บทที่ 5

สรุปผลงานวิจัยและข้อเสนอแนะ

5.1 สรุปผลการวิจัย

จากการศึกษาปัญหาระหว่าง Kerberos และ NAT แสดงให้เห็นว่า แต่ละวิธีต่างก็มีข้อดีและข้อเสียในด้านความปลอดภัยที่แตกต่างกัน ขึ้นกับผู้พัฒนาว่าจะนำวิธีการใดมาใช้เพื่อให้เหมาะสมกับสภาพแวดล้อมของตนเอง

หากเราต้องการใช้ NAT เพื่อควบคุมความปลอดภัยจากภายนอกเครือข่าย โดยป้องกันไม่ให้บุคคลภายนอกสามารถ access ไปยัง Client ปลายทางโดยตรง เราจะได้ประโยชน์จากการควบคุมความปลอดภัยด้าน Network Filtering เนื่องจาก เราสามารถควบคุมและป้องกัน Port และ IP address ที่ไหลผ่านเครือข่ายได้อย่างมีประสิทธิภาพ

หรือถ้าเราต้องการประยุกต์ใช้ Kerberos ซึ่งเป็นวิธีการควบคุมความปลอดภัยด้านการ Authentication เราก็จะมั่นใจได้ว่าผู้ที่ขอใช้บริการเป็นผู้ที่มี Authorization จริง มีความปลอดภัยเพียงพอและสะดวกแก่ผู้ใช้เนื่องจาก Kerberos สนับสนุนการ Authentication แบบ OTP ซึ่งถ้าในระบบ (หรือแต่ละ Realm) นั้น ๆ มี Kerberized Application มาก ๆ ก็จะยิ่งเพิ่มความสะดวกแก่ ผู้ใช้ เนื่องจากผู้ใช้ไม่จำเป็นต้องจำ Username และ Password มาก และยังรองรับการขยาย (Scalability) ของระบบในอนาคตได้ โดยอาจเพิ่ม Kerberos Authentication Server ให้มากกว่าหนึ่งตัว หรือเพิ่ม Kerberized Application Server ได้ในอนาคต

แต่เมื่อเรานำระบบความปลอดภัยทั้งสองวิธีนี้มาประยุกต์ร่วมกันกลับกลายเป็นปัญหา เนื่องจาก Kerberos พัฒนาขึ้นเพื่อเน้นการใช้งานภายในเครือข่ายเดียวกันเป็นหลัก ทำให้ไม่สนับสนุนการใช้งานกรณีต้นทางและปลายอยู่ต่างเครือข่ายกัน หรือถ้าเราต้องการนำทั้งสองวิธีมาประยุกต์ร่วมกันก็จำเป็นต้อง Compromise ความปลอดภัยลง โดยไม่นำ IP address มาใช้ประกอบการตรวจสอบ ซึ่งวิธีการดังกล่าว อาจไม่เหมาะสมกับ Application บางชนิดที่จำเป็นต้องระบุ IP address เป็นต้น

ดังนั้น ผู้วิจัยจึงนำเสนอและพัฒนาวิธีการทำงานร่วมกันระหว่าง Kerberos และ NAT โดยยังคงใช้ค่า IP address ในการตรวจสอบ เพื่อใช้เป็นอีกแนวทางในการพัฒนา Kerberized Application ที่จำเป็นต้องระบุ IP address อาทิ VPN เป็นต้น วิธีการดังกล่าว ถือได้ว่าเป็นการ

เพิ่มประสิทธิภาพให้แก่ Kerberos และรองรับการพัฒนา Kerberized Application ที่หลากหลายมากยิ่งขึ้น แต่ยังคงความเข้ากันได้ (Compatibility) กับการใช้งาน Kerberos ตามแบบมาตรฐาน นอกจากนี้ยังสะดวกแก่ผู้บริหารระบบ เนื่องจากไม่มีการแก้ไขใด ๆ ใน Kerberos Authentication Server และ Kerberized Application Server เลย

ผู้วิจัยจึงหวังเป็นอย่างยิ่งว่า ในอนาคต เราอาจพบ Kerberized Application ที่หลายหลายและเป็นประโยชน์แก่ผู้ใช้ แต่ยังคงความปลอดภัยแก่เครือข่ายมากยิ่งขึ้น

5.2 ปัญหาและข้อจำกัดที่พบในการวิจัย

เนื่องจากผู้วิจัยมีข้อจำกัดในด้านอุปกรณ์ ดังนั้น จึงจำเป็นต้องลดจำนวนอุปกรณ์ลงเพื่อให้เหมาะสม จากเดิม ผู้วิจัยต้องการจำลองโครงงานให้ Client ขอบริการผ่าน NAT ไปยัง Kerberos Authentication Server และ Kerberized Application Server ใน Internet โดยจำลองโครงงานเหลือเพียง ให้ Client จากเครือข่ายหนึ่งสามารถ access ไปยังอีกเครือข่ายหนึ่งผ่าน NAT เท่านั้น

จากข้อจำกัดดังกล่าว ทำให้ผู้วิจัยมิได้ทดสอบการใช้งานที่หลากหลายขึ้น อาทิ กรณีการเพิ่มจำนวน extra_address ที่มากกว่าหนึ่งตัวว่ายังสามารถทำงานได้ตามปรกติหรือไม่ ซึ่งผู้วิจัยตั้งใจจะทำเสริมจากฐานความรู้เดิมที่ศึกษาอยู่

และจากวิธีการที่ผู้วิจัยนำเสนอ ยังพบข้อจำกัดที่ Client จำเป็นต้องทราบถึง IP address ของ NAT ก่อนเพื่อใส่ค่าดังกล่าวใน extra_address ซึ่งอาจมีผู้พัฒนาให้สามารถใส่ค่าดังกล่าวโดยอัตโนมัติเพื่อป้องกันไม่ให้ Client ทราบข้อมูลต่าง ๆ ภายในเครือข่ายซึ่งอาจนำไปใช้ในทางที่ไม่ถูกต้องในอนาคต

5.3 ข้อเสนอแนะในงานวิจัยครั้งต่อไป

จากผลงานวิจัยดังกล่าว อาจเป็นพื้นฐานความรู้ในการพัฒนา Kerberized Application ที่มีความซับซ้อนและจำเป็นต้องนำ IP address ไปเป็นส่วนหนึ่งในการให้บริการ อาทิ การทำ Tunnel ระหว่าง Client ที่อยู่ภายใน NAT และ ปลายทางที่อยู่ภายนอก NAT เพื่อทำให้ Client สามารถใช้งาน VPN ที่เป็น Kerberized Application ระหว่างต้นทางและปลายทางได้ เป็นต้น

หรืออาจมีการนำความรู้ดังกล่าวไปสร้างเป็นเครื่องมือที่ใช้ตรวจสอบข้อมูลสำหรับผู้ขอบริการที่ Kerberized Application ว่ามาจากที่ใดบ้าง ซึ่งเครื่องมือดังกล่าวอาจเป็นประโยชน์ใน

การประยุกต์ร่วมกับ CRM เนื่องจาก ผู้ให้บริการสามารถทราบข้อมูลของผู้ใช้บริการว่า มีความถี่ในการขอใช้บริการแค่ไหน ในช่วงเวลาใด และนิยมใช้บริการใดที่สุด เพื่อเป็นแนวทางในการพัฒนาข้อมูลหรือทรัพยากรเครือข่ายให้เหมาะสมต่อไป

แต่ในบางกรณี อาจมีผู้นำแนวความคิดของ Kerberos ในการ compromise ให้ Authentication แบบไม่มี IP address ไปสร้างเป็นเครื่องมือดักจับ Ticket และศึกษาการจำลองตนเองเป็นผู้ใช้โดยอาศัย Ticket ที่ได้ เพื่อศึกษาถึงจุดบกพร่องของ Kerberos ซึ่งงานดังกล่าว ก็เป็นอีกงานวิจัยหนึ่งที่เป็นประโยชน์ในการพัฒนาแนวทางที่สร้างความปลอดภัยให้แก่ Kerberos ต่อไป

จากการศึกษาและทดลอง ตลอดจนการแสดงผลลัพธ์ที่ได้ ผู้วิจัยหวังเป็นอย่างยิ่งว่า งานวิจัยชิ้นนี้คงจะเป็นพื้นฐานความรู้ในการนำ Kerberos ไปประยุกต์ใช้ เพื่อให้มีความสะดวกทั้งต่อผู้ใช้และผู้บริหารระบบ มีความปลอดภัยที่เพียงพอ มีความเป็นส่วนตัว รองรับการทำงานแบบโปร่งใส ขยายระบบได้ในอนาคต และทำให้ข้อมูลในเครือข่ายเป็นหนึ่งเดียวกันได้ เพื่อก่อให้เกิดประสิทธิภาพสูงสุดแก่องค์กร