INTISARI

ANALISIS KELEMAHAN ALGORITME ENKRIPSI ADVANCED ENCRYPTION STANDARD (AES) TERHADAP SERANGAN CHOSEN PLAINTEXT PADA MODE OPERASI ELECTRONIC CODE BOOK (ECB) PADA SISTEM AUTENTIKASI

Salah satu algoritme enkripsi simetris utama yang digunakan saat ini adalah *Advanced Encryption Standard* (AES). Meskipun algoritme ini masih digunakan sampai saat ini, beberapa peneltian sebelumnya telah membuktikan bahwa algoritme enkripsi AES masih memiliki kelemahan terhadap jenis serangan tertentu.

Penelitian ini membahas tentang kelemahan dari penerapan algoritme enkripsi AES dengan menggunakan mode operasi ECB. Pada penelitian ini dibuat suatu sistem sederhana berbarsis web yang menjalankan algoritme enkripsi AES-ECB pada proses autentikasi. Serangan yang digunakan adalah *chosen plaintext.* Tujuan dari serangan ini adalah untuk mendapatkan pesan dari *cookies* yang terenkripsi pada proses autentikasi serta melakukan perubahan terhadap pesan tersebut sehingga bisa mendapatkan hak akses admin.

Dari penelitian ini, didapatkan hasil bahwa implementasi algoritme enkripsi AES-ECB dengan memberikan akses kepada *user* untuk menyisipkan *plaintext* pada proses autentikasi memiliki celah keamanan. Untuk mencegah celah keamanan ini, dibuat *security advisory* yang berisi saran perbaikan sistem. Saran perbaikan ini yaitu penyaringan *input user*, pembatasan jumlah *input user* serta melakukan pengecekan integritas data. Ketiga saran ini telah dicoba dan berhasil untuk mencegah serangan *chosen plaintext*.

Kata kunci : AES, ECB, serangan chosen plaintext, mode operasi

ABSTRACT

ANALYSIS OF WEAKNESSES OF ADVANCED ENCRYPTION STANDARD (AES) AGAINST CHOSEN PLAINTEXT ATTACK ON ELECTRONIC CODE BOOK (ECB) MODE OF OPERATION ON AUTHENTICATION SYSTEMS

One of the main symmetric encryption algorithms in use today is Advanced Encryption Standard (AES). However, several previous research have proven that the AES encryption algorithm still has weaknesses against certain types of attacks.

This research discusses the weaknesses of the application of the AES encryption algorithm using the ECB operating mode. In this research, a simple web-based system is created that runs the AES-ECB encryption algorithm in the authentication process. The attack used is the chosen plaintext. The purpose of this attack is to get messages from cookies that are encrypted in the authentication process and make changes to these messages so that they can get admin access.

From this research, it was found that the implementation of the AES-ECB encryption algorithm by giving access to the user to insert plaintext in the authentication process has a security hole. To prevent this security hole, a security advisory was made containing suggestions for system improvement. Suggestions for this improvement are filtering user input, limiting the number of user inputs and checking data integrity. These three suggestions have been implemented and succeeded to prevent chosen plaintext attack.

Keyword : AES, ECB, chosen plaintext attack, mode of operation