linux 5.10. Sebuah modifikasi dalam bentuk penambahan langkah baru dalam protokol tersebut diajukan untuk mengatasi kelemahan tersebut. Hasil verifikasi akhir menunjukkan bahwa protokol Horn- Preneel yang sudah diperbaiki berhasil memenuhi semua sifat keamanan yang diinginkan.