



INTISARI

PENGEMBANGAN MODEL MOBILE AGENT UNTUK SISTEM DETEKSI PENYUSUPAN

Bambang Sugiantoro

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 agent untuk meningkatkan sistem tersebut dalam menghadapi tantangan dan perubahan yang lebih kompleks. Beberapa studi telah mengidentifikasi bahwa mobile agent mampu mereduksi trafik jaringan, namun studi berkaitan arsitektur sistem deteksi yang memanfaatkan agen statik dan mobile dalam hal performance belum sepenuhnya tercapai. Penelitian doctoral ini mengusulkan penggunaan mobile agent, metode deteksi rule matching dilanjutkan dengan string matching dan arsitektur dengan komponen multiagen, yaitu: (i) Agen master yang bertugas sebagai koordinator (ii) Mobile agen slave yang bertugas sebagai *mobile agent* yang berkeliling jaringan untuk melakukan deteksi ke *host-host* tujuan. (iii) Mobile agen *Clone* merupakan agent yang dikirim ke semua *host* untuk membantu tugas mobile agen slave. Prototip model ini juga telah memenuhi spesifikasi kebutuhan atau kriteria model yang telah ditetapkan yaitu: penggunaan sumber daya dan tersedianya informasi deteksi penyusupan yang dimandatkan kepada agent. Hasil perbandingan penggunaan bandwidth mobile agent yang telah dikembangkan lebih unggul dari peneliti sebelumnya, sehingga dapat direkomendasikan untuk menggunakan mobile agent ini.

Kata kunci : Sistem deteksi penyusupan, Mobile Agent, Rule Matching dan String Matching.



ABSTRACT

THE DEVELOPMENT OF MOBILE AGENT MODEL FOR INTRUSION DETECTION SYSTEM

Bambang Sugiantoro

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 doctoral research proposes detection method followed by a rule matching and string matching with multi agent components, i.e. : (i) Master agent acts as the coordinator, (ii) Slave mobile agent acts as the mobile agent who walking through the network to detect the destination hosts, (iii) Clone mobile agent acts as the agent assigned to all hosts for assisting the slave mobile agent. 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.

Keyword : Intrusion detection system, Mobile Agent, Rule Matching and String Matching.