Analisis Keamanan Protokol Kriptografi Pada Aplikasi Enkripsi Desktop Menggunakan Pendekatan V erifikasi Formal: Studi Keamanan pada Aplikasi ABC = Cryptographic Protocols Security Analysis in Desktop Encryption Application Using Formal Verification Approach: Security Studies in ABC Applications

Agung Widodo, author

Abstrak

Memasuki era transformasi digital, pertukaraan informasi menjadi aspek paling vital bagi hampir seluruh organisasi, terlebih lagi informasi rahasia dan strategis. Beragam preseden buruk tentang kebocoran informasi rahasia dan strategis di Indonesia menjadi tamparan keras yang harus dijawab dengan solusi efektif. Instansi XYZ telah mengembangkan aplikasi enkripsi file ABC pada tahun 2020 untuk menjawab tantangan pengamanan informasi rahasia khususnya yang ditransmisikan pada kanal elektronik. Hingga tahun 2022, aplikasi ABC telah diimplementasikan secara terbatas dan rencananya, skala implementasi akan diperluas secara nasional. Selang 2 tahun masa operasional, Instansi XYZ telah melakukan kajian terhadap keamanan algoritma yang digunakan dalam Aplikasi ABC, namun belum melakukan kajian mendalam terhadap keamanan rangkaian protokol yang digunakan dalam Aplikasi tersebut. Pada peneitian ini dilakukan analisis keamanan protokol registrasi, verifikasi pengguna, pembangkitan kunci, dan permintaan kunci untuk proses enkripsi-dekripsi Aplikasi ABC dengan pendekatan verifikasi formal menggunakan Scyther Tool. Analisis berfokus pada aspek jaminan kerahasiaan informasi dan autentikasi dengan empat kriteria yaitu secrecy, aliveness, synchronization, dan agreement. Hasil percobaan menunjukkan bahwa protokol-protokol tersebut telah menenuhi kriteria secrecy untuk informasi rahasia yang ditransmisikan namun memiliki kelemahan umum pada pada autentikasi khususnya untuk kriteria synchronization dan agreement. Berdasarkan kelemahan tersebut, peneliti mengajukan desain konseptual protokol yang mampu mengatasi kelemahan-kelemahan yang teridentifikasi. Hasilnya, desain protokol yang diajukan peneliti terbukti provably secure berdasarkan hasil pengujian dan memenuhi empat kriteria keamanan pada aspek kerahasiaan informasi dan autentikasi entitas dan isi pesan.

.....In the era of digital transformation, information exchange, especially confidential and strategic information has become the most vital aspect for almost all organizations. Various bad precedents regarding classified and strategic information leaks in Indonesia have become a slap in the face that must be acknowledge and answered with effective solutions. In 2020, XYZ Agency developed a file encryption application (ABC Application) to address the challenge of securing confidential information, especially those transmitted on electronic channels. Until 2022, the ABC Application has been implemented in a limited scope and its implementation is planned to be expanded nationally. After 2 years of operation, the XYZ Agency has conducted a study on the security of the algorithm used in ABC Application, but unfortunately has not conducted an in-depth study regarding the security of the protocol suite used in the Application. In this research, a security analysis of ABC application protocol suites, namely the registration protocol, user verification, key generation, and key request for the encryption-decryption process protocol was conducted through formal verification approach using the Scyther Tool. The analysis focuses on aspects of guaranteeing confidentiality of information and authentication with four criteria, namely secrecy,

aliveness, synchronization, and agreement. The experimental results showed that these protocols meet the security criteria for the transmitted confidential information but have general weaknesses in the authentication aspect, especially for synchronization and agreement criteria. Based on these identified weaknesses, We proposed a robust conceptual protocol design to overcome these weaknesses. As a result, the proposed design was proved to be provably secure based on the test results and met the four security criteria in the aspects of information confidentiality and authentication in terms of entity authentication and message content integrity.