Analisis Formal dan Perancangan Peningkatan Keamanan Protokol Kriptografi pada Aplikasi Manajemen Kunci XYZ = Formal Analysis and Design Security Improvement of Cryptographic Protocol in XYZ Key Management Applications

Indra Dimas Nurdiyanto, author

Abstrak

Indonesia sejalan dengan pesatnya perkembangan teknologi dan informasi. Menjawab tantangan tersebut instansi ABC mengembangkan aplikasi XYZ sebagai salah satu solusi dalam pengamanan data dan informasi. Oleh karena itu, untuk memastikan kemampuan aplikasi tersebut dalam memberikan jaminan keamanan kepada pengguna, pada penelitian ini dilakukan analisis dan verifikasi keamanan protokol kriptografi aplikasi XYZ. Analisis dan verifikasi dilakukan melalui pendekatan verifikasi formal menggunakan alat bantu Scyther dengan focus pada protokol verifikasi pengguna, pembangkitan kunci, dan permintaan kunci untuk proses enkripsi-dekripsi. Hasil analisis menunjukan bahwa protokol-protokol tersebut telah menenuhi kriteria secrecy untuk informasi rahasia yang ditransmisikan namun memiliki kelemahan pada aspek autentikasi. Penerapan sharedsecret dan rangkaian cryptographic nonce terbukti mampu mengatasi kelemahan pada protokol verifikasi pengguna aplikasi XYZ.
.....The increasing threats and attacks that result in data leakage in Indonesia are in line with the rapid development of technology and information. Responding to these challenges, the ABC agency developed the XYZ application as a solution for data and information security. Therefore, to ensure the application's ability to provide security guarantees to users, this research analyzes and verifies the security of the XYZ application cryptographic protocol. Analysis and verification is carried out through a formal verification approach using Scyther tools with a focus on user verification protocols, key generation, and key requests for the encryption-decryption process. The results of the analysis show that these protocols have met the secrecy criteria for transmitted confidential information but have weaknesses in the authentication aspect. The application of shared secret and a series of cryptographic nonces is proven to be able to overcome weaknesses in the XYZ application user verification protocol.