โปรแกรมรับส่งสารด่วนแบบปลอดภัย

นายวรณิสร์ พงศ์จรรยานุกูล 43010365
อาจารย์ธนา หงษ์สุวรรณ อาจารย์ที่ปรึกษา
อาจารย์อัครเดช วัชระภูพงษ์ อาจารย์ที่ปรึกษา
ปีการศึกษา 2546

บทคัดย่อ

โปรแกรมรับส่งสารด่วนตัวอย่างเช่น ICQ และ AIM สามารถตอบสนองความต้องการในการสื่อสารระหว่างบุคคลได้อย่างรวดเร็วจนเป็นที่นิยมทั่วไป แม้การสื่อสารส่วนใหญ่เป็นเพื่อสันทนาการ หากแต่โปรแกรมรับส่งสารด่วนก็มีคุณค่าเชิงธุรกิจไม่น้อย อาจถือได้ว่าเป็นช่องทางการสื่อสารใหม่บนอินเทอร์เน็ตควบคู่กับจดหมายอิเล็กทรอนิกส์

แต่โปรแกรมรับส่งสารด่วนในปัจจุบันยังมิได้คำนึงถึงระบบรักษาความปลอดภัยที่ดีเพียงพอ ไม่ว่าเรื่องข้อความที่ส่งออกไปโดยไม่เข้ารหัส การแอบอ้างส่งข้อความและการรักษาความเป็นส่วนตัวของผู้ใช้งาน ในปีที่ผ่านๆ มาทางห้อง ISAG จึงได้ทำโครงงานเพื่อแก้ไขโปรแกรมฝั่งผู้ใช้ (โปรแกรม IsagQ) ให้มีการเข้ารหัสข้อความที่ได้ส่งออกและถอดรหัสปลายทาง และสามารถรองรับกับโพรโตคอลเวอร์ชั่นปัจจุบัน

แต่อย่างไรก็ตาม การใช้งานโปรแกรมรับส่งสารในปัจจุบันยังยึดติดกับการใช้งานกับเครื่องแม่ข่ายของผู้ผลิต ซึ่งผู้ใช้งานไม่สามารถสร้างเครื่องแม่ข่ายอีกตัวที่ลอกแบบการทำงานของเครื่องแม่ข่ายตัวจริงเพื่อนำโปรแกรมรับส่งสารนั้นๆไปใช้งานภายในองค์กรโดยเฉพาะได้ จึงมีการริเริ่มโครงงานโปรแกรมแม่ข่ายเพื่อรับส่งสารด่วนขึ้น จึงมีการพัฒนาโครงงาน IsagQ เพื่อให้สามารถรองรับการทำงานกับโปรแกรมแม่ข่ายดังกล่าว รวมถึงมีการออกแบบโพรโตคอลเฉพาะเพื่อให้สามารถทำงานร่วมกันได้ดีที่สุด

Isag Secure Instant Messenger

Waranis Pongjanyanukul
Thana Hongsuwan Advisor
Akkradach Watcharapupong Advisor

ABSTRACT

Instant-messaging programs, such as ICQ and AIM, can response requirement of human communication and be popular quickly. Although most of human use it for entertainment, but instant-messaging programs have helpful for business which be a new way of internet communication and work with e-mail.

But nowaday, instant-messaging programs is not considered about security system, example no sending message encryption, no sending message authentication and no authorization. In the past, ISAG offered the project for develop instant-messaging program (IsagQ program) for encrypt sending message and decrypt at destination, and it can work with current ICQ protocol's version.

However, instant-messaging programs can work with their instant-messaging server only, but users cannot duplicate it for use inside organization. So, secure instant-messaging server has borned, and begin develop IsagQ to integrated work with it, and create a new protocol for them.

กิตติกรรมประกาศ

โครงงานนี้คงไม่อาจสำเร็จได้ด้วยดี หากไม่ได้รับความช่วยเหลือและร่วมมือจากบุคคลหลายๆ ฝ่ายด้วยกัน บุคคลสองท่านแรกที่ต้องกล่าวถึงเพราะเป็นส่วนสำคัญที่ทำให้ปริญญานิพนธ์นี้สำเร็จลงได้ก็คือ อาจารย์ธนา หงษ์สุวรรณ และอาจารย์อัครเดช วัชระภูพงษ์ อาจารย์ที่ปรึกษาปริญญานิพนธ์ ที่ก่อให้เกิดโครงงานนี้ พร้อมทั้งให้คำแนะนำและให้คำปรึกษา แนะแนวทาง เคี่ยวเข็ญ เลี้ยงโออิชิ รวมถึงช่วยแก้ไขปัญหาต่างๆ อย่างต่อเนื่องตลอดโครงงาน ซึ่งต้องขอขอบพระคุณเป็นอย่างมาก

ขอขอบคุณห้องปฏิบัติการ ISAG ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ ที่ได้สนับสนุนสถานที่และอุปกรณ์เครือข่ายสำหรับใช้ในการพัฒนาโครงงาน

ขอขอบคุณคณาจารย์ในสถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบังทุกท่าน ที่ได้ประสิทธิ์ประสาทวิชาความรู้ให้กับผู้จัดทำ

ขอขอบคุณและขอบใจเพื่อนห้อง D และห้อง P รวมถึงรุ่นน้องทั้งหลายที่คอยช่วยเหลือ ให้กำลังใจและสร้างบรรยากาศที่ดีตลอดมา รวมถึงเป็นเพื่อนกินและเพื่อนเล่นเกมส์ด้วย

สุดท้ายนี้ต้องขอขอบพระคุณบุคคลสำคัญที่สุดที่ทำให้ผู้จัดทำมีวันนี้ก็คือ บิดา-มารดา อันเป็นที่เคารพรัก ซึ่งได้ให้กำเนิดและเลี้ยงดูมาเป็นอย่างดี พร้อมทั้งให้โอกาสในการศึกษาอย่างเต็มที่ คอยให้กำลังใจและเอาใจใส่เสมอมาอันหาที่เปรียบมิได้ ผู้จัดทำขอระลึกในพระคุณและขอกราบขอพระคุณมา ณ ที่นี้

วรณิสร์ พงศ์จรรยานุกูล

สารบัญ

	หน้า
บทคัดย่อ	I
ABSTRACT	II
กิตติกรรมประกาศ	III
สารบัญ	IV
สารบัญตาราง	VIII
สารบัญภาพ	IX
บทที่ 1 บทนำ	1
1.1 ความสำคัญและที่มาของโครงงาน	1
1.2 วัตถุประสงค์ของการพัฒนา	1
1.3 ขอบเขตของการพัฒนา	1
1.4 วิธีการดำเนินงาน	2
บทที่ 2 โปรแกรมรับส่งสารด่วน	3
2.1 ความสำคัญของโปรแกรมรับส่งสารด่วน	3
2.2 การทำงานในโปรแกรมรับส่งสารด่วน	3
2.3 ตัวอย่างของโปรแกรมรับส่งสารด่วน	4
2.3.1 AOL Instant Messenger	4
2.3.2 ICQ	5
2.3.3 MSN Messenger	6
2.3.4 Yahoo Messenger	7
2.4 ทิศทางของโปรแกรมรับส่งสารด่วน	8
บทที่ 3 ภาษาจาวา	10
3.1 ประวัติของภาษาจาวา	10
3.2 คุณสมบัติของภาษาจาวา	12
3.3 การใช้ภาษาจาวาสำหรับสร้างและพัฒนาในงานด้านต่าง ๆ	14
3.4 สภาพแวดล้อมเสมือน (Java Virtual Machine)	15
3.5 หลักการทำงานของภาษาจาวา	17
3.5.1 การคอมไพล์	17

3.5.2 การวางตำแหน่งในหน่วยความจำ 18
3.5.3 การรันโค้ดที่ได้จากการคอมไพล์ 18
3.5.4 คลาสโหลดเดอร์ 19
3.5.5 การตรวจสอบไบต์โค้ด 19
3.5.6 การทำงานตามโค้ด 20
3.5.7 การสร้างและรันโปรแกรม 20
3.6 Java Foundation Classes 21
3.6.1 ชุดคำสั่ง AWT 21
3.6.2 ชุดคำสั่ง Swing 21
3.6.3 ชุดคำสั่ง Java 2D 21
3.6.4 ชุดคำสั่ง Accessibility 22
3.6.5 ชุดคำสั่ง Drag and Drop 22
3.6.6 ความแตกต่างระหว่างชุดคำสั่ง AWT และชุดคำสั่ง Swing 22
3.7 เครื่องมือสำหรับพัฒนาโปรแกรมภาษาจาวา 24
3.7.1 Java Development Kit 24
3.7.2 Borland Jbuilder 24
3.7.3 Microsoft Visual J++ 25
3.7.4 IBM VisualAge for Java 26
3.7.5 VisualCafe 27
3.8 ความแตกต่างระหว่างจาวาแอพพลิเคชันและจาวาแอพเพล็ต 27
3.9 ทิศทางของจาวา 28

บทที่ 4 การเข้ารหัสข้อมูล 30
4.1 ระบบของการเข้ารหัสข้อมูล 30
4.1.1 ระบบการเข้ารหัสแบบสมมาตร 30
4.1.2 ระบบการเข้ารหัสแบบไม่สมมาตร 31
4.2 รูปแบบการเข้ารหัสสำหรับการสื่อสารข้อมูลในโพรโตคอลทีซีพี/ไอพี 32
4.2.1 การเข้ารหัสระดับการเชื่อมโยงข้อมูล 32
4.2.2 การเข้ารหัสระดับเครือข่าย 33
4.2.3 การเข้ารหัสระดับทรานสปอร์ต 33
4.2.4 การเข้ารหัสระดับโปรแกรมประยุกต์ 34

บทที่ 5 โพรโตคอลของ IsagQ และ IsagMQ 35
5.1 การติดต่อระหว่าง IsagQ กับ IsagMQ 35

5.2 การติดต่อระหว่าง IsagQ กับ IsagMQ 38
5.2.1 การเริ่มการติดต่อ 38
5.2.2 ความหมายของแพ็กเก็ตที่ใช้ติดต่อสื่อสารกับ IsagQ 39

บทที่ 6 การออกแบบและพัฒนาโครงงาน 40
6.1 แนวคิดและการออกแบบความสามารถของโปรแกรม 40
6.2 ส่วนประกอบของโปรแกรม 40
6.2.1 ส่วนการติดต่อกับผู้ใช้งานหน้ารายชื่อ 42
6.2.2 ส่วนการติดต่อกับผู้ใช้งานหน้าสนทนา 42
6.2.3 ส่วนการเข้า-ถอดรหัสข้อมูล 42
6.2.4 ส่วนติดต่อกับ ICQ 42
6.2.5 ส่วนติดต่อกับ IsagQ 42
6.3 การออกแบบและสร้างส่วนการติดต่อกับผู้ใช้งาน 42
6.4 การติดต่อเครือข่ายอินเทอร์เน็ต 44
6.5 การสร้างคีย์สำหรับทำการเข้ารหัสข้อมูล 44
6.6 การรวมส่วนประกอบของโปรแกรมเข้าด้วยกัน 46

บทที่ 7 การทดสอบโปรแกรม IsagQ 48
7.1 การทดสอบการรับส่งข้อความระหว่างผู้ใช้ IsagQ กับผู้ใช้ ICQ 48
7.1.1 การทดสอบการส่งข้อความจากผู้ใช้ IsagQ ไปยังผู้ใช้ ICQ 48
7.1.1.1 ผลจากการรับส่งข้อความจากผู้ใช้ IsagQ ไปยังผู้ใช้ ICQ 48
7.1.1.2 ผลจากการดักจับแพ็กเก็ตในการส่งข้อความจากผู้ใช้ IsagQ ไปยังผู้ใช้ ICQ 49
7.1.2 การทดสอบการส่งข้อความจากผู้ใช้ ICQ มายังผู้ใช้ IsagQ 49
7.1.2.1 ผลจากการรับส่งข้อความจากผู้ใช้ ICQ มายังผู้ใช้ IsagQ 49
7.1.2.2 ผลจากการดักจับแพ็กเก็ตในการส่งข้อความจากผู้ใช้ ICQ มายังผู้ใช้ IsagQ 50
7.2 การทดสอบการรับส่งข้อความระหว่างผู้ใช้ IsagQ กับผู้ใช้ IsagQ 51
7.2.1 ผลจากการรับส่งข้อความระหว่างผู้ใช้ IsagQ กับผู้ใช้ IsagQ 51
7.2.2 ผลจากการดักจับแพ็กเก็ตในการส่งข้อความจากผู้ใช้ ICQ มายังผู้ใช้ IsagQ 52

บทที่ 8 สรุปผลการพัฒนาโครงงาน 53
8.1 คุณสมบัติของโปรแกรม 53
8.2 ประโยชน์ของการพัฒนาโครงงาน 53
8.3 ข้อจำกัดของโครงงาน 54

8.4 ข้อเสนอแนะสำหรับผู้นำโครงงานไปพัฒนา 54

ภาคผนวก ก. ความรู้เกี่ยวกับโปรแกรม ICQ

ภาคผนวก ข. การดักจับแพ็กเก็ตโดยใช้โปรแกรม Damping ICQ

ภาคผนวก ค. การดักจับแพ็กเก็ตโดยใช้โปรแกรม Ethereal

ภาคผนวก ง. การแปลงรูปแบบของใบรับรองสิทธิ์จาก PEM เป็น PKCS12

บรรณานุกรม

สารบัญตาราง

		หน้า
ตารางที่ 4.1	แสดงข้อดีและข้อเสียในระบบของการเข้ารหัสข้อมูลแต่ละระบบ	32
ตารางที่ 5.1	คำสั่งที่ใช้ติดต่อกับ IsagMQ	36
ตารางที่ 5.1	คำสั่งที่ใช้ติดต่อกับ IsagQ	39

สารบัญภาพ

		หน้า
รูปที่ 2.1	การติดต่อกับเซิร์ฟเวอร์เพื่อใช้งาน	4
รูปที่ 2.2	โปรแกรม AOL Instant Messenger	5
รูปที่ 2.3	โปรแกรม ICQ	6
รูปที่ 2.4	โปรแกรม MSN Messenger	7
รูปที่ 2.5	โปรแกรม Yahoo Messenger	8
รูปที่ 3.1	การทำงานด้วยคอมพิวเตอร์สมมติที่จำลองโดยจาวาอินเทอร์พรีเตอร์	16
รูปที่ 3.2	การประมวลผลของโปรแกรมทั่วไปในระบบปฏิบัติการที่แตกต่างกัน	18
รูปที่ 3.3	การประมวลผลของโปรแกรมภาษาจาวา	18
รูปที่ 3.4	การทำงานของชุดคำสั่ง AWT	22
รูปที่ 3.5	การทำงานร่วมกันของคอมโพเน็นต์ top-level swing กับคอมโพเน็นต์ lightweight	23
รูปที่ 3.6	โปรแกรม Borland Jbuilder	25
รูปที่ 3.7	โปรแกรม Microsoft Visual J++	26
รูปที่ 3.8	โปรแกรม IBM VisualAge for Java	26
รูปที่ 3.9	โปรแกรม VisualCafe	27
รูปที่ 4.1	แสดงการเข้ารหัสและถอดรหัสแบบสมมาตร	30
รูปที่ 4.2	แสดงการเข้ารหัสและถอดรหัสแบบไม่สมมาตร	31
รูปที่ 4.3	การเข้ารหัสในระดับการเชื่อมโยงข้อมูล	33
รูปที่ 4.4	การเข้ารหัสในระดับเครือข่าย	33
รูปที่ 4.5	การเข้ารหัสในระดับทรานสปอร์ต	33
รูปที่ 4.6	การเข้ารหัสในระดับโปรแกรมประยุกต์	34
รูปที่ 4.7	การเข้ารหัสบนระบบโอเอสไอโมเดลของทีซีพี/ไอพี	34
รูปที่ 5.1	รูปแบบแพ็กเก็ตของโพรโตคอล	35
รูปที่ 5.2	ไดอาแกรมแสดงขั้นตอนการติดต่อเพื่อเริ่มสนทนา	38
รูปที่ 6.1	รูปแบบการติดต่อในโปรแกรม ICQ	40
รูปที่ 6.2	รูปแบบการสื่อสารโดยตรงในโปรแกรม IsagQ	41
รูปที่ 6.3	ส่วนประกอบในการทำงานของโปรแกรม IsagQ	41
รูปที่ 6.4	การออกแบบหน้าจอสำหรับติดต่อกับผู้ใช้งานในโปรแกรม IsagQ	43
รูปที่ 6.5	หน้าจอกราฟิกที่สร้างขึ้นสำหรับติดต่อกับผู้ใช้งาน	43
รูปที่ 6.6	ขั้นตอนในการสร้างคีย์ความลับสำหรับสนทนาระหว่างผู้ใช้โปรแกรม IsagQ	45
รูปที่ 6.7	การสร้างคีย์ความลับเมื่อมีผู้ใช้งานโปรแกรม IsagQ หลายคน	46

รูปที่ 7.1 ผลจากการรับส่งข้อความจากผู้ใช้ IsagQ ไปยังผู้ใช้ ICQ 48
รูปที่ 7.2 ผลจากการดักจับแพ็กเก็ตที่ทำการรับส่งในรูปที่ 7.1 49
รูปที่ 7.3 ผลจากการรับส่งข้อความจากผู้ใช้ ICQ มายังผู้ใช้ IsagQ 50
รูปที่ 7.4 ผลจากการดักจับแพ็กเก็ตที่ทำการรับส่งในรูปที่ 7.3 50
รูปที่ 7.5 ผลจากการรับส่งข้อความจากผู้ใช้ IsagQ กับผู้ใช้ IsagQ 51
รูปที่ 7.6 ผลจากการดักจับแพ็กเก็ตที่ทำการรับส่งระหว่างผู้ใช้ IsagQ กับผู้ใช้ IsagQ ในรูปที่ 7.5 52