PENCEGAHAN SESSION HIJACKING PADA SISTEM JARINGAN KOMPUTER DI WEB SERVER (STUDI KASUS PENGGUNAAN E-MAIL DAN CHATTING)

Fauziah, Ina Agustina
Jurusan Sistem Informasi Universitas Nasional
Jl. Sawo Manila No.61 Pasar Minggu Jakarta Selatan
E-Mail : fauziah_z2@yahoo.com, ina_agustina2007@yahoo.com

Abstrak
Adanya peristiwa sesi pembajakan (session hijacking) pada sistem jaringan komputer umumnya digunakan untuk menggambarkan proses sebuah koneksi TCP yang diambil alih secara langsung oleh sebuah rangkaian serangan yang sudah dapat diprediksi sebelumnya oleh rangkaian jaringan dimana serangan yang sering terjadi umumnya melakukan penyerangan memperoleh kendali melalui koneksi TCP yang sudah ada dan terkoneksi secara langsung melalui jaringan misalnya saja pada jaringan internet.
Bila diterapkan pada keamanan aplikasi web, session hijacking mengacu pada pengambilalihan sebuah session aplikasi web yang ada.Aksi yang dilakukan melalui pengambilan kendali session yang dimiliki user lain setelah aksi pembajak berhasil mendapatkan ID session dari koneksi yang akan dibajak.. Pembajakan yang digunakan oleh pada sesi ini biasanya melalui captured, reserve enggineered dengan tujuan untuk memperoleh ID yang dimiliki oleh user yang akan dibajaknya, dan secara otomatis user dapat dikendalikan oleh pembajak yang telah memiliki ID user yang bersangkutan dengan kata lain setiap user akan diremote oleh pembajak melalui jaringan. Serangan yang dilakukan secara otomatis akan bersifat fatal terhadap keamanan, firewall yang ada pada aplikasi yang sedang kita jalankan.
Ada beberapa aturan yang dapat digunakan untuk menerapkan session dan state tracking secara benar. Aturan-aturan tersebut sama sekali tidak melengkapi atau mengikat suatu aplikasi. Tetapi sebaliknya, aturan-aturan ini dapat menjadi petunjuk yang berguna untuk mendesain sebuah session dan mekanisme state tracking yang berfungsi untuk menaggulangi semua keadaan yang terjadi pada system keamanan jaringan yang ada.

Keyword : *session hijacking, session tracking, state tracking.*

1. PENDAHULUAN

1.1 Latar Belakang

Adanya Peniruan identitas yang sengaja dilakukan oleh para pembajak merupakan usaha dan kemampuan yang dimiliki oleh seseorang untuk mengambil identitas orang lain dan dapat mengendalikan semua aktifitas atau melakukan remote oleh para pembajak. Dengan terjadinya Kasus pembajakan ini sudah banyak masyarakat yang aktif di dunia internet atau jaringan mengalami hal ini lebih kurang 750.000 – 800.000 orang untuk setiap tahunnya. Kenyataannya, tindakan mengambil identitas seseorang jauh lebih mudah dilakukan melalui internet atau melalui jaringan daripada melalui dunia fisik. Hal ini terjadi karena hanya beberapa orang yang memahami resiko berkomunikasi / bertransaksi melalui internet dan bahkan sedikit pula yang berusaha mencegah resiko-resiko tersebut. Ketika *e-commerce* melebarkan sayapnya dan menjamur artinya sudah banyak orang melakukan transaksi melalui dunia maya sehingga makin banyak pula pembajkan yang terjadi, misalnya saja pembajakan melalui nomor karu kredit yang dimiliki oleh konsumen pada saat melakukan verifikasi data pembelian dan pembayaran, karena survey membuktikan bahwa Indonesia adalah pembajak nomor 2 se asia. Sehingga betapa pentingnya pembajak melakukan usaha untuk mendapatkan identitas seseorang secara akurat pada internet menjadi hal yang sangat vital bagi kerahasiaan *online* pelanggan dan pelaku bisnis.

1.2 Tujuan

Tujuan dari penulisan ini adalah untuk memahami bagaimana *session hijacking* (sesi pembajakan) dapat dilakukan dan untuk mengetahui cara pencegahannya.

2. PENGERTIAN *SESSION HIJACKING*

HTTP merupakan protokol yang *stateless,* sehingga perancang aplikasi web mengembangkan suatu cara untuk menelusuri suatu state diantara user-user yang terkoneksi secara *multiple*. Aplikasi menggunakan session untuk menyimpan parameter-parameter yang relevan terhadap user. Session akan terus ada pada server selama user masih aktif / terkoneksi. Session akan otomatis dihapus jika user logout atau melampaui batas waktu koneksi. Karena sifatnya ini, session dapat dimanfaatkan oleh seorang *hacker* untuk melakukan *session hijacking.*

I. *Pengertian Session Hijacking*

Session hijacking merupakan aksi pengambilan kendali session milik user lain setelah sebelumnya "pembajak" berhasil memperoleh autentifikasi ID session yang biasanya tersimpan dalam cookies. *Session hijacking* menggunakan metode *captured, brute forced* atau *reserve enggineered* guna memperoleh ID session*,* yang untuk selanjutnya pembajak memegang kendali atas session yang dimiliki oleh user lain tersebut selama session berlangsung

II. Pengertian Cookies

Cookies merupakan file data yang ditulis ke dalam hard disk komputer user / klien yang biasanya dilakukan oleh web server guna kepentingan mengidentifikasikan user pada situs tersebut sehingga sewaktu user kembali mengunjugi situs tersebut, situs itu akan dapat segera mengenalinya. Jadi dapat dikatakan bahwa cookies merupakan semacam *ID card* user saat koneksi pada situs-situs aktif melalui internet.Saat user mengunjungi situs yang ada cookiesnya, server akan mencari informasi yang dibuat sebelumnya dan browser membaca informasi di cookies dan menampilkannya. Cara penggunaan cookies yang tidak baik juga dapat mengakibatkan terjadinya SQL *injection* yang tidak perlu. Hal ini biasanya terjadi jika user menggunakan cookies untuk mengakses web page tertentu, dimana cookies tersebut dikirim sebagai parameter pada URL tanpa melalui proses enksipsi terlebih dahulu.

Untuk keperluan bisnis, seperti situs amazon.com,e-bay.com, gramedia.com, cikalmart.com dan situs – situs yang berbasis e-commerce lainnya banyak menggunakan fasilitas cookies yang tujuannya dapat membantu menghubungkan data pembelian yang terdahulu ke basis data yang berisi *unique* ID misalnya nomor kartu kredit yang digunakan oleh pengunjung yang sudah menjadi member dan akan melakukan belanja online dan historikal pembelian. Sehingga mampu merekomendasikan barang atau produk yang ditawarkan dan yang sesuai dengan kebutuhan serta selera user. Ini merupakan hal yang menarik, sehingga pembeli akan dengan senang hati untuk kembali ke situs e- commerce yang ada melalui internet. Situs-situs lain juga menggunakan cookies untuk mengetahui berapa orang yang mengakses mereka setiap harinya. Sehingga angka yang dihasilkan oleh cookies tersebut menunjukkan seberapa sibuknya situs mereka.

Ada beberapa cara yang dilakukan untuk dapat mengatasi dan memblok cookies, dimana pada masing-masing browser, baik Netscape maupun IE dapat diatur untuk *enable* maupun *disable* cookies. Misalnya IE, dapat diatur pada bagian Internet Options | Security.

3. HASIL DAN PEMBAHASAN

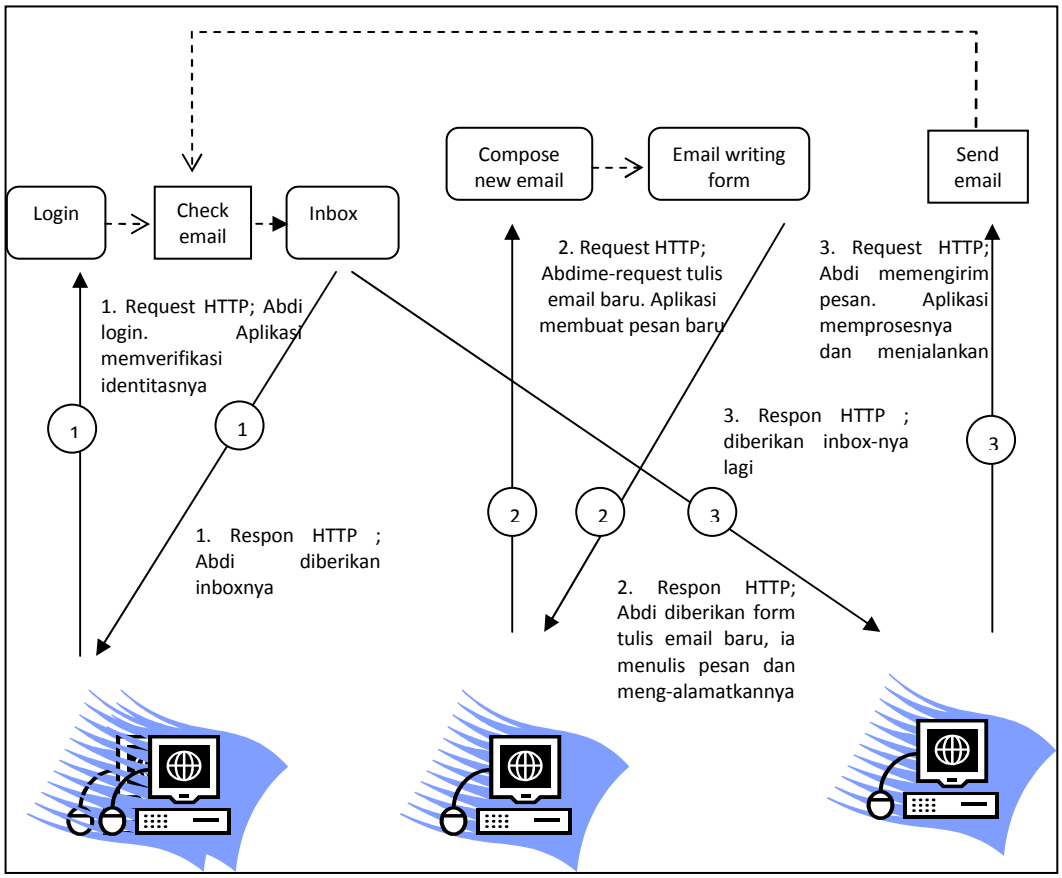
Istilah sesi pembajakan (*session hijacking*) umumnya digunakan untuk menggambarkan proses sebuah koneksi TCP yang diambil alih oleh sebuah rangkaian serangan yang sudah dapat diprediksi sebelumnya. Pada serangan seperti itu, penyerang memperoleh kendali melalui koneksi TCP yang sudah ada. Bila diterapkan pada keamanan aplikasi web, *session hijacking* mengacu pada pengambilalihan sebuah session aplikasi web.

Dibuatkan sebuah ilustrasi berikut ini untuk mengetahui bagaimana *session hijacking* dapat dilakukan, sehingga sejauh mana kelemahan dari situs web yang kita gunakan untuk melakukan komunikasi atau bertukar data. Pada waktu itu Abdi berkenalan dengan Akbar melalui media internet yaitu aplikasi *chatting online*. Keduanya saling bertukar informasi mengenai proses bisnis yang mereka jalankan selama ini. Melalui email, Akbar ingin mengajak Abdi untuk melakukan pertemuan secara langsung untuk membahas semua rencana bisnis yang akan mereka jalankan, akhirnya tiba waktunya mereka bertemu, tapi pada kenyataannya Akbar tidak muncul, nah Abdi berpendapat apakah chatting

online dan e-mail yang dia kirim tidak pernah sampai atau telah dilakukan session hijacking oleh orang yang tidak bertanggung jawab? Ternyata e-mail Abdi telah dilakukan pembajakan oleh orang yang tidak bertanggung jawab dengan cara membukanya melalui layanan eWebMail yang menggunakan java servlet. Langkah yang dilakukan adalah menuju ke halaman cookie pal.

Cookie Pal adalah aplikasi *shareware* yang tersedia pada http://www.kbura.net/. Digunakan untuk memonitor dan mengontrol cookie yang dikirim oleh situs web pada suatu browser. Pada kotak *pop-up* itu terlihat bahwa eWebMail mengirimkan cookie *string* yang panjang, dengan nama "uid" . Nilai "uid" sepertinya di-*encode* dalam heksadesimal. Cookie ini menarik untuk disimak, mengingat bahwa seringkali aplikasi web menggunakan cookie untuk melewatkan *session identifier* selama berinteraksi dengan web. Mungkin cookie ini juga semacam *session identifier* dari eWebMail.

Langkah selanjutnya adalah membersihkan browser dari semua cookie dan login ke eWebMail sebagai fauziah_z2@ewebmailexample.com. Cookie "uid" di-set, dan segera kita dapat melihat halaman inbox yang ternyata memiliki satu buah pesan email. Email ini berasal dari service eWebMail.



Gambar 1.

CARA PENCEGAHAN YANG DILAKUKAN ADALAH DENGAN

1. Dengan Cookie

Cookie ditangani melalui browser. Browser mengirimkan cookie yang diperlukan ke web server bersama dengan *request* HTTP jika sebelumnya ada cookie yang diterima dari server yang sama. Browser terkenal, seperti Netscape, Internet Explorer, dan Opera menangani cookie

secara baik. Cookie lebih menguntungkan daripada field tersebunyi. Field tersebunyi selalu memerlukan halaman form HTML untuk dikirim kembali ke server, sedangkan cookie tidak memerlukan form HTML apapun.Segi kerugiannya adalah kebanyakan situs menggunakan cookie untuk melacak tingkah laku user. Situs yang menampilkan *banner* iklan diketahui melanggar *privacy* user dengan cara mengumpulkan informasi tentang user secara berlebihan melalui pelacakan aktivitas user via cookie dan acuan-acuan HTTP. Sayangnya, browser tidak memiliki mekanisme *built-in* yang memadai untuk secara selektif hanya memilih cookie-cookie tertentu saja. Untuk maksud ini program seperti Cookie Pal dapat digunakan sebagai alat bantu.

2. Dengan Field Tersembunyi

Field tersembunyi di dalam form HTML dapat juga digunakan untuk mengirimkan dan mengembalikan informasi antara browser dan web server. Keuntungan field tersebunyi dibandingkan cookie adalah field tersebut tetap dapat bekerja walaupun browser telah diatur untuk menolak semua cookie.

4. KESIMPULAN

Serangan *session hijacking* dilakukan tidak semudah serangan aplikasi web lainnya. Tetapi efeknya bisa sangat merusak. Serangan yang dilakukan pada cara desain dan pengembangan aplikasi. Kelalaian dalam mendesain atau dalam mengimplementasikan mekanisme *session tracking* pada aplikasi.

Tak satupun *patch* sistem operasi, *firewall* atau konfigurasi web server dapat mencegah serangan *session hijacking.* Tiap pengembang web harus mengerjakan secara cermat desain dan implementasi *session* dan *state tracking*.

Server-server komersial kelas menengah sampai *high-end* memiliki mekanisme *session tracking built-in* dan menyediakan sebuah API untuk membantu developer dalam mendesain aplikasi web.

5. DAFTAR PUSTAKA

http://www.jasakom.com/Artikel.asp?ID=8,
http://www.iss.net/security_center/advice/Exploits/TCP/session_hijacking/default.htm, 12/25/2004 6:43:21AM
Mc.Clare, Stuart; Shah, Saumil; Shah, Shreejah, *Attacks and Defense*, Pearson Education Inc, 2003