IMPLEMENTASI TWO FACTOR AUTHENTICATION MENGGUNAKAN PROTOKOL ZERO KNOWLEDGE PROOF PADA SISTEM LOGIN

SKRIPSI

Oleh:

HENRY SUSILO

71120151

PROGRAM STUDI TEKNIK INFORMATIKAFAKULTAS TEKNOLOGI INFORMASI

UNIVERSITAS KRISTEN DUTA WACANA

2016

IMPLEMENTASI TWO FACTOR AUTHENTICATION MENGGUNAKAN PROTOKOL ZERO KNOWLEDGE PROOF PADA SISTEM LOGIN

SKRIPSI

Diajukan kepada Program Studi Teknik Informatika Fakultas Teknologi Informasi
Universitas Kristen Duta Wacana

Sebagai Salah Satu Syarat dalam Memperoleh Gelar Sarjana Komputer

Disusun oleh:

HENRY SUSILO

71120151

PROGRAM STUDI TEKNIK INFORMATIKAFAKULTAS TEKNOLOGI INFORMASI
UNIVERSITAS KRISTEN DUTA WACANA
2016

PERNYATAAN KEASLIAN SKRIPSI

Saya menyatakan dengan sesungguhnya bahwa skripsi dengan judul:

IMPLEMENTASI TWO FACTOR AUTHENTICATION MENGGUNAKAN PROTOKOL ZERO KNOWLEDGE PROOF PADA SISTEM LOGIN

yang saya kerjakan untuk melengkapi sebagian persyaratan menjadi Sarjana Komputer pada pendidikan Sarjana Program Studi Teknik Informatika Fakultas Teknologi Informasi Universitas Kristen Duta Wacana, bukan merupakan tiruan atau duplikasi dari skripsi kesarjanaan di lingkungan Universitas Kristen Duta Wacana maupun di Perguruan Tinggi atau instansi manapun, kecuali bagian yang sumber informasinya dicantumkan sebagaimana mestinya.

Jika dikemudian hari didapati bahwa hasil skripsi ini adalah hasil plagiasi atau tiruan dari skripsi lain, saya bersedia dikenai sanksi yakni pencabutan gelar kesarjanaan saya.

Yogyakarta, 13 Juni 2016

HENRY SUSILO
71120151

HALAMAN PERSETUJUAN

Judul Skripsi	:	IMPLEMENTASI TWO FACTOR AUTHENTICATION MENGGUNAKAN PROTOKOL ZERO KNOWLEDGE PROOF PADA SISTEM LOGIN
Nama Mahasiswa	:	HENRY SUSILO
N I M	:	71120151
Matakuliah	:	Skripsi (Tugas Akhir)
Kode	:	TIW276
Semester	:	Genap
Tahun Akademik	:	2015/2016

Telah diperiksa dan disetujui di
Yogyakarta,
Pada tanggal 13 Juni 2016

Dosen Pembimbing I	Dosen Pembimbing II
Willy Sudiarto Raharjo, S.Kom.,M.Cs.	Ignatia Dhian E K R, S.Kom, M.Eng

HALAMAN PENGESAHAN

IMPLEMENTASI TWO FACTOR AUTHENTICATION MENGGUNAKAN PROTOKOL ZERO KNOWLEDGE PROOF PADA SISTEM LOGIN

Oleh: HENRY SUSILO / 71120151

Dipertahankan di depan Dewan Penguji Skripsi
Program Studi Teknik Informatika Fakultas Teknologi Informasi
Universitas Kristen Duta Wacana - Yogyakarta
Dan dinyatakan diterima untuk memenuhi salah satu syarat memperoleh gelar
Sarjana Komputer
pada tanggal 24 Mei 2016

Yogyakarta, 13 Juni 2016
Mengesahkan,

Dewan Penguji:

1. Willy Sudiarto Raharjo, S.Kom.,M.Cs.
2. Ignatia Dhian E K R, S.Kom, M.Eng
3. Antonius Rachmat C., S.Kom.,M.Cs.
4. Kristian Adi Nugraha, S.Kom., M.T.

Dekan	Ketua Program Studi
(Budi Susanto, S.Kom., M.T.)	(Gloria Virginia, Ph.D.)

UCAPAN TERIMA KASIH

Puji syukur kepada Tuhan Yesus Kristus atassegala berkat, penyertaan, dan anugerah-Nya yang sudah diberikan kepada Penulis selama mengerjakan tugas akhir ini. Penulis juga ingin mengucapkan terima kasih kepada pihak-pihak yang telah memberikan banyak dukungan kepada Penulis, antara lain:

1. Keluarga yang senantiasa memberi dukungan dalam bentuk doa dan motivasi yang tidak henti-hentinya selama Penulis mengerjakan tugas akhir ini.
2. Bapak Willy Sudiarto Raharjo, S.Kom.,M.Cs. dan Ibu Ignatia Dhian E K R, S.Kom., M.Eng. selaku Dosen Pembimbing I dan II yang telah mendukung, membimbing, memberikan ide serta masukan-masukan bagi Penulis dalam pembuatan aplikasi, pelaksanaan penelitian, hingga penulisan laporan.
3. Teman-teman yang telah membantu menjadi responden dalam penelitian-penelitian yang dilakukan Penulis sehingga tugas akhir ini dapat berjalan dengan lancar.
4. Teman-temanseperjuangan TI UKDW angkatan 2012 (terutama kepada Vivi Citra, Monica Natasha, Valonia Inge, Tiffany Widya, Pedro Nadirio, Michael Christian, Ady Purnama, Hendy Yudhitya) yang telah bersama-sama berjuang dalam menyelesaikan studi di prodi Teknik Informatika UKDW dan tugas akhir ini.
5. Pihak-pihak lain yang yang telah membantu jalannya pengerjaan tugas akhir ini baik secara langsung ataupun tidak langsung.

Yogyakarta, 13 Juni 2016

Henry Susilo

KATA PENGANTAR

Puji syukur kepada Tuhan Yesus Kristus atas anugerah, bimbingan, dan penyertaan-Nya, Penulis dapat menyelesaikan Tugas Akhir ini yang berjudul "Implementasi *Two Factor Authentication* Menggunakana Protokol *Zero Knowledge Proof* Pada Sistem Login".

Terselesaikannya Tugas Akhir ini tidak terlepas dari bantuan berbagai pihak, sehingga pada kesempatan ini dengan segala kerendahan hati dan penuh rasa hormat, Penulis mengucapkan terima kasih bagi semua pihak yang telah memberikan bantuan baik langsung maupun tidak langsung dalam penyusunan Tugas Akhir ini hingga selesai.

Penulisan Tugas Akhir ini diajukan untuk memenuhi salah satu syarat memperoleh gelar Sarjana Komputer bagi mahasiswa program S1 pada Fakultas Teknologi Informasi Program Studi Teknik Informatika Universitas Kristen Duta Wacana Yogyakarta. Penulis menyadari bahwa Tugas Akhir ini masih jauh dari kata sempurna, oleh karena itu Penulis mengharapkan masukan dan kritik yang membangun dari para pembaca.

Akhir kata Penulis memohon maaf apabila terdapat kesalahan dan kata-kata yang kurang berkenan. Besar harapan Penulis semoga Tugas Akhir yang telah disusun oleh Penulis ini dapat bermanfaat bagi para pembaca.

Yogyakarta, 13 Juni 2016

Henry Susilo

INTISARI

IMPLEMENTASI TWO FACTOR AUTHENTICATION MENGGUNAKAN PROTOKOL ZERO KNOWLEDGE PROOF PADA SISTEM LOGIN

Password adalah kumpulan karakter atau *string* yang digunakan oleh pengguna jaringan atau sebuah sistem operasi yang mendukung banyak pengguna (*multiuser*) untuk memverifikasi identitas dirinya kepada sistem keamanan yang dimiliki oleh jaringan atau sistem tersebut, *password* merupakan informasi yang sangat berbahaya jika di salah gunakan. Untuk menanggulangi hal tersebut cara yang paling mudah digunakan adalah dengan tidak mengirimkan informasi sensitif apapun melalui jaringan yang tidak aman dan perangkat yang tidak dipercaya. Untuk alasan ini kita bisa melalukan penggabungan antara *Two Factor Authentication* dan *Zero Knowledge proof, ZeroKnowledge Proof* berguna untuk menjaga kerahasiaan password dan *Two Factor Authentication* berguna untuk mengamankan proses login pada perangkat yang tidak terpercaya.

Bahasa pemrograman yang akan digunakan dalam membangun sistem ini adalah *PHP* dan *Javascript*. Pemilihan bahasa *PHP* dan *Javascript* didasari atas pertimbangan bahwa penerapan sistem *Zero Knowledge Proof* ini akan dijalankan dengan sistem berbasis web.

Penelitian yang dilakukan bertujuan untuk mencoba mengamankan proses *login* dengan cara tidak mengirimkan *password* melalui jaringan , hal ini dapat dilakukan dengan cara menerapkan sistem *Zero Knowledge Proof* pada sistem *login*. Dari penelitian yang telah dilakukan diketahui bahwa proses *ZKP* dengan *username* dan *password* yang sesuai selalu diterima dan jika *username* dan *password* tidak sesuai akan selalu gagal, Sedangkan proses *login* dengan *username* dan *token* sesuai akan selalu berhasil , dan proses *login* dengan *username* dan *token* yang tidak sesuai akan selalu gagal.

DAFTAR ISI

DAFTAR GAMBAR

INTISARI

IMPLEMENTASI TWO FACTOR AUTHENTICATION MENGGUNAKAN PROTOKOL ZERO KNOWLEDGE PROOF PADA SISTEM LOGIN

Password adalah kumpulan karakter atau *string* yang digunakan oleh pengguna jaringan atau sebuah sistem operasi yang mendukung banyak pengguna (*multiuser*) untuk memverifikasi identitas dirinya kepada sistem keamanan yang dimiliki oleh jaringan atau sistem tersebut, *password* merupakan informasi yang sangat berbahaya jika di salah gunakan. Untuk menanggulangi hal tersebut cara yang paling mudah digunakan adalah dengan tidak mengirimkan informasi sensitif apapun melalui jaringan yang tidak aman dan perangkat yang tidak dipercaya. Untuk alasan ini kita bisa melalukan penggabungan antara *Two Factor Authentication* dan *Zero Knowledge proof, ZeroKnowledge Proof* berguna untuk menjaga kerahasiaan password dan *Two Factor Authentication* berguna untuk mengamankan proses login pada perangkat yang tidak terpercaya.

Bahasa pemrograman yang akan digunakan dalam membangun sistem ini adalah *PHP* dan *Javascript*. Pemilihan bahasa *PHP* dan *Javascript* didasari atas pertimbangan bahwa penerapan sistem *Zero Knowledge Proof* ini akan dijalankan dengan sistem berbasis web.

Penelitian yang dilakukan bertujuan untuk mencoba mengamankan proses *login* dengan cara tidak mengirimkan *password* melalui jaringan , hal ini dapat dilakukan dengan cara menerapkan sistem *Zero Knowledge Proof* pada sistem *login*. Dari penelitian yang telah dilakukan diketahui bahwa proses *ZKP* dengan *username* dan *password* yang sesuai selalu diterima dan jika *username* dan *password* tidak sesuai akan selalu gagal, Sedangkan proses *login* dengan *username* dan *token* sesuai akan selalu berhasil , dan proses *login* dengan *username* dan *token* yang tidak sesuai akan selalu gagal.

BAB 1
PENDAHULUAN

1.1 Latar Belakang

Password adalah kumpulan karakter atau string yang digunakan oleh pengguna jaringan atau sebuah sistem operasi yang mendukung banyak pengguna *(multiuser)* untuk memverifikasi identitas dirinya kepada sistem keamanan yang dimiliki oleh jaringan atau sistem tersebut, *password* merupakan informasi yang sangat berbahaya jika disalahgunakan.Sekarang sudah banyak *website* yang tidak hanya menggunakan password untuk dapat *login*, *website* tersebut menggunakan metode *Two Factor Authentication* yaitu sebuah metode di mana setelah memasukkan *password* kita harus memverifikasi bahwa kita adalah orang yang benar-benar memiliki akun tersebut. Tetapi *Two Factor Authentication* masih membutuhkan pengiriman password melewati sebuah jaringan yang tidak aman.

Untuk menanggulangi hal tersebut cara yang paling mudah digunakan adalah dengan tidak mengirimkan informasi sensitif apapun melalui jaringan yang tidak aman dan perangkat yang tidak dipercaya. Untuk alasan ini kita bisa melakukan penggabungan antara *Two Factor Authentication* dan *Zero Knowledge proof.*

Penerapan *Two Factor Authentication* dan *Zero Knowledge Proof* yang menggunakan protokol *Schnorr* pada sistem *login* akan memperkecil kemungkinan seseorang bisa masuk secara *ilegal* ke *akun* orang lain. Dalam penerapan sistem ini memerlukan beberapa perangkat dan *user* yang akan *login*, perangkat yang diperlukan antara lain adalah *trusted device* (perangkat yang dapat dipercaya), *untrusted device* (perangkat apapun yang kita gunakan untuk *login),* dan *server.* Pada sistem ini *trusted device* berguna untuk penghubung antara *user* dan *server* dalam melakukan protokol *Zero Knowledge Proof*, sedangkan *untrusted device* adalah perangkat yang kita gunakan untuk *login*.

1.2 Rumusan Masalah

Perumusan masalah yang menjadi dasar penulisan tugas akhir ini yaitu :

a. Bagaimana proses verifikasi login tanpa mengirimkan *password* melalui jaringan.
b. Berapa lama waktu yang rata-rata yang diperlukan untuk proses verifikasi *login* menggunakan protokol *zero knowledge proof.*

1.3 Batasan Masalah

Agar tulisan ini tidak menyimpang dari ruang lingkup pembahasan, diperlukan batasan masalah sebagai berikut :

a. *Password* yang dimiliki oleh *user* dipercaya aman.
b. Metode *Two Factor Authentication* menggunakan *token* yang dihasilkan dari fungsi *hash* SHA256.
c. Percobaan waktu rata-rata yang diperlukan untuk proses *zero knowledge proof* dilakukan pada kecepatan internet 10Mbps dengan ping 20ms.
d. Metode *Zero Knowledge Proof* yang digunakan adalah *Schnorr Protocol*.

1.4 Tujuan Penelitian

Tujuan dari penulisan tugas akhir ini adalah membangun sistem *login* yang mengimplementasikan *Two Factor Authentication* dan menggunakan protokol *Zero Knowledge Proof*.

1.5 Metode Penelitian

Tahapan yang dilakukan dalam penelitian ini adalah :

1. Mengumpulkan bahan-bahan referensi

   Mengumpulkan dan mempelajari bahan-bahan referensi yang berhubungan dengan kriptografi, *Zero Knowledge Proof*, *Two Factor Authentication*, *Schnorr* protokol.

2. Analisis Masalah dan Perancangan Sistem

   Melakukan analisis masalah yang dimulai dengan identifikasi masalah, memahami kerja sistem yang akan dibuat, menganalisis dan membuat laporan tentang hasil analisis, serta membuat rancangan dan *interface* sistem.

3. Implementasi Sistem

   Perancangan sistem diimplementasikan dalam bentuk kode program (*coding*).

4. Pengujian Sistem

   Pengujian dilakukan terhadap program yang telah dibuat dengan cara melakukan pendaftaran user, percobaan mendapatkan token menggunakan *Zero Knowledge Proof* , percobaan login menggunakan *token*.

5. Dokumentasi Sistem

   Penyusunan laporan lengkap dengan analisis yang didapatkan.

1.6 Sistematika Penulisan

Sistematika penulisan pada tugas akhir ini adalah :

BAB 1 PENDAHULUAN

Bab ini menjelaskan latar belakang masalah, rumusan masalah, batasan sistem, tujuan penelitian, metode penelitian, dan sistematika penulisan dari tugas akhir.

BAB 2 TINJAUAN PUSTAKA

Bab ini menjelaskan penelitian-penelitian yang pernah dilakukan sebelumnya mengenai *Zero Knowledge Proof* , *Two Factor Authentication* dan *Schnorr* protokol, serta menjelaskan teori mengenai kriptografi, *Zero Knowledge Proof* , *Two Factor Authentication* dan protokol *Schnorr*.

BAB 3 ANALISIS DAN PERANCANGAN SISTEM

Pada bab ini akan dijelaskan mengenai analisis dan perancangan yang terdapat dalam sistem, digambarkan dalam bentuk diagram alir, *activity* diagram, *mockup* (perancangan *interface* / antarmuka sistem).

BAB 4 IMPLEMENTASI DAN ANALISIS SISTEM

Bab ini menguraikan hasil implementasi dari sistem yang telah dibuat, antara lain *interface* / antarmuka sistem, serta pengujian dan analisis. Analisis dilakukan terhadap proses Two Factor Authentication dan proses verifikasi dari protokol *Schnorr*yang telah diimplementasikan ke dalam sistem.

BAB 5 KESIMPULAN DAN SARAN

Bab ini berisi kesimpulan yang didapat dari hasil pengujian yang dilakukan serta saran-saran yang diberikan untuk penelitian selanjutnya.

BAB 5
KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan hasil implementasi dan analisis yang telah dibuat dibahas pada bab sebelumnya, maka dapat disimpulkan sebagai berikut :

1. Proses verifikasi login dengan menggunakan protokol *Schnorr* bisa diterapkan dengan baik , sehingga kerahasiaan password bisa tetap terjaga. *Secret key* dan *public key* menjadi kunci utama yang dimiliki oleh *user* untuk melakukan verifikasi. Dengan kata lain jika ada pihak yang tidak memiliki *secret key* dan *public key* namun mencoba untuk melakukan verifikasi, maka sistem tidak akan memberikan hak akses untuk *user* tersebut.
2. Proses *login* menggunakan *zero knowledge proof* membutuhkan waktu rata-rata 1,798 detik untuk setiap *login* dengan perulangan *zero knowledge proof* sebanyak 20 kali. Oleh karena itu sistem *login* ini bisa diterapkan karena waktu login tidak memakan waktu yang relatif lama.

5.2 Saran

Saran yang diberikan untuk perbaikan sistem adalah :

1. Membandingkan waktu login dengan sistem login yang menggunakan protokol *zero knowledge proof* yang berbeda.
2. Bilangan prima (p) dan (q) dapat diperbesar sehingga akan semakin sulit *secret key* dipalsukan.

DAFTAR PUSTAKA

Acharya, S., Polawar, A., & P.Y.Pawar. (2013). Two Factor Authentication Using Smartphone Generated One Time Password. *IOSR Journal of Computer Engineering (IOSR-JCE)* , 6.

Aloul, F., & Zahidi, S. (2009). Two Factor Authentication Using Mobile Phones. *Department of Computer Science & Engineering* , 4.

Boneh, D. (2012). *Intro Number Theory.* California: Standford University.

Gunawan, T. (2012). *Sistem Otentikasi Berbasis Zero Knowledge Protocol Pada Sistem Operasi Android.* Salatiga: Universitas Kristen Satya Wacana.

Hao. (2013). Schnorr NIZK Proof: Non-interactive Zero Knowledge Proof for Discrete. *Internet Engineering Task Force* , 11.

Katz, J., & Lindell, Y. (2007). *Introduction to Modern.* New York.

Nugroho, S. C. (2014). Penerapan Konsep Zero Knowledge Pada Protokol E-Notary. *Prosiding Seminar Nasional Aplikasi Sains & Teknologi (SNAST) 2014* , 4.

Patel, A. (n.d.). Zero Knowledge Protocol. 13.

Sidiq, A. Z. (n.d.). Perbandingan Algoritma RSA dan Algoritma berbasis Zero Knowledge untuk Autentikasi pada Smartcard. *Teknik Informatika ITB* , 5.

Situngkir, T. N. (2013). Implementasi Zero Knowledge Proof. 135.

Stamp, M. (2005). *Crypto Basics, in Information Security: Principles and Practice.* USA: San Jose State University.