ANALISIS IMPLEMENTASI PROTOKOL HTTPS PADA WEBSITE INTERNET BANKING DI INDONESIA

Skripsi

oleh

AGUNG PRASETYA DHARAMA K.

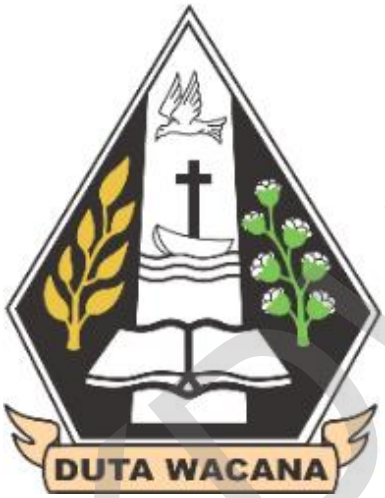
71130005

PROGRAM STUDI TEKNIK INFORMATIKA FAKULTAS TEKNOLOGI INFORMASI
UNIVERSITAS KRISTEN DUTA WACANA

2017

ANALISIS IMPLEMENTASI PROTOKOL HTTPS PADA WEBSITE INTERNET BANKING DI INDONESIA

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

AGUNG PRASETYA DHARMA K.
71130005

PROGRAM STUDI TEKNIK INFORMATIKA FAKULTAS TEKNOLOGI INFORMASI
UNIVERSITAS KRISTEN DUTA WACANA
2017

PERNYATAAN KEASLIAN SKRIPSI

Saya menyatakan dengan sesungguhnya bahwa skripsi dengan judul:

ANALISIS IMPLEMENTASI PROTOKOL HTTPS PADA WEBSITE INTERNET BANKING DI INDONESIA

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, 5 Juni 2017

AGUNG PRASETYA DHARMA K
71130005

HALAMAN PERSETUJUAN

Judul Skripsi	:	ANALISIS IMPLEMENTASI PROTOKOL HTTPS PADA WEBSITE INTERNET BANKING DI INDONESIA
Nama Mahasiswa	:	AGUNG PRASETYA DHARMA K
N I M	:	71130005
Matakuliah	:	Skripsi (Tugas Akhir)
Kode	:	TIW276
Semester	:	Genap
Tahun Akademik	:	2016/2017

Telah diperiksa dan disetujui di
Yogyakarta,
Pada tanggal 5 Juni 2017

Dosen Pembimbing I	Dosen Pembimbing II
Willy Sudiarto Raharjo, S.Kom.,M.Cs.	Junius Karel, M.T.

HALAMAN PENGESAHAN

ANALISIS IMPLEMENTASI PROTOKOL HTTPS PADA WEBSITE INTERNET BANKING DI INDONESIA

Oleh: AGUNG PRASETYA DHARMA K / 71130005

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 2017

Yogyakarta, 5 Juni 2017
Mengesahkan,

Dewan Penguji:

1. Willy Sudiarto Raharjo, S.Kom.,M.Cs.
2. Junius Karel, M.T.
3. Hendro Setiadi, M.Eng
4. Ignatia Dhian E K R, S.Kom, M.Eng

Dekan

(Budi Susanto, S.Kom., M.T.)

Ketua Program Studi

(Gloria Virginia, Ph.D.)

KATA PENGANTAR

Puji syukur penulis ucapkan kehadirat Tuhan Yang Maha Esa karena telah memberi berkah dan perlindunganNya sehingga penulis dapat menyelesaikan laporan penelitian Analisis Implementasi Protokol HTTPS pada Website Internet Banking di Indonesia. Penulisan skripsi ini diajukan untuk memenuhi salah satu syarat kelulusan jenjang perkuliahan Strata I Universitas Kristen Duta Wacana.

Dalam penulisan skripsi ini tentunya masih banyak kekurangan, baik dari aspek kualitas maupun kuantitas materi penelitian yang disajikan. Penulis menyadari bahwa skripsi ini jauh dari kata sempurna sehingga penulis membutuhkan kritik dan saran yang bersifat membangun untuk perkembangan penulis di masa mendatang.

Pada kesempatan ini penulis dengan tulus hati mengucapkan terima kasih untuk orang-orang yang telah banyak mendukung dalam penulisan ini, kepada :

1. Bapak Willy Sudiarto Raharjo, S.Kom, M.Cs selaku Dosen Pembimbing I.
2. Bapak Junius Karel, M.T. selaku Dosen Pembimbing II.
3. Orang tua penulis yang telah banyak membantu dan memberikan dukungan.
4. Teman-teman penulis yang telah membantu dan memberikan dukungan juga.

Akhir kata, semoga penelitian ini dapat berguna bagi kemajuan pendidikan dan kepentingan masyarakat umum.

Yogyakarta, 8 Mei 2017

Penulis

INTISARI

Analisis Implementasi Protokol HTTPS pada Website Internet Banking di Indonesia

HTTPS adalah sebuah protokol HTTP yang menggunakan SSL atau TLS sebagai sublayer di bawah HTTP pada layer applikasi. HTTPS menawarkan perlindungan data karena memanfaatkan *cryptography*, yang memiliki tiga inti keamanan yaitu *Confidentiality*, *Authentication*, dan *Integrity*. Seperti pada dunia perbankan, sangat diperlukan keamanan untuk perlindungan datanya. *E-banking* atau *electronic-banking* merupakan salah satu bentuk transaksi yang *sensitive*, tidak heran jika semua *website e-banking* untuk dapat dikatakan aman harus menggunakan HTTPS. Namun, HTTPS tidak bisa dikatakan sepenuhnya aman, jika HTTPS tidak dikonfigurasikan dengan benar.

Penelitian ini menganalisis keamanan *website e-banking* di Indonesia berdasarkan implementasi protokol HTTPS-nya. Pengujian dilakukan dengan bantuan tools testssl.sh dan ssllabs terhadap 10 parameter yang telah ditentukan.

Dari hasil analisis terhadap 37 domain *e-banking*, ditemukan 2,7% domain masih menggunakan protokol SSLv2 yang rawan terhadap serangan DROWN, 18,91% domain masih menggunakan protokol SSLv3 yang rawan terhadap serangan POODLE, dan hanya ada 78,37% domain yang mendukung TLSv1.1 dan 83,78% domain yang medukung TLSv1.2. Terdapat 13,51% domain rentan terhadap serangan Renegotiation, 29,72% domain rentan terhadap serangan BREACH, 17% domain masih menggunakan algoritma RC4 yang tidak aman, 91,89% domain rentan serangan BEAST, serta 2,7% domain rentan terhadap serangan Freak dan Logjam. Beberapa fitur keamanan terbaru belum banyak digunakan, seperti *forward secrecy*, HSTS, dan HPKP. Dari analisis didapatkan 40,50% domain *e-banking* masih dibawah standar yang dikeluarkan oleh NIST.

Kata kunci: *Website e-banking*, *cryptography*, HTTPS, SSL, TLS.

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

INTISARI

Analisis Implementasi Protokol HTTPS pada Website Internet Banking di Indonesia

HTTPS adalah sebuah protokol HTTP yang menggunakan SSL atau TLS sebagai sublayer di bawah HTTP pada layer applikasi. HTTPS menawarkan perlindungan data karena memanfaatkan *cryptography*, yang memiliki tiga inti keamanan yaitu *Confidentiality*, *Authentication*, dan *Integrity*. Seperti pada dunia perbankan, sangat diperlukan keamanan untuk perlindungan datanya. *E-banking* atau *electronic-banking* merupakan salah satu bentuk transaksi yang *sensitive*, tidak heran jika semua *website e-banking* untuk dapat dikatakan aman harus menggunakan HTTPS. Namun, HTTPS tidak bisa dikatakan sepenuhnya aman, jika HTTPS tidak dikonfigurasikan dengan benar.

Penelitian ini menganalisis keamanan *website e-banking* di Indonesia berdasarkan implementasi protokol HTTPS-nya. Pengujian dilakukan dengan bantuan tools testssl.sh dan ssllabs terhadap 10 parameter yang telah ditentukan.

Dari hasil analisis terhadap 37 domain *e-banking*, ditemukan 2,7% domain masih menggunakan protokol SSLv2 yang rawan terhadap serangan DROWN, 18,91% domain masih menggunakan protokol SSLv3 yang rawan terhadap serangan POODLE, dan hanya ada 78,37% domain yang mendukung TLSv1.1 dan 83,78% domain yang medukung TLSv1.2. Terdapat 13,51% domain rentan terhadap serangan Renegotiation, 29,72% domain rentan terhadap serangan BREACH, 17% domain masih menggunakan algoritma RC4 yang tidak aman, 91,89% domain rentan serangan BEAST, serta 2,7% domain rentan terhadap serangan Freak dan Logjam. Beberapa fitur keamanan terbaru belum banyak digunakan, seperti *forward secrecy*, HSTS, dan HPKP. Dari analisis didapatkan 40,50% domain *e-banking* masih dibawah standar yang dikeluarkan oleh NIST.

Kata kunci: *Website e-banking*, *cryptography*, HTTPS, SSL, TLS.

BAB 1
PENDAHULUAN

1.1. Latar Belakang

Pada era yang sudah modern ini, kebutuhan akan teknologi informasi, telekomunikasi, dan *internet* sangatlah tinggi. Berbagai bidang dan layanan umum hampir semuanya sudah menggunakan teknologi informasi terutama berbasiskan *internet*. *Internet* telah memberikan banyak kemudahan bagi manusia dalam melakukan segala kegiatan, termasuk dalam pertukaran informasi, pengiriman data, bahkan hal yang bersifat privasi. Sebuah pengiriman data pasti akan melalui sebuah *protocol* yang ada di dalam suatu jaringan tersebut. Tidak semua *protocol* menjamin data terkirim dengan baik bahkan dari segi keamanannya.

HyperText Transfer Protocol Secure (HTTPS) adalah sebuah protocol HTTP yang menggunakan *Secure Socket Layer* (SSL) atau *Transport Layer Security* (TLS) sebagai sublayer di bawah HTTP pada *layer* aplikasi. Gangan (2015) mengatakan, HTTPS merupakan protokol yang paling umum digunakan, dan sebagian besar layanan perbankan serta layanan email online menggunakannya untuk memastikan keamanan antara *server* mereka dan web browser. HTTPS digunakan untuk melindungi dari orang yang mengakses tanpa izin yaitu serangan *man-in the-middle.* Ristić (2014, hlm. 4) mengatakan, ketika *Cryptograpy* digunakan dengan benar, maka haruslah memiliki tiga inti keamanan yaitu, *Confidentiality, Authentication,* dan *Integrity*. Protocol SSL dan TLS telah menyediakan ketiga inti kemanan tersebut.

Pada dunia perbankan, sangat diperlukan keamanan untuk menjaga data-data dari pihak yang tidak berwenang. Salah satu teknologi yang digunakan perbankan adalah *e-banking* atau *electronic-banking. E-banking* merupakan contoh bentuk transaksi yang *sensitive*, jadi tidak heran jika website *e-banking* untuk dapat dikatakan aman haruslah menggunakan HTTPS. Tetapi dengan adanya perkembangan teknologi yang sangat cepat membuat HTTPS tidak bisa

lagi dikatakan sepenuhnya aman, karena beberapa algoritma enkripsi yang digunakan pada SSL atau TLS ada yang sudah bisa dipecahkan bahkan tidak dengan waktu yang lama. Tentunya hal ini perlu menjadi sorotan penting untuk segi keamanan *e-banking* walaupun website *e-banking*-nya sudah berbasis HTTPS jika tidak mengkonfigurasi HTTPS-nya dengan benar. Berdasakan latar belakang diatas peneliti akan menganalisi segi keamanan *website e-banking* di Indonesia apakah sudah benar-benar aman dan menggunakan *signature algorithm* yang *up-to-date* dan jenis-jenis serangan apa yang mungkin dilakukan.

1.2. Rumusan Masalah

Dengan didasari oleh latar belakang diatas, maka permasalahan penelitian dapat dirumuskan sebagai berikut :

1. Berapa persentase untuk setiap parameter pengujian terhadap *website e-banking* di Indonesia?
2. Apa saja macam serangan yang dapat dilakukan terhadap *website e-banking*?
3. Apa saja *website e-banking* yang diklasifikasikan memenuhi standar?

1.3. Batasan Masalah

Agar penelitian dapat mencapai hasil dan tujuan yang diharapkan, maka pemasalahan akan dibatasi sebagai berikut :

1. *Website e-banking* yang akan dianalisa adalah semua bank yang terdaftar di Bank Indonesia dan sudah memiliki *website e-banking*.
2. Pengujian terbatas tentang protokol *SSL* dan *TLS* pada *website* yang sudah menggunakan HTTPS.
3. Pengujian keamanan akan dinilai bedasarkan hasil uji dari parameter berikut yaitu, protokol-protokol yang didukung (*Support Protocols),* panjang kunci (*Key Length),* algoritma tanda tangan digital (*Digital*

Certificate), mekanisme pembatalan, *Downgrade Prevention, Secure Renegotiation, Forward Secrecy,* HSTS, HPKP, dan ancaman keamanan.

1.4. Tujuan Penelitian

Berdasarkan masalah yang dirumuskan maka tujuan dari penelitian adalah :

1. Mengetahui tingkat keamanan *website e-banking* yang dimiliki oleh bank-bank di Indonesia berdasarkan parameter pengujian.
2. Mengetahui jenis-jenis serangan terhadap protokol (*protocol attacks*).
3. Mengetahui *website e-banking* yang sudah diklasifikasikan memenuhi standar yang ada.

1.5. Metode Penelitian

Metode yang digunakan dalam Penelitian ini adalah sebagai berikut :

1. **Studi Pustaka**

   Studi Pustaka bertujuan untuk memberikan pengetahuan tentang hal-hal yang berkaitan dengan : HTTPS, SSL, TLS, *protocol attack* pada https, yang dipergunakan untuk membantu penyelesaian penelitian ini. Studi pustaka dilakukan dengan membaca buku-buku, literatur, jurnal, artikel dari internet yang berhubungan dengan masalah yang dibahas.

2. **Pengumpulan Data**

   Pada tahap pengumpulan data, peneliti mengambil data-data bank yang diakui dan terdaftar oleh Bank Indonesia. Data tersebut diambil dari *website* resmi Bank Indonesia. Selanjutnya dari semua data Bank-bank tersebut disortir kembali dan hanya diambil bank yang memiliki alamat website *E-banking.*

3. **Pengujian Sistem**

Pada tahapan ini pengujian dilakukan terhadap website *e-banking* menggunakan bantuan tools testssl.sh dan SSLLabs untuk mengetahui konfigurasi pada protokol HTTPS-nya.

4. **Analisis Data Statistik**

Setelah dilakukan pengujian terhadap semua parameter di atas, maka akan diperoleh data hasil pengujian. Lalu akan dilakukan analisis data secara analisis Kuantitatif dengan *Statistik Deskriptif*. Untuk setiap poin parameter yang diujikan berdasarkan hasil perbandingan dengan *standar* yang sudah dipaparkan. Laporan dibuat sesuai dengan hasil analisis berupa penyajian data dalam bentuk tabel atau distribusi frekuensi dan penyajian data dalam bentuk visual serta memberikan rekomendasi.

1.6. Sistematika Penulisan

Dalam penulisan penelitian ini, penulis akan membagi laporan ini menjadi 5 bab, yaitu Bab 1 Pendahuluan, Bab 2 Tinjauan Pustaka, Bab 3 Perancangan Penelitian, Bab 4 Implementasi dan Analisis, dan Bab 5 Kesimpulan dan Saran.

Bab 1 berisi Pendahuluan terhadap penelitian, antara lain latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, metode penelitian yang digunakan, dan sistematika penulisan.

Bab 2 berisi tentang Tinjauan Pustaka dan Landasan Teori yang didapatkan dari berbagai sumber pustaka dan penjelasan tentang konsep dan prinsip yang diperlukan guna membantu menyelesaikan penelitian ini.

Bab 3 berisi Perancangan penelitian, bagian ini berisi tentang analisis teori yang akan digunakan dalam penelitian.

Bab 4 berisi Implementasi dan Analisis bagian ini memuat implementasi sistem, hasil penelitian, pembahasan, dan analisis penelitian.

Bab 5 berisi Kesimpulan dari hasil penelitian yang telah didapat, dan saran yang bersifat membangun untuk pembaca serta saran untuk penelitian selanjutnya yang memiliki focus penelitian yang sama

BAB 5

KESIMPULAN DAN SARAN

5.1. Kesimpulan

Berdasarkan dari hasil pengujian dan analisis yang telah dilakukan dan dibahas pada bab-bab sebelumnya, maka dapat ditarik kesimpulan bahwa :

1. Masih terdapat situs *E-banking* di Indonesia yang melakukan dukungan terhadap protokol SSL v2 dan masih berpotensi untuk terkena serangan DROWN sebanyak 2,7%, dan cukup banyak yang masih melakukan dukungan terhadap protokol SSL v3 yang berpotensi terkena serangan POODLE sebanyak 18,91%. Namun hanya 78,37% bank mendukung protokol TLS v1.1, dan 83,78% bank mendukung protokol TLS 1.2 yang saat ini paling direkomendasikan.
2. Semua domain *e-banking* sudah menggunakan panjang kunci dan algoritma untuk tanda tangan digital yang direkomendasikan dan aman untuk digunakan, namun masih ditemukan banyak permasalahan pada implementasi baik dari sisi protokol maupun konfigurasi *web server*-nya.
3. Sebanyak 13,51% domain *e-banking* berpotensi terhadap serangan Renegotiation, 29,72% masih berpotensi tekena serangan BREACH, 16,21% masih *vulnerable* terhadap serangan POODLE SSL, 8,1% masih *vulnerable* terhadap POODLE TLS, serta 91,89% domain rentan terhadap serangan BEAST. Selain itu 2,7% domain e-banking masih *vulnerable* terhadap serangan Freak, Logjam, DROWN, serta 27% masih menggunakan algoritma RC4 yang tidak aman. Hal ini menunjukkan bahwa tingkat *awareness* pengelola domain masih kurang.
4. Sebagian besar domain *e-banking* di Indonesia masih belum banyak yang menerapkan fitur-fitur kemanan terbaru. Masih ada 27% domain belum menerapkan *forward secrecy*. Hanya sekitar 32,8% yang sudah menggunakan *HTTP Strict Transport Security* (HSTS), dan hanya 10, 81% yang sudah menerapkan *HTTP Public Key Pinning* (HPKP). Hal ini

menunjukkan bahwa tingkat *maintenance* website dalam mengikuti *update* perkembangan keamanan masih kurang.

5. Sebanyak 15 (40,50%) domain *e-banking* diklasifikasikan sebagai domain yang masih dibawah standar yang dikeluarkan oleh NIST dan 22 (59,50%) domain *e-banking* sudah memenuhi standar NIST.
6. Rekomendasi implementasi protokol HTTPS untuk website *e-banking* di Indonesia berdasarkan standarisasi NIST, hasil analisa, dan kesesuaian dengan keadaan *client* yang ada di Indonesia.

5.2. Saran

Beberapa saran yang dapat menjadi masukan untuk penelitian yang akan datang adalah :

1. Mencoba melakukan pengujian serangan kemanan secara langsung terhadap *website e-banking* yang bermasalah dengan seijin dari Bank tersebut untuk menunjukan kelemahan yang ada.
2. Menerapkan langsung hasil rekomendasi implementasi protokol HTTPS untuk *website e-banking* di Indonesia, pada salah satu *domain e-banking*.

DAFTAR PUSTAKA

Adrian, D., Bhargavan, K., Durumeric, Z., dkk. (2015). *Imperfect Forward Secrecy*. Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security.

Anas, M. (2015). *Https, SSL, dan TLS*. Diakses pada tanggal 15 September 2016 dari https://www.academia.edu/11797303/Https_SSL_dan_TLS

Aviram, N, Schinzel, S., Somorovsky J. dkk. (2016). *DROWN: Breaking TLS using SSLv2*.

Barker, E. (2016). *Recommendation for Key Management Part 1: General*. NIST Special Publication 800-57 Part 1 Revision 4.

Dierks, T., & Rescorla, E. (2008). *RFC 5246 - The Transport Layer Security (TLS) Protocol Version 1.2*. IETF.

Fielding, R., Reschke, J. (2014). RFC 7230 - *Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing*. IETF.

Gangan, S. (2015). *A Review of Man-on-the-middle Attacks*. New York : Cornell University Library.

Georgiev, M., Iyengar, S., Jana, S., dkk. (2012). *The Most Dangerous Code In The World : Validating SSL Certificates in Non-Browser Software*. ACM.

Gluck, Y., Harris, N., Prado, A. (2013). *BREACH: Reviving The CRIME Attack*.

Green, M. (2015). *Attack of the week: FREAK (or 'factoring the NSA for fun and profit')*. Diakses tanggal 15 September 2016 dari http://blog.cryptographyengineering.com/2015/03/attack-of-week-freak-or-factoring-nsa.html.

Ikhsanto, K., Amalia, M. (2009). *Analisis Keamanan Internet Banking Pada Bank Di Indonesia*, 494-498. Diakses tanggal 15 September 2016 dari http://repository.gunadarma.ac.id/839/1/ANALISIS%20KEAMANAN%20INTERNET%20BANKING%20PADA%20BANK%20DI%20INDONESIA_UG.pdf

Moller, B., Duong, T., & Kotowicz, K. (2014). *This Poodle Bites Exploiting the SSL 3.0 Fallback*.

Muhson, A. (2006) *Teknik analisis kuantitatif*. Diakses pada 15 September 2016 dari http://staffnew.uny.ac.id/upload/132232818/lainlain/Ali+Muhson+(2006)+Analisis+Kuantitatif.pdf

Polk, T., McKay, K., & Chockani, S. (2014). *Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations*. NIST Special Publication 80-52 Revision 1.

Ristić, I. (2014). *Bulletproof SSL and TLS*. London : Feisty Duck Limited.

Seggelman, R, Tuexen, M., Williams, M. (2012). *RFC 6520 - Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS) Heartbeat Extension*. IETF.

Vasan K, K. V., Kumar P, A. R. (2016). *Taxonomy of SSL/TLS Attacks*. International Journal Computer Network and Information Security. Mecs.