SKRIPSI

ANALISIS KEAMANAN PROTOKOL MEGRELISHVILI

Emmanuel Yudhistira Panjipratama

NPM: 2015730043

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNOLOGI INFORMASI DAN SAINS
UNIVERSITAS KATOLIK PARAHYANGAN
2019

UNDERGRADUATE THESIS

SECURITY ANALYSIS OF MEGRELISHVILI PROTOCOL

Emmanuel Yudhistira Panjipratama

NPM: 2015730043

DEPARTMENT OF INFORMATICS
FACULTY OF INFORMATION TECHNOLOGY AND SCIENCES
PARAHYANGAN CATHOLIC UNIVERSITY
2019

LEMBAR PENGESAHAN

ANALISIS KEAMANAN PROTOKOL MEGRELISHVILI

Emmanuel Yudhistira Panjipratama

NPM: 2015730043

Bandung, 17 Mei 2019

Menyetujui,

Pembimbing

Mariskha Tri Adithia, P.D.Eng

Ketua Tim Penguji	Anggota Tim Penguji
Chandra Wijaya, M.T.	**Raymond Chandra Putra, S.T., 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:

ANALISIS KEAMANAN PROTOKOL MEGRELISHVILI

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 17 Mei 2019

Meterai
Rp. 6000

Emmanuel Yudhistira Panjipratama
NPM: 2015730043

ABSTRAK

Protokol Megrelishvili adalah salah satu protokol yang mengatur pertukaran kunci antara entitas-entitas yang ingin berkomunikasi. Protokol ini dibangun berdasarkan adaptasi konsep protokol Diffie-Hellman serta konsep aljabar linear untuk melakukan pertukaran kunci. Pada protokol ini, kunci rahasia dibangun lewat eksponensiasi matriks serta perkalian antara matriks dan vektor. Sayangnya, sampai saat ini kepraktisan dari protokol Megrelishvili masih belum dapat dibuktikan. Masih belum terdapat pengujian eksperimental yang dapat membuktikan keamanan protokol Megrelishvili. Selain itu, protokol Megrelishvili terbukti masih memiliki kelemahan, yaitu terhadap *man in the middle attack*. *Man in the middle attack* adalah serangan yang muncul ketika seorang penyerang menempatkan diri di jalur komunikasi antara dua entitas dan mencoba mengendalikan komunikasi yang terjadi antara kedua entitas tersebut.

Untuk membuktikan kepraktisan dari protokol Megrelishvili, penelitian ini akan mencoba melakukan simulasi implementasi terhadap protokol tersebut. Simulasi akan dibuat berdasarkan prosedur protokol Megrelishvili yang telah disesuaikan agar dapat berjalan secara paralel dengan bantuan dari *thread*. Penelitian ini juga akan mencoba menerapkan mekanisme pertahanan untuk mencegah terjadinya *man in the middle attack*. Terdapat dua mekanisme pertahanan yang akan dicoba untuk diterapkan, yaitu mekanisme pertahanan yang memanfaatkan vektor verifikasi dan mekanisme pertahanan yang memanfaatkan tanda tangan digital. Kedua mekanisme pertahanan tersebut digunakan untuk melakukan verifikasi pesan untuk memastikan integritas pesan-pesan yang dipertukarkan saat terjadinya komunikasi.

Penelitian ini berhasil membangun perangkat lunak yang menyimulasikan implementasi protokol Megrelishvili. Perangkat lunak yang dihasilkan dapat menerima masukan-masukan yang sesuai dengan prosedur protokol Megrelishvili yang sudah ada dan lalu memroses masukan-masukan tersebut untuk melakukan pembangunan kunci. Perangkat lunak tersebut juga dapat melakukan verifikasi pesan untuk memastikan integritas dari pesan yang dipertukarkan sebagai bentuk usaha pertahanan terhadap *man in the middle attack*. Perangkat lunak tersebut juga sudah melewati pengujian fungsional dan eksperimental sehingga terbukti telah menerapkan protokol Megrelishvili dan mekanisme pertahanan terhadap *man in the middle attack* dengan baik.

Berdasarkan penelitian dan pembangunan perangkat lunak yang telah dilakukan, dapat disimpulkan bahwa protokol Megrelishvili merupakan protokol yang dapat dipraktikkan dan diimplementasikan. Selain itu, dapat disimpulkan pula bahwa protokol Megrelishvili dapat dikembangkan agar memiliki pertahanan terhadap *man in the middle attack*, yaitu dengan memanfaatkan vektor verifikasi atau tanda tangan digital untuk melakukan verifikasi pesan.

Kata-kata kunci: protokol Megrelishvili, *man in the middle attack*, *thread*, vektor verifikasi, tanda tangan digital, verifikasi pesan, integritas,

ABSTRACT

Megrelishvili protocol is a protocol that regulates key exchange between two communicating entities. This protocol is built based on an adapted Diffie-Hellman protocol and linear algebra concept to exchange keys. In this protocol, the secret key is built by utilizing matrix exponentiation and multiplication between matrices and vectors. Unfortunately, the practicality of Megrelishvili protocol is still not yet proven. There is still no experimental test that could prove the security of this protocol. Moreover, Megrelishvili protocol is proven to be weak against man in the middle attack. Man in the middle attack is a security attack an attacker got between the communication between two communicating entities and try to control it.

To be able to prove the practicality of Megrelishvili protocol, this research is going to simulate the implementation of Megrelishvili protocol. The simulation would be made by using the procedure of said protocol that has been adapted to be able to run in parallel using computer threads. This research is also going to try to implement a defence mechanism to try to prevent man in the middle attack from happening. There are two defence mechanism that is going to be implemented, a defence mechanism that utilizes verification vector and a defence mechanism that utilizes digital signature. Both of the defence mechanism is going to be used to do message verification to make sure of the integrity of the exchanged messages.

This research has successfully built a software to simulate the implementation of Megrelishvili protocol. The built software is able to accept inputs that conforms the procedure of Megrelishvili protocol and to process said inputs to build shared secret key. Said software is also able to do message verification to make sure of the integrity of the exchanged messages as an effort to defend itself from man in the middle attack. Said software has also been through both functional and experimental testing to make sure that it has implemented both Megrelishvili protocol and defence mechanism against man in the middle attack correctly.

According to the research and the software engineering that has been done, it could be concluded that Megrelishvili protocol is both practicable and implementable. Moreover, it could also be concluded that Megrelishvili protocol could be developed further so it could have a defence mechanism against man in the middle attack by utilizing verification vector or digital signature to do message verification.

Keywords: megrelishvili protocol, man in the middle attack, computer threads, verification vector, digital signature, message verification, integrity

Untuk keluarga, para dosen, dan teman-teman yang telah memberi dukungan dalam pembuatan skripsi ini.

KATA PENGANTAR

Puji dan syukur penulis panjatkan ke hadirat Tuhan Yang Maha Esa karena atas berkat dan rahmat-Nya penulis telah berhasil menyelesaikan penyusunan skripsi ini yang berjudul "Analisis Keamanan Protokol Megrelishvili". Penulis menyadari bahwa penyusunan skripsi ini tidak akan selesai tanpa bantuan dan dukungan dari berbagai pihak, oleh karena itu penulis ingin mengucapkan terima kasih kepada:

- Ibu Mariskha Tri Adithia, P.D.Eng yang telah memberikan banyak bimbingan selama proses penyusunan skripsi.
- Kedua orang tua penulis yang telah memberikan dukungan penuh selama proses penyusunan skripsi.
- Pak Chandra Wijaya, M.T. dan Raymond Chandra Putra, S.T., M.T. yang telah memberikan banyak kritik dan saran selaku dosen penguji.
- Segenap dosen dan teman yang telah memberikan dukungan moral maupun ilmu.

Penulis berharap semoga skripsi ini dapat berguna bagi segenap pihak yang berkepentingan. Akhir kata, penulis memohon maaf apabila terdapat kekurangan dalam hasil penyusunan skripsi ini.

Bandung, Mei 2019

Penulis

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB 1

PENDAHULUAN

1.1 Latar Belakang

Pada era digital ini, keamanan data menjadi salah satu kebutuhan yang cukup penting. Salah satu metode yang dapat dipakai untuk mengamankan data adalah dengan melakukan proses enkripsi dan dekripsi. Pada proses enkripsi, data-data yang ada akan diolah agar menjadi tidak dapat dikenali maupun dimengerti dengan bantuan kunci rahasia. Pada proses dekripsi, data-data yang telah terenkripsi akan diubah kembali seperti semula menjadi dapat dikenali dan dimengerti dengan bantuan dari kunci rahasia.

Pada pengamanan data yang menggunakan proses enkripsi dan dekripsi, kunci rahasia menjadi sebuah komponen yang sangat penting dan perlu dirahasiakan. Karena kunci rahasia merupakan komponen dan perlu dirahasiakan, maka cara pertukaran kunci rahasia tidak boleh dilakukan dengan sembarangan. Dibutuhkan suatu protokol khusus untuk mengatur cara pertukaran kunci rahasia agar kunci tersebut tidak jatuh ke tangan pihak yang salah.

Salah satu protokol yang mengatur cara pertukaran kunci rahasia adalah protokol Diffie-Hellman. Keamanan pada protokol Diffie-Hellman didasari oleh konsep *discrete logarithm problem* [1]. Dengan memanfaatkan protokol ini, dua pengguna dapat melakukan pertukaran kunci rahasia tanpa harus benar-benar mengirimkan kunci rahasia tersebut.

Salah satu protokol lain yang mengatur pertukaran kunci adalah protokol Megrelishvili. Protokol ini dibangun berdasarkan adaptasi konsep protokol Diffie-Hellman serta konsep aljabar linear untuk melakukan pertukaran kunci [1]. Pada protokol ini, kunci rahasia dibangun lewat eksponensiasi matriks serta perkalian antara matriks dan vektor. Menurut teori yang ada, tidak ada batasan terhadap matriks dan vektor yang dapat diproses oleh protokol Megrelishvili, asalkan vektor dan matriks tersebut sesuai dengan batas bilangan dan ukuran yang telah ditentukan. Namun, agar dapat diterapkan dengan baik, diperlukan pembatasan yang lebih lanjut yang mengatur ketentuan matriks dan vektor yang dapat diproses oleh protokol Magrelishvili.

Sayangnya, sampai saat ini kepraktisan dari protokol Megrelishvili masih belum dapat dibuktikan. Masih belum terdapat pengujian eksperimental yang dapat membuktikan keamanan protokol Megrelishvili. Selain itu, protokol Megrelishvili terbukti masih memiliki kelemahan, yaitu terhadap *man in the middle attack* [2]. *Man in the middle attack* adalah serangan yang muncul ketika seorang penyerang menempatkan diri di jalur komunikasi antara dua entitas dan mencoba mengendalikan komunikasi yang terjadi antara kedua entitas tersebut.

Maka dari itu, perlu dilakukan implementasi dan pengujian eksperimental terhadap protokol Megrelishvili untuk membuktikan kepraktisan dan keamanan protokol tersebut. Selain itu, perlu dilakukan juga pengembangan terhadap protokol Megrelishvili untuk meningkatkan efisiensi kerja serta meningkatkan ketahanan protokol tersebut dalam menghadapi *man in the middle attack* dan serangan-serangan kriptografi lainnya.

1.2 Rumusan Masalah

Berdasarkan deskripsi yang telah dijabarkan di atas, timbul permasalahan berupa:

1. Bagaimana cara mengimplementasikan protokol Megrelishvili?
2. Bagaimana cara melakukan pengujian eksperimental terhadap protokol Megrelishvili?
3. Bagaimana cara melakukan pertahanan terhadap *man in the middle attack* pada protokol Megrelishvili?

1.3 Tujuan

Tujuan dari penelitian yang akan dilakukan ini adalah:

1. Mengimplementasikan protokol Megrelishvili.
2. Melakukan pengujian eksperimental terhadap protokol Megrelishvili.
3. Melakukan pertahanan terhadap *man in the middle attack* pada protokol Megrelishvili?

1.4 Batasan Masalah

Batasan masalah dari penelitian yang akan dilakukan ini adalah:

1. Matriks yang dijadikan matriks publik harus menghasilkan matriks yang tiap elemennya terdiri dari bilangan bulat jika diinvers. Hal ini disebabkan karena pembangunan vektor verifikasi yang dilakukan untuk melakukan pertahanan terhadap *man in the middle attack* membutuhkan operasi invers. Jika terdapat elemen yang berupa bilangan pecahan, proses modulo yang menjadi inti dari logaritma diskrit akan sulit untuk dilakukan.
2. *Man in the middle attack* yang akan disimulasikan hanyalah kasus ketika penyerang berpura-pura menjadi server. Hal ini dilakukan untuk membatasi skenario *man in the middle attack* yang dilakukan karena terdapat terlalu banyak jenis kasus *man in the middle attack*.

1.5 Metodologi

Metodologi yang dilakukan untuk menyusun penelitian ini adalah:

1. Mempelajari dasar-dasar kriptografi, khususnya protokol Diffie-Hellman dan tanda tangan digital.
2. Mempelajari protokol Megrelishvili dan metode pengamanannya, serta dasar aljabar linear yang mendasarinya.
3. Melakukan analisis terhadap protokol Megrelishvili untuk merancang pengimplementasian protokol tersebut.
4. Membangun perangkat lunak yang mengimplementasikan protokol Megrelishvili.
5. Melakukan perancangan pengujian eksperimental untuk menganalisis keamanan protokol Megrelishvili.
6. Melakukan pengujian eksperimental terhadap protokol Megrelishvili.
7. Melakukan analisis terhadap hasil pengujian protokol Megrelishvili.

1.6 Sistematika Pembahasan

Sistematika penulisan dibagi menjadi beberapa bab yang berisikan:

1. Bab 1 Pendahuluan
   Membahas latar belakang, rumusan masalah, tujuan, batasan masalah, metodologi, serta sistematika pembahasan pada penelitian ini yang berkaitan dengan protokol Megrelishvili.

2. Bab 2 Dasar Teori
   Membahas teori mengenai protokol Diffie-Hellman, protokol Megrelishvili, serangan terhadap protokol Megrelishvili, tanda tangan digital, autentikasi entitas, *advanced encryption standard*, da *unbounded lock-free queue* yang menjadi dasar pembuatan penelitian ini.

3. Bab 3 Analisis
   Membahas segala analisis mengenai perhitungan pembangunan kunci, aktor, arsitektur, inisiasi komunikasi dan pengoptimalan protokol Megrelishvili serta analisis mengenai diagram kegiatan, diagram *use case*, dan diagram kelas awal yang dibutuhkan oleh perangkat lunak yang akan dibangun.

4. Bab 4 Perancangan
   Membahas segala perancangan *input*, antarmuka, diagram *sequence*, dan diagram kelas yang akan digunakan untuk membangun perangkat lunak yang mengimplementasikan protokol Megrelishvili berdasarkan analisis yang telah dilakukan.

5. Bab 5 Implementasi dan Pengujian Perangkat Lunak
   Membahas antarmuka perangkat lunak protokol Megrelishvili yang telah mengimplementasikan rancangan yang telah disusun serta pengujian fungsional dan eksperimental terhadap perangkat lunak tersebut.

6. Bab 6 Kesimpulan dan Saran
   Membahas kesimpulan yang timbul setelah melakukan penelitian serta saran untuk melakukan penelitian lebih lanjut mengenai protokol Megrelishvili.