PENGOPTIMUMAN ALGORITMA PENGESANAN BATU LONCATAN DALAM SISTEM PENGESANAN PENCEROBOHAN

MOHD NIZAM BIN OMAR

Tesis ini dikemukakan
sebagai memenuhi syarat penganugerahan
ijazah Sarjana Sains (Sains Komputer)

Fakulti Sains Komputer dan Sistem Maklumat
Universiti Teknologi Malaysia

MAY 2005

Buat ayah dan ibu yang tercinta.....

Omar Bin Ahmad

Seliah Binti Mat Sap

Juga sumber insiperasiku...

Zurianawati Ibrahim

Serta ...

Keluarga tersayang

PENGHARGAAN

Alhamdulillah, syukur ke hadrat Allah SWT kerana dengan limpah dan kurniaNya, penulis dapat menyiapkan tesis untuk penyelidikan dengan tajuk Pengoptimuman Algoritma Pengesanan Batu Loncatan Dalam Sistem Pengesanan Pencerobohan. Setinggi-tinggi penghargaan buat PM Dr. Mohd Aizaini Maarof yang telah membimbing serta memberi tunjuk ajar sepanjang tempoh penyelidikan ini dijalankan Bantuan dan teguran membina yang diberikan sudah pasti memberi banyak manfaat kepada penulis. Penghargaan turut diberikan kepada Pn. Anazida Zainal yang turut banyak membimbing. Kepada Pn. Subariah Ibrahim juga ucapan terima kasih diucapkan.

Terima kasih juga turut diucapkan kepad Kementrian Sains, Teknologi dan Inovasi Malaysia yang memberikan sumbangan di dalam bentuk biasiswa sepanjang tempoh penyelidikan dilakukan.

Juga penghargaan tidak terhingga untuk pensyarah-pensyarah yang turut membantu dalam usaha memantapkan lagi penyelidikan yang dijalankan. Buat keluarga juga yang memberi sokongan dalam usaha penulis menghadapi penyelidikan ini. Juga tidak ketinggalan pemberi sumber inspirasi, Zurianawati Ibrahim. Tidak ketinggalan rakan-rakan seperjuangan yang membantu, juga individu yang terlibat secara langsung dan juga tidak langsung. Terima kasih diucapkan.

ABSTRAK

Pengesanan pencerobohan rangkaian dan penindakbalasan manual tanpa tindakan selanjutnya mendatangkan masalah yang dikenali sebagai jurang masa. Jurang masa adalah tempoh masa di antara pengesanan dan penindakbalasan. Penyelidikan terdahulu menggunakan pendekatan seperti agen pintar dan adaptasi Sistem Pengesanan Pencerobohan (IDS) untuk menyelesaikan masalah jurang masa. Walaubagaimanapun, penyelidikan terdahulu tidak mengambil perhatian aspek mekanisma penindakbalasan pencerobohan. Tujuan kajian ini adalah untuk mengoptimumkan algoritma batu loncatan, yang mana ianya sebahagian daripada mekanisma penindakbalasan pencerobohan. Di dalam penyelidikan ini, metodologi khas Atas-Bawah digunakan untuk mengoptimumkan algoritma batu loncatan. Ini dicapai dengan menganalisa lima algoritma batu loncatan, di mana setiap algoritma dibahagikan kepada tiga bahagian utama. Bahagian-bahagian tersebut adalah penawanan paket, pengenalpastian dan perbandingan. Di antara algoritma-algoritma ini, pendekatan terbaik yang menghasilkan masa pemprosesan minimum untuk setiap bahagian dibangunkan dan diuji sebagai algoritma batu loncatan yang lengkap. Keputusan daripada kedua-dua pendekatan yang dioptimumkan dan algoritma sedia ada dibandingkan. Hasil daripada perbandingan, algoritma dioptimumkan memberikan keputusan yang terbaik. Penemuan daripada penyelidikan ini mencadangkan jurang masa boleh dikurangkan melalui pengoptimuman algoritma batu loncatan.

ABSTRACT

Detection of a network intrusion and manual response without any further action does create a problem known as time gap. Time gap is duration between detection and response. Previous researches have used some approaches like intelligent agent and IDS adoption to solve time gap problem. However, they do not consider the aspect of intrusion response mechanism. The purpose of this study is to optimize the stepping stone algorithm, which is part of intrusion response mechanism. In this research, special Top-Down methodology has been used to optimize the stepping stone algorithm. It is achieved by analyzing five stepping stone algorithms, in which each algorithm is divided into three main parts. The parts are packet capture, identification and comparison. Among these algorithms, the best approach which produces minimum processing time from each main part has been deployed and tested as a complete stepping stone algorithm. The results from both the optimized approach and existing algorithm are compared. From this comparison, the optimized algorithm gives the best result. The finding of this research suggests that time gap can be reduced through the optimization of the stepping stone algorithm.

KANDUNGAN

SENARAI JADUAL

SENARAI RAJAH

SENARAI SIMBOL

C	-	Identiti Unik Sambungan
j	-	Nilai Awalan
k	-	Penambahan Nilai Awalan
kbps	-	Kilo Bait Per Saat
log	-	Logaritma
ms	-	Milisaat
mak	-	Maksimum
Mhz	-	Megahetz
MB	-	Mega Bait
Min	-	Minimum
OFF_1	-	Tempoh OFF Paket
t	-	Masa
T_g	-	Jurang Masa
T_d	-	Masa Mula Pengesanan
T_r	-	Jumlah Masa Untuk Penindakbalasan
p	-	Fungsi
s	-	Saat
s	-	Saiz Tetingkap
X	-	Nilai Identiti Unik Pertama
y	-	Parameter Kawalan

Y	-	Nilai Identiti Unik Kedua
Π	-	Pai
δ_t	-	Perbezaan
T_k	-	*Thumbprint*
∑	-	Jumlah

SENARAI SINGKATAN

API	Application Programming Interface
CERT	Computer Emergency Response Team
CIS	Caller Identification System
CITRA	Cooperative Intrusion Trace back and Response Architecture
CPU	Central Processing Unit
DDoS	Distributed Denial of Service
DES	Data Encryption Standard
DOS	Denial of Service
DIDS	Distributed Intrusion Detection System
IDS	Intrusion Detection System
IRS	Intrusion Response System
IPD	Inter-Packet Delay
IPSec	IP Security
IDIP	Intrusion Identification and Isolating Protocol
LAN	Local Area Network
MMS	Min/Max Sum Ratio
NIT	National Institute of Technology
NDP 1	Normalized Dot Product 1
NDP 2	Normalized Dot Product 2

NIDS	Network Intrusion Detection System
NIC	Network Interface Card
NLANR	National Laboratory for Applied Network Research
PC	Personal Computer
SSD	Stepping Stone Detection
SA	Security Association
SWT	Sleepy Watermark Tracing
STAT	Statistical Correlation
TCP	Transmission Control Protocol
WAN	Wide Area Network

SENARAI ISTILAH

Adapter	Adapter
Adaptive	Adaptasi
Anomaly	Kejanggalan
Attack	Serangan
Attacker Filtering	Penapisan Pencerobohan
Audit log	Log audit
Automatic response	Penindakbalasan automatik
Backbone Internet	Tulang belakang Internet
Bidirectional	Dua arah
Brute-force	Cuba-jaya
Circular	Berputar
Connection	Sambungan
Connection Chain	Rantaian Sambungan
Dot product	Produk Dot
Downstream	Aliran Ke Bawah
Encryption	Penyulitan
Enhanced Notification	Peningkatan Notifikasi
False positive	Salah positif
False negative	Salah negatif
Filter	Penapis
Firewall	Dinding Api

Flood	Limpahan
Header	Kepala
Heterogeneous	Pelbagai
High-level	Aras-tinggi
Host-based	Berasaskan-hos
Network-based	Berasaskan-rangkaian
Hop	Hop
Hop-by-hop	Hop demi hop
Inbound	Sempadan dalam
Intrusion Response	Penindakbalasan Pencerobohan
Kernel Buffer	Penimbal Kernel
Kernel-managed	Selengaraan-kernel
Manual response	Penindakbalasan manual
Misuse	Penyalahgunaan
Network Analyzer	Penganalisa Rangkaian
Network Tap	Tap rangkaian
Multivariate Statistics	Statistik Perlbagaivariati
Notification	Notifikasi
Only-seen-twice	Hanya-dilihat-dua-kali
Optimize	Optimum
Outbound	Sempadan luar
Overlay network	Rangkaian
Packet	Paket
Packet Marking	Penandaan Paket
Packet Stream	Aliran paket

Payload	Muatan
Port	Pot
Principal component analysis	Analisis Komponen Asas
Tracing	Penjejakan
Real-time	Masa nyata
Remote Login	Login jauh
Router	Penghala
Scalable	Mudah alih
Stepping stone	Batu loncatan
Signature	Tandatangan
Specification-based	Berasaskan-spesifikasi
System Administrator	Pentadbir Sistem
System call	Panggilan sistem
Taxonomy	Taxonomi
Tails	Ekor
Time gap	Jurang Masa
Timing-based	Berasaskan-masa
Trust model	Model kepercayaan
Unidirectional	Satu arah
Upstream	Aliran Ke Atas
User-level	Aras-pengguna
User Buffer	Penimbal Pengguna
Window	Tetingkap

SENARAI LAMPIRAN

BAB 1

PENGENALAN

1.1 Pengenalan

Kini, serangan siber menjadi semakin rumit. Laporan tahunan daripada Computer Emergency Response Team (CERT) menerangkan pertambahan bilangan insiden keselamatan komputer setiap tahun (CERT, 2002). Sistem Pengesanan Pencerobohan (IDS) disenaraikan sebagai salah satu daripada teknologi untuk menghalang serangan terhadap rangkaian selain daripada dinding api (*firewall*) dan Identifikasi sumber pencerobohan (*intrusion source identification*) (Furguson *et al.,* 1998). IDS boleh ditakrifkan sebagai sistem yang mencuba untuk mengidentifikasikan penggunaan yang tidak dibenarkan, keganjilan dan penyalahgunaan sistem komputer (Puketza *et al.*, 1996). Sistem Penindakbalasan Pencerobohan (IRS) pula menyediakan mekanisme penindakbalasan kepada IDS. Namun demikian, kebanyakan IRS bertindak balas terhadap serangan dengan hanya melalui penjanaan laporan atau amaran (Carver, 2001). Penyelidikan oleh (Cohen, 1999) mendapati bahawa kejayaan satu-satu serangan itu adalah bergantung kepada jurang masa (*time gap*) di antara pengesanan dan penindakbalasan. Secara ringkasnya, sekiranya penceroboh diberi masa tiga puluh jam, penceroboh telah berjaya sepenuhnya menceroboh.

Masalah jurang masa wujud di antara IDS dan IRS. Ini bermakna masalah jurang masa boleh diselesaikan sama ada menerusi IDS dan IRS. Untuk menyelesaikan masalah jurang masa ini, penyelidikan yang telah dilaksanakan oleh (Carver, 2000) yang memfokuskan kepada adaptasi (*adaptive*) IDS telah menumpukan ke arah usaha untuk menghasilkan IDS yang boleh diadaptasikan.

Melalui penyelidikan ini, sekiranya IDS berada di dalam keadaan sentiasa terkemas kini dan dapat pengesanan segala jenis pencerobohan, ini seterusnya akan dapat memastikan pengesanan dapat dilakukan dengan cepat. Sekiranya pengesanan dapat dilakukan dengan cepat, maka masalah jurang masa dapat diselesaikan. Walau bagaimanapun, pengesanan semata-mata tanpa tindak balas sewajarnya adalah tidak berfaedah. Apa yang diperlukan di sini adalah unsur tindak balas yang diakui oleh (Carver, 2001) adalah lebih penting dari IDS. Oleh yang demikian, untuk penyelidikan ini, pengurangan jurang masa menerusi IRS atau penindakbalasan dilaksanakan. Selain daripada IRS dilihat lebih penting daripada IDS, pengurangan jurang masa ke atas IRS dilihat akan memperlengkapkan lagi keseluruhan penyelidikan pengurangan jurang masa yang melibatkan IDS dan IRS.

Dengan ini, dapatlah diringkaskan bahawa penyelidikan ini akan menumpukan usaha untuk mengurangkan jurang masa di antara pengesanan dan penindakbalasan dengan memfokuskan penyelidikan ke arah penindakbalasan atau IRS.

Bagi memastikan usaha ke arah pengurangan jurang masa menerusi penindakbalasan berjaya dilaksanakan, salah satu teknik penindakbalasan telah dipilih. Ini adalah berdasarkan kepada kebaikan yang ada kepada teknik penjejakan berbanding dengan teknik-teknik penindakbalasan yang telah di senaraikan oleh (Carver, 2001). Secara umumnya, kaedah penindakbalasan penjejakan menawarkan penindakbalasan seterusnya setelah punca pencerobohan diketahui. Penjejakan pencerobohan diperlukan sebagai keperluan untuk membangunkan penindakbalasan segera (Dong-li, 2002).

Teknologi penjejakan boleh dibahagikan kepada dua kategori utama, Penjejakan IP dan Penjejakan Sambungan (Buchholz, 2002). Fokus akan diberikan ke arah Penjejakan Sambungan berikutan oleh penjejakan IP memerlukan penglibatan komponen perkakasan (selalunya penghala) (Tatsuya dan Shigeyuki, 2002) sebagai komponen utama dan ini adalah tidak bersesuaian dengan persekitaran penyelidikan yang akan dilakukan dan merupakan salah satu kekangan terhadap penyelidikan ini.

Daripada tinjauan ke atas teknik-teknik penjejakan sambungan (Snap, 1991), (Staniford-Chen dan Heberlein, 1995), (Zhang dan Paxon, 2000), (Yoda dan Etoh, 2000) dan (Schnackenberg dan Djahandari, 2000), teknik penjejakan berasaskan-rangkaian (*network-based tracing*) merupakan teknik yang menjadi pilihan penyelidikan berbanding dengan teknik penjejakan berasaskan-hos (*host-based*) dan penjejakan pasif lebih digunakan berbanding dengan pendekatan aktif (Wang *et al.*, 2001). Sehingga ke saat ini, penyelidikan penjejakan sambungan seperti (Yung, 2002) dan (Dohono *et al.*, 2002) masih tertumpu kepada teknik penjejakan sambungan berasaskan-rangkaian.

Keseluruhan teknik penjejakan sambungan berasaskan-rangkaian cuba untuk menyelesaikan masalah yang dikenali sebagai pengesanan batu loncatan. Batu loncatan merupakan kaedah yang digunakan oleh penceroboh untuk melindungi jejak pencerobohannya dengan cara mempergunakan hos atau perantara sebelum melakukan pencerobohan yang sebenar (Zhang dan Paxon, 2000). Ini dapat dilihat menerusi penyelidikan yang telah dilakukan oleh penyelidik-penyelidik seperti (Snap, 1991), (Staniford-Chen dan Heberlein, 1995), (Zhang dan Paxon, 2000), (Yoda dan Etoh, 2000) dan (Schnackenberg dan Djahandari, 2000). Di sebabkan oleh penyelidik-penyelidikan menunjukkan kepentingan kajian terhadap pengesanan batu loncatan, algoritma pengesanan batu loncatan ini diselidiki dengan mendalam. Hasil daripada penyelidikan terhadap algoritma ini kemudiannya dioptimumkan ke arah untuk menghasilkan algoritma pengesanan batu loncatan yang dapat mengesan batu loncatan dengan lebih pantas.

Oleh yang demikian, keseluruhan penyelidikan ini akan bertumpu kepada pengurangan jurang masa penindakbalasan dengan mengoptimumkan algoritma pengesanan batu loncatan.

1.2 Latar Belakang

Penyelidikan yang dilakukan oleh (Cohen, 1999) mendapati bahawa kejayaan sesuatu serangan itu bergantung kepada jurang masa di antara pengesanan dan penindakbalasan.

Daripada tinjauan yang telah dilakukan oleh (Carver, 2001) menerangkan IDS semasa mempunyai mekanisme yang terhad berbanding dengan ancaman semasa. Penindakbalasan masih lagi menggunakan proses manual dan ini dibuktikan akan menghasilkan jurang masa yang besar di antara pengesanan dan penindakbalasan (Cohen, 1999).

Walaupun penyelesaian terhadap permasalahan ini telah pun diselidiki oleh (Carver, 2001) melalui pendekatan pengesanannya, namun demikian penyelidikan yang dilakukan di dalam tesis memilih untuk menyelesaikan masalah ini menerusi pendekatan penindakbalasan. Ini adalah disebabkan oleh pendekatan penindakbalasan dilihat lebih baik daripada penyelesaian sebelumnya (pendekatan pengesanan). Penyelidikan difokuskan ke arah teknik penjejakan pencerobohan yang disenaraikan oleh (Carver, 2002) sebagai salah satu teknik penindakbalasan yang perlu diambil perhatian.

Teknik penjejakan yang di dalamnya terkandung pelbagai teknik diselidiki yang hasil daripada penyelidikan yang dilakukan mendapati bahawa teknik penjejakan berasaskan rangkaian adalah lebih sesuai untuk dikaji selanjutnya. Ini adalah berdasarkan penyelidikan seperti (Staniford-Chen dan Heberlein, 1995) (Zhang dan Paxon, 2000) dan (Yoda dan Etoh, 2000) serta beberapa penyelidikan terbaru seperti (Dohono *et al.,* 2002) dan (Wang *et al*, 2002) yang masih menumpukan usaha ke arah menyediakan teknik penjejakan yang lebih berkesan.

Keseluruhan teknik penjejakan berasaskan rangkaian ini memfokuskan kepada masalah untuk menyelesaikan masalah yang dikenali sebagai pengesanan batu loncatan. Algoritma untuk menyelesaikan masalah batu loncatan ini dikaji dan penyelidikan untuk mengoptimumkannya ke arah untuk menghasilkan satu algoritma yang lebih baik dijalankan.

1.3 Pernyataan Masalah

"Adakah dengan mengoptimumkan algoritma pengesanan batu loncatan dapat mengurangkan jurang masa di antara pengesanan dan penindakbalasan"

Masalah pengesanan batu loncatan difokuskan dan dinyatakan seperti berikut

Sambungan c_i adalah sambungan tunggal daripada hos komputer H_i (sumber) kepada H_{i+1} (destinasi). Pengguna mungkin log melalui jujukan hos-hos komputer H_1, H_2, H_3,..., H_{n+1} melalui Rantaian Sambungan c_1, c_2, c_3, ..., c_{n-1} di mana sambungan c_i adalah login jauh (*remote login*) daripada hos H_i hingga ke hos H_{i+1}.

Sekiranya diberi sambungan c_n,

"Bagaimanakah kaedah untuk menawan, mengenal pasti dan membandingkan sambungan-sambungan lain c_1, c_2, c_3, ..., c_{n-1} di dalam rantaian, dan sambungan manakah yang terlibat"

"Bagaimanakah pengoptimuman dapat dilakukan untuk menjadikan algoritma pendekatan pengesanan batu loncatan dapat dilakukan dengan lebih pantas"

"Bagaimanakah menentu-ukur masa yang digunakan untuk penjejakan pencerobohan sama ada masa sebelum pengoptimuman dan selepas pengoptimuman"

1.4 Tujuan

Tujuan utama penyelidikan ini adalah untuk pengoptimuman keseluruhan penindakbalasan (IRS) dengan cara mengoptimumkan algoritma pengesanan batu loncatan bagi mengurangkan jurang masa di antara pengesanan dan penindakbalasan (IDS).

1.5 Objektif

Berikut disenaraikan objektif untuk penyelidikan ini.

i. Untuk menyelidik pendekatan mengurangkan jurang masa penindakbalasan (IRS) dengan memfokuskan kepada pendekatan pengesanan batu loncatan.
ii. Untuk mengoptimumkan algoritma pengesanan batu loncatan.
iii. Untuk membandingkan algoritma pengesanan batu loncatan sedia ada dan algoritma yang telah dioptimumkan.

1.6 Skop

Berikut disenaraikan pula skop untuk penyelidikan ini.

i. Penyelidikan ini hanya terhad kepada pengoptimuman pendekatan penindakbalasan (atau lebih tepat lagi algoritma pengesanan batu loncatan) untuk menghasilkan satu pendekatan yang lebih optimum.
ii. Pengoptimuman algoritma pengesanan batu loncatan hanya melibatkan pengesanan di dalam satu-satu segmen Kawasan Rangkaian Setempat (LAN) yang memungkinkan pencerapan paket rangkaian dilakukan hanya melalui satu titik segmen itu sahaja.
iii. Data yang digunakan di dalam algoritma pengesanan batu loncatan hanyalah tertumpu pada paket TCP (atau lebih tepat lagi paket TELNET).
iv. Data yang digunakan adalah hasil daripada penjanaan skrip TELNET (Telnet Scripting Tools v1.0) menggunakan prasarana rangkaian sebenar. Ini adalah bagi memastikan data adalah sama dengan data sebenar rangkaian dan tetap untuk setiap pengujian yang dilakukan.
v. Pencerapan data masa dalam menentu-ukur algoritma sama ada optimum atau tidak bergantung kepada fungsi (*System.milisecond()*) dalaman bahasa pengaturcaraan java versi 1.4.1_04 (Java versi 2).

1.7 Andaian

Berikut adalah andaian yang telah diberikan untuk penyelidikan ini

i. Pengesanan batu loncatan terhad untuk mengenal pasti hos yang merupakan sumber kepada serangan. Pengenalpastian dan penentusahan pengguna sebenar hos adalah di luar bidang pengesanan. Pengesanan batu loncatan adalah terhad kepada penjejakan hos yang digunakan sahaja.

ii. Persekitaran LAN yang digunakan membolehkan pencerapan maklumat keseluruhan paket rangkaian dilakukan hanya pada satu titik di dalam rangkaian tersebut.

1.8 Kepentingan Kajian

Penyelidikan pengoptimuman algoritma pengesanan batu loncatan di dalam pendekatan penindakbalasan dilakukan bagi mengurangkan masa jurang masa penindakbalasan (IRS). Kejayaan mengurangkan jurang masa penindakbalasan bukan sahaja berjaya menyelesaikan sebahagian masalah jurang masa, namun berjaya juga melengkapkan pasangan penyelidikan sebelum ini yang mengurangkan jurang masa melalui pengesanan (IDS). Kejayaan mengurangkan jurang masa ini dilihat berfaedah dari segi untuk mengurangkan kadar peratusan pencerobohan selepas pengesanan oleh IDS. Penyelidikan ini dilihat berpotensi untuk diterapkan di dalam IDS sedia ada yang hanya berkeupayaan untuk mengesan pencerobohan sahaja. Pihak yang bertanggungjawab seperti Pentadbir Sistem atau Rangkaian kini boleh memastikan pencerobohan rangkaian tidak hanya dikesan tetapi diketahui sumbernya dan diberi penindakbalasan dengan lebih cepat dan efisien.

1.9 Hasil Jangkaan

Hasil jangkaan penyelidikan ini adalah berupa algoritma pengesanan batu loncatan yang lebih optimum berbanding dengan algoritma-algoritma pengesanan batu loncatan sedia ada. Melalui pengoptimuman algoritma ini, apabila diguna-pakai sebagai komponen di dalam penindakbalasan (IRS), akan mewujudkan penindakbalasan yang lebih baik dan ini seterusnya akan mencapai matlamat mengurangkan jurang masa di antara pengesanan dan penindakbalasan secara umumnya dan mengurangkan jurang masa penindakbalasan secara khususnya.

1.11 Organisasi Tesis

Penyelidikan ini membincangkan pengurangan jurang masa penindakbalasan melalui pengoptimuman algoritma pengesanan batu loncatan. Bab 1 memberikan pengenalan, latar belakang, pernyataan masalah, tujuan, objektif, kepentingan kajian, skop, andaian dan hasil jangkaan keseluruhan penyelidikan ini. Bab 2 pula menghuraikan kajian latar belakang yang telah dilakukan sepanjang tempoh penyelidikan dilakukan. Bab 3 menerangkan kerangka kerja Penyelidikan. Bab 4 membincangkan rekabentuk yang dilakukan di dalam penyelidikan ini. Bab 5 pula menerangkan implementasi yang dilakukan. Bab 6 membincangkan pengujian yang dilakukan di dalam penyelidikan ini. Bab 7 memberikan hasil, analisa dan keputusan yang diperlolehi daripada sesi pengujian yang dijalankan. Bab 8 menutup penyelidikan ini dengan membincangkan perihal sejauh mana penyelidikan ini mencapai objektifnya, sumbangan penyelidikan, kekurangan dan diakhiri dengan cadangan masa hadapan yang boleh dilakukan.

RUJUKAN

Adam, J., A. (1992). Data security-cryptography=privacy?. *Spectrum IEEE*. 29(8): 29-35.

Arbaugh, W., A. (2003). Firewall an outdated defence. *Computer.* 36(6): 112-113.

Baba, T., dan Matsuda., S. (2002). Tracing Network Attacks to Their Sources. *IEEE Internet Computing*. 6(2): 20-26.

Burroughs, D., J., Wilson, L., F., dan Cybenko, G., V. (2002) Analysis of Distributed Intrusion Detection Systems Using Bayesian Methods. *21st IEEE International Performance, Computing, and Communications Conference*. April 3-5. Phonenix, Arizona: IEEE, 329 - 334.

Calvert, K., L., Bhattacharjee, S., Zegura, E., dan Sterbenz, J. (1998). Direction in Active Networks. *IEEE Communication Magazine*. 36(10): 72-78.

Carver., A., C., Jr., Humphries., J., W., Pooch., U., W., dan Ragsdale., D., J. (2000). Adaptation Techniques for Intrusion Detection and Intrusion Response Systems. *IEEE International Conference on Systems, Man, and Cybernetics* .October 8-11. Nashville, TN: IEEE, 2344-2349.

Carver., A., C. (2000). A Methodology for Using Intelligent Agents to provide Automated Intrusion Response. *Proceedings of the 2000 IEEE Workshop on Information Assurance and Security*. June 6-7. United State Military Academy, West Point, NY: IEEE, 110-116.

Carver, C., A. dan Pooch U., W. (2000) An Intrusion Response Taxonomy and its Role in Automatic Intrusion Response. *Proceedings of the 2000 IEEE Workshop on Information Assurance and Security*. Jun 6-7. United States Military Academy, West Point, New York: IEEE, 110-116.

Carver., A., C. (2001). Limiting Uncertainty in Intrusion Response. *Proceedings of the 2001 IEEE Workshop on Information Assurance and Security.* June 5-6. United State Military Academy, West Point, NY: IEEE, 142-147.

Carver., C., A. (2002). Intrusion Response Systems: A Survey. Department of Computer Science, Texas A&M University, College Station, USA, TX77843-3112.

CERT, (1999). Result of the Distributed System Intruder Tools Workshop. Software Engineering Institute, Carnegie Mellon University. unpublished.

Cho, S. (2002). Incorporating Soft Computing Techniques Into a Probabilistic Intrusion Detection System. *IEEE Transactions On Systems, Man, and Cybernetics – Part C: Application and Reviews*. 32(2): 154-160.

Chang., H., Y., Narayan., R., Vetter., B., Wu., S., F., Brown., M., Wang., X., Yuill., J., Sargor., C., Gong., F., Jou., F. (1999). DecIdUouS: Decentralized Source Identification for Network-Based Intrusion. *In Proceeding of the 6th IFIP/IEEE International Symposium on Integrated Network Management.* May 24-28. Boston, Mass., USA: IFIP/IEEE, 701-714.

Cohen., F. (1999). *Simulating Cyber Attacks, Defenses, and Consequences*. Fred Cohen & Associates*,* Feature Article.

Cunningham, R., K., Lippmann, R., P., dan Webster, S., E. (2001). Detecting and Displaying Novel Computer Attacks with Macroscope. *IEEE Transaction On Systems, Man, and Cybernetics – Part A: Systems And Humans,* 31(4): 275-281.

Degionni, L. (2000). *Development of an Architecture for Packet Capture and Network Traffic Analysis.* Politecnico Di Torino: Tesis Ph.D.

Degioanni, L., Baldi, M., Risso, F., dan Varenni, G. (2003) Profiling and Optimization of Software-Based Network-Analysis Applications. *Proceeding of the 15th Symposium on Computer Architecture and High Performance Computing.* November 10-12. Sao Paulo, Brazil: IEEE, 226-234.

Dohono., D., L., Flesia., A., G., Shankar., U., Paxson., V., Coit., J., Staniford., S. (2002). Multiscale Stepping-Stone Detection: Detecting Pairs of Jittered Interactive Streams by Exploiting Maximum Tolerable Delay. *Fifth International Symposium of Recent Advance in Intrusion Detection.* October 16-18. Zurich, Switzerland: Springer, 1-15.

Dong-li, S. (2002). *Trend & Technique of Intruder Traceback*. ITU-T Workshop on Security. May 13-14. Seoul, Korea: ERTI, 1-14.

Eng, P., E., dan Haug, M. (2004). *Automatic Response to Intrusion Detection*, Agder University College: Tesis Masters.

Forouzan., B., A. (2000). Data Communication and Networking. Education, North America: McGraw-Hill Higher

Foundation, Inc. (2000). *Managed Security Service*. 2 Venture Street, Suite 100, Irvine, CA 92618.

Fulvio, R. dan Loris D. (2001), An Architecture for High Performance Network Analysis, *Proceedings of the 6th IEEE Symposium on Computers and Communications.* July 3-5. Hammamet, Tunisia: IEEE, 686-693.

Furguson, P., dan Senie, D. (1998). *Network Ingress Filtering: Defeating Denial of Service Attack which employ IP Source Address Spoofing. Internet Engineering Task Force*, RFC 2267.

Jang., H. dan Kim., S. (2000). A Self-Extension Monitoring for Security Management. *Computer Security Applications 16th Annual Conference 2000.* December 11-15. New Orleans, Louisiana: ACSAC, 196-203.

Jason., W., P. (2000). *Mobile Agent Technology for Intrusion Detection and Response Systems*. Class Presentation, Department of Computer Science and Statistics University of Southern Mississippi. unpublished.

Jensen., W., Karygiannis., T., Mell., P., Marks., D. (1999). Applying Mobile Agents to Intrusion Detection and Response. National Institute of Standards and Technology – A Computer Security Division. Technical Report.

Kemmerer, R., A., dan Vigna, G. (2002) Intrusion Detection: A Brief History and Overview. *SECURITY & PRIVACY-2002*. 35(4): 27-30.

Kent, S. (2000). On the trail of intrusions into information systems. *IEEE Spectrum*. 37(12): 52-56.

Kulin, A. (2000). *A distributed security management system based on mobile agents*. Technical University of Vienna: Tesis Master.

Leckie, T., dan Yasinsac, A. (2004). Metadata for Anomaly-Based Security Protocol Attack Deduction. *IEEE Transaction On Knowledge And Data Engineering*, 16(9): 1157-1167.

Matsuda., S., Baba., T., Hayakawa., A., Nakamura., T. (2002). Design and Implementation of Unauthorized Access Tracing System. *Proceedings of the 2002 Symposium on Applications and the Internet.* January 28-Febuary 1. Nara City, Japan: IEEE, 74-81.

McCanne, S., dan Jacobson, V. (1992). The BSD Packet Filter: A New Architecture for User-level Packet Capture. *1993 Winter USENIX conference.* January 25-29. San Diego, CA: USENIX, 259-270.

Mishra, A., Nadkarni, K., dan Patcha, A. (2004) Intrusion detection in wireless ad hoc networks, *IEEE Wireless Communication.* 11(1): 48-60.

MuseMagic. (1999). MuseMagic Engineering, *An overview of optimization techniques*. United State of America, DSPworld.

Ohta., K., Mansfield., G., Takei., Y., Nemoto., Y. (2000). Detection, defence, and tracing of Internet wide illegal access in distributed manner. *In Proceeding of INET 2000*. July 18-21. Yokohama, Japan: INET, 412-420.

Park., K.dan Lee., H. (2000). *On the Effectiveness of Probabilistic Packet Marking for IP Traceback under Denial of Service Attack.* Technical Report, Purdue University¸ CSD-TR 00-013.

Paxson, V. (1999). Bro: A System for Detecting Network Intruders in Real-Time, *Computer Network.* 31(23-24): 2435-2463.

Petkac, M., dan Badger, L. (2000). Security Agility in Response to Intrusion Detection. *16th Annual Computer Security Applications Conference* December 11-15. New Orleans, Louisiana: IEEE, 11-20.

Puketza., N., J., Zhang., K., Chung., M., Mukherjee., B., dan Olsson., R., A. (1996), A Methodology for Testing Intrusion Detection Systems. *IEEE Transactions On Software Engineering.* 22(10): 719-729.

Potlapally, N., R., Ravi, S., Raghunathan, A. (2002). Optimizing Public-Key Encryption for Wireless Clients. *IEEE International Conference on Communication.* April 28-May 2. Singapore: IEEE, 1050-1056.

Rankin, A. dan Liber, S. (2004). *An Assessment of Autonomic Intrusion Detection Analysis and Response Methods in Strategic Network Defense*. unpublished.

Schnackenberg, D., dan Djahandari, K. (2002). *Cooperative Intrusion Traceback and Response Architecture (CITRA)*. San Diego, California, #02-008.

Schnackenberg, D., dan Djahandari, K. (2000). Infrastructure for Intrusion Detection and Response. *Proceeding of the DARPA Information Survivability Conference and Exposition 2000*. January 25-17. Hilton Head. S.C: IEEE, 1003-1011.

Savege., S., Wetherall., D., Karlin., A., Aderson., T. (2000). Practical Network Support for IP Traceback. *In Proceeding of the 2000 ACM SIGCOMM Conference.* August 28-September 1. Stockholm, Sweeden: ACM, 295-306.

Snap., S. (1991). DIDS (Distributed Intrusion Detection System) – Motivation, Architecture and Early Prototype. *In Proceeding of 14th National Computer Security Conference.* October 14. Washington, USA: ACM, 167-176.

Song., D., X. dan Perrig., A. (2000). *Advance and Authenticated Marking Schemes for IP Traceback*. Technical Report, University of California at Berkeley, UCB/CSD-00-1107.

Spatscheck, O., Hansen, J., S., Hartman, J., H. dan Peterson, L., L. (2000). Optimizing TCP Forwarder Performance, *IEEE/ACM Transaction On Networking*. 8(2): 146-157.

Staniford-Chen., S. dan Heberlein., L., T. (1995). Holding Intruders Accountable on the Internet. *In Proceeding of IEEE Symposium on Security and Privacy.* May 8-10. Oakland, CA: IEEE, 39-49.

Stone., R. (2000). CenterTrack: An IP Overlay Network for Tracking Dos Floods. *In Proceeding of the 9th USENIX Security Symposium.* August 14-17. Denver, Colorado: USENIX, 199-212.

Tatsuya., B. dan Shigeyuki., M. (2002). Tracing Network Attacks to Their Source. *IEEE Internet Computing Journal,* 6(2): 20-26.

Wang, X., Reeves, D., S., dan Wu, S., F. (2001). Tracing Based Active Intrusion Response. *Journal of Information Warefare.* 1(1): 50-61.

Wang, X., Reeves, D., S., dan Wu, S., F. (2002). Inter-Packet Delay Based Correlation for Tracing Encrypted Connection Through Stepping Stones. *7th European Symposium on Research in Computer Security*. October 14-16. Zurich, Switzerland: Springer, 244-263.

Watson, D., Smart, M., dan Jahanian, F. (2004). Protocol Scrubbling: Network Security Through Transparent Flow Modification. *IEEE/ACM Transaction On Networking*. 12(2): 261-273.

Wu, Y., Foo, B., Matheny, B., Olsen, T., Bagchi, S. (2004). *ADEPTS: Adaptive Intrusion Containment and Response using Attack Graphs in an E-Commerce Environment*. School of Electrical & Computer Engineering, Purdue. No 2003-33.

Yoda., K. dan Etoh., H. (2000). Finding a Connection Chain for Tracing Intruders. *6th European Sympsium on Research in Computer Security.* October 4-6. Toulouse, France: CEPIS, 191-205.

Yung., K., H. (2002). Detecting Long Connection Chains of Interactive Terminal Sessions. *Fifth International Symposium on Recent Advance in Intrusion Detection.* October 16-18. Zurich, Switzerland: Springer, 1-16.

Zhang., Y. dan Paxon., V. (2000). Detecting Stepping Stones. *In Proceedings of 9th USENIX Security Symposium*. August 14-17. Denver, Colorado: USENIX, 171-184.

BIBLIOGRAFI

Analyzer (2004). http://analyzer.polito.it/

Burks.

(2004).http://burks.brighton.ac.uk/burks/language/modula2/adps/ch2/ch23.htm

Bellovin., S., Leech., M., Taylor., T. (2001). *ICMP Traceback Message*. Internet draft, draft-ietf-itrace-02. unpublished.

CERT. (2004), http://www.cert.org/stats/cert_stats.html

Cerebro. (2004). http://cerebro.cs.xu.edu/~smbelcas/howto.html

Darvinmag (2004).

http://www.darwinmag.com/learn/curve/column.html?ArticleID=115

Digital Equipment Corporation (1992). *packetfilter(4).* Ultrix V4.1 Manual.

Ethereal. (2004). http://www.ethereal.com/

Footfall. (2004). http://footfall.csc.ncsu.edu

Flyzip. (2004) http://www.fly-zip.com/page.php?m1=Technology&m2=Technology

Huagang, X. (2000). *LIDS Hacking HOWTO. Document for LIDS*, v1.0.

Information-technology Promotion Agency. (2004).

http://www.ipa.go.jp/about/english/index.html

Libpcap. (2002). http://sourceforge.net/projects/libpcap/

Netiq. (2002). http://www.netiq.com/products/chr/default.asp

PCAUSA. (2000). http://www.rawether.net

Snort. (2004). http://www.snort.org

Sun Microsystem Inc. (1990). *SUN MICROSYSTEM INC. NIT(P4), SunOS, 4.1.1.1, Reference Manual*, Mountain View. CA, 800-5480.

Tcpdump. (2004). http://www.tcpdump.org/

Tfgen. (2004). http://www.st.rim.or.jp/~yumo/pub/tfgen.html

Webopedia. (2004). http://www.webopedia.com

Webster. (2004). http://www.webster-dictionary.org/definition/algorithm

Wikipedia. (2004a). http://en.wikipedia.org/wiki/Algorithm

Wikipedia. (2004b). http://en.wikipedia.org/wiki/Optimization_(computer_science)

Windump. (2004). http://windump.polito.it/

WinPcap. (2004). http://winpcap.polito.it/