Verifikasi protokol autentikasi andrew secure RPC dengan proverif

Pamela Indrajati Suryoputro, author

Abstrak

Protokol kriptografi adalah suatu aturan pertukaran informasi yang menggunakan operasi-operasi kriptografi dan dirancang untuk memenuhi tujuan keamanan tertentu, misalnya terjaminnya kerahasiaan informasi yang dipertukarkan (secrecy/confidentiality), autentikasi pihak-pihak yang berkomunikasi (authentication), dan lain-lain. Merancang protokol yang memenuhi tujuan keamanan yang diharapkan bukanlah pekerjaan yang mudah. Seringkali ditemukan lubang keamanan pada protokol yang diperkirakan aman. Salah satu cara yang dapat digunakan untuk memverifikasi atau menganalisa keamanan suatu rancangan protokol adalah model checking.

Fokus dari Tugas Akhir ini adalah mempelajari verifikasi protokol kriptografi dengan salah satu model checker yaitu ProVerif. Dalam Tugas Akhir ini, verifikasi dilakukan terhadap keempat varian protokol autentikasi Andrew Secure Remote Procedure Call (RPC). Keempat varian protokol tersebut dimodelkan dengan representasi process calculus yang digunakan oleh ProVerif. Selain pemodelan protokol, juga dilakukan pemodelan tujuan keamanan menurut empat definisi autentikasi yaitu aliveness, weak agreement, noninjective agreement, dan agreement.

Hasil verifikasi memberikan konfirmasi terhadap attack yang pernah diklaim sebelumnya. Selain itu, hasil analisa alur attack yang diberikan ProVerif juga menunjukkan beberapa pelanggaran definisi autentikasi di atas yang belum pernah diklaim sebelumnya. Pada protokol original Andrew Secure RPC, ditemukan pelanggaran aliveness, weak agreement, non-injective agreement, dan agreement sebuah pihak initiator oleh pihak responder. Kemudian pada protokol BAN-modified Andrew Secure RPC, ditemukan pelanggaran aliveness, weak agreement, non-injective agreement, dan agreement sebuah pihak initiator oleh pihakresponder dan sebaliknya.