Ringkasan Artikel Ilmiah

Oleh : Prastudy Mungkas Fauzi
Kelompok : 168

Judul Artikel : *The Value of Intrusion Detection Systems in Information Technology Architecture*
Sumber : Information Systems Research (Vol. 16 No.1, Maret 2005)
Penulis : H. Chavusoglu, B. Mishra, S. Raghunathan

Masalah keamanan sistem adalah isu yang sangat penting saat ini, ditandai dengan makin meningkatnya anggaran yang dimiliki perusahaan-perusahaan untuk bidang keamanan teknologi informasi (TI). Secara umum, ada dua mekanisme untuk menghadapi masalah keamanan:

a. *Preventive* : mengembangkan perisai pertahanan di sekitar sebuah sistem TI, untuk melindungi dari *intrusion* (serangan).
b. *Detective* : mencoba mendeteksi *intrusion* yang telah terjadi.

Intrusion Detection Systems (IDS) adalah sistem yang dapat memberikan peringatan tentang perilaku yang dicurigai sebagai *intrusion*. IDS mempunyai beberapa kekurangan, yaitu mungkin terjadi 2 jenis kesalahan:

a. *False Positive Errors* : memberikan peringatan saat tidak terjadi *intrusion*
b. *False Negative Errors*: tidak memberikan peringatan saat terjadi *intrusion*

Bila dimisalkan
P_D = P(diklasifikasi sebagai *hacker*| pengguna seorang *hacker*)
P_F = P(diklasifikasi sebagai *hacker*| pengguna adalah pengguna biasa)
Maka probabilitas *false positive* = 1 - $P_{D,}$ dan probabilitas *false negative* = P_F

Tujuan

Artikel ini mencoba membahas dua masalah, yaitu:

1. Apakah IDS memberikan nilai kegunaan, dan dalam kondisi apa hal itu terjadi.
2. Efek dari konfigurasi terhadap nilai kegunaan yang diberikan IDS.

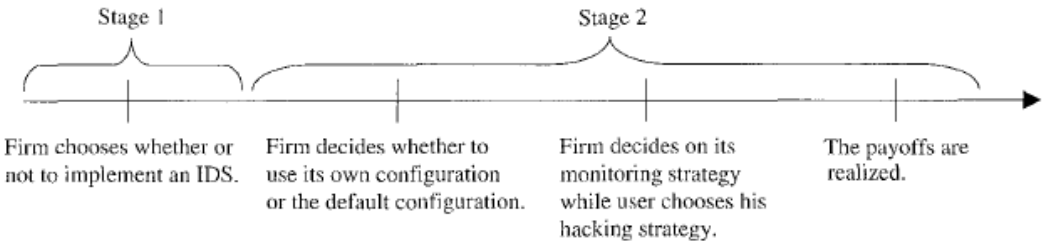
Model Penelitian

Ada 3 komponen utama dalam model ini, yaitu :

1. Pengguna sistem
2. Perusahaan
3. IDS

Dalam model ini, *intrusion detection* dikaitkan dengan *game theory* – permasalahan digambarkan sebagai sebuah permainan antara sebuah perusahaan yang mencoba memberikan pengamanan terhadap sistem, dan pengguna yang mencoba masuk ke dalam sistem perusahaan. Hal ini dapat dilihat pada gambar berikut:

The Timeline for the Game



ISR Vol. 16 No.1, Maret 2005, hal. 34
Figure 3

Tujuan dari perusahaan adalah meminimalkan perkiraan kerugian dari *intrusion*, sedangkan tujuan pengguna adalah memaksimalkan perkiraan keuntungan yang didapatkan.
Perusahaan bisa memilih :

- menggunakan IDS
- tanpa IDS, dimana deteksi *intrusion* dilakukan dengan pemeriksaan manual

Bila memilih untuk menggunakan IDS, ada 2 strategi yang dapat dilakukan :

1. Tidak melakukan konfigurasi terhadap IDS, yaitu menggunakan konfigurasi *default*
2. Melakukan konfigurasi terhadap IDS. Bila konfigurasi tidak optimal, dinamakan *out-of-box configuration*.

Metodologi Penelitian

Metodologi yang digunakan adalah *mathematical model*, yang menggunakan notasi seperti pada tabel berikut :

Table 1 List of Notations

Parameters	
d	Damage caused by an undetected intrusion
c	Cost of manual investigation
μ	Utility of intrusion for users
P_D	Probability of getting an alarm from IDS for an intrusion
P_F	Probability of getting an alarm from IDS for no intrusion
ϕ	Fraction of damage prevented or recovered by the firm when an intrusion is detected
Strategic variables	
ψ	Probability of intrusion by a user
ρ	Probability of manual investigation when there is no IDS
ρ_1	Probability of manual investigation when the IDS generates an alarm
ρ_2	Probability of manual investigation when the IDS does not generate an alarm

ISR Vol. 16 No.1, Maret 2005, hal. 34
Table 1

1. Untuk kasus tanpa IDS, diturunkan *mixed strategy Nash equilibrium*. *Strategy space* untuk pengguna adalah $\Psi \in [0,1]$ dan *strategy space* untuk perusahaan adalah $\rho \in [0,1]$. Biaya yang dikeluarkan perusahaan adalah:
$$F(\rho, \Psi) = \rho c + \rho\Psi(1-\Phi)d + \Psi(1-\rho)d,$$

sedangkan keuntungan yang didapat pengguna adalah:
$\boldsymbol{H(\rho, \Psi) = \Psi \mu - \Psi \rho \beta}$
Perusahaan akan meminimalkan $F(\rho, \Psi)$, sedangkan pengguna akan memaksimalkan $H(\rho, \Psi)$

2. Untuk kasus dengan IDS, juga diturunkan *mixed strategy Nash equilibrium*.
Strategy space untuk pengguna adalah $\Psi \in [0,1]$ dan *strategy space* untuk perusahaan adalah $(\rho_1, \rho_2) \in [0,1]x[0,1]$.
Biaya yang dikeluarkan perusahaan adalah:
$\boldsymbol{F_A(\rho_1,\Psi) = \rho_1 c + \eta_1(1- \rho_1)d + \eta\rho_1(1-\Phi)d}$ *(alarm)*
$\boldsymbol{F_N(\rho_2, \Psi)= \rho_2 c + \eta_2(1- \rho_2)d + \eta\rho_2(1-\Phi)d}$ *(no alarm)*

sedangkan keuntungan yang didapatkan pengguna adalah:
$\boldsymbol{H(\rho_1, \rho_2, \Psi) = \Psi \mu - \Psi \beta(\rho_1 P_D + \rho_2(1- P_D))}$

Perusahaan akan meminimalkan $F_A(\rho_1,\Psi)$ bila mendapatkan *alarm*, dan meminimalkan $F_N(\rho_2, \Psi)$ bila tidak mendapatkan *alarm*, sedangkan pengguna akan memaksimalkan $H(\rho_1, \rho_2, \Psi)$.

Hasil Penelitian

1. Pada *out-of-box configuration,* perusahaan bisa mendapatkan nilai positif atau negatif dari IDS. Nilai positif didapatkan dengan jika dan hanya jika *detection rate* melebihi sebuah nilai kritis, yang bergantung pada parameter pengguna.
2. Pada *out-of-box configuration,* perusahaan mendapatkan nilai positif dari IDS jika dan hanya jika IDS dapat menghalangi *hacker*, yaitu jika kemungkinan melakukan *hacking* menurun dengan adanya IDS. Jadi, nilai dari IDS adalah dalam hal membuat takut *hacker*.
3. Dalam IDS yang dikonfigurasi secara optimal, perusahaan mendapatkan nilai yang nonnegatif. Konfigirasi optimal selalu menghalangi *hacker*.

Kesimpulan

Dalam manajemen keamanan TI terdapat 3 komponen utama : *prevention, detection,* dan *response*. Secara tradisional, perusahaan menekankan pada *perevention*, sebab bila ancaman dapat dicegah, *detection* dan *prevention* tidak dibutuhkan. Namun, kini organisasi telah menyadari bahwa *prevention* tidak mungkin dilakukan secara penuh, dan sistem berbasis *detection* mulai mendapatkan popularitas.

Bila IDS tidak dikonfigurasi secara benar, perusahaan belum tentu mendapatkan nilai positif dari IDS tersebut. IDS yang tidak dikonfigurasi secara optimal akan mendorong *hacker* untuk melakukan *hacking*, menghasilkan kerugian yang lebih besar bagi perusahaan. Sebaliknya, IDS yang dikonfigurasi secara optimal dapat menghalangi *hacker*. Selain itu, konfigurasi optimal bergantung pada parameter eksternal *hacker,* bukan parameter internal perusahaan.

Referensi utama artikel ini adalah :

1. Allen, J., A. Christie, W. Fithen, J. McHugh, J. Pickel, E. Stoner. 2000. State of the practice of intrusion detection technologies. Technical Report CMU/SEI-99-TR-028 ESC-99-028, Pittsburgh, PA.
2. Lippmann, R. P., D. J. Fried, I. Graf, J. W. Haines, K. R. Kendall, D. McClung, D. Weber, S. E. Webster, D. Wyschogrod, R. K. Cunningham, M. A. Zissman. 2000. Evaluating intrusion detection systems: The 1998 DARPA off-line intrusion detection evaluation. *Proc 2000 DARPA Inform. Survivability Conf. Exposition* (DISCEX) **2** 12-26.
3. Russel, G.S, 1990.Game models for structuring monitoring and enforcement systems. *Natural Resource Modelling* **4** 143-173.