Keamanan Dalam ***Online Game***

Adrian Benigno dan B. Prabawa

Departemen Teknik Informatika
Institut Teknologi Bandung
Jalan Ganesha 10 Bandung 40132

E-mail : if11020@students.if.itb.ac.id , if11032@students.if.itb.ac.id

Abstrak

Perkembangan teknologi internet membawa suatu perubahan pula mereka yang hobi bermain *game*. Jika sebelumnya seseorang hanya bermain di dalam kamar sendirian ditemani sebuah televisi dan mesin Nintendo atau Playstation, kini mereka yang mempunyai akses internet dapat bermain bersama ribuan orang di seluruh dunia. Mereka yang tidak memiliki komputer dan akses internet pribadi pun dimanjakan dengan menjamurnya *game cente*.

Semakin berkembangnya *online game* bukannya tanpa masalah. Masalah paling besar yang dihadapi *user* adalah pencurian aset pemain dalam *game*, yang oleh *user* disebut *hacking*. Hal ini antara lain menyangkut kerahasiaan *password.* Selain masalah *hacking*, ada juga penggunaan *software* ilegal yang memang dapat membantu seseorang dalam bermain, namun tidak *fair*. Contoh untuk masalah tersebut adalah penggunaan *speed hack*, yang mempercepat respon *client* terhadap *server*, sehingga kecepatan gerak *character* milik *user* tersebut manjadi lebih cepat daripada *character* lainnya.

Penyedia layanan *online game* telah berusaha meredam kecurangan - kecurangan tersebut, antara lain dengan menggunakan *security software*. Namun masih banyak celah yang dapat ditembus.

***Kata kunci**: online game, security*

1. Pendahuluan

Peter berjalan dengan langkah ringan menuju *game center* langganannya di sebuah kompleks pertokoan di daerah Cihampelas. Hari itu dia berniat untuk bermain *Ragnarok Online*, hendak memainkan *character* – nya yang berprofesi sebagai *Hunter*. Setelah melapor pada operator, kemudian menyapa beberapa orang yang ia kenal, ia duduk di hadapan komputer dan menjalankan aplikasi *game*, kemudian memasukkan *user-id* dan *password*. Alangkah terkejutnya ia menemukan bahwa seluruh *equipment* milik *character* – nya telah hilang. Ia baru saja di – *hack*.

Kejadian yang menimpa Peter bukan cuma terjadi satu atau dua kali. Seiring dengan berkembangnya *online game*, pencurian tersebut juga makin sering terjadi. Hal ini berkaitan langsung dengan keamanan *password*. Seseorang yang berniat mengambil milik orang lain harus mengetahui *password* orang tersebut. Bagaimana caranya, serta bagaimana mengatasinya akan dijelaskan kemudian.

Masalah lain adalah penggunaan *software* ilegal. Contohnya adalah *speed-hack*, yang mampu mempercepat gerak *character*. Selain itu ada pula penggunaan *bot*, aplikasi yang dapat menjalankan *character* secara otomatis. Kedua masalah tersebut tidak

merugikan seseorang secara langsung, melainkan lebih kepada hilangnya semangat *fair play* dalam *game* tersebut.

Masalah lain yang mungkin dihadapi penyedia layanan *online game* adalah adanya penyusup ke *game database.* Namun karena masalah ini belum begitu terdengar di Indonesia, makalah ini tidak akan membahas hal tersebut.

2. Ruang lingkup

Makalah ini membahas keamanan dalam *online game*, terutama keamanan *password,* serta penggunaan *software* ilegal.

Ruang lingkup o*nline game* yang dibahas dalam makalah ini adalah *game* yang dimainkan secara *online* melalui jaringan internet. Secara spesifik, *game* yang dimaksud adalah *Ragnarok Online, Risk Your Life, Tantra Online,* serta *Gunbound,* yang semuanya memiliki server lokal Indonesia.

3. Ancaman terhadap *password*

Berikut ini adalah beberapa contoh bagaimana seseorang bisa memperoleh *password* orang lain.[1)]

3.1 *Keylogger*

Pada dasarnya, *keylogger* akan merekam penekanan tombol pada keyboard dan menyimpannya pada suatu tempat untuk selanjutnya diambil kembali. Secara teknis, *keylogger* akan merekam semua tombol keyboard yang ditekan, kecuali [ctrl]+[alt]+[del]. *Keylogger* dapat menyimpan data pada komputer tersebut, atau mengirimkannya melalui internet/jaringan.

Keylogger sulit untuk dideteksi secara manual, karena memang didesain untuk bekerja secara tersembunyi. Untuk mendeteksinya perlu digunakan *software* khusus.

Salah satu cara yang dapat dilakukan *user* untuk mengatasi *keylogger* adalah penggunaan mouse, misalnya dengan *Virtual Keyboard*

3.2 *Packet Sniffer*

Packet Sniffer adalah suatu *tool* yang digunakan untuk mengakses semua data yang dikirim melalui jaringan. Saat seorang *user* mengirimkan *user-id* dan *password* – nya untuk *login,* informasi tersebut dikirimkan ke internet melalui WinSock. Informasi yang seharusnya bersifat rahasia ini bisa diakses dengan menggunakan *packet sniffer*, sehingga *password* seseorang dapat diketahui.

Packet sniffer ini mustahil diatasi oleh user. *Tool* tersebut tidak harus berada di komputer *client,* cukup diletakkan di komputer yang menjadi *gateway* – nya.

Salah satu cara mengatasinya adalah mengenkripsi paket, dan cara ini terbukti mengurangi resiko *password* diketahui orang lain. Namun ada masalah lain dengan *packet sniffer* ini. Meskipun terenkripsi, seseorang dapat mengambil *outgoing packet* dan mengirimnya berulang – ulang (serangan ini disebut *"replaying packets"*). Bayangkan jika paket tersebut berisi perintah sebuah pesawat menembakkan sinar laser, *replaying packets* dapat memberikan keuntungan dengan membuat pesawat menembakkan sinar laser berkali – kali dengan sangat cepat.[2)]

3.3 *Peeping Tom*

Ini adalah masalah paling klasik dalam keamanan *password*, yaitu orang yang mengintip pada saat *user* memasukkan *user-*

id dan *password*. Hal ini dapat dengan mudah terjadi di *game center*. Seseorang bisa berpura – pura hendak menonton permainan orang lain, namun ternyata berniat melihat jari – jari tangan yang hendak memasukkan *password*.

Cara mengatasinya adalah dengan kesadaran *user* sendiri untuk berhati – hati.

4. Penggunaan *Software* Ilegal

Selain *packet sniffer* sebagai *software* ilegal yang telah dibahas sebelumnya, berikut ini adalah beberapa contoh lainnya.

4.1 *Speed Hack*

Secara umum software ini berfungsi mempercepat waktu respon *client* terhadap *server*. Efek yang dihasilkan, *character* yang menggunakan *speed hack* akan bergerak lebih cepat dari normal. *Speed hack* bekerja seperti *packet sniffer*, yaitu dengan memanipulasi paket yang dikirimkan ke *server*. Tentu saja aplikasi ini bergantung pada *game* itu sendiri, bagaimana komunikasi *client – server* dilakukan. *Game* yang memiliki celah untuk penggunaan *speed hack* adalah *Risk Your Life*.

4.2 *Bot*

Kualitas suatu *character* dalam *online game* antara lain ditentukan oleh levelnya. Dan untuk memperoleh level tinggi, *user* pemilik *character* tersebut wajib mencari *experience point*, yang diperoleh dengan membunuh monster. Tentu saja *user* seharusnya memainkan sendiri *character* – nya. Namun kini banyak beredar aplikasi yang dapat menjalankan *character* secara otomatis, sehingga *user* yang menggunakannya dapat memperoleh level tinggi tanpa susah payah menyisihkan waktu berburu monster. Aplikasi tersebut dinamakan *bot*. Yang perlu dilakukan hanya jalankan *bot, login* ke *game server*, lalu biarkan *character* berjalan sendiri sementara *user* pergi kuliah atau tidur. Penggunaan *bot* sangat marak dalam *Ragnarok Online*

5. Penanganan

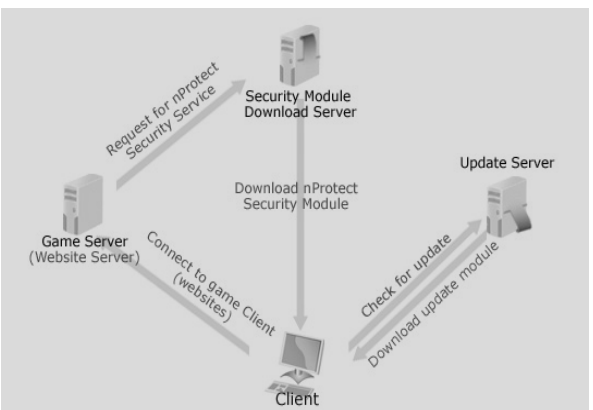
5.1 Penggunaan *Software* Khusus

Penyedia layanan *online game* pada umumnya mengintegrasikan *software* khusus ke dalam aplikasi *game* – nya untuk mengatasi masalah – masalah yang telah dijelakskan sebelumnya.

Salah satu aplikasi yang banyak dipakai di Indonesia adalah *nProtect GameGuard* yang dikembangkan oleh Inca Internet Co, Ltd., sebuah *software house* asal Korea Selatan.[3)]

Fitur utama *nProtect Gameguard* adalah sebagai berikut.

- diagnosa dan blokade paket/kode yang tidak dikenal
- blokade usaha manipulasi terhadap *game client*
- perlindungan pribadi terhadap *security modul*
- mendeteksi adanya *speed hack*
- mengoptimalkan *CPU occupancy rate*



Gambar 1. *system flow chart nProtect GameGuard*

System Flow Chart nProtect GameGuard dapat dilihat di gambar 1.

NProtect GameGuard terbukti efektif mengatasi *keylogger* dan beberapa aplikasi *sniffer, speed hack,* dan *bot.* Meskipun demikian, masih ada beberapa versi aplikasi *speed hack* dan *bot* yang dapat menembus proteksi *nProtect GameGuard*

Di Indonesia, *nProtect GameGuard* dipakai oleh Lyto sebagai penyedia *Ragnarok Online* dan serta Cib Net sebagai penyedia *Risk Your Life.*[4)]

Aplikasi proteksi sejenis antara lain adalah *AhnLab HackShield* dan *Fortinet's Fortigate™-3000.*

AhnLab HackShield merupakan produk dari AhnLab, Inc., pesaing Inca Internet yang juga berasal dari Korea Selatan. *HackShield* antara lain dipakai dalam sebuah *online game* bertipe pacuan kuda bernama *Derby Owners Club Online,* keluaran Sega Corp., Jepang. *Game* tersebut tidak dikenal di Indonesia, selain karena pacuan kuda kurang populer di Indonesia, *game* itu sendiri baru dirilis pada tanggal 16 Desember 2004.[5)]

Fortinet's Fortigate™-3000 merupakan produk dari Fortinet Inc., sebuah *software house* yang berpusat di Sunnyvale, California. *Fortigate™-3000* antara lain digunakan oleh AsiaSoft Int'l Co. Ltd., penyedia layanan *Ragnarok Online* di Thailand.[6)]

5.2 Perbaikan *Game*

Cara lain mengatasi masalah keamanan *online game* adalah dengan menutup celah – celah yang ada. Contohnya adalah untuk mencegah *packet replaying* dengan *sniffer* serta *speed hack*, adalah dengan memberikan *sequence number* pada tiap paket. Jadi apabila *server* menerima paket dengan *sequence number* yang tidak tepat, maka otomatis dianggap sebagai kecurangan.

5.3 Kesadaran *user*

Sebagian besar kasus yang terjadi di Indonesia adalah karena kelalaian *user* dalam menjaga *password* – nya. Bisa karena *password* yang gampang ditebak, atau karena *peeping tom.* Dibutuhkan kesadaran *user* untuk membuat *password* yang tidak mudah ditebak, serta kehati – hatian dalam menyimpannya. Ada baiknya dilakukan penggantian *password* secara berkala.

6. Kesimpulan dan Saran

Kesenangan dalam bermain *online game* kadang terganggu oleh orang – orang yang serakah. Pencurian aset dalam *online game* tentu sangat merugikan. Kemudian adanya *user* yang dengan mudah mencapai level tinggi tanpa harus susah payah menyisihkan waktu tentu dapat merusak suasana *fair play.* Yang dapat dilakukan adalah mencegah. Peyedia layanan *online game* telah mengintegrasikan *software* khusus. Yang harus dilakukan oleh user adalah meningkatkan kesadaran pentingnya menjaga *password.* Alangkah baiknya jika semua *user* sadar akan pentingnya bermain dengan *fair,* tanpa melakukan kecurangan.

[1] C. Kenni, *Security Tips*, http://www.ragnafilia.com, diakses tanggal 9 Januari 2005 pukul 11.15
[2] Andrew and C. Kirmse, *Security in Online Game*, http://www.gamasutra.com, diakses tanggal 9 Januari 2005 pukul 11.20
[3] -----, *nProtect GameGuard*, http://eng.nprotect.co.kr, diakses tanggal 9 Januari 2005 pukul 10.50
[4] -----, *nProtect Partners*, http://eng.nprotect.co.kr, diakses tanggal 9 Januari 2005 pukul 10.53
[5] -----, *AhnLab to Guard Sega's Online Game*, http://www.ahnlab.com/english, diakses tanggal 9 Januari 2005 pukul 11.30
[6] -----, *Press Releases*, http://www.fortinet.com, diakses tanggal 9 Januari 2005 pukul 11.35