บทคัดย่อ

ไฟร์วอลล์นับว่าเป็นอุปกรณ์เครือข่ายที่สำคัญที่จะช่วยให้เครือข่ายมีความปลอดภัย โดยระดับความปลอดภัยนั้นจะขึ้นอยู่กับกฎที่ได้กำหนดไว้ในไฟร์วอลล์ซึ่งการเขียน/ออกแบบกฎนั้นจะต้องทำอย่างระมัดระวัง เพราะการเขียนกฎผิดลำดับอาจจะทำให้ความหมายของกฎเปลี่ยนไป กลุ่มกฎของไฟร์วอลล์มักจะมีสิ่งผิดปกติหรือข้อขัดแย้งที่แอบแฝงอยู่ซึ่งเรียกว่า Anomaly ได้มีงานวิจัยหลายชิ้นที่คิดค้นกรรมวิธีเพื่อนำมาใช้ในการวิเคราะห์กฎของไฟร์วอลล์ และเพื่อใช้ค้นหา Anomaly ต่าง ๆ ภายในกฎของไฟร์วอลล์ แต่ก็ยังไม่มีงานวิจัยชิ้นใด ที่จะค้นหา Anomaly ได้ครอบคลุมทุกกรณี เช่นไม่สามารถหา Rule ที่ถูกบัง (Shadowed Rule) โดยหลาย Rule ที่อยู่ก่อนหน้า และไม่สามารถค้นหา Correlation Anomaly ที่เกิดจากการ correlate ภายในฟิลต์เดียวกัน ซึ่งสามารถที่จะเกิดได้กับผลิตภัณฑ์ไฟล์วอลล์หลายยี่ห้อเช่น IPTABLES และ Check Point Firewall-1 ซึ่งผลที่ตามมาก็คือไม่สามารถที่จะออกแบบกฎของไฟร์วอลล์ที่มีความปลอดภัยสูงได้

งานวิจัยนี้จะนำเสนอการวิเคราะห์กฎของไฟร์วอลล์โดยใช้รีเลชันแนลอัลจีบรา และอัลกอริทึมที่ใช้ในการค้นหา Anomaly ชนิดต่าง ๆ ซึ่งสามารถที่จะค้นหา Anomaly ได้อย่างครอบคลุม มันสามารถที่จะค้นหา Anomaly โดยการพิจารณาทีละหลาย ๆ Rule พร้อมกันได้ จากนั้นก็จะนำเสนอวิธีการกำจัด Anomaly ต่าง ๆ รวมทั้งวิธีการยุบรวมกฎ เพื่อลดจำนวนบรรทัดของ Rule List ให้สั้นลงด้วย

ABSTRACT

TE162827

Firewall is an important device for network security. However managing and writing firewall rules must be carefully done in order to implement the security policy correctly. Alternating rule order incorrectly may change meaning of the policy. Many research works proposed methods for finding anomalies within Rule List by using several approaches, but they are not cover all anomalies. For example, it could not find shadowed rule which might be shadowed by more than one previous rule, and could not find correlation anomaly that is a correlation within the same attribute. This kind of correlation can be occurred in many firewall products, such as port-range in IPTABLES or using multi-address in Check Point FW-1. Many researches consider only two rules. This could possibly get incorrectly results.

In this research, we propose a firewall rules analyzing and a new anomaly discovery algorithm using Relational Algebra technique. It can find all anomalies by considering more than two rules at the same time. We also propose an approach to remove anomalies within the Rule List, and to combine rules to reduce the Rule List's size.