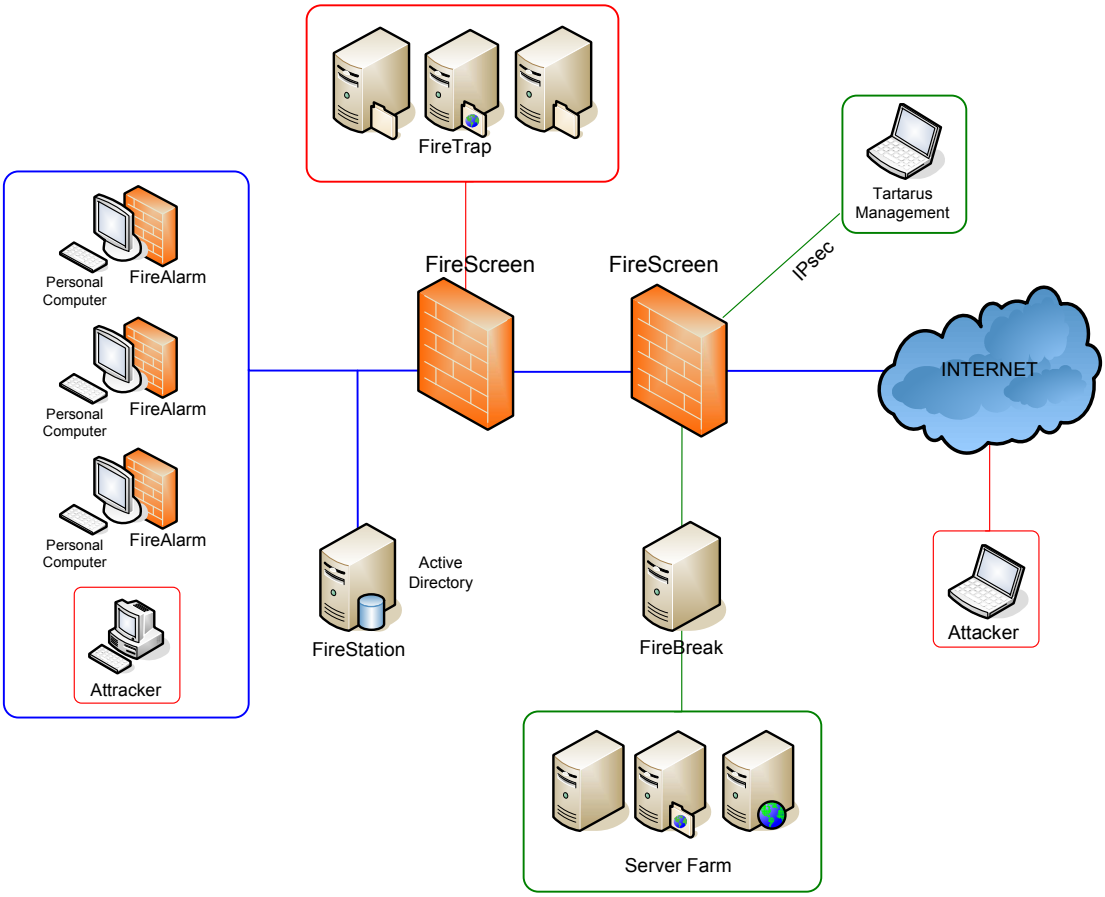
บทที่ 3
การออกแบบและพัฒนา

3.1 โครงสร้างของโครงงาน



รูปที่ 3.1 รูปภาพแสดงโครงสร้างของชุดโปรแกรมรักษาความปลอดภัยเครือข่าย

จากภาพเป็นลักษณะโครงสร้างโดยรวมของชุดโปรแกรมรักษาความปลอดภัยเครือข่ายซึ่งมีการทำงานที่ติดต่อทั้งกับส่วนของผู้ใช้ที่มาจากอินเตอร์เน็ตและผู้ใช้ที่อยู่ภายในองค์กร และเป็นชุดโปรแกรมที่สามารถดักกรองแพ็คเก็ตที่เข้ามาในระบบพร้อมทั้งดักจับแยกแยะผู้บุกรุกออกจากผู้ใช้งานจริงเพื่อทำการศึกษาพฤติกรรมของผู้บุกรุกที่ทำกับระบบได้ต่อไป

3.2 การออกแบบและพัฒนาซอฟแวร์

โครงสร้างของชุดโปรแกรมจะแบ่งออกเป็น 7 ส่วนใหญ่ ๆ ดังนี้

3.2.1 ไฟร์สเตชั่น (FireStation)

เป็นโปรแกรมที่ทำงานอยู่บนระบบปฏิบัติการวินโดวส์เซิร์ฟเวอร์ 2003 ทำหน้าที่ในการกำหนดกฎของเกตเวย์ไฟร์วอล (FireScreen) และเพอร์ซันนอลไฟร์วอล (FireAlarm) ซึ่งกฎของเพอร์ซันนอลไฟร์วอลสามารถที่จะกำหนดกฎให้กับกลุ่มผู้ใช้และผู้ใช้แต่ละคนได้ นอกจากนี้ยังทำหน้าที่รับรายละเอียดการโจมตีจากเครื่องต่าง ๆ ที่อยู่ในระบบ ซึ่งเป็นข้อมูลจากส่วนไฟร์อลาร์ม (FireAlarm) และ ไฟร์สกรีน (FireScreen) ซึ่งข้อมูลเหล่านี้ ได้แก่ ข้อมูลการ Allow , Deny หรือ Redirect แพ็คเก็ตที่ผ่านเข้ามายังส่วนไฟร์สกรีนและไฟร์อลาร์ม รวมถึงการบุกรุกที่ตรวจจับได้จากไฟร์อลาร์ม พร้อมทั้งจัดการเกี่ยวกับการนำล็อกไฟล์จากฐานข้อมูลขึ้นมาแสดงผล

ไฟร์สเตชั่นจะพัฒนาบนระบบปฏิบัติการวินโดวส์โดยใช้ความสามารถของเทคโนโลยีที่ชื่อแอ็คทีฟไดเร็คทอรีในการเก็บกฎของโปรแกรมส่วนต่าง ๆ ภายในระบบ และใช้เครื่องมือที่พัฒนา คือ Microsoft Visual C++ 6.0

3.2.2 ไฟร์อลาร์ม (FireAlarm)

ทำงานบนระบบปฏิบัติการวินโดวส์ XP โดยจะทำหน้าที่ในการป้องกันเครื่องคอมพิวเตอร์ตามกฎที่ได้รับมาจากไฟร์สเตชั่น ส่วนระบบตรวจจับผู้บุกรุกจะทำหน้าที่ตรวจจับการโจมตีและทำการแจ้งเตือนโดยการแสดงรูปแบบการโจมตีไว้ในล็อกไฟล์ และสามารถทำการส่งล็อกไฟล์นี้ไปยังเซิร์ฟเวอร์กลางเพื่อแจ้งให้ผู้ดูแลระบบได้ทราบ นอกจากนี้ยังสามารถทำงานแบบวินโดวส์เซอร์วิส (Windows Service) ทำให้ป้องกันเครื่องของผู้ใช้ได้แม้ว่ายังไม่ได้ทำการล็อกอินเข้าระบบก็ตาม

ไฟร์อลาร์มจะพัฒนาบนระบบปฏิบัติการวินโดวส์ โดยใช้เครื่องมือที่พัฒนา คือ Microsoft Visual C++ 6.0

ส่วนประกอบต่าง ๆ ของไฟร์อลาร์ม มีดังนี้

- ในส่วนของการกรองแพ็คเก็ต จะใช้ Firewall Hook Driver ซึ่งเป็นการนำ API (Application Program Interface) ที่มีใน Microsoft SDK มาใช้ในการพัฒนาโปรแกรม โดย API นี้จะทำงานในส่วนของเคอร์เนลโหมด
- ในการดักจับแพ็คเก็ตจะใช้ความสามารถของ WinPcap ดักจับแล้วนำมาวิเคราะห์
- ส่วนที่ใช้ในการรับกฎจากไฟร์สเตชั่น จะใช้ LDAP ในการติดต่อกับแอคทีฟไดเรคทอรี

3.2.3 ไฟร์สกรีน (FireScreen)

เป็นการรวมความสามารถของส่วนไฟร์สกรีนจากโครงงาน ISAG Firewall Suite 2548 และความสามารถในส่วนเกตเวย์ฮันนี่วอล จากโครงงาน ISAG Honeypot Suite 2548 เข้าไว้ด้วยกัน

โดยจะพัฒนาและออกแบบให้เป็นเกตเวย์ไฟร์วอลทำหน้าที่ป้องกันการโจมตีตามกฎที่รับมาจากเครื่องไฟร์สเตชั่นซึ่งเก็บไว้ในแอคทีฟไดเรคทอรีดาต้าเบสได้ โดยสามารถเข้าถึงผ่านทางโพรโตคอล LDAP โดยอาศัยไลบรารี่ OpenLDAP ซึ่งจะทำการตรวจสอบแพ็คเก็ตที่ผ่านเข้ามาในระบบเครือข่ายว่าเป็นไปตามกฎที่ตั้งไว้หรือไม่ แต่ถ้าไม่ตรงกับกฎใด ๆ เลยก็จะทำการตรวจสอบโดยอาศัยระบบตรวจจับผู้บุกรุก เพื่อทำการจำแนกผู้บุกรุกออกจากผู้ใช้ปรกติ ถ้าเข้าข่ายผู้บุกรุกก็จะทำการเปลี่ยนให้ผู้บุกรุกไปใช้งานในส่วนของไฟร์แทรป (FireTrap) แทน

ในการจำแนกผู้บุกรุกนั้น แพ็คเก็ตที่ไม่ตรงกับกฎใด ๆ ที่รับมาจากไฟร์สเตชั่นเลยจะถูกส่งมาตรวจสอบว่ามีพฤติกรรมเข้าข่ายเป็นผู้บุกรุกหรือไม่ โดยใช้กฎของโปรแกรมตรวจจับผู้บุกรุก (Snort_inline) ซึ่งเป็นเครื่องมือประเภท IDS (Intrution Detection System) โดยหากว่าการเชื่อมต่อใดมีลักษณะตรงตามกฎของโปรแกรมตรวจจับผู้บุกรุก จะถือว่าเจ้าของการเชื่อมต่อนั้นมีพฤติกรรมเข้าข่ายเป็นผู้บุกรุก และระบบจะทำการเปลี่ยนทิศทางการเชื่อมต่อดังกล่าวไปยังส่วนไฟร์แทรป (FireTrap) เพื่อทำการบันทึกพฤติกรรมของผู้บุกรุกที่กระทำต่อระบบต่อไป

3.2.4 ไฟร์เบรก (FireBreak)

ออกแบบให้เป็นโปรแกรมซีเคียวรีเวิร์สเว็บพร็อกซี่สำหรับเพิ่มความปลอดภัยให้กับเว็บเซิร์ฟเวอร์ซึ่งอยู่ภายในโซน DMZ มีความสามารถตรวจจับผู้บุกรุกในระดับแอปพลิเคชั่น และเมื่อมีการบุกรุกจะส่งข้อมูลการบุกรุกกลับไปที่เครื่องแม่ข่าย ในการพัฒนาจะใช้โปรแกรม Squid-cache ในการใช้งานเป็นรีเวิร์สเว็บพร็อกซี่ทั่ว ๆ ไป

3.2.5 ไฟร์แทรป (FireTrap)

เป็นระบบจำลองซึ่งแพ็คเก็ตที่ถูกส่วนไฟร์สกรีนจำแนกว่าเข้าข่ายผู้รุกจะถูกส่งมาที่ส่วนนี้และทำการหลอกล่อให้ผู้บุกรุกเข้าใจผิดว่าเป็นเครื่องที่ให้บริการจริง โดยจะจำลองการบริการต่าง ๆ ให้เหมือนจริงมากที่สุด พร้อมทั้งเปิดบริการหรือช่องโหว่ เพื่อให้ผู้บุกรุกหลงเชื่อและแสดงพฤติกรรมในการบุกรุกต่าง ๆ ออกมาซึ่งพฤติกรรมเหล่านั้นจะถูกบันทึกจะส่งไปเก็บไว้ยังระบบล็อกมอนิเตอร์เพื่อเก็บบันทึกและนำไปศึกษาต่อไป นอกจากนี้จะมีการตรวจสอบสภาพและความเสียหายของเครื่องไฟร์แทรปตลอดเวลาจากโปรแกรม S2I ซึ่งอยู่ในส่วนของไฟร์สกรีน

3.2.6 ล็อกมอนิเตอร์ (Log Monitor)

ออกแบบให้รับรายละเอียดการโจมตีจากเครื่องลูกข่ายในระบบและจากภายนอกระบบ โดยล็อกไฟล์จากส่วนต่างๆ จะถูกนำมาแสดงผลซึ่งจะแบ่งการแสดงผลออกเป็นสองส่วนคือ ส่วนที่เป็นล็อกไฟล์ที่อยู่ในระบบแอ็คทีฟไดเร็คทอรี่และส่วนที่เป็นล็อกไฟล์ที่เก็บอยู่ในส่วนของดาต้าเบส Mysql

3.2.7 Tartarus Management (TM)

โปรแกรม Tartarus Management (TM) เป็นโปรแกรม Front-end ที่สร้างขึ้นเพื่อแก้ปัญหาความยุ่งยากในการดูแลและจัดการระบบจำแนกผู้บุกรุกที่อยู่ในส่วนไฟร์สกรีน การจัดการเครื่องกับดักของระบบไฟร์แทรป รวมถึงการแสดงล็อกไฟล์จากระบบตรวจจับผู้บุกรุก และล็อกไฟล์จากการบันทึกพฤติกรรมของผู้บุกรุกในเครื่องกับดัก ซึ่งในการทำงานร่วมกับระบบอื่น ๆ นั้นทำงานผ่านทางช่องทาง IPsec เพื่อความปลอดภัย