INTISARI

PEMBUATAN *COUNTEREXAMPLE* PADA ALGORITMA PENGUJIAN KEAMANAN PROTOKOL *PING-PONG*

Oleh

ERWIN EKO WAHYUDI
12/334631/PA/14864

Penggunaan protokol pengiriman pesan yang "kurang benar" akan rentan terhadap serangan aktif terhadap jaringan. Suatu protokol pengiriman pesan dikatakan aman jika seorang penyabot Z tidak bisa memperoleh pesan asli M yang dikirim. Pada tugas akhir ini, dilakukan implementasi algoritma pengujian protokol pengiriman pesan yang diajukan oleh Dolev dkk. (1982), yaitu mengecek apakah terdapat *string* γ sehingga $\overline{\gamma} = \lambda$. Pembuatan algoritma pencarian *counterexample* untuk protokol yang telah teruji tidak aman juga dilakukan. Algoritma yang diajukan sedikit modifikasi dari Algoritma BFS (*Breadth-First Search*). Jika k adalah panjang *string* γ yang memenuhi $\overline{\gamma} = \lambda$ dan l adalah banyak perulangan dari protokol, algoritma yang diajukan memiliki kompleksitas waktu $\mathcal{O}\left(\frac{kn^{k+1} - (k+1)n^k + 1}{(n-1)^2}\right)$ dan kompleksitas memori $\mathcal{O}(kn^{k-1})$ dengan $n = 10 + 6l$.

Kata kunci: keamanan protokol, protokol *ping-pong*, kriptografi, *finite state automata* (FSA)

ABSTRACT

COUNTEREXAMPLE GENERATION FOR PING-PONG PROTOCOL SECURITY CHECKING ALGORITHM

By

ERWIN EKO WAHYUDI
12/334631/PA/14864

An improperly designed protocol for sending a message could be vulnerable to an active saboteur. A protocol for sending a message is called secure if for any saboteur Z, one cannot obtain plaintext M. In this research, the implementation of an algorithm for checking protocol security which is proposed by Dolev et. al. (1982), stated that whether string γ exists so that $\overline{\gamma} = \lambda$, has been done. The design of an algorithm for searching counterexample in insecure protocol is proposed. The algorithm is slightly modified from BFS (Breadth-First Search) Algorithm. Let k be the length of string γ satisfies $\overline{\gamma} = \lambda$ and l be the number of looping in a protocol, the proposed algorithm runs in $\mathcal{O}\left(\frac{kn^{k+1} - (k+1)n^k + 1}{(n-1)^2}\right)$ time-complexity and $\mathcal{O}(kn^{k-1})$ memory-complexity, where $n = 10 + 6l$.

Keyword: protocol security, ping-pong protocol, cryptography, finite state automata (FSA)