Verifikasi formal protokol otentikasi dan komunikasi suara perangkat X menggunakan Scyther Tool = Formal verification of the authentication and voice communication protocol security on device X using Scyther Tool

Muhamad Al Fikri, author

Abstrak

Di era saat ini, kepemilikan terhadap informasi strategis dan kemampuan untuk mengelola informasi tersebut secara efektif telah menjadi suatu keunggulan yang signifikan. Berkaca dari pengalaman mengenai serangan terhadap komunikasi strategis di Indonesia diantaranya penyadapan percakapan Presiden Susilo Bambang Yudhoyono melalui jaringan Selular dan penyadapan rumah dinas Presiden Jokowi, kemudian Indonesia menaruh perhatian lebih terhadap keamanan pada sektor ini. Perangkat X adalah salah satu alat komunikasi strategis rahasia yang digunakan di Indonesia. Penggunaan perangkat ini digagas oleh Instansi XYZ. Hingga tahun 2020, telah terdapat 1.284-unit Perangkat X yang digunakan secara luas oleh TNI, POLRI, dan instansi lain yang bersifat strategis di Indonesia. Dalam selang 5 tahun operasional, Instansi XYZ telah melakukan kajian terhadap keamanan algoritma yang digunakan dalam Perangkat X, namun di satu sisi belum pernah dilakukan kajian terhadap keamanan protokol otentikasi dan komunikasi dari perangkat tersebut. Pada peneitian ini dilakukan analisis keamanan protokol komunikasi suara dan otentikasi Perangkat X dengan pendekatan verifikasi formal menggunakan Scyther Tool untuk melengkapi kajian keamanan Perangkat X sebagai salah satu perangkat komunikasi strategis rahasia di Indonesia. Analisis berfokus pada aspek jaminan kerahasiaan informasi dan otentikasi dengan empat kriteria yaitu secrecy, aliveness, synchronization, dan agreement. Hasil percobaan menunjukkan bahwa protokol otentikasi dan komunikasi suara Perangkat X dinilai telah menenuhi kriteria secrecy untuk informasi rahasia yang ditransmisikan namun belum memenuhi kriteria aliveness, synchronization, dan agreement pada beberapa entitas yang terlibat dalam protokol tersebut. Sehingga, protokol otentikasi dan komunikasi suara Perangkat X dapat dikatakan aman berdasarkan aspek kerahasiaan informasi, namun belum aman dilihat dari aspek otentikasi.

<hr>

In the current era, the ownership of strategic information and the ability to effectively manage it has become a significant advantage. Reflecting on the experience of attacks on strategic communications in Indonesia, including the tapping of President Susilo Bambang Yudhoyono's conversation through the Cellular network and the tapping of President Jokowi's official residence, therefore Indonesia pays more attention to security in this sector. Device X is one of the secret strategic communication tools used in Indonesia. The XYZ Agency initiated the use of this device. Until 2020, there have been 1,284 X Device units widely used by the Army, Police Officer, and other strategic agencies in Indonesia. In 5 years of operation, the XYZ Agency has researched the algorithm security used in Device X, but on the one hand, there has never been a study of the security regarding the authentication and communication protocols of this device. This research aims to make a security analysis of voice communication and authentication protocols of Device X. The research was implemented using Scyther Tool as a formal verification approach. The analysis focuses on aspects of guaranteeing the confidentiality of information and authentication with four criteria, namely secrecy,

aliveness, synchronization, and agreement. The experimental results show that the authentication and voice communication protocol of Device X is considered to have satisfied the secrecy criteria for transmitted confidential information but does not satisfy the criteria of aliveness, synchronization, and agreement on several entities involved in the protocol. Thus, the authentication and voice communication protocol of Device X can be claimed to be provably secure based on the confidentiality aspect of information but is not from the authentication aspect.