INTISARI

Proof of Concept Serangan *Padding Oracle* Pada Penyandian AES Dengan Mode PCBC

Oleh

Rafie Muhammad
16/398524/PA/17485

Advanced Encryption Standard (AES) merupakan salah satu algoritme kriptografi kunci simetris untuk mengamankan pengiriman data pada perangkat lunak dan perangkat keras. AES sendiri memiliki beberapa mode aplikasi yang dapat digunakan, salah satunya adalah mode *Propagating Cipher Block Chaining* (PCBC). Meskipun bersifat standar, algoritme ini dengan beberapa penerapannya masih rentan terhadap serangan kriptanalisis. Sejumlah penelitian pada penyandian AES menggunakan berbagai macam teknik serangan untuk membuktikan celah keamanan pada penerapan AES. Salah satu teknik yang digunakan adalah serangan *padding oracle* yang memanfaatkan informasi pesan *error* pada validasi *padding*.

Penelitian ini menjabarkan sebuah *proof of concept* eksploitasi pada suatu penerapan AES-PCBC yang menampilkan informasi terkait validasi *padding* dari *plaintext*. *Proof of concept* diawali dengan usaha untuk mendapatkan pesan asli dari suatu pesan yang terenkripsi dan melakukan modifikasi terhadap pesan yang terenkripsi agar menjadi pesan asli yang diinginkan pada saat proses dekripsi. Pada percobaannya, digunakan sebuah *webservice* sederhana sebagai target serangan dengan menerapkan kustom enkripsi pada *cookies* autentikasi menggunakan AES-PCBC.

Dari hasil penelitian yang diperoleh, didapatkan bahwa penerapan AES-PCBC secara independen untuk proses autentikasi ditambah dengan diberikannya informasi terkait validitas suatu *padding* dapat menimbulkan celah keamanan *padding oracle*. Selain itu, dari hasil eksperimen didapatkan bahwa waktu eksekusi untuk eksploitasi cukup singkat sehingga memungkinkan untuk terjadinya serangan secara masif. Untuk mencegah celah kemanan yang telah diteliti, akan diberikan beberapa *security advisory*.

Kata kunci : *kriptografi, AES, PCBC, serangan kriptografi, padding oracle, exploit, proof of concept, security advisory*

ABSTRACT

PROOF OF CONCEPT ORACLE PADDING ATTACK ON AES ENCRYPTION WITH PCBC MODE

By

Rafie Muhammad

Advanced Encryption Standard (AES) is one of the symmetric key cryptographic algorithms to secure data transmission on software and hardware. AES itself has several application modes that can be used, one of which is the Propagating Cipher Block Chaining (PCBC) mode. Although standard, this algorithm with some applications is still vulnerable to cryptanalysis. A number of studies on AES encryption use a variety of attack techniques to prove security loopholes in the application of AES. One of the techniques used is the padding oracle attack that uses error message information on padding validation.

This study describes a proof of concept exploitation of an AES-PCBC application that displays information related to validation padding from the text. Proof of concept begins with an attempt to get the original message from an encrypted message and modifies the encrypted message to make the original message desired during the decryption process. In the experiment, a simple webservice was used as an attack target by implementing custom encryption on authentication cookies using AES-PCBC.

From the research results obtained, it was found that the application of AES-PCBC independently for the authentication process coupled with the provision of information related to the validity of a padding can lead to padding oracle vulnerability. In addition, the experimental results show that the execution time for exploitation is short enough to allow for massive attacks. To prevent security holes that have been studied, several security advisory will be given.

Keywords : *cryptography, AES, PCBC, cryptographic attack , padding oracle, exploit, proof of concept, security advisory*