

JURNAL PENELITIAN

IMPLEMENTASI *SINGLE HANDSHAKING* DALAM MENGHUBUNGKAN *WEBSERVER* BERBASIS PHP DENGAN KLIEN BERBASIS DELPHI PADA *ANIMATION STORE* EDUKREASI



Disusun Oleh:

HENRI SUSANTO

NIM. A11.2009.04712

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS ILMU KOMPUTER

UNIVERSITAS DIAN NUSWANTORO

2013

IMPLEMENTASI *SINGLE HANDSHAKING* DALAM MENGHUBUNGKAN *WEBSERVER* BERBASIS PHP DENGAN KLIEN BERBASIS DELPHI PADA *ANIMATION STORE* EDUKREASI

Penulis : Henri Susanto
Pembimbing : Elkaf Rahmawan P, M. Kom

ABSTRAK

Berawal dari keinginan untuk meningkatkan daya guna *website* Edukreasi yang semula hanya sebagai *company profile*, muncul satu gagasan untuk menciptakan *animation store* Edukreasi. Yakni sebuah system terpadu jual-beli konten animasi pendidikan *online*, yang juga didistribusikan melalui aplikasi klien berbasis Delphi. Sistem tersebut menuntut adanya komunikasi yang *well known* (saling mengenal) antara aplikasi klien dengan *webservice*. Edukreasi berbasis PHP. Implementasi sub-sistem *single handshaking* kedalam aplikasi klien dan *server* berfungsi untuk memastikan bahwa kedua aplikasi hanya dapat terhubung dengan *intended person* (aplikasi pasangan yang dikehendaki). Sub-sistem *single handshaking* diperoleh beberapa manfaat yakni proses *upload* dan *download* konten animasi melalui protokol FTP serta penyeragaman struktur materi pembelajaran klien dan *server*, tanpa mempengaruhi kenyamanan *user interface*, performa maupun kecepatan komunikasi data kedua aplikasi. Kedepan diharapkan penelitian ini dapat menjadi dasar pengetahuan dan dapat dilakukan penelitian lanjut implementasi sub-sistem *handshaking* menggunakan protokol yang lebih aman seperti halnya SSL (*secure socket layer*).

Kata kunci :*Handshaking*, AnimasiPendidikan, Delphi, PHP, *Animation Store*, *Socket*

1. PENDAHULUAN

1.1 Latar belakang

Animation Store Edukreasi adalah sebuah sistem jual beli animasi pendidikan *online* yang dimiliki oleh CV. Edukreasi. Sistem jual beli ini berbasis *web* dan

menggunakan aplikasi desktop berbasis *delphi*. Sistem ini diharapkan dapat menjamin sekuritas proteksi konten di sisi klien dari upaya duplikasi dan pembajakan. Dalam mewujudkan sistem tersebut dibutuhkan adanya komunikasi antara *website* edukasi berbasis PHP dengan aplikasi *client desktop* edukasi berbasis *Delphi*. Sedangkan, agar *webserver* dapat mengidentifikasi pengguna yang terhubung, dibutuhkan sebuah proses autentikasi perangkat yang terhubung ke *server*.

Dalam penelitian ini, protokol komunikasi yang dipilih untuk mengimplementasikan prosedur *handshaking* ialah *socket*. Berdasarkan masalah tersebut, diimplementasikan penggunaan *single handshaking* agar *webserver* Edukresi dapat mengidentifikasi pengguna yang terhubung.

2.1 KajianTeori

4.1. Bahasa Pemrograman PHP (*php hypertext pre-processor*)

Keunggulan penggunaan bahasa pemrograman PHP, antara lain :

- 1) gratis dan *open source*,
- 2) *compatible*,
- 3) sederhana,
- 4) tingkat ketersediaan yang tinggi.

Tim *developer* Edukresi telah memilih merealisasikan *website* edukasi menggunakan *web server apache* dengan bahasa pemrograman PHP dalam pengembangan sistem di sisi *server*.

4.2. Bahasa Pemrograman Delphi (*Embarcadero Delphi*)

Secara detail, aplikasi klien ini berfungsi untuk :

- 1) menayangkan konten animasi yang telah dienkrpsi sedemikian rupa guna menghindari pemanfaatan *illegal*.
- 2) melakukan enkripsi konten animasi yang di-upload oleh pengguna.
- 3) sebagai identitas klien di dalam sistem animation store edukasi.

Keseluruhan proses dalam sistem *animation store* yang saling berkaitan namun harus terjadi dalam lingkungan yang berbeda, mengharuskan adanya interkoneksi antara kedua *environment* tersebut melalui sebuah jalur protokol

jaringan yang dapat dikenali dan ditangani oleh kedua jenis bahasa pemrograman yang digunakan.

4.3. Metode *Handshaking*

Berdasarkan kebutuhan dan karakteristik komunikasi yang hendak dilakukan, diputuskan untuk menggunakan *single handshaking*, dengan pertimbangan sebagai berikut :

- a) kedua lingkungan aplikasi hanya membutuhkan otentikasi diawal *running* tidak dilakukan setiap kali klien dan *server* berkomunikasi
- b) aplikasi diharapkan menggunakan sumber daya *bandwidth* dan saling bertukar data seminimal mungkin.

4.4. Socket

Socket merupakan *endpoint* dari suatu jalur komunikasi dua arah antara dua program yang berkomunikasi dalam suatu jaringan komputer, dimana aplikasi dapat menuliskan data yang akan dikirimkan melalui jaringan komputer serta dapat membaca data yang diterima. Dengan menggunakan *socket*, dua proses yang berjalan pada dua computer berbeda, yang terhubung dengan jaringan komputer, dapat melakukan *Interprocess Communication* (IPC) dengan mengirimkan pesan dari *socket* pada suatu proses ke *socket* pada proses lainnya.

4.5. Metode *Prototyping*

Pengembangan perangkat lunak menggunakan metode *prototyping* merupakan sebuah siklus yang diawali dengan pengumpulan kebutuhan sistem, pembangunan *prototype* dan evaluasi, jika masih terdapat kekurangan dari *prototype* yang dibangun maka kembali ke tahap awal, demikian hingga *prototype* telah memenuhi seluruh ekspektasi pengguna.

Dalam hal ini, pengguna sub-system *single handshaking* ialah aplikasi *server* PHP dan aplikasi klien *Delphi*, maka satu demi satu *prototype* dibangun dan dievaluasi hingga memenuhi kebutuhan keduanya.

2. METODE PENELITIAN

Karena proses *handshaking* dalam penelitian ini merupakan sebuah sub-sistem dari dua buah sistem yang telah terbentuk sebelumnya, maka digunakan metode *prototyping*.

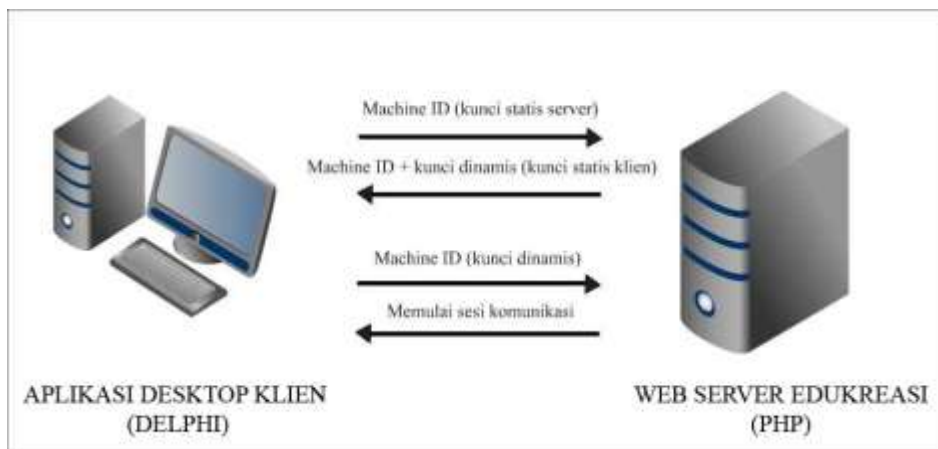
2.1 Pengumpulan Kebutuhan

Dalam tahap awal ini dapat dirumuskan sekurangnya 6 (enam) *point requirement*, antara lain :

- 1) Kedua aplikasi membutuhkan jaminan bahwa masing-masing keduanya hanya dapat terhubung dengan aplikasi pasangannya.
- 2) *Webserver* membutuhkan informasi untuk mengenali apakah pengguna telah terdaftar sebagai member.
- 3) Proses *handshaking* harus mampu mencegah akses dan atau proses *illegal*.
- 4) *Webserver* membutuhkan informasi mengenai *application id* yang dimiliki oleh aplikasi klien.
- 5) *Webserver* membutuhkan memasang pengenalan kepada aplikasi klien berupa session untuk otorisasi proses-proses selanjutnya.

2.2 Desain

Pada fase development, digunakan sebuah PC klien dengan sistem operasi microsoft windows8 dan sebuah webserver dengan sistem operasi linux mint v11 yang terhubung melalui sebuah jaringan lokal. Sedangkan pada fase implementasi digunakan server production berupa VPS (virtual private server) dengan sistem operasi CentOS yang terhubung ke internet dengan nama domain edukreasi.co.id.



Gambar 2.1: Data Flow Proses *Handshaking*

2.3 Coding

1. Aplikasi *Desktop* Klien Menggunakan *Delphi*

Langkah-langkah yang dilakukan sebagai berikut :

- 1) Mengirimkan *machine id* yang telah dienkripsi ke *server*
- 2) Mengambil *dynamic key* dari *response server*
- 3) Mengenkripsi *machine id* dengan *dynamic key* dan mengirimnya kembali ke *server* bersama dengan *record id* yang telah diterima bersamaan dengan *dynamic key*

2. Aplikasi *Web* di *Server* Menggunakan *PHP*

Adapun detail masing-masing *function* adalah sebagai berikut :

1) *Function identify*

url:edukreasi.co.id/cloader/identify/<encrypted_machine_id>

Langkah yang dilakukan :

- a) Mendekripsi *encrypted_machine_id*
- b) Menyimpannya dalam tabel *machine_connect* (lebih detail akan dijelaskan pada bahasan selanjutnya)
- c) Memberikan response berupa *dynamic key* yang telah dienkripsi, yakni kombinasi antara *machine id*, *record id* dan waktu koneksi yang diambil dari tabel *machine_connect*

2) *Function identified*

url:edukreasi.co.id/cloader/identified/<encrypted_machine_id|shifted_record_id>

Langkah yang dilakukan :

- a) Mengambil *record id* dan membuat *dynamic key* dari data yang diambil dari tabel *machine_connect*
- b) Mendekripsi *machine id*
- c) Apabila *machine id* telah terdaftar atas seorang pengguna, maka *server* memberikan identitas pada *user* tersebut berupa *session* kemudian mengarahkannya ke halaman utama. Sebaliknya jika *machine id* belum terdaftar maka *server* mengarahkan *user* ke halaman *login*.

3) Database

DBMS yang digunakan adalah MySQL, strukturnya sebagai berikut :

- a) *id : integer(11)*
- b) *machineId : varchar(50)*
- c) *last_connect : timestamp*
- d) *userdata : text* (untuk menyimpan identitas *user* dari *session*)

2.4 Evaluasi Prototype

Tahapan evaluasi prototype merupakan tahapan yang membedakan metode pengembangan perangkat lunak prototyping dengan metode pengembangan perangkat lunak lainnya, sekaligus menjadi nilai tambah, karena melalui evaluasi prototyping, pengguna yang dalam hal ini adalah tim developer Edukreasi dapat memahami dan menguji secara langsung terhadap unit yang disajikan.

2.5 Unit Testing

Adapun beberapa poin pengujian yang dilakukan antara lain sebagai berikut:

- a. Membuktikan bahwa proses handshaking melakukan login system menggunakan *machine id*
- b. Menguji transaksi jual-beli dan *upload-download* tanpa melalui prosedur *handshaking*
- c. Mencoba melakukan penggandaan konten animasi secara *illegal* tanpa melalui *animation store* Edukreasi

3. HASIL PENELITIAN

Berikut adalah perbandingan antara komunikasi aplikasi klien Delphi ke *webserver* Edukreasi, melalui proses *handshaking* dan akses langsung tanpa melalui proses *handshaking*.

Table 3.1. Perbandingan Teknis Penggunaan *Handshaking*

No	Fitur	Akses <i>Handshaking</i>	Tanpa <i>Handshaking</i>
1	Authentikasi Pengguna	Otomatis melalui identifikasi <i>machineid</i>	manual melalui prosedur login (<i>username</i> dan <i>password</i>)
2	Proteksi konten animasi	binding <i>machine id</i>	<i>Binding username /</i>

		dengan konten animasi	<i>password</i> dengan konten animasi
3	Protokol <i>upload-download</i> konten animasi	FTP	HTTP
4	Integrasi konten <i>upload-download</i> dengan struktur materi pembelajaran	Konten animasi yang di- <i>download</i> pengguna dapat langsung terintegrasi ke dalam struktur pembelajaran yang seragam dengan yang disediakan server Edukreasi	Pengguna harus membuat struktur materi pembelajaran sendiri untuk menata konten animasinya sehingga struktur yang dibuat tidak seragam

4. PEMBAHASAN

4.1 Pengumpulan Data

4.1.1 Pengambilan *Machine Id*

Hal ini bertujuan untuk melakukan *binding* antara pengguna dengan perangkat miliknya, sehingga konten animasi yang dibeli hanya dimiliki oleh sebuah *device* saja,

4.1.2 Pengambilan Identitas Pengguna

Identitas pengguna didapatkan saat pengguna melakukan registrasi melalui formulir pendaftaran

4.2 Implementasi Desain *Handshaking*

Agar aplikasi *server*Edukreasi dapat mengidentifikasi aplikasi klien yang terhubung guna melakukan autentikasi *user*, maka dilakukan proses pra-komunikasi antara kedua aplikasi tersebut.

4.2.1 Langkah Pertama: Pengiriman *MachineId* dengan Enkripsi Kunci Statis oleh Aplikasi Delphi

4.2.2 Langkah Kedua : Pengiriman Machine Id, Waktu Koneksi dan Record Id dengan Enkripsi Kunci Statis oleh Aplikasi PHP

4.2.3 Langkah Ketiga : Pengiriman Machine Id dengan Enkripsi Kunci Dinamis oleh Aplikasi Delphi

4.2.4 Langkah Keempat : Pengiriman URL dan Akses FTP Server dengan Enkripsi Kunci Statis oleh Aplikasi PHP

4.3 Coding

Proses implementasi design single handshaking kedalam kode dilakukan 2(dua) kali, yakni pada sisi server menggunakan bahasa PHP dan pada sisi klien menggunakan bahasa pascal/Delphi,

4.3.1 Proses Coding di Sisi Klien

- a) *Generate dan matching machine id*
- b) *Enkripsi dan dekripsi machineid*
- c) *Mengirim machineid ke web server Edukreasi melalui socket*
- d) *Menerima setiap response dari web server Edukreasi*

4.3.2 Proses Coding di Sisi Server

- a) Identify, menerima *machine id* terenkripsi, mendekripsinya dan menyimpannya kedalam basis data, kemudian menyediakan response bagi aplikasi klien sesuai dengan langkah kedua
- b) Identified, menerima *request* berisi *machine id* yang dienkripsi menggunakan kunci dinamis, mendekripsinya dan melakukan autentikasi pengguna serta menyediakan response berupa akses FTP, dan url menuju halaman penulisan session beserta session yang akan ditulis.

4.3.3 Menambahkan Tabel kedalam Database Server Edukreasi

Dalam melakukan autentikasi pengguna menggunakan *machine id* perlu adanya *binding* antara pengguna dengan *machine id* perangkat yang digunakan dengan relasi *one to one*, oleh karena itu perlu ditambahkan sebuah field *machine Id* kedalam tabel *users* di basis data Edukreasi.

4.4 Evaluasi *Prototype*

Melalui evaluasi yang dilakukan bersama dengan tim developer edukreasi, didapatkan kesimpulan bahwa *prototype* yang dihasilkan sudah memenuhi semua aspek requirement kedua sistem,

4.5 *Unit Testing*

4.5.1 Membuktikan bahwa proses handshaking melakukan login sistem menggunakan *machine id*

- 4.5.2 Menguji transaksi jual-beli dan upload-download tanpa melalui prosedur handshaking
- 4.5.3 Melakukan penggandaan konten animasi secara illegal tanpa melalui animation store Edukreasi
- 4.5.4 Melakukan Interupsi Terhadap Proses Handshaking
- 4.5.5 Mengakses Halaman animation store Edukreasi Menggunakan Parameter Aplikasi Klien Delphi

5. KESIMPULAN

Melalui hasil unit testing yang dilakukan terhadap implementasi sub-sistem *single handshaking* kedalam *animation store* Edukreasi, dapat dibuktikan bahwa sub-sistem *single handshaking* mampu melindungi konten animasi pendidikan dari upaya duplikasi dan dekompile *illegal*. Mampu menjaga integritas data antara aplikasi klien dan *webserver* Edukreasi, Menyediakan sarana autentikasi klien, serta melindunginya dari upaya koneksi *illegal*. Sehingga dapat disimpulkan bahwa sub-sistem *handshaking* yang diimplementasikan telah memenuhi kebutuhan aplikasi baik di sisi *server* (PHP) maupun di sisi klien (Delphi).

6. DAFTAR PUSTAKA

- Asmuni, Idris. 2006. Kajian Teoritis Pendekatan *Prototyping* dan Relevansinya Terhadap Pengembangan Sistem Informasi Bisnis. Seminar Nasional Aplikasi Teknologi Informasi, ISSN : 1907-5022, e47-e52
- Bergamo. 2004. "Socket and Network Programming : Introduction and Definitions". UCLA
- Dwijaksana, Made Harta. Studi dan Implementasi Kriptografi Kunci-Publik untuk Otentikasi Perangkat dan Pengguna pada Komunikasi Bluetooth.
<http://informatika.stei.itb.ac.id/~rinaldi.munir/TA/makalah-TA%20Made.pdf>.
Diakses tanggal 1 April 2013
- Hartono, Herman. 2005. Studi Evaluasi Kinerja File Transfer di atas Protokol TCP dengan Menggunakan Winsock 2.2. Jakarta : Universitas Indonesia

- Hower, Chad Z. and the Indy Pit Crew. 2005. Indy Knowledge Base.
<http://indyproject.org/docsite>. Diakses tanggal 1 april 2013
- Kendall, Kenneth. E dan Julie E. Kendall. 2003. Analisis dan Perancangan Sistem Edisi Bahasa Indonesia. Jakarta : PT. Prenhallindo
- Koskie, Sarah. 2003. Handshaking for asynchronous data
transfer.engr.iupui.edu/~skoskie/ECE362/lecture_notes/LNB20_html/11-20-03lecture.html. Diakses tanggal 1 April 2013
- Soelistijanto, Bambang. 2010. Implementasi Autentikasi Client dengan Metode “two way challenge-response” pada Transaksi Perbankan Elektronik. Seminar Nasional Informatika, ISSN: 1979-2328, c-15 – c-20
- Supriyanto, Aji. 2005. Model Pengujian Komunikasi Socket dengan Protocol TCP/IP. Jurnal Teknologi Informasi DINAMIK, ISSN : 0854-9524, 10-18
- Quinn, Bob. 1998. Winsock 2 Information. <http://www.sockets.com/winsock2.htm>.
Diakses tanggal 1 april 2013