Implementasi *Threshold Cryptography* dalam *Autonomous Network Defense*

Perkembangan teknologi informasi yang semakin masif berpotensi mendorong juga peningkatan terjadinya serangan siber. Salah satu cara dalam menghadapi hal tersebut dengan menjalankan *Security Operation Center* (SOC) untuk untuk memantau, mendeteksi, mencegah, dan merespon ancaman siber secara *real-time*. SOC tidak harus dijalankan secara internal tetapi dapat melalui pihak ketiga. *Managed SOC* merupakan pelaksanaan SOC yang diserahkan kepada pihak ketiga/layanan *outsourcing*. Sebuah perusahaan yang menyediakan layanan SOC tentu akan memasang perangkat *Intrusion Detection System* (IDS) untuk memantau trafik pada jaringan kliennya. Hal ini tentunya memiliki beberapa tantangan, karena semakin banyak klien tentu perlu semakin banyak IDS yang terpasang dan sumber daya manusia untuk memantaunya. Namun, apabila sumber daya perusahaan tidak mencukupi tentunya pelaksaan SOC menjadi tidak optimal.

Setiap jaringan internet tentunya memiliki sebuah *firewall* yang berfungsi untuk menyaring dan memblokir akses atau konten yang berbahaya berdasarkan *rule* yang diterapkan. *Rule* yang diterapkan pada *firewall* dapat bersumber dari IDS. Namun, IDS memiliki kemungkinan untuk menghasilkan banyak false positive dan apabila hasil dari IDS secara langsung diterapkan pada firewall tentunya tidak akan efektif. Oleh karena itu, diperlukan sebuah sistem yang dapat melakukan evaluasi terhadap temuan anomali pada IDS serta memanfaatkan setiap temuan anomali trafik pada IDS dapat digunakan secara secara langsung pada *firewall*. *Threshold cryptography* dapat diterapkan pada setiap IDS ketika beberapa IDS menemukan *hint* anomali yang terindikasi sebagai anomali trafik dan memenuhi nilai *threshold*-nya maka sistem dapat otomatis menambahkan *rule* pada *firewall*. Hal tersebut, tetap memiliki tantangan pada akurasi IDS dalam menentukan *false positif* atau true positif. Apabila terdapat *hint false positive* yang memenuhi *threshold* maka *rule* yang ditambahkan pada *firewall* akan melakukan blok pada trafik komunikasi yang salah. Oleh karena itu tetap dibutuhkan sistem atau mekanisme untuk mengurangi *false positif* pada IDS.

Tentunya menerapkan *threshold cryptography* pada perangkat IDS memiliki dampak terhadap performa pada perangkat tersebut.Selain itu, diperlukan sebuah sistem atau mekanisme untuk mengurangi *hint false positive* pada IDS serta pengaruhnya terhadap peningkataan keamanan sebuah jaringan dibandingkan dengan pendekatan *single decision maker* dari IDS. Hasil penelitian diharapkan dapat menunjukkan pengaruh penerapan *threshold cryptography* dan sebuah sistem atau mekanisme *multi decision maker* dengan jumlah angka anomali trafik yang *false positif*, penggunaan *firewall* yang lebih efektif, serta penggunaan sumber daya dalam menerapkan Managed SOC.

Implementation Threshold Cryptography for Autonomous Network Defense

The increasingly rapid development of information technology has the potential to drive an increase in cyberattacks. One way to address this is by operating a Security Operations Center (SOC) to monitor, detect, prevent, and respond to cyber threats in real time. A SOC does not have to be operated internally but can be managed by a third party. A Managed SOC refers to the operation of a SOC that is outsourced to a third party. A company that provides SOC services will, of course, install Intrusion Detection System (IDS) devices to monitor traffic on its clients' networks. This naturally presents several challenges, as a growing number of clients requires more IDS installations and human resources to monitor them. However, if a company's resources are insufficient, SOC operations will inevitably be suboptimal.

Every internet network has a firewall that filters and blocks harmful access or content based on applied rules. The rules applied to the firewall may originate from an IDS. However, IDS systems are prone to generating many false positives, and if the results from the IDS are applied directly to the firewall, they will not be effective. Therefore, a system is needed that can evaluate anomaly detections from the IDS and ensure that any detected traffic anomalies can be directly applied to the firewall. Threshold cryptography can be applied to each IDS; when multiple IDSs detect anomalies that meet the threshold value, the system can automatically add a rule to the firewall. However, this approach still faces challenges regarding the accuracy of IDS in distinguishing between false positives and true positives. If a false positive hint meets the threshold, the rule added to the firewall will block legitimate traffic. Therefore, a system or mechanism is still needed to reduce false positives in the IDS.

Of course, implementing threshold cryptography on an IDS device has an impact on the device's performance. In addition, a system or mechanism is needed to reduce false positives in the IDS and to assess its impact on improving network security compared to the IDS's single-decision-maker approach. The research results are expected to demonstrate the impact of implementing threshold cryptography and a multi-decision-maker system or mechanism on the number of false-positive traffic anomalies, more effective firewall usage, and resource utilization in implementing a Managed SOC.