TELEMATIKA, Vol. 14, No. 02, OKTOBER, 2017, Pp. 83 – 88
ISSN 1829-667X

PENGEMBANGAN DETEKSI PENYUSUPAN MENGGUNAKAN MULTIAGENT

Bambang Sugiantoro
Teknik Informatika UIN Sunan Kalijaga
Alamat Jl Marsda Adisucipto Yogyakarta
e-mail : bambang.sugiantoro@uin-suka.ac.id

Abstract

As challenges and problems surround intrusion arises rapidly, the intrusion detection system has been gradually developed. Agent-based approach for intrusion detection system has developed from single to multi agent, and later developed to mobile agent in order to increase system's capability to face with a more complex challenge and change. A number of study had been identified that mobile agent can reduce network traffic, however the study related to intrusion detection using static and mobile agent for finding intruder has not been fully achieved. This research proposes detection method followed by a rule matching and string matching with multi agent components. The prototype has fulfilled the requirements specification or the defined model criteria, i.e. : resource usage and the provision of intrusion detection information which are mandated to agent.

Keywords : Multiagent, Intrusion detection, intruder

Sistem deteksi penyusupan telah berkembang seiring dengan berkembangnya tantangan dan permasalahan yang perlu diakomodasi oleh sistem tersebut. Pendekatan teknologi agen dalam sistem deteksi penyusupan telah berkembang dari agen tunggal ke multiagen, dan kemudian berkembang lagi ke mobile agen untuk meningkatkan sistem tersebut dalam menghadapi tantangan dan perubahan yang lebih kompleks. Beberapa studi telah mengidentifikasikan bahwa mobile agen mampu mereduksi trafik jaringan, namun studi berkaitan arsitektur sistem deteksi yang memanfaatkan agen statik dan mobile dalam dalam hal performance belum sepenuhnya tercapai. Penelitian doktoral ini mengusulkan penggunaan mobile agent, metode deteksi rule matching dilanjutkan dengan string matching dan arsitektur dengan komponen multiagen

Kata Kunci : ***Multiagent, Deteksi Penyusupan, Penyusup***

1. PENDAHULUAN

Menurut data dari annual report panda lab 2013 melaporkan adanya penyusupan yang berkaitan dengan tindakan ilegal untuk login di jejaring sosial khususnya twitter sebanyak 250.000 pengguna (Pandalabs, 2014). Kerugian non materil maupun materil adalah dampak yang akibatkan adanya tindakan ilegal yang dilakukan oleh penyusup. Riset di bidang keamanan untuk mendeteksi adanya penyusup menjadi hal yang penting mendapat perhatian, karena kerugian yang diakibatkan oleh intrusion. Penyusupan/intrusion didefinisikan kegiatan yang berusaha merusak atau menyalahgunakan sistem atau setiap usaha yang melakukan compromise integritas, kepercayaan atau ketersediaan suatu sumber daya komputer. Definisi ini tidak bergantung pada sukses atau gagalnya aksi tersebut, sehingga berkaitan dengan suatu serangan pada sistem komputer (Bace dan Mell, 2001). Keberadaan penyusup perlu dideteksi sejak awal, maka diperlukan sistem yang mampu untuk mendeteksi adanya penyusup atau biasa disebut IDS. IDS singkatan dari Intrusion Detection System. Saat ini model IDS secara umum terdiri dari tiga komponen: sumber informasi IDS, analisis IDS dan respon IDS (Maskat et al., 2011). Sumber informasi yang dikumpulkan IDS terdiri dari dua komponen, yang pertama network based IDS (NIDS) dan host based IDS (HIDS). NIDS akuisisi data dari jaringan, yaitu menangkap paket yang lewat. HIDS akuisisi data dari sumber di host, contoh file log atau keadaan memori. Adapun analisis IDS terdiri dari misuse detection (signature/pattern analysis) dan anomaly detection. Setelah IDS mengumpulkan informasi dan melakukan proses deteksi tahap selanjutnya respon IDS. Respon IDS terdiri dari respon pasif dan aktif, respon pasif jika hasil dari proses deteksi yang dihasilkan sebatas alert. Sedangkan respon aktif sistem akan mengambil tindakan tidak hanya sebatas alert tetapi disertai tindakan tertentu. Teknologi IDS bekerja dengan melakukan proses identifikasi terhadap aktivitas yang dianggap mencurigakan

sesuai dengan aturan yang sesuai kebijakan aturan yang berlaku, IDS menganalisa dari sejumlah data yang dikoleksi dari sumber paket jaringan dan dari sumber pada host atau multihost komputer (Jachak dan Barua, 2012).

2. Metode Penelitian

Dewasa ini penggunaan IDS untuk membantu mendeteksi adanya aktifitas penyusupan oleh administrator jaringan sangat diperlukan. Adapun kondisi saat ini IDS yang banyak digunakan adalah IDS dengan sistem terpusat dan terdapat *false alarm*. IDS dengan sistem terpusat mempunyai kelemahan dalam hal skalabilitas dan adanya potensi lonjakan penggunaan jaringan untuk komunikasi, untuk mengatasi problem ini *mobile agent* mampu mengatasi hal tersebut diatas. Penelitian-penelitian yang menggunakan pendekatan *mobile agent* untuk mendukung IDS mempunyai kelebihan dan kekurangan. Kelebihan yang bisa didapatkan diantaranya berkaitan dengan skalabilitas dan mampu mengurangi *trafik* jaringan. Adapun kelemahan dari pendekatan *mobile agent* untuk sistem deteksi adalah masalah keamanan.

Klasifikasi celah keamanan terbagi menjadi empat bagian yaitu : *agent to agent*, *agent to platform*, *platform to agent* dan *other to platform*. Salah satu kelemahan yang berhasil diidentifikasi yang akan dijadikan esensi penelitian ini adalah adanya potensi intruder yang akan melakukan penyusupan, jika *mobile agent* telah berpindah dari *host* yang telah dikunjunginya. Jika hal tersebut terjadi akan mengakibatkan gagalnya *mobile agent* mendeteksi adanya penyusupan.

Berdasarkan gambaran umum tersebut, pada penelitian ini, kerangka utama pengembangan model mobile agen untuk IDS seperti analisis kebutuhan diatas, maka untuk mendesain menggunakan M-UML. M-UML adalah *extension* dari UML yang dapat digunakan untuk membantu para analis dibidang *mobile agent* baik secara umum maupun detail setiap bagian *mobile agent*. AgletMaster sebagai *class* utama di *server* menginstansiasi *user interface* dari *class* AgletMasterGUI. *Class* ini berhubungan dengan beberapa *class* yang masing-masing memiliki fungsi tertentu. Pertukaran data antar class dilakukan melalui objek dari class Informasi.

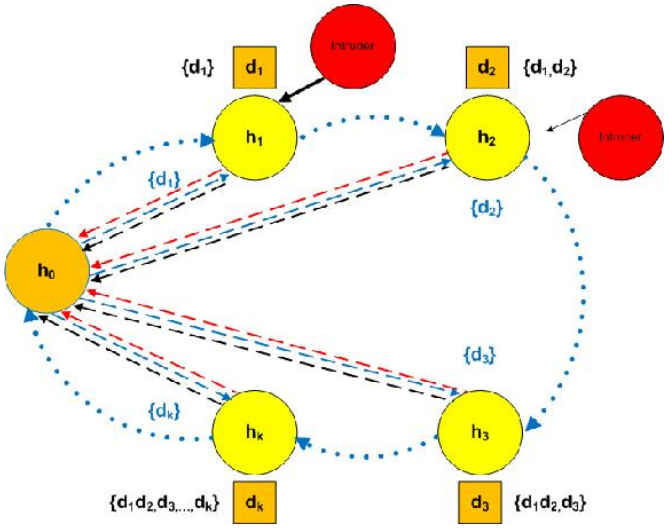
AgletSlave bertugas sebagai *mobile agent* yang bisa melakukan *dispatch* melalui jaringan ke *host-host* tujuan. Informasi yang diambil pada setiap jaringan disimpan dalam objek dari *class* Report. AgletCloned merupakan aglet yang dikirim ke semua *host* tujuan secara serempak. Pada *remote host*, AgletCloned bisa melakukan komunikasi dengan AgletMaster melalui AgletMessenger. Hal ini dilakukan untuk memantau lokasi *host* tempat AgletCloned melakukan deteksi.

Objek dari *class* AgletSlave kemudian berpindah dari satu *host* ke *host* yang lain sesuai dengan rencana perjalanan yang telah ditentukan. Langkah-langkah deteksi yang dilakukan oleh agen digambarkan dengan *collaboration* diagram pengiriman agen pada Gambar 1. Agen melakukan *dispatch*() ke setiap *host* tujuan.

Arsitektur secara umum model dengan mekanisme kerja sama antar *multiagent* dan untuk analisis IDS memanfaatkan *misuse detection* dengan teknik *string matching*. Himpunan *host* yang akan dideteksi adalah $\{h_1, h_2, h_3,\ldots, h_k\}$, dengan himpunan data D yang diperoleh adalah $\{d_1, d_2, d_3,\ldots, d_k\}$. *Mobile agent* (agen *slave*) yang di*create* dari *host* asal, akan melakukan deteksi penyusupan pada masing-masing *host* tersebut, kemudian akan kembali lagi ke *host* asal h_0. Data yang diperoleh oleh *mobile agen*t (agen slave) akan bertambah seiring dengan bertambahnya *host* yang telah dideteksi. Himpunan rencana perjalanan *mobile agent* (agen *slave*) adalah $\{h_0, h_1, h_2, h_3,\ldots, h_k, h_0\}$. Setelah mengeksekusi deteksi penyusupan disemua *host, mobile agen*t (agen *slave*) akan kembali ke *host* asal h_0, informasi hasil deteksi yang diperoleh adalah $\{d_1, d_2, d_3,\ldots, d_k\}$.

Ketika *mobile agent* (agen *slave)* telah selesai mendeteksi penyusupan di h_1, agen *slave* meminta bantuan ke agen statik (agen master) agar dikirim agen pembantu untuk ditempatkan di h_1, kemudian agen statik (agen master) mengirimkan *mobile agent* (agen *clone*)

ke h_1, Setelah itu *mobile agent* (agen *slave*) melanjutkan ke *host* berikutnya. Mekanisme ini berulang sampai *host* yang terakhir h_k. *Mobile agent* (agen *clone*) sejumlah h_k akan dibuat untuk membantu *mobile agent* (agen *slave*). Apabila terjadi penyusupan masing-masing *mobile agent* (agen *clone*) akan mengirimkan hasil deteksinya ke agen statik (agen master) untuk ditampilkan sebagai hasil deteksi penyusupan.



Gambar 1 Arsitektur

3. Hasil dan Pembahasan

Dewasa Pengujian dilakukan pada 5 komputer pada jaringan lokal dengan konfigurasi sebagai berikut: (i) satu komputer sebagai host asal dengan IPaddress 192.168.231.1 sistem operasi windows, database Mysql server, Aglets SDK dan JDK. (ii) host sebagai komputer destinasi pertama yang akan dideteksidengan IP address 192.168.231.18 sistem operasi windows, Aglets SDK dan JDK. (iii) host sebagai komputer destinasi kedua yang akan dideteksi dengan IP address 192.168.231.17 sistem operasi linux, Aglets SDK, JDK dan Ossec hids. (iii) host sebagai komputer destinasi terakhir yang akan dideteksi dengan IP address 192.168.231.24 sistem operasi linux, Aglets SDK, JDK dan Ossec hids.(v) IP komputer sebagai intruder 192.168.231.180.Kebutuhan adanya mobile agen server di setiap host, Jika mobile agen telah menjadi cukup populer, makasetiap host bisa dianggap berada dalam keadaan default terinstal dengan mobile agen. Seperti halnya browser yang telah mendukung interpreter Java. Untuk melakukan instalasi Java Virtual Machine dan server aglet memerlukan waktu kurang lebih sekitar 1 menit.

Komunikasi antara agen master dengan mobile agen menggunakan standard KQML (*Knowledge query and manipulation language*). Mobile agen diimplementasikan menggunakan aglet. Aglet menggunakan JKQML yang digunakan komunikasi dan pertukaran pesan. Implementasi dalam pertukaran pesan antara agen master dengan mobile agen menggunakan proxy. Argumen pesan yang dikirim dari agen master ke mobile agen atau sebaliknya berupa argumen yang dapat diserialisasi, dengan mengimplementasikan *java.io.serializable.* Pesan yang dikirim berupa obyek. Obyek pesan dikenali dari jenisnya (kind). Properti string ini digunakan untuk membedakan antara pesan satu dengan pesan yang lainnya. Obyek pesan juga dapat berupa argumen opsional unutk data yang berhubungan dengan pesan tertentu, Argumen dapat berupa argumen atomik bertipe *string, integer* dan tipe data lain atau tabular berupa *hashtable.* Dalam menanganani pesan yang datang, agen master maupun mobile agen menggunakan *method handle message (message msg).* Pada layer komunikasi agen master dan mobile agen menggunakan ATP (*agen tranfer protocol*) sebagai implementasi komunikasi default dari layer komunikasi.

Adapun komponen agen ditinjau dari segi ukuran yang dihasilkan adalah sebagai berikut : *AgletMaster.java* mempunyai ukuran 9.31 KB (9,539 *bytes*), *AgletCloned.java*

memiliki ukuran 5.71 KB (5,848 *bytes*) dan *AgletSlave.java* berukuran 3.66 KB (3,749 *bytes*) dapat dilihat pada Tabel . Ukuran mobile agen yang relatif kecil memungkinkan untuk menjelajah dengan gesit di jaringan komputer, hal ini salah satu faktor tidak mengkonsumsi *bandwidth* yang tinggi.

Tabel 1 Ukuran Multiagen

Nama	Ukuran
AgletMaster.java	9.31 KB (9,539 bytes)
AgletCloned.java	5.71 KB (5,848 bytes)
AgletSlave.java	3.66 KB (3,749 bytes)

Uji beda telah dilakukan antara dua jenis *mobile agent* : agen *slave* dan agen *clone*, lebih detail dapat dilihat pada lampiran. Alat uji yang digunakan : uji mann *whitney* (uji non parametik) sepadan dengan uji t

Uji t = uji parametik ==> perlu asumsi ; asumsi data normal

Ho : Tidak ada perbedaan

H1 : Terdapat perbedaan

Dasar pengambilan keputusan Ho ditolak jika nilai Asymp. Sig < 0.05 (tingkat kepercayaan 95%). Tampak nilai sig. = 0.037 < 0.05. Artinya Ho ditolak (h1 diterima). Terdapat perbedaan *bytes* antara 2 *mobile agent* tersebut, dimana Agen *Clone* cenderung lebih besar dari pada Agen *Slave* Hasil experimen agen *slave*, pertambahan per *host* diperlihatkan pada Tabel , menghasilkan rata-rata per *host* 491 *bytes*.

Tabel 2. Mobile agen slave

No	Host yang dikunjungi	Rata-rata ukuran hasil deteksi (bytes)
1 2	192.168.231.18 192.168.231.17	491 bytes
3	192.168.231.24	

Jika terjadi penambahan jumlah host, asumsi rata-rata per host terjadi penambahan 491 bytes, maka perhitungan total adalah 3749 bytes + (jumlah host* 491 bytes) diperlihatkan pada Tabel .

Tabel 3 Jumlah host vs ukuran agen slave

No.	Jumlah host dikunjungi	Total ukuran agen slave (bytes)
1	3	5222
2	5	6204
3	7	7186
4	9	8168
5	11	9150
6	13	10132
7	15	11114

Hasil experimen mobile agen *clone*, rata-rata per *host* menghasilkan 770 *bytes*. diperlihatkan pada Tabel .

Tabel 4 Mobile agen clone

No	Host yang dikunjungi	Rata-rata ukuran hasil deteksi
1	192.168.231.18	770 bytes
2	192.168.231.17	
3	192.168.231.24	

Jika terjadi penambahan jumlah *host,* asumsi rata-rata per *host* 770 *bytes*, maka perhitungan adalah jumlah *host* * (5848 + 770) bytes diperlihatkan pada Tabel .

Tabel 5 Jumlah host vs ukuran agen clone

No.	Jumlah host dikunjungi	Total ukuran agen clone (bytes)
1	3	19854
2	5	33090
3	7	46326
4	9	59562
5	11	72798
6	13	86034
7	15	99270

Jumlah host yang dikunjungi bervariasi mulai dari tiga, lima, tujuh, sembilan, sebelas, tigabelas dan limabelas. Sedangkan ukuran dari mobile agent dalam satuan bytes, terlihat terjadi peningkatan seiring dengan banyaknya jumlah host yang dikunjungi secara signifikan.

4. KESIMPULAN

Prototip model multiagent untuk deteksi penyusupan yang dikembangkan telah mempertimbangkan aspek adanya potensi intruder yang memanfaatkan kepergian mobile agent telah berhasil dikembangkan untuk menyediakan informasi deteksi penyusupan. Informasi yang mewakili aspek integritas dalam hal ini kasus mengenai celah port yang telah dibuka oleh intruder dan informasi yang mewakili aspek authentication dalam hal ini kasus mengenai adanya ilegal login. Terdapat satu agen statik yaitu agen master dan dua mobile agent: agen slave dan agenclone. Pemanfaatan teknik string matching digunakan proses analisis deteksi mobile agent slave yang telah dibangun dan mampu menjalankan tugas secarabaik dan benar dalam berinteraksi. Adapun kemampuan agen terdapat pada bab perancangan tentang kemampuan multiagen.berisi saran yang berupa rekomendasi akademik atau tindak lanjut nyata atas kesimpulan yang diperoleh.

DAFTAR PUSTAKA

Al Rajeh, N.A. and Loret, J.L., 2013, Intrusion Detection system Based on Artificial Intelligence Techniques in Wirelles Sensor Network, International Journal of Distributed Sensor Network, 1, 2013, 1-6

Anderson, J.P., 1980, Computer Security Threat Monitoring and Surveillance, Technical Report James P Anderson Co, Fort Washington

Apostolico, A and Galil, Z., 1997, Pattern Matching Algorithms, Oxford University Press, Uk

Asaka, M., Okazawa, S., Taguchi, A. and Goto, S., 1999, A Method of Tracing Intruders by use of mobile agents, Internet Society Conference, San Jose, June 1999

Bace, R. and Mell, P., 2001, Intrusion Detection System, National Institute of Standard and Technology, Scott Valley

Balasubramaniyan, J., Fernandez, J.O.G., Isacoff, D., Spafford, E.H. and Zamboni, D., 1998, An Architecture for Intrusion Detection system is Using Autonomous Agents, Technical Report no TR 98-05, Purdue University USA

Brahmi, I., Yahia, A. and Poncelet, P., 2011, A Snort-Based Mobile Agent For A Distributed Intrusion Detection System, Proceedings of 6th International Conference on Security and Cryptography, Seville Spain, 18 -21 July 2011

Deeter, K., Singh, K., Filipozzi, S. and Vuong, S., 2004, APHIDS: A A Mobile Agent-Based Programable Hybrid Intrusion Detection System, Proceedings of the International Workshop on Mobility Aware Technologies and Applications (MATA'04), Florianopolis Bresil, Month 2004

Denning, D., 1987, An Intrusion Detection Detection Model, IEEE Transactions on Software Engineering, 2, 13, 244-253

El mourabit, Y., Toumanari, A. and Zougagh, H., 2014, A Mobile Agent Approach for IDS in Mobile Ad Hoc Network, International Journal of Computer Science Issue (IJCSI), 1, 11, 148-152

Foukia, N., Hulaas, J. and Harm, J., 1999, Intrusion Detection With Mobile agents, Internet Society Conference (INET 2001), Stockholm Sweeden, June 2001

Fritzson, R., McKay, D. and McEntire, R., 1994, KQML as an Agent Communication Language, Conference on Information and Knowledge Management (CIKM'94), USA, November 1994

Ghorbani, A.A., 2010, Network Intrusion Detection and Prevention: Concepts and Techniques,Advances in Information Security, Springer Science + Business Media, Country

Hay, A., Daniel, B.C. and Bray, R., 2007, Log Analysis Using OSSEC, Syngress, Country

Jachak, K. and Barua, A., 2012, Distributed Intrusion Detection using Mobile Agent in Distributed System, Emerging Trend in Computer Science and Information Techonolgy, India, 18 Nov 2012