Distribusi Intrusion Detection System *Rules* Dengan Menggunakan Algoritma RSA pada *Cloud* Computing

SKRIPSI

Diajukan untuk Memenuhi Sebagian dari Syarat untuk Memperoleh Gelar Sarjana Komputer Program Studi Ilmu Komputer

Oleh

Zakka Muhammad Shiddiq

1405201

PROGRAM STUDI ILMU KOMPUTER

FAKULTAS PENDIDIKAN MATEMATIKA DAN ILMU PENGETAHUAN ALAM

UNIVERSITAS PENDIDIKAN INDONESIA

BANDUNG

2018

DISTRIBUSI INTRUSION DETECTION SYSTEM RULES MENGGUNAKAN ALGORITMA RSA PADA CLOUD COMPUTING

Oleh
Zakka Muhammad Shiddiq

Sebuah skripsi yang diajukan untuk memenuhi salah satu syarat memperoleh gelar Sarjana Pendidikan pada Fakultas Pendidikan Bahasa dan Seni

Zakka Muhammad Shiddiq

1405201

DISTRIBUSI INTRUSION DETECTION SYSTEM *RULES* DENGAN MENGGUNAKAN ALGORITMA RSA PADA *CLOUD* COMPUTING

DISETUJUI DAN DISAHKAN OLEH PEMBIMBING:

Pembimbing I,

Rizky Rachman Judhie Putra, M.Kom.

NIP. 197711252006041002

Pembimbing II,

Wahyudin, MT.

NIP : 197304242008121001

Mengetahui,

Ketua Departemen Pendidikan Ilmu Komputer

Prof. Dr. H. Munir, M.IT.

NIP. 196603252001121001

DISTRIBUSI INTRUSION DETECTION SYSTEM *RULES* MENGGUNAKAN ALGORITMA RSA PADA *CLOUD* COMPUTING

ABSTRAK

Pada penelitian sebelumnya telah dilakukan perubahan log honeypot menjadi rules Intrusion Detection System (IDS). Pada penelitian ini, dilakukan pengembangan lebih lanjut pada rules IDS tersebut. Rules IDS yang telah diubah kemudian didistribusikan dan diaplikasikan ke dalam lingkungan cloud computing. Pada proses pendistribusian, algoritma RSA diaplikasikan untuk melakukan verifikasi keaslian dari rules yang didistribusikan. Selain itu, pada penelitian ini algoritma BFS digunakan untuk mempercepat proses pendistribusian rules pada Virtual Machine di dalam cloud. Hasil dari penelitian ini menunjukkan bahwa RSA layak digunakan sebagai algortima verifikasi rules. Penelitian ini juga membuktikan bahwa penggunaan algoritma BFS dapat mempercepat proses distribusi rules.

Kata Kunci: *Rivest-Shamir-Adleman, SHA-256 Digital signature, Breadth first search, Cloud computing*

DISTRIBUTION OF INTRUSION DETECTION SYSTEM RULES USING RSA ALGORITHM ON *CLOUD* COMPUTING

ABSTRACT

On previous research, honeypot logs were converted into Intrusion Detection System (IDS) rules. On this research that matters were developed further more. IDS rules that were converted, then distributed and aplicated into cloud computing environment. At the distribution process, RSA algorithms were used for verificating the authenticity of the rules that was distributed. Other than RSA, this research were using Breadth First Search (BFS) to speed up the distribution process. This research proves that RSA algorithm can be used as rules verificator. This research also proves that BFS algorithm are able to speed up the distribution process.

Keyword: *Rivest-Shamir-Adleman, SHA-256 Digital signature, Breadth first search, Cloud computing*

KATA PENGANTAR

Puji dan syukur penulis panjatkan kehadirat Allah swt. karena hanya dengan kehendak, berkat, serta karunia-Nya lah penulis dapat menyelesaikan skripsi yang berjudul "Distribusi Intrusion Detection System Rules Dengan Menggunakan Algoritma RSA pada Cloud Computing" ini dapat terselesaikan.

Penyusunan skripsi ini ditunjukan untuk memenuhi dan melengkapi salah satu syarat untuk penyusunan skripsi yang merupakan syarat untuk mendapatkan gelar sarjana komputer atas jenjang studi S1 pada Program Studi Ilmu Komputer Fakultas Pendidikan Matematika dan Ilmu Pengetahuan Alam Universitas Pendidikan Indonesia.

Penulis menyadari bahwa dalam penyusunan proposal ini masih terdapat banyak kekurangan dan keterbatasan yang perlu disempurnakan. Oleh karena itu, penulis sangat mengharapkan saran maupun kritik yang membangun agar tidak terjadi kesalahan yang sama dikemudian hari dan dapat meningkatkan kualitas ke tahap lebih baik.

Bandung, Januari 2018

Penulis

UCAPAN TERIMA KASIH

Alhamdulillahhirabilalamin, puji dan syukur kehadirat Allah SWT. Yang telah melimpahkan rahmat dan hidayah-Nya sehingga penulis diberikan kelancaran dalam menyelesaikan penulisan skripsi ini. Dalam proses menyelesaikan penelitian dan penyusunan skripsi ini, peneliti banyak mendapat bimbingan, dorongan, serta bantuan dari berbagai pihak. Oleh karena itu, pada kesempatan ini peneliti mengucapkan terimakasih serta penghargaan yang setinggi-tingginya, kepada:

1. Kedua orang tua serta kakak dan adik penulis yang tanpa henti-hentinya memberikan doa dan dukungan, baik itu dukungan moral, materil maupun spiritual sehingga dapat memotivasi penulis dalam menyelesaikan skripsi ini.
2. Bapak Rizky Rachman Judhie Putra, M.Kom selaku pembimbing I atas segala waktu yang dicurahkan untuk membimbing penulis demi terselesaikannya skripsi ini.
3. Bapak Wahyudin, M.T., selaku pembimbing II yang telah memberikan saran kepada penulis selama proses penyelesaian penelitian dan penulisan skripsi.
4. Bapak Prof. Dr. H. Munir, M.IT., selaku Kepala Departemen Pendidikan Ilmu Komputer FPMIPA Universitas Pendidikan Indonesia.
5. Bapak Eddy Prasetyo Nugroho, M.T., selaku Ketua Program Studi Ilmu Komputer.
6. Bapak Eki Nugraha, M.Kom., selaku dosen pembimbing akademik yang telah memberikan arahan juga bimbingan selama penulis menjalani perkuliahan.
7. Bapak dan Ibu Dosen Prodi Pendidikan Ilmu Komputer dan Ilmu Komputer yang telah berbagi ilmu yang sangat bermanfaat kepada penulis.
8. Chintia Kulsum yang selalu memberikan segala dukungan untuk penulis dalam menjalani hidup, perkuliahan serta proses penulisan skripsi ini.
9. Sahabat selama di UPI Fikry, Ridwan, Zulfikar, Reinaldy, Fidela, Faisal, Eagan, Agung yang senantiasa memberikan dukungan, semangat, canda dan tawa kepada penulis baik selama proses perkuliahan maupun selama proses pengerjaan skripsi ini.

Bandung, Januari 2018

Zakka Muhammad Shiddiq

DAFTAR ISI

KATA PENGANTAR vi
BAB I PENDAHULUAN 1
1.1 Latar Belakang 1
1.2 Rumusan Masalah 5
1.3 Tujuan Penelitian 5
1.4 Manfaat Penelitian 5
1.5 Batasan Masalah 5
1.6 Sistematika Penulisan 6
2 BAB II KAJIAN PUSTAKA 7
2.1 *Cloud* Computing 7
2.1.1 Karakteristik *Cloud* Computing 9
2.1.2 *Service Models Cloud computing* 10
2.1.3 *Deployment Models Cloud Computing* 11
2.2 *Honeypot* 11
2.3 Router 13
2.4 IP Address 13
2.5 Kriptografi 13
2.5.1 Hash 16
2.5.2 SHA-256 18
2.5.3 *Digital signature* 18
2.5.4 RSA 19
2.6 Intrusion Detection System 19
2.6.1 Snort 20
2.6.2 Snort *rules* 21
2.7 Breadth First Search 22
2.8 Man In The Middle 23
3 BAB III METODO*LOG*I PENELITIAN 25
3.1 Desain Penelitian 25

3.1.1 Identifikasi masalah 26
3.1.2 Studi literatur 27
3.1.3 Penelitian 28
3.1.4 Pengujian 32
3.1.5 Analisis hasil penelitian 34
3.1.6 Penarikan kesimpulan 34
3.2 Alat Penelitian 34
4 BAB IV HASIL PENELITIAN DAN PEMBAHASAN 36
4.1 Pembahasan Distribusi *Rules* Menggunakan Algoritma RSA dan Algoritma BFS 36
4.2 Implementasi Algoritma RSA 37
4.2.1 Hashing *rules* dengan SHA-256 37
4.2.2 Pembuatan Public dan *Private key* 38
4.2.3 Pembuatan *Digital signature* 38
4.2.4 Verifikasi *Digital signature* 39
4.3 Implementasi Algoritma BFS 40
4.4 Pembuatan rules IDS dari *log* honeypot 41
4.5 Pengujian Perangkat Lunak 42
4.5.1 Pengujian *rules* baru dengan melakukan verifikasi kelayakan *rules* menggunakan snort dan penyerangan menggunakan nmap 43
4.5.2 Pengujian verifikasi *digital signature* 47
4.5.3 Pengujian kecepatan penggunaan algoritma BFS 53
4.5.4 Pengujian dengan menggunakan penyerangan *Man-In-The-Middle* 56
4.6 Pembahasan hasil penelitian 60
5 BAB V KESIMPULAN DAN SARAN 63
5.1 Kesimpulan 63
5.2 Saran 63
6 DAFTAR PUSTAKA 64

DAFTAR GAMBAR

Gambar 2.1 NIST Visual Model of *Cloud* Computing Definition (Security Guidance For Critical Areas Of Focus In *Cloud* Computing V3.0, 2011). 9
Gambar 2.2 Proses enkripsi (Piper, 1997) 15
Gambar 2.3 Proses hashing 16
Gambar 2.4 Perubahan pada input yang menghasilkan digest yang sangat berbeda 17
Gambar 2.5 ilustrasi perputaran sha-256 (Sanadhya, 2008) 18
Gambar 2.6 *Rules* pada snort 21
Gambar 2.7 proses penjelajahan tree oleh BFS (Rahim, 2018) 23
Gambar 3.1 Desain penelitian 25
Gambar 3.2 Insiden serangan XSS terhadap OSN (gupta, 2016). 26
Gambar 3.3 RSA 27
Gambar 3.3.4 Model Linear *Sequential Model* (Pressman, 2001) 28
Gambar 3.5 Desain perangkat lunak 31
Gambar 4.1 ilustrasi proses kerja aplikasi 36
Gambar 4.2 Proses hashing sha-256 38
Gambar 4.3 Pembuatan kunci 38
Gambar 4.4 pembuatan *digital signature* dan verifikasi *digital signature*. 39
Gambar 4.5 pembagian file menggunakan BFS 40
Gambar 4.6 pembuatan rules dari *log* 41
Gambar 4.7 Struktur VM 42
Gambar 4.8 Pemeriksaan konfigurasi 44
Gambar 4.9 *alert* snort 46
Gambar 4.10 *Rules* asli 47
Gambar 4.11 Public key asli 48
Gambar 4.12 *Digital signature* asli 48
Gambar 4.13 Verifikasi *digital signature* 49
Gambar 4.14 *Digital signature* modifikasi 49
Gambar 4.15 Hasil modifikasi pada *digital signature* yang dimodifikasi 50
Gambar 4.16 *Rules* modifikasi 51
Gambar 4.17 Hasil verifikasi *rules* yang dimodifikasi 51
Gambar 4.18 Public key modifikasi 52
Gambar 4.19 Hasil verifikasi public key yang dumodifikasi 52
Gambar 4.20 *Man-In-The-Middle* 57
Gambar 4.21 Pengiriman *rules* 57
Gambar 4.22 file yang diterima MITM 58
Gambar 4.23 *rules* sebelum dimodifikasi 58
Gambar 4.24 *rules* setelah dimodifikasi 59
Gambar 4.25 pengiriman file oleh MITM 59
Gambar 4.26 Verifikasi file dari MITM 60

DAFTAR TABEL

Tabel 4.1 Flag snort..... 44
Tabel 4.2 Perintah pada nmap..... 45
Tabel 4.3 uji coba *digital signature*, plain *text* dan public key..... 53
Tabel 4.4 hasil perbandingan kecepatan 54
Tabel 4.5 Perbandingan kecepatan cluster A 55
Tabel 4.6 Perbandingan kecepata pada *cluster* B..... 55
Tabel 4.7 Perbandingan kecepatan pada *cluster* C..... 56

DAFTAR PUSTAKA

P. Mell and T. Grance, “The NIST Definition of *Cloud* Computing,” National Institute of Standards and Techno*log*y Draft (NIST) Special Publication 800-145, 2011

“Security guidance for critical areas of focus,” *Cloud* Security Alliance (CSA), 2011.

N. Ahmad, "*Cloud computing*: Techno*log*y, security issues and solutions," 2017 2nd International Conference on Anti-Cyber Crimes (ICACC), Abha, 2017, pp. 30-35.

H. Orman, “Both Sides Now: Thinking about *Cloud* Security,” IEEE Internet Comput., vol. 20, no. 1, pp. 83–87, 2016.

S. Campbell and M. Jeronim, “An Introduction to Virtualization,” 2006.

S.J.Vaughan-Nichol, “Virtualization Sparks Security Concerns,”Computer, vol.41, no.8,13-15, Auguest 2008.

Gao Xiaopeng, Wang Sumei and Chen Xianqin, "VNSS: A network security sandbox for virtual computing environment," 2010 IEEE Youth Conference on Information, Computing and Telecommunications, Beijing, 2010, pp. 395-398.

M. S. Dildar, N. Khan, J. B. Abdullah and A. S. Khan, "Effective way to defend the hypervisor attacks in *cloud computing*," 2017 2nd International Conference on Anti-Cyber Crimes (ICACC), Abha, 2017, pp. 154-159.

Provos, Niels. "A Virtual *Honeypot* Framework." USENIX Security Symposium. Vol. 173. 2004.

MELL, Peter, et al. The NIST definition of *cloud computing*. 2011.

S. Roschke, F. Cheng and C. Meinel, "Intrusion Detection in the *Cloud*," 2009 Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing, Chengdu, 2009, pp. 729-734.

29

Garcia-Teodoro, Pedro, et al. "Anomaly-based network intrusion detection: Techniques, systems and challenges." computers & security 28.1 (2009): 18-28.

Grønland, Vidar Ajaxon. Building IDS *rules* by means of a *honeypot*. MS thesis. 2006.

Standard, Secure Hash. "The Cryptographic Hash Algorithm Family: Revision of the Secure Hash Standard and Ongoing Competition for New Hash Algorithms." (2009).

Ariyus, D. (2008). pengantar ilmu kriptografi: teori analisis & implementasi. Penerbit Andi.

M. I. Aziz and S. Akbar, "Introduction to Cryptography," 2005 International Conference on Microelectronics, 2005, pp. 144-147.

Fred Piper, Introduction to crypto*log*y, Information Security Technical Report, Volume 2, Issue 2, 1997, Pages 10-13.

Katz, Jonathan, and Yehuda Lindell. Introduction to modern cryptography. CRC press, 2014.

Yaksic, Vladimir Omar Calderón. "A study on hash functions for cryptography." Global Information Assurance Certification Paper, SANS Institute (2003).

Sobti, Rajeev, and G. Geetha. "Cryptographic hash functions: a review." IJCSI International Journal of Computer Science Issues 9.2 (2012): 461-479.

Roesch, Martin. "Snort: Lightweight intrusion detection for networks." Lisa. Vol. 99. No. 1. 1999.

Snort user manual 2.9.11, [online] Available: www.Snort.org.

Dahal, Ram Krishna, Jagdish Bhatta, and Tanka Nath Dhamala. "Performance Analysis of SHA-2 and SHA-3 finalists." The International Journal on Cryptography and Information Security 3.3 (2013): 1-10.

Dobraunig, Christoph, Maria Eichlseder, and Florian Mendel. "Analysis of SHA512/224 and SHA-512/256." International Conference on the Theory and Application of Crypto*log*y and Information Security. Springer Berlin Heidelberg, 2014

Provos, Niels, and Thorsten Holz. "Virtual *honeypot*s: from botnet tracking to intrusion detection." (2007).

Srivastava, A., et al. "A recent survey on DDoS attacks and defense mechanisms." *Advances in Parallel Distributed Computing*. Springer, Berlin, Heidelberg, 2011. 570-580.

Rahim, Robbi, et al. "Breadth First Search Approach for Shortest Path Solution in Cartesian Area." *Journal of Physics: Conference Series*. Vol. 1019. No. 1. IOP Publishing, 2018.

Sanadhya, Somitra Kumar, and Palash Sarkar. "Attacking reduced round SHA-256." *International Conference on Applied Cryptography and Network Security*. Springer, Berlin, Heidelberg, 2008.

Stinson, Douglas R. *Cryptography: theory and practice*. CRC press, 2005.

Pressman, R. S. (2001). *Software Enginering A Practitioner's Approach*. (B. Jones & E. Gray, Eds.) (FIFTH EDIT). Palgrave Macmillan.

Preetha, M., and M. Nithya. "A study and Performance Analysis of RSA Algorithm." *IJCSMC* 2 (2013): 126-139.

Gupta, Shashank, and Brij Bhooshan Gupta. "XSS-secure as a service for the platforms of online social network-based multimedia web applications in cloud." *Multimedia Tools and Applications* 77.4 (2018): 4829-4861.