SKRIPSI

PEMBANGUNAN PERANGKAT LUNAK YANG MENGIMPLEMENTASIKAN METODE SECRET SHARING UNTUK BERBAGI PASSWORD

Abraham Sri Paskah Ageng Wahono

NPM: 2012730072

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNOLOGI INFORMASI DAN SAINS
UNIVERSITAS KATOLIK PARAHYANGAN

2017

UNDERGRADUATE THESIS

SECRET SHARING METHODS SOFTWARE IMPLEMENTATION FOR DISTRIBUTING PASSWORD

Abraham Sri Paskah Ageng Wahono

NPM: 2012730072

DEPARTMENT OF INFORMATICS
FACULTY OF INFORMATION TECHNOLOGY AND SCIENCES
PARAHYANGAN CATHOLIC UNIVERSITY
2017

LEMBAR PENGESAHAN

PEMBANGUNAN PERANGKAT LUNAK YANG MENGIMPLEMENTASIKAN METODE SECRET SHARING UNTUK BERBAGI PASSWORD

Abraham Sri Paskah Ageng Wahono

NPM: 2012730072

Bandung, 20 Desember 2017

Menyetujui,

Pembimbing

Mariskha Tri Adithia, P.D.Eng

Ketua Tim Penguji

Rosa De Lima, M.Kom.

Anggota Tim Penguji

Husnul Hakim, M.T.

Mengetahui,

Ketua Program Studi

Mariskha Tri Adithia, P.D.Eng

PERNYATAAN

Dengan ini saya yang bertandatangan di bawah ini menyatakan bahwa skripsi dengan judul:

PEMBANGUNAN PERANGKAT LUNAK YANG MENGIMPLEMENTASIKAN METODE SECRET SHARING UNTUK BERBAGI PASSWORD

adalah benar-benar karya saya sendiri, dan saya tidak melakukan penjiplakan atau pengutipan dengan cara-cara yang tidak sesuai dengan etika keilmuan yang berlaku dalam masyarakat keilmuan.

Atas pernyataan ini, saya siap menanggung segala risiko dan sanksi yang dijatuhkan kepada saya, apabila di kemudian hari ditemukan adanya pelanggaran terhadap etika keilmuan dalam karya saya, atau jika ada tuntutan formal atau non-formal dari pihak lain berkaitan dengan keaslian karya saya ini.

Dinyatakan di Bandung,
Tanggal 20 Desember 2017

Abraham Sri Paskah Ageng Wahono
NPM: 2012730072

ABSTRAK

Password adalah salah satu teknik otentikasi entitas yang umum digunakan untuk memperoleh hak akses pada suatu sistem. Teknik otentikasi menggunakan *password* masih memiliki kelemahan dari segi keamanan. Permasalahan yang sering kali ditemui adalah hilangnya *password* atau rusaknya kerahasiaan *password* karena adanya serangan dari pihak yang tidak bertanggung jawab. *Password* bisa saja dibuat salinannya dan disimpan di beberapa tempat, namun cara ini tidak aman karena berisiko menurunkan tingkat kerahasiaan *password*. Karena itu diperlukan cara untuk membagikan *password* tanpa merusak kerahasiaan dari *password*.

Metode *secret sharing* dapat digunakan untuk membagikan pesan rahasia kepada sejumlah partisipan tanpa memberikan informasi mengenai pesan rahasia tersebut. Pada skema *threshold secret sharing* (k, n), pesan rahasia akan dibagikan ke sejumlah n partisipan. Setiap partisipan akan memperoleh bagian dari pesan rahasia yang berupa *share*. Pesan rahasia hanya dapat diperoleh kembali dengan menggabungkan minimal k buah *share*.

Pada skripsi ini akan dibangun perangkat lunak yang dapat mengimplementasikan penggunaan metode *secret sharing* untuk membagikan *password*. Skripsi ini akan menggunakan dua buah metode *secret sharing* yaitu metode *secret sharing* Shamir dan metode *secret sharing* Blakley. Berdasarkan hasil pengujian yang dilakukan, dapat disimpulkan bahwa perangkat lunak yang dibangun dapat mengimplementasikan penggunaan metode *secret sharing* Shamir dan metode *secret sharing* Blakley untuk membagikan *password*.

Kata-kata kunci: *Password*, Otentikasi Entitas, *Secret Sharing*, metode *Secret Sharing* Shamir, metode *secret sharing* Blakley

ABSTRACT

Password is one of the most commonly used entity authentication technique to prove identity or access approval to gain access to a system. The usage of password as an authentication technique somehow still have several flaws. Some problems that may occur are lost/forgotten password or on several ocassions, malicious attack from intruders that can corrupt the anonymous password. Copies of password can be created and stored on various places, but by doing this the secrecy of password can be harmed.

Secret sharing methods can be used to distribute a secret message to several participants while maintaining the secrecy of said message by not giving any information about the secret message to any participants. By using (k, n) threshold secret sharing scheme, secret message can be distributed amongst group of n participants. Every participants will receive part of the secret message called "share" and secret message can be reconstructed only when a sufficient k number of participants come together and combine their part of the share.

In this undergraduate thesis, a software is developed to implement the usage of secret sharing methods for distributing password. There are two different secret sharing methods that are used in this undergraduate thesis, those methods are Shamir's secret sharing and Blakley's secret sharing. Based on the tests done, it can be concluded that the software built in this undergraduate thesis can implement password distribution using Shamir's secret sharing and Blakley's secret sharing.

Keywords: Password, Entity Authentication, Secret Sharing, Shamir's Secret Sharing, Blakley's Secret Sharing

Dipersembahkan untuk Tuhan Yang Maha Esa, orang tua, pembimbing, dan semua orang yang telah membantu pembuatan skripsi ini

KATA PENGANTAR

Puji syukur penulis panjatkan ke hadirat Tuhan Yang Maha Esa karena atas berkat dan rahmat-Nya penulis berhasil menyelesaikan penyusunan skripsi yang berjudul "Pembangunan Perangkat Lunak yang Mengimplementasikan Metode *Secret Sharing* untuk Berbagi *Password*". Penulis menyadari bahwa penyelesaian penyusunan skripsi ini tidak terlepas dari bantuan dan dukungan berbagai pihak, oleh karena itu penulis ingin mengucapkan terima kasih kepada:

- Bu Mariskha atas bimbingannya yang sangat membantu penulis sepanjang proses penyusunan skripsi ini.
- Kedua orang tua atas dukungan dan kesabarannya.
- Gavrila yang selalu setia mendampingi dan memberi semangat kepada penulis selama proses penyusunan skripsi.
- Bu Rosa dan Pak Husnul atas masukan dan saran yang telah diberikan sebagai dosen penguji.
- Sahabat-sahabat Kansup B2 yang selalu menghibur dan memberikan kebahagiaan sepanjang masa perkuliahan.
- Semua pihak yang tidak mungkin disebutkan satu-persatu yang sudah memberikan bantuan dan dukungan dalam pengerjaan dan penyusunan skripsi ini.

Semoga segala bantuan dan dukungan dari semua pihak tersebut mendapat berkah dari Tuhan Yang Maha Esa. Akhir kata, penulis memohon maaf apabila terdapat kekurangan dalam penyusunan skripsi ini. Semoga skripsi ini berguna bagi semua pihak yang memerlukan.

Bandung, Desember 2017

Penulis

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB 1

PENDAHULUAN

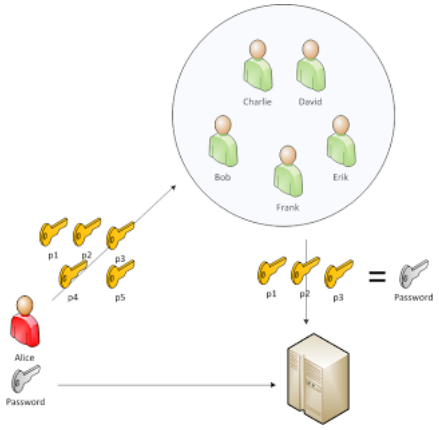
1.1 Latar Belakang

Otentikasi adalah suatu proses verifikasi untuk menentukan keaslian identitas dari pihak yang ingin mengakses sumber daya atau informasi yang terdapat pada sebuah sistem. Dengan otentikasi, dapat ditentukan apakah seseorang berhak atau tidak untuk mengakses sumber daya atau informasi pada sistem tersebut [1]. Terdapat dua jenis proses otentikasi yaitu otentikasi pesan dan otentikasi entitas. Perbedaan utama dari kedua proses otentikasi tersebut terdapat pada saat proses-proses otentikasi tersebut dilakukan. Pada proses otentikasi pesan, proses otentikasi tidak perlu dilakukan secara *real time* yang artinya pesan yang dikirim dapat diotentikasi kapan saja setelah pesan tersebut diterima. Sementara pada proses otentikasi entitas, proses verifikasi hanya dapat berjalan apabila pihak yang ingin diotentikasi berkomunikasi secara langsung dengan pihak yang mengotentikasi.

Salah satu teknik otentikasi entitas yang umum digunakan adalah *password*. *Password* adalah kode rahasia atau kata sandi yang diketahui oleh entitas (dalam hal ini dapat berupa orang atau proses), yang merupakan kunci untuk bisa mengakses atau membuka suatu sistem yang dikunci [2]. *Password* dapat berupa kombinasi dari karakter alfabet, angka, dan simbol. Teknik otentikasi menggunakan *password* memiliki beberapa kelemahan dari segi keamanan. Permasalahan yang sering kali ditemui adalah hilangnya *password* atau rusaknya kerahasiaan *password* karena adanya serangan dari pihak yang tidak bertanggung jawab. *Password* bisa saja dibuat salinannya dan disimpan di beberapa tempat, namun cara ini tidak aman karena berisiko menurunkan tingkat kerahasiaan *password* [2]. Salinan *password* dapat mengalami kebocoran dan dapat disalahgunakan oleh pihak yang tidak berwenang. Selain itu, untuk suatu sistem yang di dalamnya terdapat informasi yang bersifat sangat penting diperlukan proses otentikasi yang tingkat keamanannya lebih tinggi. Proses otentikasi yang hanya membutuhkan satu entitas tidak cukup aman untuk mengamankan sistem tersebut. Diperlukan suatu cara untuk membagikan *password* ke beberapa entitas tanpa menurunkan tingkat kerahasiaan *password*.

Cara yang dapat digunakan untuk mengatasi permasalahan tersebut adalah dengan menggunakan metode *secret sharing*. *Secret sharing* merupakan metode untuk merahasiakan pesan dengan cara membagikan pesan rahasia kepada beberapa partisipan di mana setiap partisipan akan memperoleh bagian dari pesan rahasia yang disebut dengan *share* [3]. Setiap partisipan akan mendapatkan *share* yang berbeda-beda dan partisipan-partisipan tersebut sama sekali tidak memiliki informasi mengenai pesan rahasia yang dibagikan. Pada skema *threshold secret sharing* (k, n), pesan rahasia S akan dibagikan ke n buah partisipan dan pesan rahasia hanya dapat diperoleh kembali dengan mengumpulkan k buah *share* atau lebih [4]. Metode ini dapat meningkatkan tingkat keamanan sistem yang proses otentikasinya menggunakan *password* karena dengan membagikan pesan rahasia ke beberapa partisipan, proses otentikasi yang dibutuhkan untuk memperoleh akses ke suatu sistem menjadi berlapis-lapis. Ilustrasi skema *threshold secret sharing* dapat dilihat pada Gambar 1.1.

Terdapat beberapa metode *threshold secret sharing* (k, n) yang dapat digunakan untuk membagikan pesan rahasia. Pada skripsi ini akan dibahas dua buah metode *threshold secret sharing* (k, n) yang dapat digunakan untuk membagikan pesan rahasia. Metode-metode tersebut adalah metode *secret sharing* Shamir dan metode *secret sharing* Blakley. Pada bab selanjutnya akan



Gambar 1.1: Skema *threshold secret sharing* $(3, 5)$

dibahas secara lebih dalam mengenai perbedaan antara kedua metode *threshold secret sharing* (k, n) tersebut beserta cara kerja masing-masing metode *secret sharing* Shamir dan *secret sharing* Blakley.

Pada skripsi ini akan dibangun perangkat lunak yang dapat mengimplementasikan metode-metode *secret sharing* yang digunakan untuk membagikan *password*. Perangkat lunak yang dibangun akan mengimplementasikan dua buah metode *secret sharing* yaitu metode *secret sharing* Shamir dan metode *secret sharing* Blakley. Perangkat lunak yang mengimplementasikan metode-metode tersebut akan diuji dengan berbagai kasus. Pengujian yang dilakukan akan menggunakan teknik pengujian fungsional dan pengujian eksperimental. Dari hasil pengujian tersebut akan ditarik kesimpulan apakah perangkat lunak yang dibangun dapat mengimplementasikan metode *secret sharing* Shamir dan metode *secret sharing* Blakley dengan tepat.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah dijelaskan di atas, rumusan masalah pada skripsi ini adalah:

1. Bagaimana cara kerja metode *secret sharing* Shamir?
2. Bagaimana cara kerja metode *secret sharing* Blakley?
3. Bagaimana cara mengimplementasikan penggunaan skema *secret sharing* Shamir dan *secret sharing* Blakley untuk membagikan *password*.

1.3 Tujuan

Untuk menjawab rumusan masalah di atas, maka tujuan yang ingin dicapai dari skripsi ini adalah:

1. Mempelajari cara kerja metode *secret sharing* Shamir.
2. Mempelajari cara kerja metode *secret sharing* Blakley.
3. Membangun perangkat lunak yang dapat mengimplementasikan pembagian *password* menggunakan metode *secret sharing* Shamir dan metode *secret sharing* Blakley.

1.4 Batasan Masalah

Batasan masalah untuk skripsi ini adalah sebagai berikut:

1. Untuk metode *secret sharing* Blakley, skema *threshold secret sharing* yang dapat digunakan adalah skema (3,3) di mana terdapat 3 *threshold* dan 3 buah partisipan.

1.5 Metodologi

Metodologi yang digunakan dalam penyusunan skripsi ini adalah sebagai berikut:

1. Melakukan studi literatur mengenai dasar-dasar kriptografi.
2. Melakukan studi literatur mengenai *secret sharing*, seperti metode-metode *secret sharing* dan cara kerjanya, beserta cara mengimplementasikan metode-metode *secret sharing*.
3. Melakukan perancangan kelas yang akan digunakan untuk mengimplementasikan *secret sharing* Shamir dan *secret sharing* Blakley.
4. Mengimplementasikan hasil perancangan kelas ke dalam bahasa pemrograman *Java*.
5. Melakukan pengujian terhadap perangkat lunak yang telah mengimplementasikan metode *secret sharing* Shamir dan *secret sharing* Blakley.
6. Menarik kesimpulan berdasarkan hasil pengujian.

1.6 Sistematika Pembahasan

Skripsi ini disusun secara sistematis ke dalam 6 bab yang terdiri dari pendahuluan, dasar teori, analisis, perancangan, implementasi dan pengujian, dan kesimpulan. Sistematika pembahasan dari skripsi ini adalah:

1. Bab 1 Pendahuluan
   Bab ini berisi latar belakang, rumusan masalah, tujuan, batasan masalah, metodologi, dan sistematika pembahasan.
2. Bab 2 Dasar Teori
   Bab ini berisi dasar teori tentang kriptografi, otentikasi pesan, *secret sharing*, metode *secret sharing* Shamir, metode *secret sharing* Blakley, dan pengkodean ASCII.
3. Bab 3 Analisis
   Bab ini berisi analisis masalah, analisis metode *secret sharing*, dan analisis perangkat lunak yang didalamnya membahas diagram aliran proses, dan diagram kelas awal.
4. Bab 4 Perancangan
   Bab ini berisi perancangan perangkat lunak yang akan dibangun yang di dalamnya meliputi kebutuhan masukan dan keluaran perangkat lunak, perancangan antarmuka perangkat lunak, diagram kelas rinci, beserta rincian metode.
5. Bab 5 Implementasi dan Pengujian
   Bab ini berisi implementasi antarmuka perangkat lunak, pengujian fungsional perangkat lunak yang mengimplementasikan metode *secret sharing* Shamir dan metode *secret sharing* Blakley, serta pengujian eksperimental perangkat lunak.
6. Bab 6 Kesimpulan
   Bab ini berisi kesimpulan dari awal hingga akhir skripsi dan saran untuk pengembangan selanjutnya.