OTENTIKASI PASSWORD PENGGUNA MENGGUNAKAN ZERO KNOWLEDGE PROTOCOL

Sandromedo Christa Nugroho1), Wahyu Indah Rahmawati 2)
Lembaga Sandi Negara
Jl. Harsono RM No.70 Ragunan Ps.Minggu Jakarta Selatan -12550
Telp.021-7805814, Fax.021-78844104
major.ruft@gmail.com1) , indah.as.ayu@gmail.com2)

Abstract

Globalization has an impact on the development of science and technology, where the mentioned development also given impact to the development of information security. Information security has 3 (three) main aspects, among others confideality, integrity, and authentication. Authentication is a process that ensures that both parties believe (with evidence) the identity of the first party. There are several ways to perform authentication, like using something known, something possessed, and something inherent. Practically, authentication is generally done by using password that consists of 6 (six) to 10 (ten) characters. The use of passwords in authenticated user have less secure and weaker, beside that there are some attacks that can be applied by the use of password for authentication, including replays of fixed passwords, passwords exhaustive search, and password-guessing and dictionary attacks. The use of passwords also has some drawbacks, among others a person tends to be difficult to remember long passwords, where password generally consist of date or things that are easy to remember and liked by the user, making it easier for an unauthorized person to guess the password. One solution that can be used to address the weaknesses found in the use of passwords as an authentication is by using the Zero Knowledge Protocol.

Keywords: Information Security, Authentication, Password, Zero Knowledge Protocol

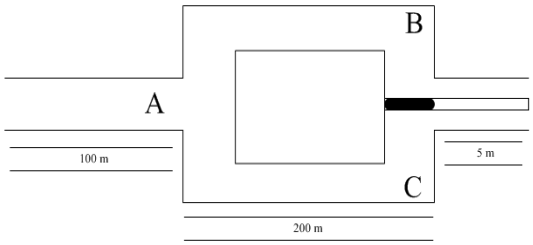
1. Pendahuluan

Perkembangan teknologi dan informasi di era globalisasi telah memberikan dampak pada perkembangan keamanan informasi. Dahulu orang-orang mungkin merasa aman dengan penggunaan password sebagai teknik otentikasi dalam pelindungan data-data yang bersifat pribadi, namun seiring dengan perkembangan jaman dan dengan ditemukannya serangan-serangan yang dapat membreak password seseorang dengan sangat mudah dan cepat, seperti replay of fixed password, exhaustive password search, dan password-guessing and dictionary attacks, maka penggunaan password sudah dianggap kurang aman dan lemah.

Selain itu penggunaan password juga memiliki kelemahan utama, yaitu sulitnya mengingat atau menghapal password yang digunakan, hal ini tentunya dapat merugikan diri kita sendiri, terlebih jika data-data yang kita amankan dengan menggunakan password tersebut adalah data-data yang bersifat penting dan rahasia. Kekurangan lainnya dalam penggunaan password adalah penggunaan satu password yang sama untuk banyak account atau proteksi data, hal ini memang memudahkan kita dalam mengingat password, namun dapat juga menjadi bumerang, jika satu saja account kita dapat dipecahkan oleh pihak-pihak yang tidak berwenang, dimana password tersebut akan dapat digunakan untuk membuka account-account kita yang lain. Masalah keamanan pada penggunaan password, bukan merupakan masalah yang tidak dapat diselesaikan. Dengan menggunakan teknik dan ilmu kriptografi, kita dapat memanfaatkan sebuah protokol keamanan yang dapat berfungsi sebagai teknik otentikasi pengganti password yang tentu saja tingkat keamannya lebih kuat daripada penggunaan password semata. Protokol tersebut adalah protokol Zero Knowledge.

2. Gambaran Umum Protokol *Zero Knowledge*

Protokol Zero Knowledge adalah mekanisme atau protokol, dimana seorang dengan rahasia tertentu, yaitu Denis, dapat meyakinkan pengujinya, yaitu Erlang, bahwa Denis mengetahui rahasia tersebut, tanpa membuka rahasianya kepada Erlang atau orang lain. Rahasia yang diketahui oleh Denis sebagai pihak *prover* memiliki konsekuensi yang dapat diperiksa oleh Erlang sebagai pihak *verifier*. Konsep protokol Zero Knowledge dapat dijelaskan dengan menggunakan analogi gua atau terowongan yang memiliki percabangan pada jalan keluarnya. Konsep protokol Zero Knowledge ditunjukkan pada Gambar 1.



Gambar 1. Konsep Protokol Zero Knowledge