การรวบรวมและจัดหมวดหมู่ประเด็นการรักษาความปลอดภัยของระบบคอมพิวเตอร์

นาย สุรสิทธิ์ มัลลิกานิล

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต
สาขาวิชาวิทยาศาสตร์คอมพิวเตอร์ ภาควิชาวิศวกรรมคอมพิวเตอร์
คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
ปีการศึกษา 2546

ISBN 974-17-4870-1

ลิขสิทธิ์ของจุฬาลงกรณ์มหาวิทยาลัย

COLLECTION AND CATEGORIZATION OF TOPICS IN COMPUTER SECURITY

Mr. Surasit Manlikanin

A Thesis Submitted in Partial Fulfillment of the Requirements
for the Degree of Master of Science in Computer Science
Department of Computer Engineering
Faculty of Engineering
Chulalongkorn University
Academic Year 2003

ISBN 974-17-4870-1

จุฬาลงกรณ์มหาวิทยาลัย

หัวข้อวิทยานิพนธ์	การรวบรวมและจัดหมวดหมู่ประเด็นการรักษาความปลอดภัยของระบบคอมพิวเตอร์
โดย	นายสุรสิทธิ์ มัลลิกานิล
สาขาวิชา	วิทยาศาสตร์คอมพิวเตอร์
อาจารย์ที่ปรึกษา	อาจารย์ ดร.ยรรยง เต็งอำนวย
อาจารย์ที่ปรึกษา (ร่วม)	อาจารย์ ปริญญา หอมเอนก

คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย อนุมัติให้นับวิทยานิพนธ์ฉบับนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญามหาบัณฑิต

..... คณบดีคณะวิศวกรรมศาสตร์
(ศาสตราจารย์ ดร. ดิเรก ลาวัณย์ศิริ)

คณะกรรมการสอบวิทยานิพนธ์

..... ประธานกรรมการสอบ
(อาจารย์ ดร.ณัฐวุฒิ หนูไพโรจน์)

..... อาจารย์ที่ปรึกษา
(อาจารย์ ดร.ยรรยง เต็งอำนวย)

..... อาจารย์ที่ปรึกษา (ร่วม)
(อาจารย์ ปริญญา หอมเอนก)

..... กรรมการ
(อาจารย์ ธงชัย โรจน์กังสดาล)

สถาบันวิทยบริการ
จุฬาลงกรณ์มหาวิทยาลัย

สุรสิทธิ์ มัลลิกานิล : การรวบรวมและจัดหมวดหมู่ประเด็นการรักษาความปลอดภัยของระบบคอมพิวเตอร์ (COLLECTION AND CATEGORIZATION OF TOPICS IN COMPUTER SECURITY) อ. ที่ปรึกษา : อ.ดร. ยรรยง เต็งอำนวย , 66 หน้า ISBN 974-17-4870-1

การรักษาความปลอดภัยของระบบคอมพิวเตอร์ มีพัฒนาการที่รวดเร็ว ยากต่อผู้บริหารระบบจะติดตามข่าวสารและวิทยาการในด้านนี้ได้ทัน การวิจัยนี้จึงจัดหมวดหมู่ประเด็นการรักษาความปลอดภัยของระบบคอมพิวเตอร์ โดยทำการรวบรวมประเด็นจากแหล่งข้อมูลต่างๆทั้งที่มีการจัดหมวดหมู่ไว้แล้วและที่นำเสนอเฉพาะประเด็นที่กำลังได้รับความสนใจ เช่น เว็บไดเรกทรอรี หลักสูตรการเรียนการสอน การประชุมวิชาการและเว็บไซต์ต่างๆ โดยใช้หลักการทางสถิติคือการวิเคราะห์การจัดกลุ่มแบบลำดับชั้นมาช่วยในการจัดกลุ่มประเด็นที่กำลังได้รับความสนใจหรือกำลังให้ความสำคัญจากแหล่งข้อมูลดังกล่าว

จากกรรมวิธีดังกล่าวทำให้ได้ผลลัพธ์ทั้งหมด 15 ประเด็นในหมวดหมู่หลัก และวิทยานิพนธ์ฉบับนี้ได้กล่าวถึงการหาประเด็นย่อยภายใต้ประเด็นหลักโดยใช้วิธีการค้นหาข้อมูลจากระบบค้นหาข้อมูล (Search Engine) ได้เป็นประเด็นรองในชั้นที่สองจำนวน 10 ถึง 16 ประเด็น

กรรมวิธีที่ใช้ในวิทยานิพนธ์ฉบับนี้เป็นวิธีการจัดหมวดหมู่ตามประเด็นที่กำลังได้รับความสนใจจากแหล่งข้อมูลต่างๆ ทำให้สามารถรองรับกับปัญหาทางด้านการรักษาความปลอดภัยของระบบคอมพิวเตอร์ที่เกิดขึ้นมาใหม่อยู่เสมอตามเทคโนโลยีที่เปลี่ยนไป และผลที่ได้ทำให้ทราบถึงกลุ่มของประเด็นการรักษาความปลอดภัยของระบบคอมพิวเตอร์ที่หน่วยงานและองค์กรต่างๆจะต้องศึกษาและให้ความสำคัญ

สถาบันวิทยบริการ
จุฬาลงกรณ์มหาวิทยาลัย

ภาควิชา วิศวกรรมคอมพิวเตอร์ ลายมือชื่อนิสิต .....

สาขาวิชา วิทยาศาสตร์คอมพิวเตอร์ ลายมือชื่ออาจารย์ที่ปรึกษา .....

ปีการศึกษา 2546 ลายมือชื่ออาจารย์ที่ปรึกษาร่วม .....

4471460121 : MAJOR COMPUTER SCIENCE

KEY WORD : Computer Security Topic / Category / Classification / Taxonomy / Cluster Analysis

SURASIT MANLIKANIN : COLLECTION AND CATEGORIZATION OF TOPICS IN COMPUTER SECURITY. THESIS ADVISOR : YUNYONG TENG-AMNUAY, Ph.D, 66 pp. ISBN 974-17-4870-1

Computer Security is continuously rapidly developed. System administrator can hardly monitor and update this change. This research is to categorize and represent the classified topics or hot issues on computer security topics, for example, web directories, classes and curriculums, security conferences, and various types of web sites by using the statistical principal, *hierarchical cluster analysis*, as a tool for classifying the hot topics from sources.

This methodology generated and provided 15 main topics. This research explained the sub-categorization method within the main topics by using the Search Engine. It generated 10 to 16 sub-topics.

The methodology provided in this research is to organize the worth topics from sources so that it can cope with categorization in computer security changes. The result led us to know the group of computer security topics that should be concerned by other organizations.

สถาบันวิทยบริการ
จุฬาลงกรณ์มหาวิทยาลัย

Department of Computer Engineering
Field of study Computer Science
Academic year 2003

Student's signature .....
Advisor's signature .....
Co-advisor's signature .....

กิตติกรรมประกาศ

วิทยานิพนธ์ฉบับนี้สำเร็จลุล่วงไปได้ด้วยความช่วยเหลืออย่างดียิ่งของอาจารย์ ดร.ยรรยง เต็งอำนวย อาจารย์ที่ปรึกษาวิทยานิพนธ์ ซึ่งท่านได้ให้คำแนะนำและข้อคิดเห็นต่าง ๆ ในการวิจัยด้วยดีตลอด และขอขอบคุณ อ. ดร. ณัฐวุฒิ หนูไฟโรจน์ และ อ.ธงชัย โรจน์กังสดาล กรรมการวิทยานิพนธ์ที่กรุณาสละเวลาให้คำแนะนำ ตรวจและแก้ไขวิทยานิพนธ์ และที่สำคัญ อ.ปริญญา หอมเอนก อาจารย์ที่ปรึกษาร่วม ที่ได้ให้คำแนะนำเกี่ยวกับแหล่งข้อมูลต่างๆที่เกี่ยวข้องกับเรื่องการรักษาความปลอดภัยของระบบคอมพิวเตอร์ ซึ่งท่านเป็นผู้เชี่ยวชาญด้านการรักษาความปลอดภัยคอมพิวเตอร์ในประเทศ โดยได้ใบรับรองจากสถานบันต่างๆที่มีชื่อเสียง เช่น CISSP, CISA, SANS GIAC GCFW, CCSA 2000, CCNS, MCSE Windows 2000, MCDBA SQL Server 2000, MCP+Internet, Master CNE, CNI, CNA เป็นต้น

ขอขอบคุณ ผศ.ดร. วินิจ เทือกทอง จากสถานบันราชภัฏสวนสุนันทา อาจารย์ภัทรินี ไตรสถิตย์ จากมหาวิทยาลัยเชียงใหม่ และคุณกิตติกร ทองนิมิตสวัสดิ์ ที่ได้ให้คำปรึกษาเกี่ยวกับสถิติ คุณดวงสมร พันธ์พิกุล ที่ได้เอื้อเฟื้อเวลาในการช่วยผู้วิจัยแปลและเรียบเรียงภาษาต่างประเทศ และขอขอบคุณท่านอื่นๆที่มีส่วนช่วยเหลือในการทำวิทยานิพนธ์ที่ไม่ได้กล่าวนามา ณ โอกาสนี้ด้วย

ท้ายนี้ผู้วิจัยใคร่ขอกราบขอบพระคุณบิดามารดาซึ่งให้การเลี้ยงดูอบรมสั่งสอน รวมทั้งสนับสนุนและให้กำลังใจแก่ผู้วิจัยเสมอมา

สถาบันวิทยบริการ
จุฬาลงกรณ์มหาวิทยาลัย

สารบัญ

สารบัญ (ต่อ)

หน้า

สถาบันวิทยบริการ
จุฬาลงกรณ์มหาวิทยาลัย

สารบัญตาราง

หน้า

สารบัญตาราง (ต่อ)

หน้า

สถาบันวิทยบริการ
จุฬาลงกรณ์มหาวิทยาลัย

สารบัญรูปภาพ

หน้า

สถาบันวิทยบริการ
จุฬาลงกรณ์มหาวิทยาลัย

บทที่ 1

บทนำ

1.1. ความเป็นมาและความสำคัญของปัญหา

ปัจจุบันคอมพิวเตอร์ได้ถูกนำมาใช้ในการส่งข้อมูลข่าวสารหรือประมวลผลข้อมูลทั้งด้านธุรกิจและธุรกรรมส่วนบุคคลอย่างแพร่หลาย โดยมีเครือข่ายคอมพิวเตอร์และเทคโนโลยีการสื่อสารเป็นตัวสนับสนุนการใช้งาน เช่นเครือข่ายอินเทอร์เน็ต ทำให้เกิดความสะดวกและรวดเร็วในการส่งข้อมูล ไม่ว่าจะเป็นการส่งอีเมล์ การซื้อขายออนไลน์ การทำธุรกรรมทางอิเล็กทรอนิกส์ การเผยแพร่ข้อมูลขององค์กร จากความสามารถในการเชื่อมต่อกันของคอมพิวเตอร์นี้เองที่เปิดโอกาสให้เกิดภัยคุกคามที่มากับเทคโนโลยีเหล่านี้ ซึ่งภัยคุกคามนี้เกิดจากการกระทำของผู้ไม่ประสงค์ดีโดยอาจจะทำการลักลอบดูข้อมูล แก้ไขข้อมูล การใช้เทคนิคต่างๆ ที่ทำให้เกิดผลเสียหายต่อเจ้าของข้อมูลและผู้ได้รับข้อมูล หรืออาจจะมีการทำลายข้อมูลของฝ่ายตรงกันข้าม เช่นการส่งไวรัสหนอนอินเทอร์เน็ต เข้าไปก่อกวนหรือทำลาย รวมถึงการบุกรุกระบบที่ไม่มีการรักษาความปลอดภัยที่ดี จากปัญหาดังกล่าวนี้ทำให้สถาบันการศึกษา หน่วยงาน และองค์กรต่างๆ ได้หันมาให้ความสำคัญเกี่ยวกับปัญหาทางด้านนี้ เช่น สถาบันการศึกษาหลายแห่งได้ทำการเปิดสอนวิชา Computer Security เพื่อพัฒนาบุคลากรให้สามารถรองรับกับปัญหาทางด้านนี้หรือหน่วยงานที่เกี่ยวข้องในด้านการรักษาความปลอดภัยของระบบคอมพิวเตอร์ทั้งในประเทศและต่างประเทศที่จัดตั้งขึ้นมา รวมถึงการจัดทำเว็บไซต์ที่เป็นแหล่งรวบรวมข้อมูลที่กล่าวถึงประเด็นการรักษาความปลอดภัยของระบบคอมพิวเตอร์ โดยมีทั้งการรวบรวมเว็บไซต์ที่เกี่ยวข้องกับการรักษาความปลอดภัยของระบบคอมพิวเตอร์ เช่น directory.google.com www.yahoo.com หรือเป็นแหล่งข้อมูลการแจ้งและแก้ไขปัญหาทางด้านการรักษาความปลอดภัยของระบบคอมพิวเตอร์เช่น thaicert.nectec.or.th เป็นต้น

ปัจจุบันแหล่งข้อมูลที่เกี่ยวข้องกับการรักษาความปลอดภัยของระบบคอมพิวเตอร์นั้นมีอยู่มากมายและแสดงข้อมูลที่แตกต่างกันไปขึ้นอยู่กับว่าแหล่งข้อมูลนั้นให้ความสำคัญเกี่ยวกับเรื่องใดเป็นพิเศษ เช่น www.cert.org ก็จะกล่าวถึงเพียงจุดอ่อนหรือรูโหว่ของระบบต่างๆ เช่นระบบปฏิบัติการ ระบบฐานข้อมูล แนวทางการแก้ไขปัญหา หรือเว็บไซต์ที่รวมรวบเว็บไซต์ต่างๆ ก็มีการรวบรวมและจัดหมวดหมู่ที่แตกต่างกันไป และเว็บไซต์ที่รวบรวมนั้นเป็นเพียงเว็บไซต์ที่สร้างขึ้นในแต่ละเรื่องที่ผู้สร้างเว็บไซต์รู้หรือชำนาญเกี่ยวกับประเด็นนั้นๆ แต่ยังไม่มีแหล่งข้อมูลไหนที่รวบรวมและครอบคลุมประเด็นที่เกี่ยวข้องกับการรักษาความปลอดภัยของระบบคอมพิวเตอร์ทั้งหมดที่มีอยู่ในปัจจุบัน

จากสาเหตุนี้ทำให้เกิดแนวคิดของวิทยานิพนธ์ฉบับนี้ที่จะนำประเด็นของการรักษาความปลอดภัยของระบบคอมพิวเตอร์มารวบรวมและจัดกลุ่มของเนื้อหาข้อมูลที่มีลักษณะเดียวกันให้อยู่ด้วยกัน โดยให้ครอบคลุมถึงเนื้อหาที่เกี่ยวข้องกับเรื่องการรักษาความปลอดภัยของระบบคอมพิวเตอร์ที่มีอยู่ในปัจจุบัน ซึ่งผลจากการวิจัยนี้ทำให้เกิดผลดีหลายด้านเช่น

1) ทำให้ทราบถึงภาพรวมของประเด็นการรักษาความปลอดภัยของระบบคอมพิวเตอร์
2) ทำให้เนื้อหาที่มีลักษณะเกี่ยวเนื่องกันหรือสัมพันธ์กันอยู่รวมในกลุ่มเดียวกัน ซึ่งช่วยให้ผู้สนใจมีโอกาสได้เลือกหรือทราบถึงประเด็นอื่นๆไปด้วย
3) เป็นแหล่งข้อมูลพื้นฐานของเรื่องการรักษาความปลอดภัยของระบบคอมพิวเตอร์

1.2. วัตถุประสงค์

เพื่อรวบรวมและจัดหมวดหมู่ให้ครอบคลุมของเรื่องการรักษาความปลอดภัยของระบบคอมพิวเตอร์จากแหล่งข้อมูลที่มีอยู่ในปัจจุบัน

1.3. ขอบเขตวิทยานิพนธ์

1) จัดหมวดหมู่ของประเด็นการรักษาความปลอดภัยของระบบคอมพิวเตอร์ที่มีอยู่ในปัจจุบัน โดยใช้แนวทางของจากแหล่งข้อมูลทั้ง 5 แหล่งดังนี้
   - เว็บไซต์ที่รวบรวมเว็บไซต์ต่างๆ เช่น dmoz.org
   - เว็บไซต์ที่เกี่ยวข้องกับการรักษาความปลอดภัยของระบบคอมพิวเตอร์โดยตรง เช่น thaicert.nectec.or.th www.securityfocus.com เป็นต้น
   - หนังสือที่เกี่ยวกับการรักษาความปลอดภัยของระบบคอมพิวเตอร์
   - หลักสูตรที่เปิดสอนตามสถาบันการศึกษาต่างๆ
   - การประชุมวิชาการและวารสารที่เกี่ยวข้อง
2) ค้นคว้าหาประเด็นการรักษาความปลอดภัยของระบบคอมพิวเตอร์ที่มีอยู่ในปัจจุบันและจัดให้อยู่ในหมวดหมู่ โดยพิจารณาจากคุณลักษณะ
3) พัฒนาเว็บไซต์ ที่ประกอบด้วยข้อมูลหมวดหมู่ของประเด็นการรักษาความปลอดภัยของระบบคอมพิวเตอร์

1.4. ประโยชน์ที่คาดว่าจะได้รับ

1) ได้ทราบถึงประเด็นการรักษาความปลอดภัยของระบบคอมพิวเตอร์ทั้งหมดในปัจจุบัน
2) เพื่อเป็นแนวทางในการเรียนการสอนของวิชา 2110639 Computer System Security ของคณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
3) เพื่อเป็นแหล่งข้อมูลอ้างอิงสำหรับผู้ทำวิทยานิพนธ์ในเรื่องการรักษาความปลอดภัยของระบบคอมพิวเตอร์

สถาบันวิทยบริการ
จุฬาลงกรณ์มหาวิทยาลัย

บทที่ 2

แนวคิด ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

ปัจจุบันมีแหล่งข้อมูลมากมายที่ได้รวบรวมประเด็นทางด้านความปลอดภัยของคอมพิวเตอร์ แต่แหล่งข้อมูลเหล่านั้นส่วนใหญ่ไม่ได้จัดแบ่งประเด็นไว้เป็นโครงสร้างที่ชัดเจนหรือเป็นแค่เพียงการจัดทำเฉพาะกิจเท่านั้น (ad hoc) การที่อัตราของประเด็นถูกรวบรวมขึ้นอย่างไม่มีโครงสร้างได้เพิ่มขึ้นเรื่อยๆ ทำให้ยากที่จะหาข้อมูลที่มีความเชื่อมโยงกันในการที่จะช่วยในการทำธุรกรรมใดๆ หรือใช้ในการตัดสินใจ การจัดหมวดหมู่เป็นการอธิบายอย่างละเอียดถึงความเชื่อมโยงที่มีอยู่ภายในและระหว่างประเด็นต่างๆ เหล่านั้นซึ่งถูกจำกัดอยู่ในข้อมูลที่ไม่เป็นโครงสร้างในเอกสารจำนวนมาก และการที่จะทำได้ต้องมีกระบวนการในการจัดแบ่งหมวดหมู่ เพื่อที่จะแบ่งกลุ่มข้อมูลที่มีความสัมพันธ์กันเข้าไว้ด้วยกัน การจัดแบ่งหมวดหมู่นั้นมีประโยชน์หลายประการ ดังนี้คือ [1][29]

- สามารถเข้าถึงข้อมูลได้อย่างรวดเร็ว
- เข้าถึงข้อมูลได้อย่างถูกต้อง
- หลีกเลี่ยงการค้นหาที่ซับซ้อนที่มีกลุ่มแยกเป็นอิสระหลายกลุ่ม
- แสดงให้เห็นถึงภาพรวมในขณะเดียวกันก็เห็นรายละเอียดของแต่ละ subject
- แสดงให้เห็นความสัมพันธ์ของข้อมูล
- ลดความซ้ำซ้อน
- ค้นหาได้ดีกว่าการใช้ search engine ในกรณีที่เราไม่รู้คำสำคัญ (keyword)

และปัจจุบันแหล่งข้อมูลที่เผยแพร่ความรู้ เทคโนโลยี และแนวทางการป้องกันต่างๆ เพื่อรองรับกับปัญหาต่างๆทางด้านการรักษาความปลอดภัยของระบบคอมพิวเตอร์ที่เกิดขึ้นมาใหม่อยู่เสมอตามเทคโนโลยีที่เปลี่ยนไป ดังนั้นงานวิจัยนี้จึงมีแนวคิดในการจัดหมวดหมู่ตามประเด็นที่กำลังได้รับความสนใจหรือกำลังได้รับความสำคัญจากแหล่งข้อมูลต่างๆ งานวิจัยนี้จึงได้ทำการศึกษาทฤษฎีและงานวิจัยต่างๆเพื่อสนับสนุนแนวคิดนี้ โดยมีรายละเอียดดังนี้

2.1. แนวทางในการรวบรวมประเด็นและจัดหมวดหมู่ [25]

ก่อนที่จะทำการจัดหมวดหมู่จะต้องมีการรวบรวมประเด็นจากแหล่งข้อมูลต่างๆ โดยมีขั้นตอนดังนี้

- ขีดเส้นใต้หรือทำเครื่องหมายคำศัพท์ที่สามารถใช้ในการจัดหมวดหมู่
- พิมพ์คำศัพท์เหล่านั้นในเอกสารแยกไปต่างหาก
- ระบุแหล่งที่มาของคำศัพท์เหล่านั้น
- นับจำนวนครั้งที่พบคำศัพท์เหล่านั้น
- ควรจะแสดงรายการทุกอย่างที่คิดว่าน่าจะใช้ได้โดยยังไม่ต้องกังวลถึงความซ้ำซ้อน
- ไม่ต้องวิเคราะห์ให้มากเกิดไป ให้พิมพ์ทุกอย่างที่คิดว่ามีความเชื่อมโยงกับการจัดหมวดหมู่
- ทำการจัดหมวดหมู่ในระดับบนสุดก่อน (Top Down) การออกแบบแบบ Top-down นั้น จะพิจารณาหัวข้อหลักก่อน จากนั้นก็จะแตกลงไปในรายละเอียดของแต่ละหัวข้อ [11]

2.2. ทฤษฎีการจัดหมวดหมู่

หลังจากที่ได้ทำการรวบรวมประเด็นทางด้านความปลอดภัยของคอมพิวเตอร์แล้ว จากนั้นจะทำการจัดกลุ่มหรือหมวดหมู่ของประเด็น ซึ่งงานวิจัยนี้ได้ทำการศึกษาถึงทฤษฎีที่จะสามารถนำมาใช้ในการจัดหมวดหมู่ดังนี้ [49]

2.2.1 Discriminant Analysis

- เป็นเทคนิคที่ทำการแบ่งกลุ่มข้อมูลหรือหน่วยตัวอย่าง ออกเป็นกลุ่มย่อยๆหลายๆกลุ่ม โดยใช้หลักเกณฑ์ของการวิเคราะห์ความถดถอยเชิงพหุนามที่มีความสัมพันธ์เชิงเส้น โดยที่ตัวแปรตามเป็นตัวแปรเชิงกลุ่ม โดยที่ตัวแปรต้นหรือตัวแปรอิสระควรเป็นตัวแปรเชิงปริมาณ
- โดยที่หน่วยที่อยู่กลุ่มเดียวกันจะมีความคล้ายคลึงกัน
- ต้องทราบว่าก่อนว่าแต่ละหน่วยอยู่ในกลุ่มใดมาก่อนและมีจำนวนกี่กลุ่ม
- คาดว่าตัวแปร/ปัจจัยใดบ้างที่ทำให้หน่วยอยู่ต่างกัน

2.2.2 Factor Analysis

แบ่งกลุ่มตัวแปร กรณีที่มีตัวแปรเป็นจำนวนมากๆ จะมีการแบ่งกลุ่มตัวแปรออกเป็น factor หลายๆ factor โดยตัวแปรที่อยู่ใน factor เดียวกันจะมีความสัมพันธ์กัน

2.2.3 Cluster Analysis

เป็นเทคนิคการจำแนกหรือแบ่ง Case หรือแบ่งตัวแปรออกเป็นกลุ่มย่อยๆตั้งแต่ 2 กลุ่มขึ้นไป โดยที่ case ที่อยู่ในกลุ่มเดียวกันจะมีลักษณะที่คล้ายกัน ส่วน case ที่อยู่ต่างกันจะมีลักษณะที่แตกต่างกัน โดยการแบ่งกลุ่มจะขึ้นอยู่กับตัวแปรที่จะนำมาพิจารณา Cluster Analysis มีลักษณะดังนี้

- เป็นเทคนิคการแบ่งกลุ่มข้อมูลออกเป็นกลุ่มย่อย
- ไม่จำเป็นต้องทราบจำนวนกลุ่มมาก่อน
- ไม่ต้องทราบว่าแต่ละหน่วยอยู่กลุ่มใด
- ใช้แบ่งกลุ่มลูกค้าที่มีลักษณะ/พฤติกรรมการบริโภคที่เหมือนกันหรือคล้ายกัน

ขั้นตอนของการแบ่งกลุ่ม

1) เลือกตัวแปรหรือ factor ที่คาดว่ามีอิทธิพลที่ทำให้ case ต่างกัน
2) เลือกวิธีการวัดระยะห่าง จะขึ้นกับชนิดของข้อมูลซึ่งมีอยู่ 3 ประเภท
   - Interval ใช้กับข้อมูลชนิด Interval หรือ Ratio scale มีหลายวิธี เช่น Euclidean distance Squre Euclidean distance เป็นต้น

หลักเกณฑ์ในการรวมกลุ่มหรือรวม cluster มีขั้นตอนดังนี้

เริ่มต้นกำหนดให้ 1 case เท่ากับ 1 cluster มีทั้งหมด n cluster

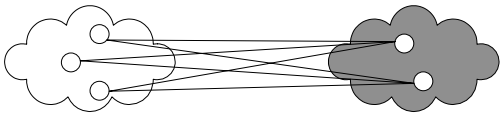
ขั้นที่ 1 รวม case 2 case ให้อยู่ในกลุ่มเดียวกันหรือ cluster เดียวกัน โดยพิจารณาจากค่าระยะห่าง

ขั้นที่ 2 พิจารณาว่าควรจะรวม case ที่ 3 เข้าอยู่ในกลุ่มเดียวกับ 2 case แรกหรือควรจะรวม 2 case ใหม่เข้าอยู่ในกลุ่มใหม่อีกกลุ่มหนึ่ง โดยพิจารณาจากค่าระยะห่าง

ทำขั้นที่ 3,4, … โดยใช้เกณฑ์เดียวกับขั้นที่ 2 ทำไปเรื่อยๆจนกระทั่งได้ทุก case อยู่ในกลุ่มเดียวกัน

วิธีในการรวมกลุ่ม มีอยู่หลายวิธี เช่น

Between-groups linkage หรือ Average linkage between groups



รูปที่ 2-1: Average linkage

วิธีนี้จะคำนวณหาระยะห่างเฉลี่ยของทุกคู่ของ case โดยที่ case หนึ่งอยู่ใน cluster ที่ i ส่วนอีก case หนึ่งอยู่ใน cluster ที่ j โดยที่ i<>j ถ้า cluster ที่ i มีระยะห่างเฉลี่ยจาก cluster ที่ j สั้นกว่าระยะห่างจาก cluster อื่นๆจะนำ cluster ที่ i และ j รวมกันเป็น cluster เดียวกัน

ยังมีวิธีในการรวมกลุ่มอื่นอีกเช่น Nearest neighbor, Single linkage Further neighbor หรือ Complete linkage

จากทฤษฎีการจัดหมวดหมู่ที่ได้ศึกษามาข้างต้นสามารถนำมาเปรียบในแต่ละประเด็นได้ดังนี้

ตารางที่ 2-1: แสดงการเปรียบเทียบของวิธีการจัดกลุ่มข้อมูล

ประเด็น	Discriminant	Factor Analysis	Cluster Analysis
ทราบถึงลักษณะการแบ่งกลุ่ม	จะต้องทราบลักษณะของการแบ่งกลุ่มมาก่อน (เป็นกลุ่มที่มีอยู่แล้ว)	ไม่จำเป็น	ไม่จำเป็น
จำนวนกลุ่ม	ต้องทราบจำนวนกลุ่มมาก่อน แล้วใช้ข้อมูลในอดีตมาคำนวณค่าที่ใช้ในการแบ่งกลุ่ม	ไม่จำเป็น	ไม่จำเป็น
ลักษณะข้อมูลที่ใช้ในการจัดกลุ่ม	จัดกลุ่มข้อมูลหรือหน่วยตัวอย่างๆ/จัดกลุ่มตัวแปร	จัดกลุ่มตัวแปรที่มีจำนวนมากๆ	จัดกลุ่มข้อมูลหรือหน่วยตัวอย่าง

Cluster Analysis เป็นการแบ่งกลุ่มของข้อมูลที่มีลักษณะคล้ายกันโดยวิธีการวัดระยะห่างระหว่าง case แต่ละคู่ สามารถแบ่งออกเป็น 2 เทคนิคย่อย คือ Hierarchical Cluster Analysis และ K-Means Cluster Analysis สามารถเปรียบเทียบ 2 เทคนิคนี้ดังตารางที่ 2-2

ตารางที่ 2-2: แสดงการเปรียบเทียบเทคนิคย่อยของ Cluster Analysis

ประเด็น	Hierarchical	K-Means
จำนวนของ Case	<200	>200
จำนวนกลุ่ม	ไม่เป็นจำเป็นต้องทราบมาก่อน	ต้องกำหนดหรือทราบจำนวนกลุ่ม
Standardized	ไม่ต้อง	ต้อง
หาระยะห่าง	ได้หลายวิธี	Euclidean Distance
ชนิดของข้อมูลหรือตัวแปร	- Interval scale/Ratio scale - Count Data - Binary	Interval scale/Ratio scale

2.3. งานวิจัยในการจัดหมวดหมู่ของเว็บไซต์

เนื่องจากงานวิจัยจะนำผลของการจัดหมวดหมู่มาเป็นชื่อหมวดหมู่ต่างๆที่จะนำมาแสดงบนเว็บไซต์ โดยการพัฒนาเว็บไซต์หมวดหมู่ของประเด็นการรักษาความปลอดภัยของระบบคอมพิวเตอร์จะใช้แนวทางในการจัดหมวดหมู่ของเว็บไซต์ โดยได้ทำการสำรวจหลักการต่างๆจากเว็บไซต์ที่ได้รับความนิยม เช่น yahoo dmoz โดยมีหลักการดังต่อไปนี้

2.3.1. โครงสร้างของหัวข้อ [11]

โครงสร้างของหัวข้อที่จัดทำขึ้นจะมีผลต่อกระบวนการและประสิทธิภาพในการค้นหาข้อมูล โดยที่โครงสร้างของหัวข้อจะแบ่งออกเป็น 3 ระดับ ต่อไปนี้คือ

หัวข้อในระดับบนสุด (Top-level)

หัวข้อหลักเป็นเหมือนกับแกนหลักของการจัดหมวดหมู่ซึ่งจะเป็นหัวข้อสูงสุดที่ระบุในโครงสร้างและนำเสนอถึงขอบเขตของการค้นหา โดยการจัดหมวดหมู่ของเว็บไซต์ทั่วไปจะมีประมาณ 10-16 หัวข้อ ซึ่งถ้ามากกว่านี้จะทำให้ผู้เยี่ยมชมมีทางเลือกมากเกินไป [42]

หัวข้อย่อย (Subtopics)

หัวข้อย่อยจะอยู่ระหว่างหัวข้อหลักและรายละเอียด [25][28]

- ชื่อของหัวข้อย่อยควรจะบ่งบอกถึงรายละเอียดภายใต้หัวข้อย่อยนั้น
- จำนวนความลึกของควรจะอยู่ระหว่าง 3 ถึง 5
- จะสร้างหัวข้อย่อยก็ต่อเมื่อมีรายละเอียดอยู่ระหว่าง 5-20
- ไม่ควรให้ผู้เยี่ยมคลิกเลือกดูข้อมูลมากกว่า 3 ครั้ง
- ไม่ควรใช้ชื่อซ้ำกับหัวข้อหลัก
- ควรพิจารณาการจัดหมวดหมู่จากแหล่งข้อมูลต่างๆ

รายละเอียดภายใต้หัวข้อ (Evidence Topics)

รายละเอียดภายใต้หัวข้อจะเป็นประเด็นต่างๆภายใต้หมวดหมู่นั้น ซึ่งประเด็นนั้นจะแสดงถึงข้อความหรือคำอธิบาย งานวิจัยนี้ได้นำเอามาตรฐานดับลินคอร์เมทาดาทา (Dublin Core Metadata) ในการนำเสนอข้อมูล ซึ่งดับลินคอร์เมทาดาทาเป็นมาตรฐานสำหรับพรรณนาสารสนเทศอิเล็กทรอนิกส์ในการพัฒนาห้องสมุดดิจิตัล หนังสือและวารสารอิเล็กทรอนิกส์ของหน่วยงานต่างๆ ทำให้สามารถสืบค้นและแลกเปลี่ยนข้อมูลระหว่างกันได้ [51]

ดับลินคอร์เมทาดาทาประกอบด้วยหน่วยข้อมูลย่อยพื้นฐาน 15 หน่วย (15 Dublin Core Metadata Elements) [52] ดังนี้

1) TITLE ชื่อเรื่อง ชื่อของทรัพยากรสารสนเทศที่กำหนดโดยเจ้าของผลงาน หรือ สำนักพิมพ์
2) AUTHOR OR CREATOR ผู้แต่ง หรือ เจ้าของผลงาน บุคคล หรือ หน่วยงานที่รับผิดชอบเนื้อหาเชิงปัญญาของสารสนเทศ
3) SUBJECT OR KEYWORDS หัวเรื่อง คำสำคัญ หัวข้อ วลี รหัสวิชา เลขหมู่ ที่อธิบายเรื่อง และเนื้อหา
4) DESCRIPTION ลักษณะ รายละเอียดของสารสนเทศ เช่น บทคัดย่อ หรือ บรรยายรูปร่าง ลักษณะการใช้งาน
5) PUBLISHER สำนักพิมพ์ หน่วยงานที่ผลิตสารสนเทศชิ้นที่เผยแพร่ในรูปแบบปัจจุบัน เช่น สำนักพิมพ์ มหาวิทยาลัย บริษัท
6) OTHER CONTRIBUTORS ผู้ร่วมงาน หรือ หน่วยงานอื่นนอกจากผู้แต่ง หรือ เจ้าของผลงานที่มีชื่อปรากฏในข้อผู้แต่ง หมายถึงบุคคล หรือ หน่วยงาน ที่มีส่วนร่วมสร้างผลงานในระดับรองจากผู้แต่ง
7) DATE ปี ปีที่ผลิตผลงานในรูปแบบปัจจุบัน ประกอบด้วย [50]
   - วันที่ผลิต (Created)
   - วันที่มีผลบังคับใช้ (Valid)
   - วันที่ เข้าถึงได้ (Available)
   - วันที่เผยแพร่ (Issued)
   - วันที่แก้ไข (Modified)
8) RESOURCE TYPE ประเภทของสารสนเทศ เช่น HomePage นวนิยาย คำประพันธ์ บทความ รายงานทางวิชาการ เรียงความ พจนานุกรม
9) FORMAT รูปแบบที่บันทึกสารสนเทศ เช่น Text , HTML
10) RESOURCE IDENTIFIER รหัส สัญลักษณ์ หรือ เลข ที่ระบุเฉพาะว่าหมายถึงสารสนเทศอิเล็คทรอนิกส์รายการนั้นๆ เช่น URL และ URN
11) SOURCE ต้นฉบับ ผลงานที่มาของสารสนเทศไม่ว่าจะเป็นเอกสารหรืออยู่ในรูปของอิเล็กทรอนิกส์
12) LANGUAGE ภาษา ที่ใช้ในการเรียบเรียงสารสนเทศ
13) RELATION เรื่องที่เกี่ยวข้อง สารสนเทศเรื่องอื่นๆที่เกี่ยวข้อง
14) COVERAGE สถานที่ และ เวลา
15) RIGHT MANAGEMENT สิทธิ ระเบียบปฏิบัติเรื่องสิทธิ เพื่อให้ผู้ใช้สารสนเทศรับทราบ และยอมรับข้อปฏิบัติเรื่องสิทธิขณะที่สารสนเทศเรื่องนั้นๆปรากฏบนจอภาพ

ความสำคัญของ Dublin Core

- ง่ายต่อการใช้ และ ไม่ซับซ้อนยุ่งยาก ผู้ที่ไม่ใช่ผู้เชี่ยวชาญเกี่ยวกับการจัดหมวดหมู่ของทรัพยากรสารสนเทศเลย ก็สามารถใช้ได้ เพราะว่าหน่วยของ Dublin Core เข้าใจง่าย
- ง่ายต่อการจัดหมวดหมู่ และ การใช้ที่จะบรรยายถึง ทรัพยากร Resource นั้นๆ
- เป็นมาตรฐานซึ่งกำหนดขึ้นโดย W3C (World Wide Web Consortium)
- ช่วยพัฒนาการจัดทรัพยากรสารสนเทศให้มีคุณภาพ
- สามารถใช้งานได้ร่วมกับมาตรฐานอื่นๆ
- จะใช้คำสำคัญต่างๆในการค้นหาสื่อสารสนเทศอิเล็กทรอนิกส์
- เป็นมาตรฐานที่สามารถนำไปใช้ได้อย่างแพร่หลายและประยุกใช้ได้กับงานทุกประเภทบนอินเทอร์เน็ต ซึ่งปัจจุบันมีคำจำกัดความที่ไม่ใช่มาตรฐาน ทำให้การค้นหายุ่งยาก แต่ Dublin Core ทำให้เกิดมาตรฐานที่เป็นอันหนึ่งอันเดียวกัน เพราะมีการใช้มากกว่า 20 ประเทศทั่วโลก เช่นในทวีป อเมริกา ยุโรป เอเชีย ออสเตเลีย
- สามารถยืดหยุ่นได้ตามต้องการ ขึ้นอยู่กับว่าต้องการนำไปใช้ในงานแบบใด

2.3.2. การตั้งชื่อ

การกำหนดมาตรฐานการตั้งชื่อหัวข้อ และเข้มงวดกับการใช้มาตรฐานนี้ จะทำให้สามารถจัดหมวดหมู่ให้เข้าใจได้ง่ายและมีความผิดพลาดน้อยลง [11][19][25][28]

- ความยาวของชื่อหัวข้อ
  - ชื่อของประเด็นควรมีความยาวไม่เกิน 128 ตัวอักษร ซึ่งรวมถึง hyphens และ underscores ด้วย
- Case Sensitivity
  - ชื่อหัวข้อและชื่อหัวข้อย่อยโดยปกติแล้วจะเป็น case-insensitive ไม่ควรนำ Case มาเป็นตัวกำหนดเงื่อนไขในการค้นหา แต่การใช้ตัวพิมพ์ใหญ่ในหัวข้อหลักก็จะช่วยให้อ่านง่ายขึ้น
- หลีกเลี่ยงความซ้ำซ้อน
  - การจัดแบ่งหมวดหมู่ที่แยกคำศัพท์ที่แตกต่างกันแต่จริงๆแล้วพูดถึงเรื่องเดียวกัน จะทำให้ทั้งผู้อ่านและผู้จัดหมวดหมู่เกิดความสับสนได้
- หมวดหมู่ที่มีความเกี่ยวข้องกัน
  - ใช้ *@link* ถ้ามีหมวดย่อยใน area อื่นๆ ที่คล้ายคลึงกับในหมวดย่อย
- ข้อพิจารณาอื่นๆ ในการตั้งชื่อ
  - ชื่อที่ใช้ควรจะใช้คำที่รู้จักกันทั่วไป (เช่น ใช้คำว่า e-commerce แทนคำว่า Electronic commerce)
  - พยายามอย่าใช้ตัวย่อ นอกจากตัวย่อนั้นจะเป็นที่รู้จักกันโดยทั่วไป
  - อย่าใช้คำย่อหรือสัญลักษณ์ (เช่น &, + or etc.) ในการนำเสนอคำใดๆ
  - อย่าใช้ชื่อซ้ำกับชื่อที่เป็นหัวข้อของหมวดหมู่ระดับก่อนหน้า
  - อย่าใช้คำที่สื่อถึงความหมายที่กว้างเกินไปหรือสื่อถึงการไม่เกี่ยวข้องกัน เช่น “เบ็ดเตล็ด” หรือ “ประเด็นอื่นๆ”
  - อย่าใช้คำศัพท์ที่สื่อถึงสิ่งผิดกฎหมาย

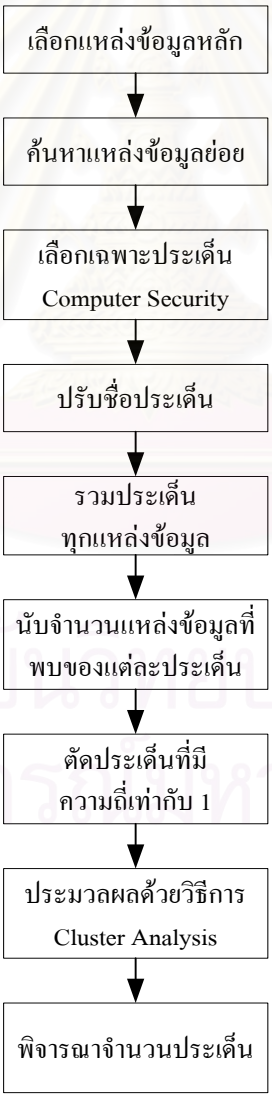
บทที่ 3

การออกแบบการจัดหมวดหมู่

บทนี้จะกล่าวถึงการออกแบบการจัดหมวดหมู่เพื่อเป็นกรรมวิธีที่จะใช้การสำรวจของข้อมูลและนำข้อมูลที่ได้ไปจัดหมวดหมู่ โดยจะทำการจัดหมวดหมู่ตามประเด็นที่กำลังได้รับความสนใจจากแหล่งข้อมูลต่างๆที่ได้สำรวจมา ซึ่งมีรายละเอียดดังนี้

3.1. กรรมวิธีการจัดหมวดหมู่

ผู้วิจัยได้ทำการออกแบบกรรมวิธีในการจัดหมวดหมู่เพื่อเป็นแนวทางในการจัดหมวดหมู่ประเด็นการรักษาความปลอดภัยของระบบคอมพิวเตอร์มาเป็นหมวดหมู่หลัก โดยมีขั้นตอนดังรูปที่ 3-1



รูปที่ 3-1: กรรมวิธีการจัดหมวดหมู่หลัก

สถาบันวิทยบริการ
จุฬาลงกรณ์มหาวิทยาลัย

3.1.1. เลือกแหล่งข้อมูลหลัก

มีแหล่งข้อมูลมากมายที่เกี่ยวข้องกับข้อมูลด้านความปลอดภัยของระบบคอมพิวเตอร์ ซึ่งแต่ละแหล่งข้อมูลจะเน้นประเด็นที่แตกต่างกันไป เพื่อให้เกิดความหลากหลายและชัดเจนมากขึ้นงานวิจัยนี้จึงได้ทำการสำรวจประเด็นจากแหล่งข้อมูลที่ได้จัดหมวดหมู่ไว้แล้วหรือมีประเด็นที่เกี่ยวข้องทั้ง 6 แหล่งข้อมูล คือ ไดเรกทอรีเวบ (web directory) ตำราเรียนหรือหนังสือ หลักสูตรต่างๆ ระบบค้นหาข้อมูล (Search Engine) การประชุมทางวิชาการ และเว็บไซต์ โดยมีรายละเอียดดังนี้

1) ไดเรกทอรีเวบ (Web directories) เป็นแหล่งข้อมูลที่มีรวบรวมเว็บไซต์ต่างๆเข้าเป็นหมวดหมู่หรือไดเรกทอรี เว็บไซต์เหล่านี้จะมีไดเรกทอรีต่างๆให้เลือกมากมายรวมถึงประเด็นในเรื่องความปลอดภัยของระบบคอมพิวเตอร์
2) ระบบค้นหาข้อมูล (Search Engine) เป็นแหล่งข้อมูลที่ใช้เก็บรายชื่อและรายละเอียดต่างๆของเว็บไซต์ โดยผู้ค้นหาจะทำการป้อนคำสำคัญในการค้นหาข้อมูล
3) ตำราเรียนหรือหนังสือ เป็นอีกแหล่งข้อมูลที่มีประเด็นทางด้านความปลอดภัยของระบบคอมพิวเตอร์ ซึ่งสามารถนำประเด็นมาได้จากสารบัญของตำรานั้น
4) หลักสูตรต่างๆที่สอนในมหาวิทยาลัยและสถาบันการสอนเรื่องการรักษาความปลอดภับของระบบคอมพิวเตอร์ โดยพิจารณาถึงเนื้อหาที่ใช้สอน
5) การประชุมวิชาการ เป็นอีกแหล่งข้อมูลหนึ่งที่มีประชุมหรือสัมมนาเกี่ยวกับเรื่องการรักษาความปลอดภัยของระบบคอมพิวเตอร์ ซึ่งเป็นเวทีที่สะท้อนถึงประเด็นที่มีผลต่อสถานการณ์ปัจจุบัน
6) เว็บไซต์ทางด้านการรักษาความปลอดภัยของระบบคอมพิวเตอร์ เป็นอีกแหล่งข้อมูลหนึ่งที่ปัจจุบันคนส่วนใหญ่อาศัยแหล่งข้อมูลในการศึกษาเรื่องความปลอดภัยของระบบคอมพิวเตอร์

3.1.2. ค้นหาแหล่งข้อมูลย่อย

เป็นการค้นหาแหล่งข้อมูลภายใต้แหล่งข้อมูลหลักเพื่อใช้สำหรับหาประเด็นต่างๆที่เกี่ยวข้องกับการรักษาความปลอดภัยของระบบคอมพิวเตอร์ โดยการค้นหาจะใช้เว็บไซต์ Google ในการค้นหาเพราะเป็นเว็บไซต์ที่คนส่วนใหญ่นิยมใช้ (Google 54.86%, Yahoo 33.12%) [12] โดยการเลือกแหล่งข้อมูลย่อยแต่ละแหล่งข้อมูลจะต้องมีจำนวนประเด็นที่ปรากฏไม่ต่ำกว่า 10 ประเด็นเพราะจำนวนประเด็นของหมวดหมู่หลักจะต้องอยู่ระหว่าง 10 ถึง 16 ประเด็น (หัวข้อที่ 2.3.1) และเลือกจากเอกสารที่ถูกเรียงตามลำดับตรงตามคำสำคัญที่ป้อนลงไป (Ranked List) [48] ดังนี้

1) ไดเรกทอรีเวบ (Web directories) งานวิจัยนี้จะเลือกเอาเฉพาะแหล่งข้อมูลที่มีหมวดหมู่เป็นของตัวเอง และมีหมวดหมู่ของเรื่องการรักษาความปลอดภัยของระบบคอมพิวเตอร์ โดยการค้นหาจะใช้คำสำคัญ "Web Directory" เป็นคำสำคัญในการค้นหา
2) ระบบค้นหาข้อมูล (Search Engine) งานวิจัยนี้ได้เลือกเว็บไซต์ที่แสดงผลการค้นหาแบบคลัสเตอร์ลิ่ง (Clustering) คือการแสดงผลแบบลำดับชั้นซึ่งช่วยให้ผู้ค้นหาข้อมูลได้สะดวกและรวดเร็ว โดยการค้นหาจะใช้คำสำคัญ “Search Engine Clustering” เป็นคำสำคัญในการค้นหา
3) ตำราเรียนหรือหนังสือ งานวิจัยนี้จะเลือกหนังสือที่แต่งล่าสุดเพื่อให้ทันกับสถานการณ์ปัจจุบัน โดยการค้นหาจะใช้คำสำคัญ “Information Security Book” หรือ "Computer Security Book" เป็นคำสำคัญในการค้นหา

4) หลักสูตรต่างๆ งานวิจัยนี้จะเลือกหลักสูตรที่เปิดสอนในมหาวิทยาลัยและสถาบันการอบรมต่างๆที่เกี่ยวข้องกับเรื่องการรักษาความปลอดภัยของระบบคอมพิวเตอร์ และต้องเปิดสอนปีล่าสุด โดยการค้นหาจะใช้คำสำคัญ “Information Security Syllabus” เป็นคำสำคัญในการค้นหา
5) การประชุมวิชาการ การค้นหาจะใช้คำสำคัญ "Information Security Conference" เป็นคำสำคัญในการค้นหา และต้องทำการสัมมนาในปีปัจจุบัน
6) เว็บไซต์ทางด้านการรักษาความปลอดภัยของระบบคอมพิวเตอร์ การค้นหาจะใช้คำสำคัญ "Information Security Category" เป็นคำสำคัญในการค้นหา

3.1.3. เลือกเฉพาะประเด็นการรักษาความปลอดภัยของระบบคอมพิวเตอร์

ทำการหาประเด็นจากหมวดหมู่หลักของแหล่งข้อมูลทั้งหมด โดยมีแนวทางดังนี้

1) ตัดประเด็นที่ไม่ใช่เรื่องการรักษาความปลอดภัยของระบบคอมพิวเตอร์ เช่น Product and Tools Company and Organization เป็นต้น เพราะงานวิจัยนี้จะเลือกเอาประเด็นที่เกี่ยวข้องกับทฤษฎี เทคโนโลยี วิธีการรับมือหรือกระบวนการต่างๆที่เกี่ยวข้องกับด้านความปลอดภัยของระบบคอมพิวเตอร์
2) ตัดประเด็นที่เป็นชื่อผลิตภัณฑ์ออกไป เช่น Microsoft Symantec
3) เลือกเฉพาะประเด็นที่เป็นหมวดหมู่หรือหัวข้อหลักของแต่ละแหล่งข้อมูล แต่ถ้าหมวดหมู่หรือหัวข้อหลักเป็นประเด็นที่กว้างมากๆก็ให้พิจารณาถึงหมวดหมู่หรือหัวข้อย่อยอีกหนึ่งระดับ เช่น หนังสือให้เอาบทหลักแต่ถ้าถ้าบทหลักเป็นเรื่องกว้างให้ลงลึกไปอีก 1 ระดับ

3.1.4. ปรับชื่อประเด็น

การพิจารณาชื่อประเด็นสามารถนำเอาแนวทางในการตั้งชื่อจากหัวข้อ 2.3.2

1) รวมเป็นประเด็นเดียวกันถ้าชื่อที่แสดงมีความหมายเดียวกัน เช่น Network and Network Security
2) ถ้าชื่อประเด็นสามารถแบ่งออกเป็น 2 ชื่อได้ให้ทำการแบ่งออกเป็น 2 ประเด็น เช่น “Threats Analysis and Risk Management” เป็น “Threat Analysis” and “Risk Management”
3) ถ้าชื่อประเด็นไม่เหมือนกันของแต่ละแหล่งข้อมูล แต่มีความหมายเดียวกันให้ปรับเป็นชื่อเดียวกัน เช่น Security Assessment กับ Assessment ให้เปลี่ยนเป็น Assessment
4) ถ้าชื่อประเด็นนั้นเน้นไปเรื่องใดเรื่องหนึ่งให้ใช้ชื่อนั้นแทน เช่น Encryption Policy ให้เปลี่ยนเป็น Policy
5) ถ้าชื่อประเด็นเป็นชื่อเฉพาะให้หาชื่อที่เป็นคำกลาง เช่น Unix Windows Linux ใช้คำว่า Operating System
6) เปลี่ยนชื่อจากประเด็นที่เป็นภาษาไทยให้เป็นภาษาอังกฤษ

3.1.5. รวมประเด็นทุกแหล่งข้อมูล

ทำการรวมประเด็นจากทุกแหล่งข้อมูลเข้าด้วย

3.1.6. นับจำนวนแหล่งข้อมูลพี่พบของแต่ละประเด็น

ทำการนับจำนวนแหล่งข้อมูลที่กล่าวถึงประเด็นเดียวกัน

3.1.7. ตัดประเด็นที่มีความถี่เป็น 1

ตัดประเด็นที่มีความถี่เป็น 1 เพราะงานวิจัยจะเลือกเฉพาะประเด็นที่ได้รับความสนใจซึ่งก็คือประเด็นนั้นต้องมีแหล่งข้อมูลกล่าวถึงมากกว่า 1 ที่

3.1.8. ประมวลผลด้วยวิธี Cluster Analysis

งานวิจัยนี้ได้เลือกวิธี Cluster analysis เนื่องจากวิธีนี้ไม่จำเป็นต้องทราบจำนวนกลุ่มมาก่อน จากนั้นนำผลของการสำรวจข้อมูลที่ได้มาประมวลผลด้วยวิธีการ Cluster Analysis โดยใช้ความถี่เป็นตัวแปรในการพิจารณา

3.1.9. พิจารณาจำนวนประเด็น

ในการที่จะพิจารณาว่าจะมีจำนวนประเด็นในหมวดหมู่หลักเป็นเท่าไหร่นั้น อาจใช้แผนภาพ Dendogram มาพิจารณาในการแบ่งจำนวนกลุ่มข้อมูลโดยพิจารณาจากระยะห่าง แต่งานวิจัยนี้ใช้จำนวนประเด็นที่เหมาะสมในการแสดงข้อมูลบนหน้าแรกของเว็บไต์ (Top-level) นั้นก็คือ 10 ถึง 16 ประเด็นและใช้การแบ่งกลุ่ม (Cluster) มาร่วมพิจารณา

สถาบันวิทยบริการ
จุฬาลงกรณ์มหาวิทยาลัย

บทที่ 4

การจัดหมวดหมู่

บทนี้จะเป็นการนำเอากรรมวิธีจากบทที่ 3 มาเป็นขั้นตอนในการจัดหมวดหมู่ และนำผลการจัดหมวดหมู่ที่ได้มาเป็นประเด็นของหมวดหมู่หลักของงานวิจัยนี้ และนำมาเป็นแนวทางในการหาหมวดหมู่ย่อย (Second-level) โดยมีรายละเอียดของการจัดหมวดหมู่ดังนี้

4.1. การจัดหมวดหมู่หลัก

ขั้นตอนของการหาแหล่งข้อมูลงานวิจัยนี้ได้เลือกไว้แล้ว 6 ที่ตามที่ได้กล่าวไว้ใน 3.1.1. ดังนั้นจะเริ่มการจัดหมวดหมู่ตั้งแต่ขั้นตอนค้นหาแหล่งข้อมูลย่อย (หัวข้อ 3.1.2.)

4.1.1. ค้นหาแหล่งข้อมูลย่อย

จากแนวทางของการค้นหาแหล่งข้อมูลย่อยในหัวข้อ 3.1.2 สามารถหาแหล่งข้อมูลย่อยของแต่ละแหล่งข้อมูลหลักดังนี้

1) ไดเรกทอรีเวบ (Web directories) มีแหล่งข้อมูลย่อยดังนี้
   - DMOZ[30]
   - Yahoo [47]
   - Looksmart [23]
   - Galaxy [22]
   - Best of The Web [3]
2) ระบบค้นหาข้อมูล (Search Engine) มีแหล่งข้อมูลย่อยดังนี้
   - Vivisimo [44]
   - Infonetware [16]
   - iBoogie [14]
   - Killerinfo [20]
   - Wisenut [46]
3) ตำราเรียนหรือหนังสือ มีสารบัญของหนังสือที่ใช้เป็นแหล่งข้อมูลย่อยดังนี้
   - Secrets and Lies: Digital Security in a Networked World [5]
   - Computer Security: Art and Science [24]
   - Cryptography and Network Security: Principles and Practice (3rd Edition) [37]
   - Corporate Computer and Network Security [31]
   - The CISSP Prep Guide: Mastering the CISSP and ISSEP Exams, 2nd Edition [32]
4) หลักสูตรต่างๆ มีแหล่งข้อมูลย่อยดังนี้
   - Cyber Security Group Training Conference (CERIAS Purdue) [6]

สถาบันวิทยบริการ
จุฬาลงกรณ์มหาวิทยาลัย

- Network and Computer Security (MIT) [26]
- 07017311 Computer Security (สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง) [7]
- Csci 4407- Networks Security (Minessota) [43]
- Security Essentials Course Topics (SANS) [33]

5) การประชุมวิชาการ มีแหล่งข้อมูลย่อยดังนี้
   - IEEE Symposium on Security and Privacy [15]
   - Annual Computer Security Application Conference [2]
   - European Symposium on Research in Computer Security (ESORICS) [10]
   - International Conference on Information and Communications Security [18]
   - The Internet Security Conference [39]
6) เว็บไซต์ทางด้านการรักษาความปลอดภัยของระบบคอมพิวเตอร์ งานวิจัยจะให้น้ำหนักกับเว็บไซต์มากกว่าแหล่งข้อมูลอื่น เพราะแหล่งข้อมูลประเภทนี้จะเป็นแหล่งข้อมูลที่คอยรับมือกับปัญหาทางด้านความปลอดภัยของระบบคอมพิวเตอร์ การใช้วิธีการค้นหาแหล่งข้อมูลย่อยจาก Search Engine อาจทำให้ได้ข้อมูลไม่ตรงนัก ซึ่งอาจเกิดจากคำสำคัญ (Keyword) ในการค้นหาไม่ตรงกับเว็บไซต์ที่เผยแพร่อยู่ในปัจจุบัน ดังนั้นผู้วิจัยจึงได้ขอคำแนะนำจากอาจารย์ หอมเอนก (อาจารย์ที่ปรึกษาร่วม) โดยท่านได้แนะนำเว็บไซต์ที่หน่วยงานและผู้เชี่ยวชาญส่วนใหญ่เข้าศึกษาและหาวิธีการรับมือกับปัญหาทางด้านความปลอดภัยของระบบคอมพิวเตอร์ ซึ่งมีแหล่งข้อมูลย่อยดังนี้
   - InfosysSec [17]
   - SecurityFocus [36]
   - The SANS Institute [40]
   - CISSP [8]
   - NIST [27]
   - CERIAS Perdue [38]
   - Bitpipe [4]
   - ITSecurity [41]
   - Network Security Library [45]
   - SC Magazine [34]

จากนั้นทำตามขั้นตอนในหัวข้อที่ 3.1.3 ถึง 3.1.6 ในบทที่ 3 จะได้ผลลัพธ์ทั้งหมดในภาคผนวก ก และสามารถสรุปจำนวนประเด็นของหมวดหมู่ในแหล่งข้อมูลต่างๆในตารางที่ 4-1 และเมื่อทำการตัดประเด็นที่มีความถี่เท่ากับ 1 จะได้ผลดังตารางที่ 4-2

ตารางที่ 4-1: เปรียบเทียบจำนวนหัวข้อในแต่ละระดับ

Source	Top level categories	Second Level Categories	All categories	Depth of hierarchy
Web directories				
DMOZ [30]	15	106	283	5
Yahoo [47]	24	78	180	4
LookSmart [23]	12	31	62	3
Best of The Web [3]	10	-	10	-
Galaxy [22]	17	-	20	-
Search Engine				
Vivisimo [44]	46	56	118	3
Infonetware [16]	25	0	25	-
WiseNut [46]	21	0	21	-
iBoogie [14]	48	104	208	3
KillerInfo [20]	30	29	59	1
Books				
Secrets and Lies: Digital Security in a Networked World [5]	20	-	20	-
Computer Security: Art and Science [24]	18	-	18	-
Cryptography and Network Security [37]	20	-	20	-
Corporate Computer and Network Security [31]	13	-	13	-
The CISSP Prep Guide: Mastering the CISSP and ISSEP Exams, 2nd Edition [32]	18	-	18	-
Courses				
Cyber Security Group Training Conference[6]	10	-	10	-
Network and Computer Security [26]	18	-	18	-
07010311 Computer Security [7]	15	-	15	-
Csci 4407- Networks Security [43]	20	-	20	-
SANS Security Essentials Course Topics [33]	19	-	19	-
Conference				
IEEE Symposium on Security and Privacy [15]	23	-	23	-
Annual Computer Security Application Conference [2]	15	-	15	-
European Symposium on Research in Computer Security (ESORICS) [10]	42	-	42	-
International Conference on Information and Communications Security [18]	27	-	27	-
The Internet Security Conference [39]	19	-	19	-
Web site				
InfosysSec [17]	42	-	42	-
SecurityFocus [36]	20	-	20	-
The SANS Institute [40]	47	-	47	-
CISSP [8]	12	-	12	-
NIST [27]	23	-	23	-
CERIAS [38]	22	-	22	-
Bitpipe [4]	35	-	35	-
ITSecurity [41]	20	-	20	-
Network Security Library [45]	29	-	29	-
SC Magazine [34]	22	-	22	-

ตารางที่ 4-2: การจัดลำดับประเด็นการรักษาความปลอดภัยของแต่ละแหล่งข้อมูล

No	Topics	Fequency	Web Directories					Search Engines					Books					Courses					Conferences					Websites									
			[30]	[47]	[23]	[3]	[22]	[44]	[16]	[46]	[14]	[20]	[5]	[24]	[37]	[31]	[32]	[6]	[26]	[7]	[43]	[33]	[15]	[2]	[10]	[18]	[39]	[17]	[36]	[40]	[8]	[27]	[38]	[50]	[41]	[45]	[34]
1	Cryptography	28		X	X	X		X			X	X	X	X	X	X	X	X	X	X	X			X	X	X		X	X	X	X	X	X	X	X	X	X
2	Intrusion Detection Systems	21	X		X		X	X						X				X	X	X	X	X	X		X	X	X	X				X	X	X	X	X	
3	Network Security	21						X	X	X	X	X	X	X	X		X			X	X	X	X		X	X		X			X		X	X	X		X
4	Firewalls	20	X	X		X	X				X				X	X		X	X	X		X		X	X		X	X		X			X		X	X	X
5	Policy	20	X	X		X	X		X		X	X	X	X						X	X	X						X		X		X	X	X	X	X	X
6	Authentication and Identification	18	X			X							X	X	X				X				X	X	X	X	X	X	X	X		X		X		X	X
7	Viruses Worms and Trojan Malicious Code	17		X	X	X		X			X			X	X				X	X	X		X					X		X			X	X	X	X	
8	Email	14		X		X									X	X			X	X	X						X	X		X			X	X	X		X
9	Privacy	14		X				X		X	X									X			X		X	X	X	X		X			X		X	X	
10	Access Control	13												X		X	X				X		X	X	X				X		X	X			X	X	X
11	Biometrics	13	X		X	X	X	X										X					X	X		X		X						X	X		X
12	Risk Assessment and Analysis	13		X				X	X				X				X		X	X		X				X		X		X				X	X		
13	e-Commerce	12			X											X			X		X			X	X	X	X		X	X			X		X		
14	Operating System	12		X			X			X									X	X		X					X	X	X	X			X			X	
15	Virtual Private Networks	11	X		X	X	X									X				X							X	X		X						X	X
16	World Wide Web Security	10		X							X				X				X	X	X	X											X	X		X	
17	Anonymity and Pseudonymity	9		X		X		X				X											X		X	X		X					X				
18	Auditing	9												X								X	X	X				X	X	X					X	X	
19	Incident response and Handling	9						X		X	X	X				X						X				X			X	X							
20	Internet Security	9	X			X	X		X	X	X																	X			X			X			
21	Certification and Accreditation (C&A)	8											X				X	X						X		X		X				X			X		
22	Hacking and Hackers	8	X	X		X		X			X																X	X		X							
23	Information Warfare	8		X																	X		X	X			X	X	X					X		
24	Law, Investigation, and Ethics	8															X			X							X	X		X		X	X		X	
25	Anti Virus	7	X				X			X	X										X														X	X
26	Digital Signatures	7		X	X	X									X				X	X	X															
27	PGP – Pretty Good Privacy	7		X	X			X												X		X					X					X				
28	Physical Security	7						X									X			X							X		X	X		X				
29	System Security	7						X	X		X				X									X								X	X				
30	Threat	7						X					X							X	X		X						X		X						
31	Wireless Security	7																X								X			X		X	X	X			X
32	Denial of Service	6																					X	X	X		X	X					X				
33	Disaster Recovery	6															X			X							X		X				X		X		
34	Forensics	6																						X		X	X			X						X	X
35	Protocols	6						X															X		X	X		X		X							
36	Security Management	6								X															X						X			X		X	X
37	Security Models	6															X		X						X	X				X	X						
38	Smart Cards	6																				X		X	X		X				X						X
39	Steganography	6		X	X																X			X			X		X								
	…																																				
97	Software Engineering	2																										X							X	
98	trust models and trust Management	2																							X	X											
99	Watermarking	2																								X		X									

จากตารางที่ 4-2 จะได้ผลของความถี่ของประเด็นที่ปรากฏในแหล่งข้อมูลทั้งหมด จากนั้นจะทำการประมวลด้วยวิธีการ Cluster Analysis ตามหัวข้อที่ 3.1.8 ซึ่งจะนำเอาข้อมูลที่ได้มาทำการแบ่งกลุ่มข้อมูลออกเป็นกลุ่มย่อย โดยใช้วิธี Hierarchical Cluster

Analysis เพราะมีประเด็นน้อยกว่า 200 และใช้ความถี่เป็นตัวแปรในการแบ่งกลุ่มเนื่องจากต้องการพิจารณาถึงกลุ่มของประเด็นที่กำลังได้รับความนิยมหรือความสนใจ

งานวิจัยนี้ได้ใช้โปรแกรมสำเร็จรูป SPSS เวอร์ชัน 11.5 ซึ่งเป็นโปรแกรมที่นิยมใช้ในการวิเคราะห์ข้อมูลทางสถิติ ซึ่งสามารถประมวลผลโดยใช้วิธี Cluster Analysis ได้ โดยในงานวิจัยนี้ได้เลือก Between-groups เป็นวิธีการรวมกลุ่มและใช้ Square Euclidean distance เป็นวิธีการวัดระยะห่าง จากการประมวลผลจะได้ดังตารางที่ 4-3 Proximity Matrix ตารางที่ 4-4 Agglomeration Schedule และรูปที่ 4-1 Dendogram

ตารางที่ 4-3: Proximity Matrix

Proximity Matrix									
Case	Squared Euclidean Distance								
	1:Cryptography	2:Intrusion Detection	3:Network Security	4:Firewalls	⋮	11:Biometrics	12:Risk Assessment and	⋮	99:Watermarking
1:Cryptography	0	49	49	64		225	225		676
2:Intrusion Detection	49	0	0	1		64	64		361
3:Network Security	49	0	0	1		64	64		361
4:Firewalls	64	1	1	0		49	49		324
5:Policy	64	1	1	0		49	49		324
6:Authentication and	100	9	9	4		25	25		256
7:Viruses Worms and Trojan	121	16	16	9		16	16		225
8:Email	196	49	49	36		1	1		144
9:Privacy	196	49	49	36		1	1		144
10:Access Control	225	64	64	49		0	0		121
11:Biometrics	225	64	64	49		0	0		121
12:Risk Assessment and	225	64	64	49		0	0		121
13:e-Commerce	256	81	81	64		1	1		100
14:Operating System	256	81	81	64		1	1		100
15:Virtual Private Network	289	100	100	81		4	4		81
16:World Wide Web Security	324	121	121	100		9	9		64
17:Anonymity and Pseudo	361	144	144	121		16	16		49
18:Auditing	361	144	144	121		16	16		49
19:Incident response an	361	144	144	121		16	16		49
20:Internet Security	361	144	144	121		16	16		49
…									
98:trust models and trust Management	676	361	361	324		121	121		0
99:Watermarking	676	361	361	324		121	121		0

จากตารางที่ 4-3 Proximity Matrix จะแสดงถึงระยะห่างแต่ละคู่โดยนำเอาความถี่มาเข้าสูตรการคำนวณระยะห่าง Square Euclidean distance ซึ่งสามารถนำมาใช้ในการพิจารณาในการรวมกลุ่มได้ เช่น ประเด็น Cryptography และ ประเด็น Watermarking ห่างกันเท่ากับ 676 ขณะที่ ประเด็น Cryptography และ ประเด็น Intrusion Detection ห่างกันเพียง 49 ดังนั้นควรจัดให้ ประเด็น Cryptography และประเด็น Intrusion Detection ให้อยู่กลุ่มเดียวกัน ในขณะเดียวกันควรจัดให้ ประเด็น Cryptography และประเด็น Watermarking อยู่ต่างกลุ่มกัน

ตารางที่ 4-4 Agglomeration Schedule

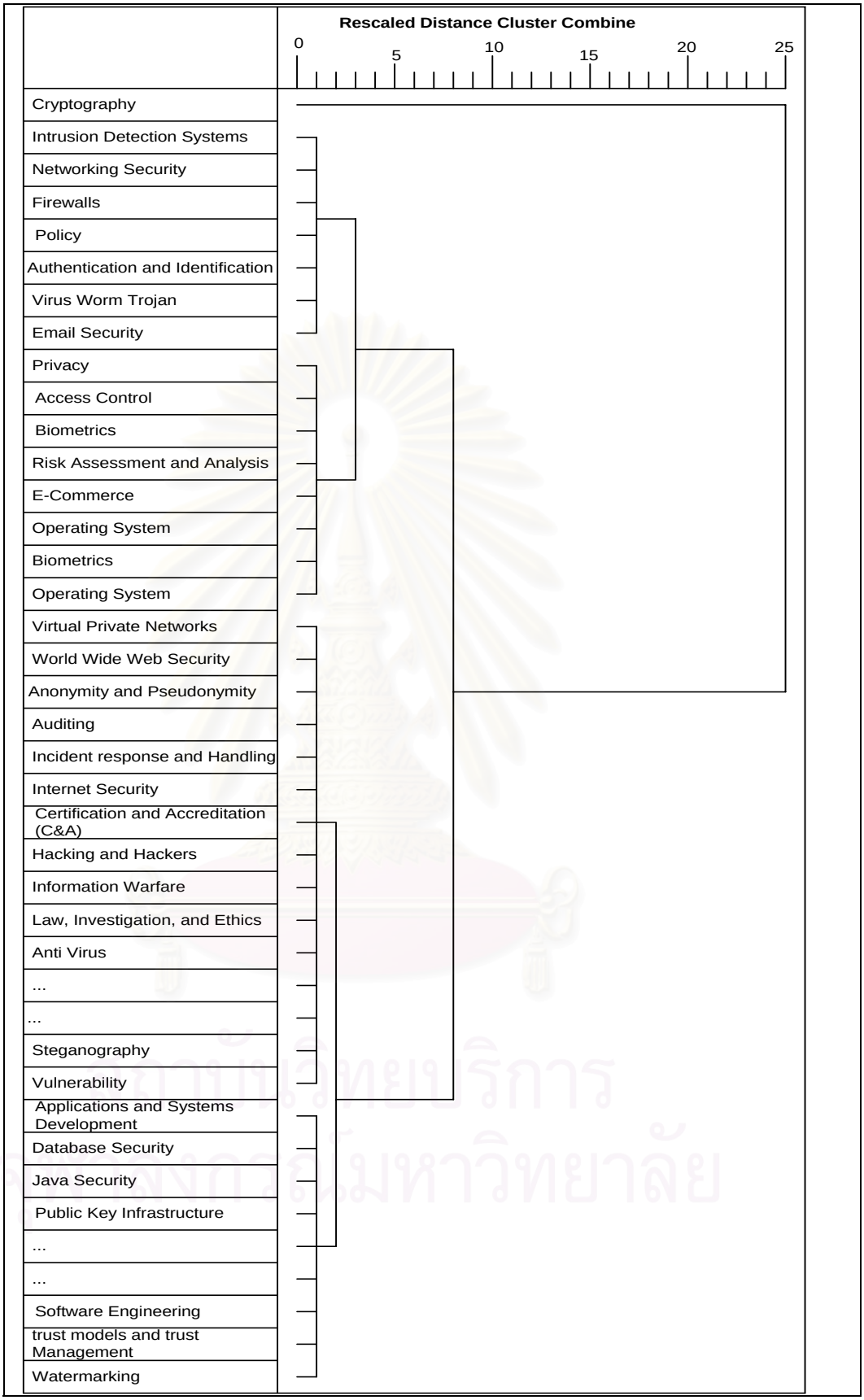
Agglomeration Schedule						
Stage	Cluster Combined		Coefficients	Stage Cluster First Appears		Next Stage
	Cluster 1	Cluster 2		Cluster 1	Cluster 2	
1	98	99	0	0	0	2
2	73	98	0	0	1	4
3	96	97	0	0	0	4
4	73	96	0	2	3	6
5	94	95	0	0	0	6
6	73	94	0	4	5	8
7	92	93	0	0	0	8
8	73	92	0	6	7	10
9	90	91	0	0	0	10
10	73	90	0	8	9	12
11	88	89	0	0	0	12
12	73	88	0	10	11	14
13	86	87	0	0	0	14
14	73	86	0	12	13	16
15	84	85	0	0	0	16
16	73	84	0	14	15	18
17	82	83	0	0	0	18
18	73	82	0	16	17	20
19	80	81	0	0	0	20
20	73	80	0	18	19	22
21	78	79	0	0	0	22
22	73	78	0	20	21	24
23	76	77	0	0	0	24
24	73	76	0	22	23	26
25	74	75	0	0	0	26
26	73	74	0	24	25	82
27	71	72	0	0	0	28
	…					
95	15	41	23.29204694	93	91	97
96	2	8	45.07142857	94	90	97
97	2	15	155.5520362	96	95	98
98	1	2	514.8673469	0	97	0

จากตารางที่ 4-4 Agglomeration Schedule แสดงถึงการรวมกลุ่มของประเด็นต่างๆ ในแต่ละ Stage จะบอกว่ามีการรวมกลุ่มประเด็นคู่ใดบ้างให้อยู่กลุ่มเดียวกัน เช่น

Stage ที่ 1 จะจัดให้ประเด็นที่ 98 และประเด็นที่ 99 อยู่ในกลุ่มเดียวกัน เนื่องจากประเด็นที่ 98 และ 99 มีระยะห่างที่สั้นที่สุด ซึ่งเท่ากับ 0 และค่า Next Stage ใน column สุดท้ายเท่ากับ 2 หมายถึงกลุ่มหรือ cluster ที่มีประเด็นที่ 98 และ 99 จะรวมกับประเด็นอื่นต่อไปใน stage ที่ 2

Stage ที่ 2 มีการจัดให้ประเด็นที่ 73 และประเด็น ที่ 98 ให้อยู่ในกลุ่มหรือ cluster เดียวกัน ซึ่งประเด็นที่ 73 และประเด็นที่ 98 มีระยะห่างเท่ากับ 0 โดยที่ประเด็นที่ 98 มาจาก Stage ที่ 1 และกลุ่มที่มีประเด็นที่ 73 และประเด็นที่ 98 อยู่จะรวมกับ case อื่นอีกใน stage ที่ 4

ทำเช่นนี้ไปเรื่อยๆจนถึง Stage ที่ 98 จะเป็นการรวมทุกประเด็นอยู่ในกลุ่มเดียวกัน ซึ่งผลการรวมกลุ่มสามารถดูได้ที่รูปที่ 4-1 Dendogram และตารางที่ 4-5 การแบ่งกลุ่ม การแบ่งกลุ่มด้วย Dendogram ทำได้โดยเลือกระยะห่างระหว่างกลุ่มที่ต้องการแบ่ง ซึ่งค่าที่อยู่ในภาพจะเป็นค่าที่แปลงแล้ว (Rescale)



รูปที่ 4-1: Dendogram using Average Linkage

ตารางที่ 4-5 แสดงการจัดกลุ่มของหัวข้อหลักของทุกแหล่งข้อมูล

ลำดับ	ประเด็น	ความถี่	Cluster								
			2	3	4	5	6	7	8	9	10
1	Cryptography	28	1	1	1	1	1	1	1	1	1
2	Intrusion Detection Systems	21	2	2	2	2	2	2	2	2	2
3	Network Security	21	2	2	2	2	2	2	2	2	2
4	Firewalls	20	2	2	2	2	2	2	2	2	2
5	Policy	20	2	2	2	2	2	2	2	2	2
6	Authentication and Identification	18	2	2	2	2	3	3	3	3	3
7	Viruses Worms and Trojan Malicious Code	17	2	2	2	2	3	3	3	3	3
8	Email	14	2	2	3	3	4	4	4	4	4
9	Privacy	14	2	2	3	3	4	4	4	4	4
10	Access Control	13	2	2	3	3	4	4	4	4	5
11	Biometrics	13	2	2	3	3	4	4	4	4	5
12	Risk Assessment and Analysis	13	2	2	3	3	4	4	4	4	5
13	e-Commerce	12	2	2	3	3	4	4	4	4	5
14	Operating System	12	2	2	3	3	4	4	4	4	5
15	Virtual Private Networks	11	2	3	4	4	5	5	5	5	6
16	World Wide Web Security	10	2	3	4	4	5	5	5	5	6
17	Anonymity and Pseudonymity	9	2	3	4	4	5	5	6	6	7
18	Auditing	9	2	3	4	4	5	5	6	6	7
19	Incident response and Handling	9	2	3	4	4	5	5	6	6	7
20	Internet Security	9	2	3	4	4	5	5	6	6	7
21	Certification and Accreditation (C&A)	8	2	3	4	4	5	5	6	6	7
22	Hacking and Hackers	8	2	3	4	4	5	5	6	6	7
23	Information Warfare	8	2	3	4	4	5	5	6	6	7
24	Law, Investigation, and Ethics	8	2	3	4	4	5	5	6	6	7
25	Anti Virus	7	2	3	4	4	5	6	7	7	8
26	Digital Signatures	7	2	3	4	4	5	6	7	7	8
27	PGP - Pretty Good Privacy	7	2	3	4	4	5	6	7	7	8
28	Physical Security	7	2	3	4	4	5	6	7	7	8
29	System Security	7	2	3	4	4	5	6	7	7	8
30	Threat	7	2	3	4	4	5	6	7	7	8
31	Wireless Security	7	2	3	4	4	5	6	7	7	8
32	Denial of Service	6	2	3	4	4	5	6	7	7	8
	…										
97	Software Engineering	2	2	3	4	5	6	7	8	9	10
98	trust models and trust Management	2	2	3	4	5	6	7	8	9	10
99	Watermarking	2	2	3	4	5	6	7	8	9	10

ต่อไปเป็นขั้นตอนของการพิจารณาจำนวนประเด็นที่จะเป็นหมวดหมู่หลักของงานวิจัยนี้ โดยทำตามขั้นตอนที่ 3.1.9 ในบทที่ 3 การพิจารณาว่าควรจะเอากี่กลุ่มหรือกี่ประเด็นเป็นหมวดหมู่หลักนั้น ทำได้โดยพิจารณาว่ามีช่วงแบ่งกลุ่มที่ประเด็นใดในช่วงประเด็นที่ 10 ถึง 16 โดยพิจารณาเรียงลำดับตาม Cluster เช่น ถ้าพิจารณาที่ Cluster ที่ 2 จะพบว่าไม่มีช่วงการแบ่งข้อมูล ให้พิจารณาใน Cluster ถัดไปคือ Cluster ที่ 3 จะพบว่ามีช่วงแบ่งกลุ่มที่ประเด็นที่ 14 ซึ่งจะได้กลุ่มข้อมูลที่ 1 และ 2 ซึ่งมีจำนวนรวมกันแล้วอยู่ระหว่าง 10 ถึง 16 ดังนั้นประเด็นที่อยู่ในหมวดหมู่หลักของงานวิจัยนี้คือ Access Control, Authentication and Identification, Biometrics, Cryptography, e-Commerce, Email, Firewalls, Intrusion Detection Systems, Network Security, Operating System, Policy, Privacy, Risk Assessment and Analysis, Viruses Worms and Trojan Malicious Code

4.2. การจัดหมวดหมู่ย่อย

จากการสำรวจข้อมูลที่ผ่านมาจะพบว่าข้อมูลที่เป็นหมวดหมู่ย่อยของแต่ละแหล่งข้อมูลจะมีประเด็นอยู่น้อยมาก ซึ่งส่วนใหญ่จะอยู่ใน Web Directories ดังนั้นงานวิจัยนี้จะทำการสำรวจข้อมูลจากระบบค้นหาข้อมูล (Search Engine) โดยใช้คำสำคัญคือชื่อประเด็นต่างๆของหมวดหมู่หลักมาทำการค้นหาข้อมูลหรือเอกสารที่เกี่ยวข้อง การทำเช่นจะทำให้ทราบถึงประเด็นอื่นๆที่มีความสัมพันธ์กับประเด็นที่ใช้ในการค้นหา

งานวิจัยนี้จะใช้ Vivisimo ช่วยในการค้นหาข้อมูลเพราะผลของการค้นหาจะมีการจัดหมวดหมู่หรือจัดกลุ่มให้ โดยการค้นหาจะให้ Search Engine เข้าไปค้นหาทีละแหล่งข้อมูลเพราะต้องการให้ Search Engine จัดกลุ่มของผลลัพธ์ของแต่ละแหล่งข้อมูล เพื่อให้เกิดความหลากหลายต่อผลลัพธ์ของแต่ละแหล่งข้อมูลทำให้เกิดความชัดเจนในหาประเด็นที่จะอยู่หมวดหมู่ย่อยของประเด็นในหมวดหมู่หลัก โดยแหล่งข้อมูลที่ทำการค้นหาคือ MSN, Netscape, Lycos, Looksmart และ DMOZ

ขั้นตอนของการค้นหาเพื่อหาหมวดหมู่ย่อยของงานวิจัยสามารถสรุปได้ดังนี้

1) ทำการค้นหาโดยใช้ชื่อประเด็นในหมวดหมู่หลักเป็นคำสำคัญในการค้นหา ถ้าชื่อประเด็นเป็นคำทั่วไปที่สามารถใช้ในเรื่องอื่นๆได้ให้เพิ่มคำสำคัญ "Security" ช่วยในการค้นหาด้วย เช่น ประเด็น Policy ผลลัพธ์ของการค้นหาจะแสดงดังรูปที่ 4-2
2) พิจารณาเฉพาะผลลัพธ์ระดับแรกเพราะกำลังทำการค้นหาหมวดหมู่ย่อยรองจากหมวดหมู่หลัก
3) ตัดประเด็น Computer, Security และชื่อประเด็นของหมวดหมู่หลัก และเลือกเฉพาะหมวดหมู่ที่เกี่ยวข้องกับการรักษาความปลอดภัย
4) ใช้จำนวนเอกสารที่พบเป็นตัวแปรความถี่ของแต่ละประเด็น
5) ปรับชื่อประเด็นให้เป็นคำเฉพาะ เช่น LDAP authentication เป็น LDAP
6) รวมประเด็นทุกแหล่งข้อมูล
7) รวมจำนวนเอกสารหรือความถี่ของทุกแหล่งข้อมูลและเรียงลำดับประเด็นตามตัวแปรความถี่
8) เข้ากรรมวิธี Cluster Analysis
9) พิจารณาจำนวนประเด็นที่เหมาะสม

จากขั้นตอนข้างต้นจะพบว่าคล้ายกับวิธีการหมวดหมู่หลัก จะต่างกันตรงที่การสำรวจข้อมูลและตัวแปรที่ใช้

สถาบันวิทยบริการ
จุฬาลงกรณ์มหาวิทยาลัย

รูปที่ 4-2 แสดงผลการค้นหาจาก Vivisimo

จากกรรมวิธีข้างต้นจะได้ข้อมูลที่จะนำมาเป็นหมวดหมู่ย่อยและมีจำนวนความถี่ประกอบ จากนั้นนำผลที่ได้เข้าวิธีการจัดกลุ่มโดยใช้วิธีการ Cluster analysis

ในวิทยานิพนธ์ฉบับนี้ได้ยกตัวอย่างการหาหมวดหมู่ย่อยของเรื่อง Authentication ซึ่งผลจากการค้นหาและกระทำตามกรรมวิธีข้างต้นและได้ผลของการทำ Cluster Analysis ด้วยเทคนิค Hierarchical Cluster Analysis ดังตารางที่ 4-6

ตารางที่ 4-6 แสดงการจัดกลุ่มของประเด็นย่อยต่อหัวข้อหลัก Authentication

ลำดับ	ประเด็น	ความถี่	Cluster								
			2	3	4	5	6	7	8	9	10
1	Password	41	1	1	1	1	1	1	1	1	1
2	Biometric	24	2	2	2	2	2	2	2	2	2
3	Network Authentication	24	2	2	2	2	2	2	2	2	2
4	Digital Signatures	18	2	2	3	3	3	3	3	3	3
5	RFC	18	2	2	3	3	3	3	3	3	3
6	Kerberos	15	2	2	3	3	4	4	4	4	4
7	Encryption	9	2	3	4	4	5	5	5	5	5
8	Fingerprint	8	2	3	4	4	5	5	5	6	6
9	Smart card	6	2	3	4	5	6	6	6	7	7
10	Access Controls	6	2	3	4	5	6	6	6	7	7
11	RADIUS	6	2	3	4	5	6	6	6	7	7
12	Single sign	5	2	3	4	5	6	6	7	8	8
13	Two-factor authentication	5	2	3	4	5	6	6	7	8	8
14	Java	5	2	3	4	5	6	6	7	8	8
15	NTLM Authentication	4	2	3	4	5	6	6	7	8	9
16	Privacy	4	2	3	4	5	6	6	7	8	9
17	Intrusion detection	3	2	3	4	5	6	7	8	9	10
18	PPP	2	2	3	4	5	6	7	8	9	10
19	Remote Acess Network	2	2	3	4	5	6	7	8	9	10

ต่อไปเป็นขั้นตอนของการพิจารณาจำนวนประเด็นของหมวดหมู่ Authentication จะพิจารณาเหมือนกับหมวดหมู่หลัก จากตารางที่ 4-6 จะพบว่าประเด็นที่ 16 จะเป็นช่วงที่แบ่งกลุ่ม ซึ่งได้จำนวนประเด็นอยู่ระหว่าง 10 ถึง 16 ประเด็นใน Cluster 7 ที่ ทำให้ได้กลุ่มข้อมูลที่ 1 ถึง 6 เป็นประเด็นย่อยของหมวดหมู่ Authentication ดังนี้ Access Controls, Biometric, Digital Signatures, Encryption, Fingerprint, Java, Kerberos, Network Authentication, NTLM Authentication, Password, Privacy, RADIUS, RFC, Single sign, Smart card, Two-factor authentication

ส่วนหมวดหมู่อื่นๆก็ให้ทำในลักษณะเดียวกันกับ Authentication โดยผลจะอยู่ที่ภาคผนวก ข

สถาบันวิทยบริการ
จุฬาลงกรณ์มหาวิทยาลัย

บทที่ 5

ผลการจัดหมวดหมู่

5.1. ผลการจัดหมวดหมู่

จากผลการหาประเด็นเพื่อนำมาเป็นหมวดหมู่หลักของงานวิจัยนี้ในหัวข้อที่ 4.1 จะได้หมวดหมู่หลักทั้งหมด 16 ประเด็น แต่จากตารางที่ 4-5 จะพบว่ามีประเด็นทั้งหมด 99 ประเด็น ซึ่งยังเหลืออยู่ 85 ประเด็น จึงต้องมีประเด็น Miscellaneous ขึ้นมาเพื่อรองรับกับประเด็นที่ยังเหลืออยู่ ดังนั้นสามารถสรุปประเด็นหรือหัวข้อหลักของการรักษาความปลอดภัยคอมพิวเตอร์ทั้งหมด 15 ประเด็นดังนี้

1) Access Control
2) Authentication and Identification
3) Biometrics
4) Cryptography
5) e-Commerce
6) Email Security
7) Firewalls
8) Intrusion Detection Systems
9) Network Security
10) Operating System
11) Policy
12) Privacy
13) Risk Assessment and Analysis
14) Viruses Worms and Trojan Malicious Code
15) Miscellaneous

จากตารางที่ 4-1 จะพบว่าค่าเฉลี่ยของจำนวนประเด็นของหมวดหมู่หลักทุกแหล่งข้อมูลคือ 23.34 และค่า S.D. คือ 10.52 งานวิจัยนี้มีจำนวน 15 ประเด็นซึ่งเป็นค่าที่น้อยกว่าแหล่งข้อมูลอื่นๆ แต่ถ้าพิจารณาจากจำนวนความถี่ของประเด็นที่ได้เลือกมาเป็นหมวดหมู่หลักของงานวิจัยนี้ต่อประเด็นทั้งหมดของแหล่งข้อมูลที่ไปสำรวจมาจะพบว่า งานวิจัยนี้ใช้จำนวนประเด็น 14 ประเด็นเป็นหมวดหมู่ซึ่งคิดเป็นร้อยละ 10 ของประเด็นทั้งหมดแต่ประเด็นทั้ง 14 ประเด็นนั้นจะมีความสำคัญหรือความสนใจจากแหล่งข้อมูลทั้งหมดถึง 40%

และจากวิธีการหาประเด็นเพื่อมาเป็นหมวดหมู่ย่อยในหัวข้อที่ 4.2 ซึ่งงานวิจัยนี้ได้ทำกับทุกประเด็นในหมวดหมู่หลักยกเว้น Miscellaneous สามารถดูผลการจัดกลุ่มได้จากภาคผนวก ข

จากการจัดหมวดหมู่ที่ผ่านกระบวนข้างต้นซึ่งจะมีทั้งที่เป็นหัวข้อหลักและหัวข้อย่อยภายใต้หัวข้อหลัก ผลการจัดหมวดหมู่ทั้งหมดสามารถแสดงได้ดังตารางที่ 5-1 ซึ่งจะนำผลที่ได้มาจัดทำข้อมูลที่แสดงบนหน้าเว็บไซต์

ตารางที่ 5-1 แสดงหัวข้อหลักและหัวข้อย่อย

หัวข้อหลัก	หัวข้อย่อย
Access Control	Access Control Lists, Authentication, Barcode, Camera & CCTV, Detection, Door entry, Fingerprint Recognition, Firewall, Htaccess, Network, Port, Role Based Access Control, Smart Card & Plastic Card, XML
Authentication and Identification	Access Controls, Biometric, Digital Signatures, Encryption, Fingerprint, Java, Kerberos, Network Authentication, NTLM Authentication, Password, Privacy, RADIUS, RFC, Single sign, Smart card, Two-factor authentication
Biometrics	Access Control, Authentication, CCTV & Cameras, Crypto-Gram, Face Recognition, Finger Print, Hand Geometry, Information security, Iris, Privacy, Smart Cards, Voice biometrics, XML
Cryptography	Digital Signatures, Information Security, Java Cryptography, Key Cryptography, Network Security, PGP, Policy, Privacy, Quantum, Steganography
e-Commerce	Digital Certificates, Hosting, Internet Security, Law, Network Security, PKI, Programming, Seal, Security Audit, SSL, Web Hosting
Email Security	Anonymous, Anti-Spam, Anti-Virus, Encryption, Filtering, Information Security, MIME, Network Security, PGP, Policy, Privacy, Spam, Virus
Firewalls	Anti-Virus, Filtering, IDS, Information security, Internet Security, Linux, Network, Personal Firewalls, Router, Scan Port, VPN, Windows
Intrusion Detection Systems	Audit, Detection signatures, Firewall, Hackers & Hacking, Honeypot, Information Systems, Internet Security, Network security, Scanner, Snort, Vulnerability
Network Security	Anti Virus & Virus, Encryption, Firewalls, Hacking, Information security, Internet Security, Intrusion detection, Penetration Testing, Policy, Scanning, Wireless Network
Operating System	Access control, Audit, Exploits, FreeBSD, Hackers & Hacking, Information Security, Linux, Mac, Microsoft, Network Security, Patches, Security Checklist, Solaris, Unix, Windows
Policy	Access Control, HIPAA, Information security, Law, Network Security, Privacy, Rfc 2196, Windows
Privacy	Anonymous and Anomymity, Cookies, Digital Privacy, GNU Privacy, HIPAA, Internet Privacy, Law, P3P, Personal privacy, PGP, Privacy Policy, Privacy Statement, Rights
Risk Assessment and Analysis	HIPAA, Information Security, Internet Security, Investigation, Network Security, Privacy, Security Audits, Threat, Virus, Vulnerability
Viruses Worms and Trojan (Malicious Code)	Anti-Trojan, Anti-Virus, Firewall, Information Security, Internet Security, Network Security, Patch, Privacy, Security Scan, Vulnerabilities

สถาบันวิทยบริการ
จุฬาลงกรณ์มหาวิทยาลัย

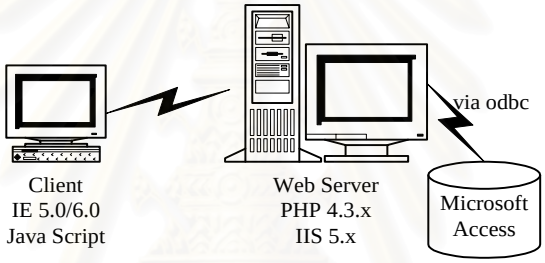
บทที่ 6

การออกแบบระบบต้นแบบ

งานวิจัยนี้ได้ทำการออกแบบระบบต้นแบบเพื่อนำเสนอเรื่องประเด็นการรักษาความปลอดภัยของระบบคอมพิวเตอร์ โดยใช้ผลของการจัดหมวดหมู่ที่ได้จากบทที่ 5 มาเป็นข้อมูลที่นำเสนอในระบบต้นแบบนี้ โดยมีรายละเอียดดังนี้

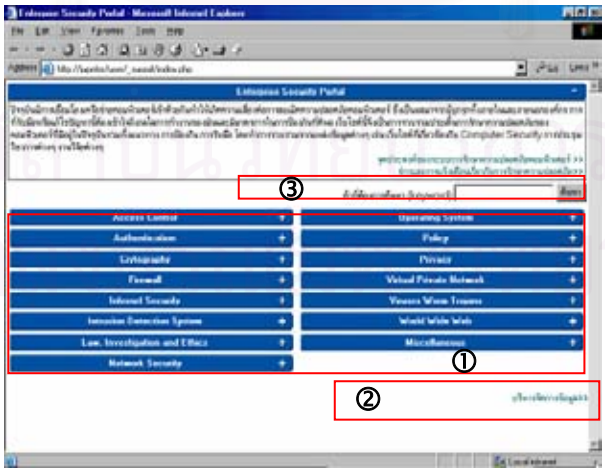
6.1. โครงสร้างรวมของระบบ

ในการพัฒนาระบบต้นแบบหมวดหมู่ประเด็นการรักษาความปลอดภัยของระบบคอมพิวเตอร์ งานวิจัยนี้ได้เลือกใช้เทคโนโลยีเว็บในการสร้างระบบ เนื่องจากผู้ใช้สามารถใช้งานจากที่ใดก็ได้โดยไม่จำเป็นต้องมีโปรแกรมทำให้สะดวกในการใช้งาน โดยโครงสร้างของระบบประกอบด้วยส่วนหลักๆ ดังรูปที่ 6-1



รูปที่ 6-1: โครงสร้างของระบบต้นแบบ

เทคโนโลยีที่ใช้ในการพัฒนาเว็บเพจ คือ PHP เหตุผลที่เลือกใช้ PHP เพราะภาษานี้สามารถ execute ได้ทั้ง web server ที่ติดตั้งในระบบปฏิบัติการ Microsoft Linux หรือ UNIX ซึ่งในการพัฒนาได้ใช้ IIS 5.0 เป็น web server และใช้ฐานข้อมูล Microsoft Access ในการเก็บข้อมูล การทำงานของเว็บไซต์ที่นำเสนอประกอบด้วย 3 ส่วนหลักๆดังรูปที่ 6-2



รูปที่ 6-2: การทำงานของเว็บไซต์

- นำเสนอ: เป็นส่วนที่นำเสนอเรื่องต่างๆของประเด็นการรักษาความปลอดภัยของระบบคอมพิวเตอร์
- บันทึกข้อมูล: เป็นส่วนที่ใช้สำหรับนำข้อมูลหรือเอกสารต่างๆเข้าไปในเว็บไซต์
- ค้นหา: ใช้สำหรับค้นหาข้อมูลทั้งหมดที่อยู่ในเว็บไซต์นี้

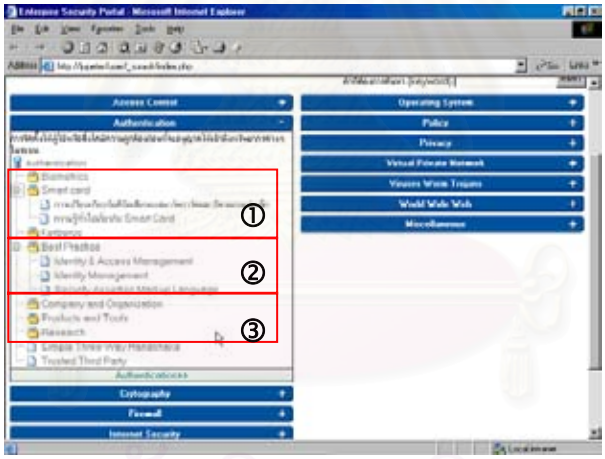
โดยแต่ละส่วนสามารถอธิบายโดยละเอียดดังนี้

6.1.1. นำเสนอ

จากรูปที่ 6-2 แสดงถึงรูปแบบของการนำเสนอเนื้อหาในเว็บไซต์ของหมวดหมู่ของประเด็นการรักษาความปลอดภัยของระบบคอมพิวเตอร์ โดยนำเอาหัวข้อหลักที่ได้จากผลการวิจัยมาแสดงเป็นข้อมูลในหน้าหลัก โดยรูปแบบของการนำเสนอในแต่ละหัวข้อหลักนั้นสามารถยืดและหดได้ [13] โดยข้อมูลที่อยู่ภายในหัวข้อหลักนั้นคือหัวข้อย่อยและรายละเอียดภายใต้หัวข้อนั้นซึ่งจะแสดงในรูปแบบของไดเร็กทรอรี [21] แต่ข้อเสียถ้ามีข้อมูลจำนวนจะทำให้การแสดงผลช้า

จากการนำเสนอแบบกำหนดให้แสดงใน 1 หน้าจอ ทำให้ผู้ใช้สามารถเห็นภาพรวมทั้งหมดของประเด็นการรักษาความปลอดภัยของระบบคอมพิวเตอร์และสะดวกต่อการค้นหาข้อมูล

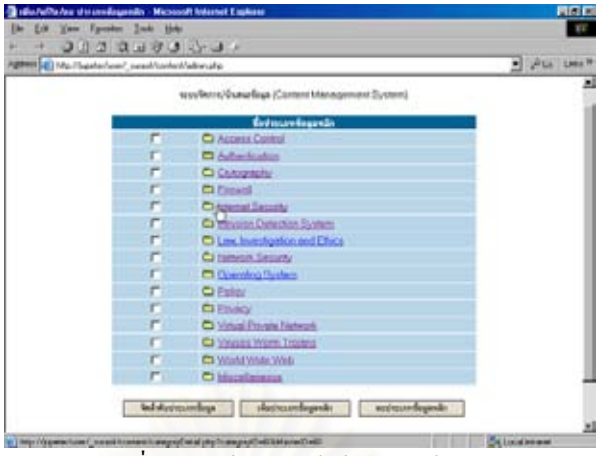
งานวิจัยนี้ได้ทำการเพิ่มหัวข้อย่อยลงในแต่ละหัวข้อหลัก 2 ประเด็นคือ Tutorial และ Best practices โดยที่ Tutorial จะเป็นข้อมูลที่แสดงถึงความรู้เบื้องต้นของหัวข้อหลัก และ Best practices จะเป็นแนวทางวิธีการปฏิบัติที่สามารถนำมาปฏิบัติได้จริง ดังรูปที่ 6-3



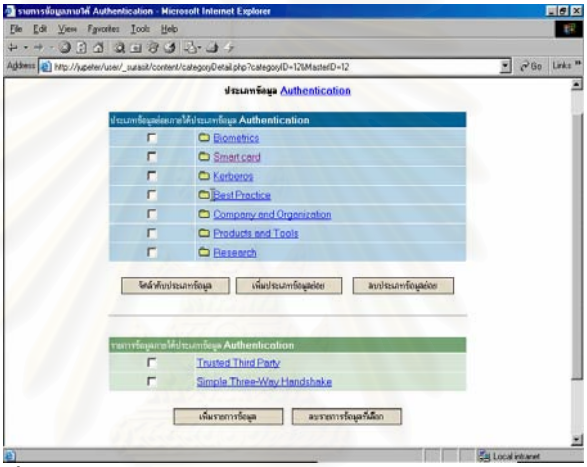
รูปที่ 6-3: การแสดงข้อมูลในเว็บไซต์

6.1.2. บันทึกข้อมูล

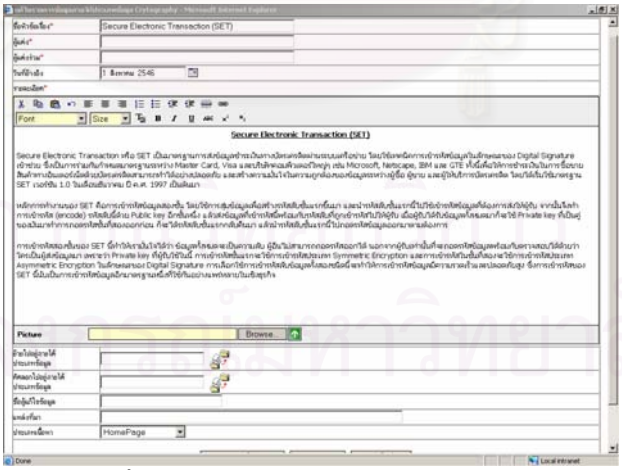
เป็นส่วนที่ใช้สำหรับบันทึกข้อมูลและนำเอกสารเข้าไปในแต่ละประเด็น ซึ่งสามารถเปลี่ยนแปลงหมวดหมู่จากหน้าจอนี้ได้ โดยรูปที่ 6-4 แสดงถึงประเด็นในหมวดหมู่หลัก และรูปที่ 6-5 แสดงหน้าจอการบันทึกหัวข้อย่อยและการนำเข้าเอกสารภายใต้หัวข้อหลัก และรูปที่ 6-6 แสดงการบันทึกรายละเอียดข้อมูล โดยการบันทึกรายละเอียดข้อมูลได้นำเอามาตรฐานดับลินคอร์เมทาดาทา (Dublin Core Metadata) มาประยุกต์ใช้ และคำแปลหรือความหมายส่วนใหญ่จะอ้างอิงจากหนังสือศัพท์เฉพาะทางด้านความปลอดภัยคอมพิวเตอร์ (เวอร์ชัน 1.5) ซึ่งจัดโดยศูนย์ประสานงานการรักษาความปลอดภัยคอมพิวเตอร์ประเทศไทย [53]



รูปที่ 6-4: หน้าจอนำเข้าข้อมูลหัวข้อหลัก



รูปที่ 6-5: หน้าจอนำเข้าประเด็นย่อยและรายละเอียดภายใต้หัวข้อ



รูปที่ 6-6: หน้าจอการบันทึกรายละเอียดข้อมูล

6.1.3. Search

ในกรณีที่ไม่สามารถค้นหาข้อมูลจากหน้าจอหลักได้ แต่ทราบถึงคำที่ต้องการหาสามารถใช้ในส่วนของการค้นหาจากคำสำคัญ โดยระบบจะทำการค้นหาคำจากคำอธิบายและในไฟล์ที่แนบเข้ามากับประเด็นนั้นๆ งานวิจัยนี้ได้โดยใช้ Library ของ Digital Genesis Technologies มาใช้ในการค้นหา [9] แต่ข้อเสียตรงที่ไม่สามารถค้นหาข้อมูลที่เป็นภาษาไทยในไฟล์ที่แนบมาได้

สถาบันวิทยบริการ
จุฬาลงกรณ์มหาวิทยาลัย

บทที่ 7

สรุปผลการวิจัยและข้อเสนอแนะ

7.1. สรุปผลการวิจัย

งานวิจัยนี้ได้ทำการออกแบบการจัดหมวดหมู่โดยใช้วิธีการจัดลำดับประเด็นที่ได้รับความสนใจ โดยใช้วิธีการทางสถิติคือ Hierarchical Cluster Analysis ในการจัดกลุ่มและหลักการจัดหมวดหมู่เว็บไซต์มาช่วยในการพิจารณาจำนวนประเด็นที่ปรากฏในหมวดหมู่หลัก งานวิจัยนี้มีเหตุผลอยู่ 3 ประการที่เลือกใช้วิธีนี้คือ

1) เทคโนโลยีทางด้านคอมพิวเตอร์และการสื่อสารมีการพัฒนาอย่างรวดเร็วและไม่หยุดนิ่ง เช่นเดียวกันกับปัญหาทางด้านความปลอดภัยของระบบคอมพิวเตอร์ ซึ่งจะแปรเปลี่ยนไปตามเทคโนโลยีใหม่ๆที่เกิดขึ้น ดังนั้นการที่จะใช้หลักการจัดหมวดหมู่ทั่วๆไป เช่น Ontology ที่จะต้องอาศัยปัจจัยต่างๆ เช่น Attribute Weight ซึ่งอาจปัจจัยเหล่านี้อาจจะแปรเปลี่ยนไปตามสถานการณ์ต่างๆ ณ ขณะนั้น ทำให้ไม่รองรับถึงปัญหาใหม่ๆที่จะเกิดขึ้นมา
2) จากการสำรวจประเด็นทางด้านความปลอดภัยของระบบคอมพิวเตอร์จากแหล่งข้อมูลต่างๆ จะมีความแตกต่างและหลากหลายมาก การที่จะนำประเด็นต่างๆมาจัดหมวดหมู่ใหม่ให้เป็นหนึ่งเดียวจะเป็นสิ่งที่เป็นไปได้ยาก เนื่องจากแนวคิดของแต่ละแหล่งข้อมูลไม่เหมือนกัน
3) คุ้มค่าที่จะจัดหมวดหมู่แบบนี้เพราะได้อ้างอิงจากการจัดหมวดหมู่ที่มีอยู่แล้ว วิธีการนี้เป็นวิธีที่ง่ายและครอบคลุมกับสถานการณ์ปัจจุบัน โดยแหล่งข้อมูลที่งานวิจัยนี้ได้สำรวจก็เป็นแหล่งของผู้เชี่ยวชาญจากสาขาต่างๆ ซึ่งมีรายละเอียดของแต่ละแหล่งข้อมูลดังนี้
    - Web Directory มีคนจากหลายสาขาอาชีพมาช่วยจัดหมวดหมู่
    - ระบบค้นหาข้อมูล (Search Engine) เป็นแหล่งข้อมูลที่คนนิยมในการค้นหาข้อมูล
    - หนังสือและตำราเรียน ผู้เชี่ยวชาญได้ทำการกำหนดเนื้อหาต่างๆที่เกี่ยวข้องกับกับเรื่องการรักษาความปลอดภัยคอมพิวเตอร์
    - หลักสูตรต่างๆ อาจารย์จากมหาวิทยาลัยต่างๆและผู้เชี่ยวชาญได้กำหนดเนื้อหาเรื่องการรักษาความปลอดภัยคอมพิวเตอร์ที่กำลังได้รับสนใจในปัจจุบัน
    - งานสัมมนาและประชุมวิชาการ เป็นการสะท้อนถึงเทคโนโลยี ปัญหาและเทคโนโลยีต่างๆทางด้านการรักษาความปลอดภัยของระบบคอมพิวเตอร์
    - Web sites เป็นแหล่งข้อมูลที่เกี่ยวข้องกับเรื่องการรักษาความปลอดภัยของระบบคอมพิวเตอร์โดยตรง

ผลของการจัดหมวดหมู่หลักทำให้ทราบถึงประเด็นต่างๆที่โลกกำลังประสบปัญหาหรือให้ความสนใจอยู่ ซึ่งสามารถนำไปประยุกต์ใช้ประโยชน์ได้ เช่น

- เมื่อต้องทำการเรียนการสอนเรื่องการรักษาความปลอดภัยคอมพิวเตอร์สามารถนำไปกำหนดเป็นบทเรียนในการสอนได้ หรือถ้าต้องการทราบภาพรวมก็สามารถนำไปอ้างอิงได้

- องค์กรต่างๆได้ตระหนักถึงปัญหาที่จะต้องเผชิญในปัจจุบันและมีการวางแผนและมาตรการรองรับในการรับมือกับปัญหานั้นๆ

ส่วนผลการจัดหมวดหมู่ย่อยทำให้ทราบถึงความสัมพันธ์ของประเด็นต่างๆภายใต้หมวดหมู่หลักนั้น อาจจะมีบางประเด็นที่อยู่ในหลายหมวดหมู่ แต่ไม่จำเป็นว่าจะต้องเป็นเนื้อหาเดียวกัน เช่น ประเด็น Policy ใน หมวดหมู่หลัก e-mail Security จะเป็นเนื้อหาเกี่ยวกับการนโยบายทางการใช้อีเมลล์ แต่ Policy ใน หมวดหมู่หลัก Privacy จะเป็นเนื้อหาเกี่ยวกับนโยบายของสิทธิส่วนบุคคล

7.2. ข้อเสนอแนะในการพัฒนาระบบ

จากการจัดหมวดหมู่ที่ได้จัดทำขึ้นตามกรรมวิธีของงานวิจัยนี้และการออกแบบระบบต้นแบบ ทางผู้วิจัยได้ตั้งข้อเสนอแนะในการพัฒนาระบบเพิ่มเติม ดังนี้

การจัดหมวดหมู่

1) การจัดหมวดหมู่ข้างต้นอาจจะทำการปรับหมวดหมู่ใหม่ทุก 2-3 ปี เพราะว่าเทคโนโลยีทางด้านคอมพิวเตอร์มีการพัฒนาอย่างรวดเร็ว และมีเทคนิคใหม่ๆเกิดขึ้นมาอย่างมากมาย

2) จากการสำรวจข้อมูลทั้งในหมวดหมู่หลักและหมวดหมู่ย่อยของแต่ละแหล่งข้อมูล จะมีประเด็นอื่นๆที่ไม่ใช่เรื่องการรักษาความปลอดภัยคอมพิวเตอร์อยู่เป็นจำนวนมาก เช่น Research, Product and Tool, Company, Consultants เป็นต้น ทางผู้วิจัยเห็นว่าที่มีหมวดหมู่เหล่านี้เกิดขึ้นเพราะแหล่งข้อมูลเหล่านั้นจะมีข้อมูลรองรับให้กับสาขาอาชีพและผู้สนใจต่างๆ ซึ่งสามารถนำเอาประเด็นเหล่านี้มาเป็นหมวดหมู่ย่อยของแต่ละหมวดหมู่

3) ผู้จะทำการวิจัยต่อไปอาจจะต้องนำเอาผลการจัดหมวดหมู่ที่ได้นำไปเสนอให้กับผู้เชี่ยวชาญด้านการรักษาความปลอดภัยของคอมพิวเตอร์ เพื่อขอข้อเสนอแนะและความต้องหมวดหมู่เพิ่มเติม หรือทำเป็นแบบสอบถามเพื่อขอคำแนะนำจากสายชีพต่างๆ เช่น อาจารย์ ผู้เชี่ยวชาญด้านการรักษาความปลอดภัย นิสิตนักศึกษา ผู้ออกแบบระบบหรือโปรแกรมเมอร์ เป็นต้น

4) การใช้วิธีนับจำนวนผลลัพธ์จากการค้นหาอาจจะไม่ใช่วิธีที่ดีเนื่องจากผลการค้นหาของแต่แหล่งข้อมูลอาจจะเป็นเอกสารเดียวกัน

5) วิธีการนี้จะนำเอาจำนวนผลลัพธ์หรือเอกสารมาพิจารณามาเป็นตัวแปรความถี่ที่ใช้ในการจัดกลุ่ม ซึ่งแต่ละแหล่งข้อมูลจะมีการจัดเก็บเอกสารมากน้อยแตกต่างกันทำให้ผลที่ได้มีความไม่เสมอภาคกัน ดังนั้นจะต้องทำการสมดุลของจำนวนข้อมูลก่อนที่จะทำการจัดกลุ่ม

6) ผลลัพธ์ของเอกสารที่ค้นหาอาจเป็นเอกสารที่เก่ามากหรือล่าสมัยไปแล้ว อาจจะต้องตรวจสอบถึงวันที่ผลิตเอกสาร ซึ่งจะต้องเป็นเอกสารที่ผลิตไม่เกิน 2-3 ปี

7) ในกรณีที่ผลการค้นหามีมากอาจจะต้องทำหาหมวดหมู่ย่อยในระดับถัด เพราะถือว่ามีความสนใจในประเด็นนั้นมาก

การพัฒนาระบบ

1) จากการจัดหมวดหมู่จะอยู่ในลักษณะที่จัดโดยผู้วิจัยเอง (Manual) ซึ่งผู้ที่จะวิจัยต่อไปอาจจะนำเอากรรมวิธีเบื้องต้นมาพัฒนาเป็นโปรแกรมที่จัดหมวดหมู่อัตโนมัติ

2) การจัดหมวดหมู่อาจใช้ความสนใจของผู้เข้าเยี่ยมชมเว็บไซต์ โดยทำสถิติในการเข้าเยี่ยมชมหมวดหมู่หรือรายการข้อมูลต่างๆ จากนั้นนำสถิติที่ได้มาทำการจัดหมวดหมู่ใหม่

3) การนำเอกสารหรือข้อมูลเข้าไปในแต่ละประเด็น งานวิจัยได้จัดทำระบบต้นแบบและได้ทดลองนำรายการเข้าบางส่วน ซึ่งจะมีปัญหาในการพิจารณาในการเลือกหมวดหมู่ที่จะจัดลงไป อาจจะแก้ปัญหาโดยใช้หลักการ "Training set" เพื่อให้ระบบสามารถจัดเอกสารไว้ในประเด็นต่างๆที่มีอยู่แล้วโดยอัตโนมัติ [35]

4) การออกแบบระบบต้นแบบนี้เมื่อมีเอกสารที่ต้องปรากฏในหลายประเด็นจะต้องทำการสำเนาเอกสารนั้นไปอยู่ประเด็นต่างๆที่ต้องการ ซึ่งจะเป็นการซ้ำซ้อนและไม่ประหยัดเนื้อที่การจัดเก็บ การวิจัยต่อไปจะต้องออกแบบให้รองรับกับการมีประเด็นของแต่ละเอกสาร (Overlapping clustering)

7.3. ปัญหาและอุปสรรค

1) การพิจารณาว่าประเด็นที่กำลังพิจารณาเป็นเรื่องเดียวกันหรือไม่ ต้องอาศัยความรู้ความชำนาญเกี่ยวกับเรื่องการรักษาความปลอดภัยของคอมพิวเตอร์ ซึ่งผู้วิจัยยังมีความชำนาญในด้านนี้น้อย

สถาบันวิทยบริการ
จุฬาลงกรณ์มหาวิทยาลัย

รายการอ้างอิง

[1] A Delphi Group White Paper, Taxonomy & Content Classification Market Milestone Report, 2002.

[2] Annual Computer Security Application Conference, 20th Annual Computer Security Applications Conference, [Online] Available from: http://www.acsac.org/, [2004, April 6].

[3] Best of the Web, BOTW, [Online] Available from: http://botw.org/top/Computers/Security/, [2004, April 6].

[4] bitpipe, IT Research White Papers, Product Information, Webcasts, and Case Studies, [Online] Available from: http://www.bitpipe.com/data/tlist?b=blat_security, [2004, April 6].

[5] Bruce Schneier, Secrets and Lies: Digital Security in a Networked World, Wiley, 2004.

[6] CERIAS, Cyber Security Group Training Conference, [Online] Available from: http://www.cerias.purdue.edu/news_and_events/events/calendar/details.php?calendar=20&event=716, [2004, April 6].

[7] Chanboon Sathitwiriyawong, Ph.D., 07017311 Computer Security, คณะเทคโนโลยีสารสนเทศ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง, 2003.

[8] CISSP Certification, CISSP Exam Structure, [Online] Available from: https://www.isc2.org/cgi/content.cgi?category=19, [2004, April 7].

[9] Digital Genesis Technologies, DGS Search v0.9.6, [Online] Available from: http://www.digitalgenesis.com/software/dgssearch.html, [2004, April 6].

[10] European Symposium on Research in Computer Security (ESORICS), 9th European Symposium on Research in Computer Security, [Online] Available from: http://esorics04.eurecom.fr/, [2004, April 8].

[11] eXcelon Corporation, Designing the Initial Topic, [Online] Available from : http://support.exln.com/doc/full/dm/vdk/doc/topics/ch053.htm, [2004, April 6].

[12] GITS, Truehits, [Online] Available from : http://www.truehits.net, [2004, April 6].

[13] Government Information Techonology Services, Template of Operations Center, [Online] Available from: http://www.thaigov.net/templateoc/, [2004, April 6].

[14] iBoogie , iBoogie MetaSearch Engine, [Online] Available from: http://iboogie.tv/, [2004, April 6].

[15] IEEE Computer Society Technical Committee on Security and Privacy, 2004 IEEE Symposium on Security and Privacy, [Online] Available from: http://www.cs.berkeley.edu/~daw/oakland04-cfp.html, [2004, April 6].

[16] Infonetware, Search the Web and Find with RealTerm, [Online] Available from: http://www.infonetware.com, [2004, April 6].

[17] INFOSYSSEC, The Security Portal for Information System Security Professionals, [Online] Available from: http://www.infosyssec.org, [2004, April 6].

[18] International Conference on Information and Communications Security, ICICS'04 Sixth International Conference on Information Communication Security, [Online] Available from: http://icics04.lcc.uma.es/, [2004, April 6].

[19] ITPapers CNET Networks, Inc, The Yellow Pages of White Papers, [Online] Available from: http://www.itpapers.com, [2004, April 6].

[20] Killerinfo, KillerInfo easy web searching, [Online] Available from: http://www.killerinfo.com/, [2004, April 6].

[21] Landro G., dTree, [Online] Available from: http://www.destroydrop.com/javascripts/tree/, [2003, May 15].

[22] LOGIKA Corporation, the Internet's First Searchable Directory, [Online] Available from: http://www.galaxy.com/directory/, [2004, April 6].

[23] Looksmart, Computer and Network Security , [Online] Available from: http://www.looksmart/Computers/Security/, [2004, April 6].

[24] Matt Bishop, Computer Security: Art and Science, Addison-Wesley-Longman, 2003.

[25] Mcgovern G., A step-by-step approach to web classification design. Learn how you can effectively design a robust, reader-friendly web classification, October, 2002.

[26] MIT, 6.857 Network and Computer Security - Fall 2003, [Online] Available from : http://theory.lcs.mit.edu/classes/6.857/announce.html, [2004, April 6].

[27] National Institute of Standards and Technology, Computer Security Resource Center, [Online] Available from: http://csrc.nist.gov/, [2004, April 6].

[28] Netscape Communications Corporation, Open Directory Editorial Guidelines, [Online] Available from: http://dmoz.org/guidelines/subcategories.html, [2004, April 6].

[29] Office of Information Technology, Information Management - Classification Guideline, Issue No:1.0, May, 2002.

[30] Open Directory Project, Security, [Online] Available from: http://www.dmoz.org/Computers/Security/, [2004, April 6].

[31] Raymond R. Panko, Corporate Computer and Network Security, Prentice Hall, 2003.

[32] Ronald L. Krutz, Russell Dean Vines, The CISSP Prep Guide: Mastering the CISSP and ISSEP Exams 2nd Edition, Wiley, 2004.

[33] SANS, Security Essentials Course Topics, [Online] Available from: http://www.sans.org/vancouver04/description.php?tid=23, [2004, April 6].

[34] SC MAGAZINE, Global Awards 2004, [Online] Available from: http://www.scawards.com/finalists/rta.asp, [2004, April 6].

[35] Search Tools. Taxonomies, Categorization, Classification, Categories, and Directories for Searching, [Online] Available from : http://www.searchtools.com/info/classifiers.html, [2004, January 20].

[36] SecurityFocus, SecurityFocus ONLINE Library Archive, [Online] Available from: http://www.securityfocus.com/library, [2004, April 6].

[37] Stallings W., Cryptography and Network Security: Principles and Practice (3rd Edition), Prentice Hall, August , 2002.

[38] The Center for Education and Research in Information Assurance and Security, CERIAS Hotlist, [Online] Available from: http://www.cerias.purdue.edu/tools_and_resources/hotlist/, [2004, April 6].

[39] The Internet Security Conference, Security Resource & Links, [Online] Available from: http://www.tisc2001.com/links.html, [2004, April 6].

[40] The SANS Institute, SANS' Information Security Reading Room, [Online] Available from: http://www.sans.org/rr/, [2004, April 6].

[41] Townsend & Taphouse, The ITsecurity Show, [Online] Available from: http://www.itsecurity.com/show/foyer.htm, [2004, April 6].

[42] Trabalka M. and Bielikova, M., Using Salient Words to Perform Categorization of Web sites, 2002.

[43] University of Minnesota, Csci 4407- Networks Security Course Outline, [Online] Available from: http://cda.mrs.umn.edu/~andy/cs4407S2004outline.pdf, Spring 2004.

[44] Vivisimo Inc., Vivisimo Clustering Engine, [Online] Available from: http://vivisimo.com, [2004, April 6].

[45] WindowsSecurity.com, Network Security Library, [Online] Available from: http://www.secinf.net/, [2004, April 6].

[46] Wisenut, Wisenut Search Exactly, [Online] Available from: http://www.wisenut.com, [2004, April 6].

[47] Yahoo! Directory, Security and Encryption , [Online] Available from: http://www.yahoo.com/Security/, [2004, April 6].

[48] กฤษณี อริยชาญศิลป์, ระบบค้นคืนสารสนเทศภาษาไทย-อังกฤษ สำหรับคำทับศัพท์และแสดงผลลัพธ์ด้วยวิธีการจัดกลุ่มข้อมูล, 2545.

[49] กัลยา วานิชย์บัญชา, SPSS for Windows, Cluster Analysis, Page 197-248, 2001.

[50] กัลลิสรา เอกวัฒน์พานิชย์, ประดิษฐา ศิริพันธ์, ตัวขยายดับลินคอร์ ภาษาไทย (qualifiers), 2544.

[51] ประดิษฐา ศิริพันธ์, การประยุกต์ดับลินคอร์เมทาดาทาเพื่อการสืบค้นสารสนเทศ, ศูนย์บริการสารสนเทศทางเทคโนโลยี, 2546.

[52] ประดิษฐา ศิริพันธ์, ดับลินคอร์เมทาดาทาฉบับ 1.1 ภาษาไทย, 2544.

[53] ศูนย์ประสานงานการรักษาความปลอดภัยคอมพิวเตอร์ประเทศไทย ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ, ศัพท์เฉพาะทางด้านความปลอดภัยคอมพิวเตอร์ (เวอร์ชัน 1.5), 2545.

ภาคผนวก ก

ผลของการสำรวจข้อมูล

ตารางที่ ก-1: แสดงผลการสำรวจประเด็นของหมวดหมู่หลักของ Web Directories

ลำดับ	ประเด็น	ความถี่	แหล่งข้อมูล				
			[30]	[47]	[23]	[3]	[22]
1	Biometrics	4	X		X	X	X
2	Firewalls	4	X	X		X	X
3	Policy	4	X	X		X	X
4	Virtual Private Networks	4	X		X	X	X
5	Cryptography	3		X	X	X	
6	Digital Signatures	3		X	X	X	
7	Hacking	3	X	X		X	
8	Internet	3	X			X	X
9	Intrusion Detection Systems	3	X		X		X
10	News	3			X	X	X
11	Anonymous Mailers	2		X		X	
12	Anti Virus	2	X				X
13	Authentication	2	X			X	
14	Digital Money	2		X		X	
15	Email	2		X		X	
16	Java	2	X	X			
17	Kerberos	2		X	X		
18	Operating System	2		X			X
19	Patches	2	X			X	
20	PGP - Pretty Good Privacy	2		X	X		
21	Public Key Infrastructure	2	X			X	
22	Steganography	2		X	X		
23	Viruses & Trojans	2			X	X	
24	Viruses Worms and Trojan	2		X	X		
25	Counter Measures	1	X				
26	Dongles	1			X		
27	Hackers	1	X				
28	Information Warfare	1		X			
29	Phreaking	1				X	
30	Piracy	1		X			
31	Privacy	1		X			
32	Rijndael	1		X			
33	Risks	1		X			
34	RSA	1		X			
35	S/KEY	1		X			
36	World Wide Web Security	1		X			

ตารางที่ ก-2: แสดงผลการสำรวจประเด็นของหมวดหมู่หลักของ Search Engine

ลำดับ	ประเด็น	ความถี่	แหล่งข้อมูล				
			[44]	[16]	[46]	[14]	[20]
1	Network Security	5	X	X	X	X	X
2	Incident Response	4	X		X	X	X
3	Information Security	4	X	X	X		X
4	Cryptography	3	X			X	X
5	Internet Security	3		X	X	X	
6	policies	3		X		X	X
7	Privacy	3	X		X	X	
8	Security Systems	3	X	X		X	
9	Administration	2	X		X		
10	Anonymous	2	X				X
11	Camera	2	X				X
12	CERT Coordination Center	2	X				X
13	Home security	2		X		X	
14	National Security	2		X	X		
15	Password	2				X	X
16	Risk	2	X	X			
17	Security services	2			X	X	
18	Virus	2	X			X	
19	Alerts	1				X	
20	Anti	1				X	
21	Anti virus	1			X		
22	Applications	1	X				
23	Awareness	1	X				
24	Biometric	1	X				
25	Crypto-Gram	1	X				
26	Doe-Ciac	1					X
27	e – business	1		X			
28	e – Security	1		X			
29	File	1				X	
30	Firewall	1				X	
31	Hacker	1				X	
32	Hacking	1	X				
33	Homeland Security	1			X		
34	Intrusion detection	1	X				
35	Java Security	1	X				
36	Management	1			X		
37	mobile phone	1		X			
38	news	1				X	
39	Operating System	1			X		
40	Personal computer security	1				X	
41	PGP	1	X				
42	Physical Security	1	X				

ลำดับ	ประเด็น	ความถี่	แหล่งข้อมูล				
			[44]	[16]	[46]	[14]	[20]
43	Protocol	1	X				
44	Security measures	1		X			
45	security program	1				X	
46	Security Programs	1			X		
47	Social Security	1			X		
48	Surveillance and Counter Measure	1			X		
49	Theft	1	X				
50	Web	1				X	

ตารางที่ ก-3: แสดงผลการสำรวจประเด็นของหมวดหมู่หลักของ Book

ลำดับ	ประเด็น	ความถี่	แหล่งข้อมูล				
			[5]	[24]	[37]	[31]	[32]
1	Cryptography	5	X	X	X	X	X
2	Network Security	4	X	X	X		X
3	Access Control	3		X		X	X
4	Authentication and Identification	3	X	X	X		
5	Attacks	2	X			X	
6	e-mail	2			X	X	
7	Firewalls	2			X	X	
8	Key Management	2		X	X		
9	Policies	2	X	X			
10	Vulnerabilities	2	X	X			
11	AES	1			X		
12	Applications and Systems Development	1					X
13	Architecture	1					X
14	Assessment	1					X
15	Auditing	1		X			
16	Business Continuity Planning	1					X
17	Certificates and Credentials	1	X				
18	Certification and Accreditation (C&A)	1					X
19	Cipher Techniques	1		X			
20	Countermeasures	1	X				
21	Digital Signatures	1			X		
22	Disaster Recovery Planning	1					X
23	e-commerce	1				X	
24	Evaluating Systems	1		X			
25	Hardware	1	X				
26	Hash Algorithms	1			X		
27	Host security	1				X	
28	Incident response	1				X	
29	Information Flow	1		X			
30	Intruders	1			X		
31	Intrusion Detection	1		X			
32	IP Security	1			X		
33	Kerberos	1				X	
34	Law, Investigation, and Ethics	1					X
35	Malicious	1		X			
36	Message Authentication and Hash Functions	1			X		

ลำดับ	ประเด็น	ความถี่	แหล่งข้อมูล				
			[5]	[24]	[37]	[31]	[32]
37	Models	1					X
38	Network Defenses	1	X				
39	Number Theory	1			X		
40	Operations Security	1					X
41	Physical Security	1					X
42	Product Testing	1	X				
43	Program Security	1		X			
44	Public-Key Cryptography	1			X		
45	Risk Assessment	1	X				
46	Security Framework	1				X	
47	Security Processes	1	X				
48	SSL/TLS	1				X	
49	Symmetric Ciphers	1			X		
50	System Security	1			X		
51	Systems Security Engineering	1					X
52	TCP/IP internetworking	1				X	
53	Technical Management	1					X
54	Telecommunications	1					X
55	The Human Factor	1	X				
56	Threat Modeling	1	X				
57	Threats	1	X				
58	User Security	1		X			
59	Verification	1	X				
60	Viruses	1			X		
61	VPNs	1				X	
62	Web Security	1			X		

ตารางที่ ก-4: แสดงผลการสำรวจประเด็นของหมวดหมู่หลักของ Course

ลำดับ	ประเด็น	ความถี่	แหล่งข้อมูล				
			[6]	[26]	[7]	[43]	[33]
1	Intrusion Detection	5	X	X	X	X	X
2	Firewall	4	X	X	X		X
3	World Wide Web	4		X	X	X	X
4	e-mail	3		X	X	X	
5	Network Security	3			X	X	X
6	Policy	3			X	X	X
7	Cryptography	2	X	X			
8	Cryptography	2			X	X	
9	Digital Signature	2			X	X	
10	e-Commerce	2		X		X	
11	Operating System Security	2		X	X		
12	PGP	2			X		X
13	Risk Assessment	2		X			X
14	Threats	2			X	X	
15	Viruses	2		X	X		
16	Access Control	1				X	
17	Administration	1					X

ลำดับ	ประเด็น	ความถี่	แหล่งข้อมูล				
			[6]	[26]	[7]	[43]	[33]
18	AES	1				X	
19	Anti-Virus	1					X
20	Auditing	1					X
21	Authentication	1		X			
22	Awareness	1	X				
23	Biometrics	1	X				
24	Certification	1	X				
25	Certification and Accreditation	1	X				
26	Cisco Router Filters	1					X
27	Configuration Management	1	X				
28	Contingency Planning and Disaster Recovery	1			X		
29	Cryptography	1				X	
30	Cyber Security	1	X				
31	Database Security	1			X		
32	DES	1				X	
33	digital signatures	1		X			
34	distributed computer systems	1		X			
35	e-cash	1		X			
36	e-Payment Systems	1				X	
37	Hashing Functions	1				X	
38	Honeypots	1					X
39	IIS Security	1					X
40	Incident Handling	1					X
41	Information Warfare	1					X
42	IP Security	1			X		
43	Legal and Ethical Issues	1			X		
44	Malicious Code	1				X	
45	models	1		X			
46	Operating System Security	1					X
47	Password	1					X
48	Patch	1	X				
49	payment protocols	1		X			
50	Perimeter Protection	1					X
51	Personal Computer Security	1			X		
52	Physical Security	1			X		
53	Privacy	1			X		
54	public-key	1		X			
55	Risk Management and analysis	1			X		
56	RSA	1				X	
57	S/MIME	1			X		
58	secret-key	1		X			
59	SET	1			X		
60	SSL	1			X		
61	Steganography	1					X
62	TCP attacks	1				X	
63	Virtual Private Network (VPN)	1			X		
64	Wireless Security	1	X				

ตารางที่ ก-5: แสดงผลการสำรวจประเด็นของหมวดหมู่หลักของ Conference

ลำดับ	ประเด็น	ความถี่	แหล่งข้อมูล				
			[15]	[2]	[10]	[18]	[39]
1	Authentication and Identification	5	X	X	X	X	X
2	Denial of Service	4	X	X	X		X

ลำดับ	ประเด็น	ความถี่	แหล่งข้อมูล				
			[15]	[2]	[10]	[18]	[39]
3	e-commerce	4		X	X	X	X
4	Intrusion Detection	4	X		X	X	X
5	Privacy	4	X		X	X	X
6	Access Control	3	X	X	X		
7	Anonymity and Pseudonymity	3	X		X	X	
8	Biometrics	3	X	X		X	
9	Cryptography	3		X	X	X	
10	Data Integrity	3	X		X	X	
11	Firewalls	3		X	X		X
12	Forensics	3		X		X	X
13	Network Security	3	X		X	X	
14	Smartcards	3	X		X	X	
15	Audit	2	X	X			
16	Database Security	2	X	X			
17	Information Flow	2	X		X		
18	Information Survivability	2		X	X		
19	information warfare	2		X	X		
20	Language-Based Security	2	X		X		
21	Mobile Communications Security	2	X			X	
22	Models	2			X	X	
23	Peer-to-Peer Security	2	X		X		
24	Protocols	2			X	X	
25	trust models and trust Management	2			X	X	
26	accountability	1			X		
27	administration	1			X		
28	application security	1			X		
29	Certification and accreditation	1		X			
30	Covert channels	1			X		
31	Critical Infrastructures Protection	1				X	
32	Cybercrime	1			X		
33	Desktop Security	1					X
34	digital right management	1			X		
35	Distributed Systems Security	1	X				
36	DNS	1					X
37	E-Business	1					X
38	Email	1					X
39	Enterprise Security	1		X			
40	Fraud Control	1				X	
41	Hacking	1					X
42	Hardware Security	1	X				
43	Host Scanners	1					X
44	identity management	1			X		
45	Incident Response	1				X	
46	inference control	1			X		
47	information dissemination control	1			X		

ลำดับ	ประเด็น	ความถี่	แหล่งข้อมูล				
			[15]	[2]	[10]	[18]	[39]
48	Information Hiding	1				X	
49	Intellectual Property Protection	1				X	
50	Key Management	1				X	
51	Key Recovery	1				X	
52	Malicious Code	1	X				
53	management	1			X		
54	Mobile Code and Agent Security	1	X				
55	Operating System Security	1					X
56	PKI	1					X
57	Programming	1					X
58	Risk Evaluation	1				X	
59	Secure Broadband Local Access	1					X
60	Security Assurance	1				X	
61	Security Certification	1				X	
62	security evaluation	1			X		
63	Security Protocols	1	X				
64	security requirements engineering	1			X		
65	Security Verification	1	X				
66	steganography	1			X		
67	subliminal channels	1			X		
68	system security	1			X		
69	threat	1		X			
70	transaction management	1			X		
71	trustworthy user devices	1			X		
72	verification	1			X		
73	Viruses	1	X				
74	VPNs	1					X
75	Watermarking	1				X	
76	Wireless LAN Security	1					X

ตารางที่ ก-6: แสดงผลการสำรวจประเด็นของหมวดหมู่หลักของ Web Sites

ลำดับ	ประเด็น	ความถี่	แหล่งข้อมูล									
			[17]	[36]	[40]	[8]	[27]	[38]	[4]	[41]	[45]	[34]
1	Cryptography	10	X	X	X	X	X	X	X	X	X	X
2	Policy	8	X		X		X	X	X	X	X	X
3	Intrusion Detection	7	X	X	X			X	X	X	X	
4	Authentication	6	X	X	X		X		X		X	
5	E-Mail Security	6	X		X			X	X	X		X
6	Firewalls	6	X		X			X		X	X	X
7	Law, Investigation, and Ethics	6	X	X		X		X	X		X	
8	Network Security	6	X			X		X	X	X		X
9	Virus Worms Trojans Malicious Code	6	X		X			X	X	X	X	
10	Access Control	5		X		X	X			X	X	
11	Audit	5	X	X	X					X	X	
12	Operating System	5	X	X	X			X			X	
13	Wireless Security	5			X		X	X	X			X

ลำดับ	ประเด็น	ความถี่	แหล่งข้อมูล									
			[17]	[36]	[40]	[8]	[27]	[38]	[4]	[41]	[45]	[34]
14	Assessment	4	X		X				X	X		
15	Biometrics	4	X						X	X		X
16	Disaster Recovery	4	X		X				X		X	
17	E-Commerce	4		X	X			X		X		
18	Information Warfare	4	X	X	X						X	
19	Physical Security	4	X		X	X		X				
20	Privacy	4	X					X		X	X	
21	Security Management	4				X			X		X	X
22	VPN's-Virtual Private Networks	4	X		X						X	X
23	Vulnerabilities	4		X	X		X		X			
24	Business Continuity Planning	3	X			X						X
25	Certification and Accreditation	3	X				X			X		
26	Content security	3								X	X	X
27	Cybercrime	3	X	X					X			
28	Forensics	3			X						X	X
29	Internet Security	3	X			X			X			
30	Smart Cards	3	X				X					X
31	Standards	3			X				X		X	
32	WWW	3						X	X		X	
33	Anonymity	2	X					X				
34	Anti Virus and Spam	2									X	X
35	Application Security	2			X	X						
36	Backup Strategies	2			X					X		
37	Database Security	2			X				X			
38	Denial of Service and DDOS	2	X						X			
39	Hacker	2	X		X							
40	Incident Handling	2		X	X							
41	Intrusion Prevention	2			X				X			
42	IPSec	2					X		X			
43	Java Security	2	X					X				
44	Penetration Testing	2	X		X							
45	PGP-Pretty Good Privacy	2	X					X				
46	PKI-Public Key Infrastructure	2	X							X		
47	Protocols	2	X		X							
48	RFC-Request for Comments	2	X	X								
49	Security Architecture	2				X			X			
50	Security Modeling	2			X	X						
51	Security Standards	2	X	X								
52	Software Engineering	2		X							X	
53	Steganography	2	X		X							
54	system security	2						X	X			
55	Telecommunication	2	X			X						
56	Threats	2			X		X					
57	Access Control	1										X
58	Advanced Encryption Standard (AES)	1					X					
59	Attacking Attackers	1			X							
60	Automated Security Functional Testing	1					X					
61	Automated Security Self-Evaluation Tool (ASSET)	1					X					
62	Awareness	1								X		
63	Backups	1							X			
64	CCTV Video Surveillance Cameras	1	X									
65	Communications Security	1										X

ลำดับ	ประเด็น	ความถี่	แหล่งข้อมูล									
			[17]	[36]	[40]	[8]	[27]	[38]	[4]	[41]	[45]	[34]
66	Covert Channels	1			X							
67	Cryptographic Module Validation Program (CMVP)	1					X					
68	Data Replication	1							X			
69	Data Storage and Recovery Solution	1										X
70	Digital Certificates	1			X							
71	Digital Privacy	1			X							
72	DNS	1			X							
73	FIRST	1						X				
74	Hacking	1	X									
75	Hardware	1							X			
76	Harmless hacking book	1									X	
77	HIPAA	1			X							
78	Homeland	1							X			
79	Honeypots	1									X	
80	Hostile Code	1		X								
81	ICAT Vulnerability Database	1					X					
82	Identity Management	1										X
83	Information Assurance	1			X							
84	Information Hiding	1		X								
85	Infrastructure	1							X			
86	Intrusion Solution	1										X
87	Mac	1						X				
88	Mobile Computing Security (formerly known as MAIDS)	1					X					
89	National Information Assurance Partnership (NIAP)	1					X					
90	NCSC&DoD Rainbow series	1									X	
91	Network Devices	1			X							
92	Operations Security	1				X						
93	Password	1							X			
94	Patch Management	1									X	
95	PDAs	1			X							
96	Perimeter Protection	1			X							
97	Public Key Infrastructure	1					X					
98	RSA Security	1										X
99	S/MIME	1					X					
100	Scripting	1			X							
101	Securing Code	1			X							
102	Security Awareness	1			X							
103	Security Events	1					X					
104	Security Management Assistance (PRISMA)	1					X					
105	Security Service	1										X
106	Security Testing	1					X					
107	Single Sign-on	1							X			
108	Social Engineering	1			X							
109	Spam	1					X					
110	SSL	1							X			
111	Tokens	1							X			
112	Watermarks	1	X									
113	WEP	1							X			
114	WIN NT Security Files	1	X									

ตารางที่ ก-7: แสดงผลการสำรวจประเด็นของหมวดหมู่หลักของทุกแหล่งข้อมูลเรียงตามความถี่

ลำดับ	ประเด็น	ความถี่	ลำดับ	ประเด็น	ความถี่	ลำดับ	ประเด็น	ความถี่
1	Cryptography	28	39	Steganography	6	77	DNS	2
2	Intrusion Detection Systems	21	40	Vulnerabilities	6	78	e-Payment Systems	2
3	Network Security	21	41	Applications and Systems Development	5	79	Hash Algorithms	2
4	Firewalls	20	42	Database Security	5	80	Home security	2
5	Policy	20	43	Java Security	5	81	Homeland Security	2
6	Authentication and Identification	18	44	Public Key Infrastructure	5	82	Honeypots	2
7	Viruses Worms and Trojan Malicious Code	17	45	Security Standards	5	83	Information Hiding	2
8	Email	14	46	Administration	4	84	Information Survivability	2
9	Privacy	14	47	Business Continuity Planning	4	85	Language-Based Security	2
10	Access Control	13	48	Cybercrime	4	86	Mobile Communications Security	2
11	Biometrics	13	49	Information Security	4	87	National Security	2
12	Risk Assessment and Analysis	13	50	IP Security	4	88	Operations Security	2
13	e-Commerce	12	51	News	4	89	Peer-to-Peer Security	2
14	Operating System	12	52	Password	4	90	Penetration Testing	2
15	Virtual Private Networks	11	53	Patches	4	91	Perimeter Protection	2
16	World Wide Web Security	10	54	Telecommunications	4	92	Personal Computer Security	2
17	Anonymity and Pseudonymity	9	55	AES	3	93	RFC-Request for Comments	2
18	Auditing	9	56	Attacking Attackers	3	94	S/MIME	2
19	Incident response and Handling	9	57	Awareness	3	95	Securing Code	2
20	Internet Security	9	58	Backups	3	96	Security Architecture	2
21	Certification and Accreditation (C&A)	8	59	CCTV Video Surveillance Cameras	3	97	Software Engineering	2
22	Hacking and Hackers	8	60	Content security	3	98	trust models and trust Management	2
23	Information Warfare	8	61	Data Integrity	3	99	Watermarking	2
24	Law, Investigation, and Ethics	8	62	Hardware Security	3	100	Accountability	1
25	Anti Virus	7	63	Information Flow	3	101	Alerts	1
26	Digital Signatures	7	64	Intrusion Prevention	3	102	Architecture	1
27	PGP – Pretty Good Privacy	7	65	Kerberos	3	103	Automated Security Functional Testing	1
28	Physical Security	7	66	Key Management	3	104	Automated Security Self-Evaluation Tool (ASSET)	1
29	System Security	7	67	Public Key Infrastructure	3	105	Cipher Techniques	1
30	Threat	7	68	RSA	3	106	Cisco Router Filters	1
31	Wireless Security	7	69	Security Service	3	107	Configuration Management	1
32	Denial of Service	6	70	Security Verification	3	108	Contingency Planning	1
33	Disaster Recovery	6	71	SSL/TLS	3	109	Critical Infrastructures Protection	1
34	Forensics	6	72	Surveillance and Counter Measure	3	110	Crypto-Gram	1
35	Protocols	6	73	CERT Coordination Center	2	111	Cryptographic Module Validation Program (CMVP)	1
36	Security Management	6	74	Covert channels	2	112	Cyber Security	1
37	Security Models	6	75	Digital Money	2	113	Data Replication	1
38	Smart Cards	6	76	Distributed Systems Security	2	114	Data Storage and Recovery Solution	1

ตารางที่ ก-7: แสดงผลการสำรวจประเด็นของหมวดหมู่หลักของทุกแหล่งข้อมูลเรียงตามความถี่ (ต่อ)

ลำดับ	ประเด็น	ความถี่	ลำดับ	ประเด็น	ความถี่	ลำดับ	ประเด็น	ความถี่
115	DES	1	139	Mac	1	163	Security Management Assistance (PRISMA)	1
116	Desktop Security	1	140	Message Authentication and Hash Functions	1	164	Security measures	1
117	Digital Certificates	1	141	Mobile Code and Agent Security	1	165	Security Processes	1
118	Digital right management	1	142	Mobile Computing Security (formerly known as MAIDS)	1	166	security requirements engineering	1
119	Doe-Ciac	1	143	mobile phone	1	167	Security Testing	1
120	Dongles	1	144	National Information Assurance Partnership (NIAP)	1	168	SET	1
121	e – Security	1	145	NCSC&DoD Rainbow series	1	169	Single Sign-on	1
122	e-cash	1	146	Network Defenses	1	170	Social Engineering	1
123	Enterprise Security	1	147	Network Devices	1	171	Social Security	1
124	File	1	148	Number Theory	1	172	Spam	1
125	FIRST	1	149	PDAs	1	173	subliminal channels	1
126	Fraud Control	1	150	Phreaking	1	174	Symmetric Ciphers	1
127	Harmless hacking book	1	151	Piracy	1	175	Systems Security Engineering	1
128	HIPAA	1	152	Product Testing	1	176	TCP attacks	1
129	Host Scanners	1	153	Program Security	1	177	TCP/IP internetworking	1
130	Host security	1	154	Rijndael	1	178	Technical Management	1
131	Hostile Code	1	155	S/KEY	1	179	The Human Factor	1
132	IIS Security	1	156	secret-key	1	180	Tokens	1
133	inference control	1	157	Secure Broadband Local Access	1	181	transaction management	1
134	Information Assurance	1	158	Security Assurance	1	182	trustworthy user devices	1
135	information dissemination control	1	159	Security Awareness	1	183	User Security	1
136	Infrastructure	1	160	security evaluation	1	184	WEP	1
137	Intellectual Property Protection	1	161	Security Events	1	185	WIN NT Security Files	1
138	Intruders	1	162	Security Framework	1			

ตารางที่ ก-8: แสดงผลการสำรวจประเด็นของหมวดหมู่หลักของทุกแหล่งข้อมูลเรียงตามตัวอักษร

ลำดับ	ประเด็น	ความถี่	ลำดับ	ประเด็น	ความถี่	ลำดับ	ประเด็น	ความถี่
1	Access Control	13	16	Backups	3	31	Cryptography	28
2	Accountability	1	17	Biometrics	13	32	Cyber Security	1
3	Administration	4	18	Business Continuity Planning	4	33	Cybercrime	4
4	AES	3	19	CCTV Video Surveillance Cameras	3	34	Data Integrity	3
5	Alerts	1	20	CERT Coordination Center	2	35	Data Replication	1
6	Anonymity and Pseudonymity	9	21	Certification and Accreditation (C&A)	8	36	Data Storage and Recovery Solution	1
7	Anti Virus	7	22	Cipher Techniques	1	37	Database Security	5
8	Applications and Systems Development	5	23	Cisco Router Filters	1	38	Denial of Service	6
9	Architecture	1	24	Configuration Management	1	39	DES	1
10	Attacking Attackers	3	25	Content security	3	40	Desktop Security	1
11	Auditing	9	26	Contingency Planning	1	41	Digital Certificates	1
12	Authentication and Identification	18	27	Covert channels	2	42	Digital Money	2
13	Automated Security Functional Testing	1	28	Critical Infrastructures Protection	1	43	Digital right management	1
14	Automated Security Self-Evaluation Tool (ASSET)	1	29	Crypto-Gram	1	44	Digital Signatures	7
15	Awareness	3	30	Cryptographic Module Validation Program (CMVP)	1	45	Disaster Recovery	6

ตารางที่ ก-8: แสดงผลการสำรวจประเด็นของหมวดหมู่หลักของทุกแหล่งข้อมูลเรียงตามตัวอักษร (ต่อ)

ลำดับ	ประเด็น	ความถี่	ลำดับ	ประเด็น	ความถี่	ลำดับ	ประเด็น	ความถี่
46	Distributed Systems Security	2	93	Law, Investigation, and Ethics	8	140	security evaluation	1
47	DNS	2	94	Mac	1	141	Security Events	1
48	Doe-Ciac	1	95	Message Authentication and Hash Functions	1	142	Security Framework	1
49	Dongles	1	96	Mobile Code and Agent Security	1	143	Security Management	6
50	e - Security	1	97	Mobile Communications Security	2	144	Security Management Assistance (PRISMA)	1
51	e-cash	1	98	Mobile Computing Security (formerly known as MAIDS)	1	145	Security measures	1
52	e-Commerce	12	99	mobile phone	1	146	Security Models	6
53	Email	14	100	National Information Assurance Partnership (NIAP)	1	147	Security Processes	1
54	Enterprise Security	1	101	National Security	2	148	security requirements engineering	1
55	e-Payment Systems	2	102	NCSC&DoD Rainbow series	1	149	Security Service	3
56	File	1	103	Network Defenses	1	150	Security Standards	5
57	Firewalls	20	104	Network Devices	1	151	Security Testing	1
58	FIRST	1	105	Network Security	21	152	Security Verification	3
59	Forensics	6	106	News	4	153	SET	1
60	Fraud Control	1	107	Number Theory	1	154	Single Sign-on	1
61	Hacking and Hackers	8	108	Operating System	12	155	Smart Cards	6
62	Hardware Security	3	109	Operations Security	2	156	Social Engineering	1
63	Harmless hacking book	1	110	Password	4	157	Social Security	1
64	Hash Algorithms	2	111	Patches	4	158	Software Engineering	2
65	HIPAA	1	112	PDAs	1	159	Spam	1
66	Home security	2	113	Peer-to-Peer Security	2	160	SSL/TLS	3
67	Homeland Security	2	114	Penetration Testing	2	161	Steganography	6
68	Honeypots	2	115	Perimeter Protection	2	162	subliminal channels	1
69	Host Scanners	1	116	Personal Computer Security	2	163	Surveillance and Counter Measure	3
70	Host security	1	117	PGP – Pretty Good Privacy	7	164	Symmetric Ciphers	1
71	Hostile Code	1	118	Phreaking	1	165	System Security	7
72	IIS Security	1	119	Physical Security	7	166	Systems Security Engineering	1
73	Incident response and Handling	9	120	Piracy	1	167	TCP attacks	1
74	inference control	1	121	Policy	20	168	TCP/IP internetworking	1
75	Information Assurance	1	122	Privacy	14	169	Technical Management	1
76	information dissemination control	1	123	Product Testing	1	170	Telecommunications	4
77	Information Flow	3	124	Program Security	1	171	The Human Factor	1
78	Information Hiding	2	125	Protocols	6	172	Threat	7
79	Information Security	4	126	Public Key Infrastructure	5	173	Tokens	1
80	Information Survivability	2	127	Public Key Infrastructure	3	174	transaction management	1
81	Information Warfare	8	128	RFC-Request for Comments	2	175	trust models and trust Management	2
82	Infrastructure	1	129	Rijndael	1	176	trustworthy user devices	1
83	Intellectual Property Protection	1	130	Risk Assessment and Analysis	13	177	User Security	1
84	Internet Security	9	131	RSA	3	178	Virtual Private Networks	11
85	Intruders	1	132	S/KEY	1	179	Viruses Worms and Trojan Malicious Code	17
86	Intrusion Detection Systems	21	133	S/MIME	2	180	Vulnerabilities	6
87	Intrusion Prevention	3	134	secret-key	1	181	Watermarking	2
88	IP Security	4	135	Secure Broadband Local Access	1	182	WEP	1
89	Java Security	5	136	Securing Code	2	183	WIN NT Security Files	1
90	Kerberos	3	137	Security Architecture	2	184	Wireless Security	7
91	Key Management	3	138	Security Assurance	1	185	World Wide Web Security	10
92	Language-Based Security	2	139	Security Awareness	1			

ตารางที่ ก-9: แสดงผลการสำรวจประเด็นที่ตัดความถี่เท่ากับ 1 เรียงตามความถี่

ลำดับ	ประเด็น	ความถี่	ลำดับ	ประเด็น	ความถี่
1	Cryptography	28	51	News	4
2	Intrusion Detection Systems	21	52	Password	4
3	Network Security	21	53	Patches	4
4	Firewalls	20	54	Telecommunications	4
5	Policy	20	55	AES	3
6	Authentication and Identification	18	56	Attacking Attackers	3
7	Viruses Worms and Trojan Malicious Code	17	57	Awareness	3
8	Email	14	58	Backups	3
9	Privacy	14	59	CCTV Video Surveillance Cameras	3
10	Access Control	13	60	Content security	3
11	Biometrics	13	61	Data Integrity	3
12	Risk Assessment and Analysis	13	62	Hardware Security	3
13	e-Commerce	12	63	Information Flow	3
14	Operating System	12	64	Intrusion Prevention	3
15	Virtual Private Networks	11	65	Kerberos	3
16	World Wide Web Security	10	66	Key Management	3
17	Anonymity and Pseudonymity	9	67	Public Key Infrastructure	3
18	Auditing	9	68	RSA	3
19	Incident response and Handling	9	69	Security Service	3
20	Internet Security	9	70	Security Verification	3
21	Certification and Accreditation (C&A)	8	71	SSL/TLS	3
22	Hacking and Hackers	8	72	Surveillance and Counter Measure	3
23	Information Warfare	8	73	CERT Coordination Center	2
24	Law, Investigation, and Ethics	8	74	Covert channels	2
25	Anti Virus	7	75	Digital Money	2
26	Digital Signatures	7	76	Distributed Systems Security	2
27	PGP - Pretty Good Privacy	7	77	DNS	2
28	Physical Security	7	78	e-Payment Systems	2
29	System Security	7	79	Hash Algorithms	2
30	Threat	7	80	Home security	2
31	Wireless Security	7	81	Homeland Security	2
32	Denial of Service	6	82	Honeypots	2
33	Disaster Recovery	6	83	Information Hiding	2
34	Forensics	6	84	Information Survivability	2
35	Protocols	6	85	Language-Based Security	2
36	Security Management	6	86	Mobile Communications Security	2
37	Security Models	6	87	National Security	2
38	Smart Cards	6	88	Operations Security	2
39	Steganography	6	89	Peer-to-Peer Security	2
40	Vulnerabilities	6	90	Penetration Testing	2
41	Applications and Systems Development	5	91	Perimeter Protection	2
42	Database Security	5	92	Personal Computer Security	2
43	Java Security	5	93	RFC-Request for Comments	2
44	Public Key Infrastructure	5	94	S/MIME	2
45	Security Standards	5	95	Securing Code	2
46	Administration	4	96	Security Architecture	2
47	Business Continuity Planning	4	97	Software Engineering	2
48	Cybercrime	4	98	trust models and trust Management	2
49	Information Security	4	99	Watermarking	2
50	IP Security	4			

ตารางที่ ก-10: แสดงผลการสำรวจประเด็นที่ตัดความถี่เท่ากับ 1 เรียงตามตัวอักษร

ลำดับ	ประเด็น	ความถี่	ลำดับ	ประเด็น	ความถี่
1	Access Control	13	51	Kerberos	3
2	Administration	4	52	Key Management	3
3	AES	3	53	Language-Based Security	2
4	Anonymity and Pseudonymity	9	54	Law, Investigation, and Ethics	8
5	Anti Virus	7	55	Mobile Communications Security	2
6	Applications and Systems Development	5	56	National Security	2
7	Attacking Attackers	3	57	Network Security	21
8	Auditing	9	58	News	4
9	Authentication and Identification	18	59	Operating System	12
10	Awareness	3	60	Operations Security	2
11	Backups	3	61	Password	4
12	Biometrics	13	62	Patches	4
13	Business Continuity Planning	4	63	Peer-to-Peer Security	2
14	CCTV Video Surveillance Cameras	3	64	Penetration Testing	2
15	CERT Coordination Center	2	65	Perimeter Protection	2
16	Certification and Accreditation (C&A)	8	66	Personal Computer Security	2
17	Content security	3	67	PGP - Pretty Good Privacy	7
18	Covert channels	2	68	Physical Security	7
19	Cryptography	28	69	Policy	20
20	Cybercrime	4	70	Privacy	14
21	Data Integrity	3	71	Protocols	6
22	Database Security	5	72	Public Key Infrastructure	5
23	Denial of Service	6	73	Public Key Infrastructure	3
24	Digital Money	2	74	RFC-Request for Comments	2
25	Digital Signatures	7	75	Risk Assessment and Analysis	13
26	Disaster Recovery	6	76	RSA	3
27	Distributed Systems Security	2	77	S/MIME	2
28	DNS	2	78	Securing Code	2
29	e-Commerce	12	79	Security Architecture	2
30	Email	14	80	Security Management	6
31	e-Payment Systems	2	81	Security Models	6
32	Firewalls	20	82	Security Service	3
33	Forensics	6	83	Security Standards	5
34	Hacking and Hackers	8	84	Security Verification	3
35	Hardware Security	3	85	Smart Cards	6
36	Hash Algorithms	2	86	Software Engineering	2
37	Home security	2	87	SSL/TLS	3
38	Homeland Security	2	88	Steganography	6
39	Honeypots	2	89	Surveillance and Counter Measure	3
40	Incident response and Handling	9	90	System Security	7
41	Information Flow	3	91	Telecommunications	4
42	Information Hiding	2	92	Threat	7
43	Information Security	4	93	trust models and trust Management	2
44	Information Survivability	2	94	Virtual Private Networks	11
45	Information Warfare	8	95	Viruses Worms and Trojan Malicious Code	17
46	Internet Security	9	96	Vulnerabilities	6
47	Intrusion Detection Systems	21	97	Watermarking	2
48	Intrusion Prevention	3	98	Wireless Security	7
49	IP Security	4	99	World Wide Web Security	10
50	Java Security	5			

ตารางที่ ก-11: แสดงการจัดกลุ่มของหัวข้อหลักของทุกแหล่งข้อมูลทั้งหมด

ลำดับ	ประเด็น	ความถี่	Cluster								
			2	3	4	5	6	7	8	9	10
1.	Cryptography	28	1	1	1	1	1	1	1	1	1
2.	Intrusion Detection Systems	21	2	2	2	2	2	2	2	2	2
3.	Network Security	21	2	2	2	2	2	2	2	2	2
4.	Firewalls	20	2	2	2	2	2	2	2	2	2
5.	Policy	20	2	2	2	2	2	2	2	2	2
6.	Authentication and Identification	18	2	2	2	2	3	3	3	3	3
7.	Viruses Worms and Trojan Malicious Code	17	2	2	2	2	3	3	3	3	3
8.	Email	14	2	2	3	3	4	4	4	4	4
9.	Privacy	14	2	2	3	3	4	4	4	4	4
10.	Access Control	13	2	2	3	3	4	4	4	4	5
11.	Biometrics	13	2	2	3	3	4	4	4	4	5
12.	Risk Assessment and Analysis	13	2	2	3	3	4	4	4	4	5
13.	e-Commerce	12	2	2	3	3	4	4	4	4	5
14.	Operating System	12	2	2	3	3	4	4	4	4	5
15.	Virtual Private Networks	11	2	3	4	4	5	5	5	5	6
16.	World Wide Web Security	10	2	3	4	4	5	5	5	5	6
17.	Anonymity and Pseudonymity	9	2	3	4	4	5	5	6	6	7
18.	Auditing	9	2	3	4	4	5	5	6	6	7
19.	Incident response and Handling	9	2	3	4	4	5	5	6	6	7
20.	Internet Security	9	2	3	4	4	5	5	6	6	7
21.	Certification and Accreditation (C&A)	8	2	3	4	4	5	5	6	6	7
22.	Hacking and Hackers	8	2	3	4	4	5	5	6	6	7
23.	Information Warfare	8	2	3	4	4	5	5	6	6	7
24.	Law, Investigation, and Ethics	8	2	3	4	4	5	5	6	6	7
25.	Anti Virus	7	2	3	4	4	5	6	7	7	8
26.	Digital Signatures	7	2	3	4	4	5	6	7	7	8
27.	PGP - Pretty Good Privacy	7	2	3	4	4	5	6	7	7	8
28.	Physical Security	7	2	3	4	4	5	6	7	7	8
29.	System Security	7	2	3	4	4	5	6	7	7	8
30.	Threat	7	2	3	4	4	5	6	7	7	8
31.	Wireless Security	7	2	3	4	4	5	6	7	7	8
32.	Denial of Service	6	2	3	4	4	5	6	7	7	8
33.	Disaster Recovery	6	2	3	4	4	5	6	7	7	8
34.	Forensics	6	2	3	4	4	5	6	7	7	8
35.	Protocols	6	2	3	4	4	5	6	7	7	8
36.	Security Management	6	2	3	4	4	5	6	7	7	8
37.	Security Models	6	2	3	4	4	5	6	7	7	8
38.	Smart Cards	6	2	3	4	4	5	6	7	7	8
39.	Steganography	6	2	3	4	4	5	6	7	7	8
40.	Vulnerabilities	6	2	3	4	4	5	6	7	7	8
41.	Applications and Systems Development	5	2	3	4	5	6	7	8	8	9
42.	Database Security	5	2	3	4	5	6	7	8	8	9
43.	Java Security	5	2	3	4	5	6	7	8	8	9
44.	Public Key Infrastructure	5	2	3	4	5	6	7	8	8	9
45.	Security Standards	5	2	3	4	5	6	7	8	8	9
46.	Administration	4	2	3	4	5	6	7	8	8	9
47.	Business Continuity Planning	4	2	3	4	5	6	7	8	8	9
48.	Cybercrime	4	2	3	4	5	6	7	8	8	9
49.	Information Security	4	2	3	4	5	6	7	8	8	9
50.	IP Security	4	2	3	4	5	6	7	8	8	9

ลำดับ	ประเด็น	ความถี่	Cluster								
			2	3	4	5	6	7	8	9	10
51.	News	4	2	3	4	5	6	7	8	8	9
52.	Password	4	2	3	4	5	6	7	8	8	9
53.	Patches	4	2	3	4	5	6	7	8	8	9
54.	Telecommunications	4	2	3	4	5	6	7	8	8	9
55.	AES	3	2	3	4	5	6	7	8	9	10
56.	Attacking Attackers	3	2	3	4	5	6	7	8	9	10
57.	Awareness	3	2	3	4	5	6	7	8	9	10
58.	Backups	3	2	3	4	5	6	7	8	9	10
59.	CCTV Video Surveillance Cameras	3	2	3	4	5	6	7	8	9	10
60.	Content security	3	2	3	4	5	6	7	8	9	10
61.	Data Integrity	3	2	3	4	5	6	7	8	9	10
62.	Hardware Security	3	2	3	4	5	6	7	8	9	10
63.	Information Flow	3	2	3	4	5	6	7	8	9	10
64.	Intrusion Prevention	3	2	3	4	5	6	7	8	9	10
65.	Kerberos	3	2	3	4	5	6	7	8	9	10
66.	Key Management	3	2	3	4	5	6	7	8	9	10
67.	Public Key Infrastructure	3	2	3	4	5	6	7	8	9	10
68.	RSA	3	2	3	4	5	6	7	8	9	10
69.	Security Service	3	2	3	4	5	6	7	8	9	10
70.	Security Verification	3	2	3	4	5	6	7	8	9	10
71.	SSL/TLS	3	2	3	4	5	6	7	8	9	10
72.	Surveillance and Counter Measure	3	2	3	4	5	6	7	8	9	10
73.	CERT Coordination Center	2	2	3	4	5	6	7	8	9	10
74.	Covert channels	2	2	3	4	5	6	7	8	9	10
75.	Digital Money	2	2	3	4	5	6	7	8	9	10
76.	Distributed Systems Security	2	2	3	4	5	6	7	8	9	10
77.	DNS	2	2	3	4	5	6	7	8	9	10
78.	e-Payment Systems	2	2	3	4	5	6	7	8	9	10
79.	Hash Algorithms	2	2	3	4	5	6	7	8	9	10
80.	Home security	2	2	3	4	5	6	7	8	9	10
81.	Homeland Security	2	2	3	4	5	6	7	8	9	10
82.	Honeypots	2	2	3	4	5	6	7	8	9	10
83.	Information Hiding	2	2	3	4	5	6	7	8	9	10
84.	Information Survivability	2	2	3	4	5	6	7	8	9	10
85.	Language-Based Security	2	2	3	4	5	6	7	8	9	10
86.	Mobile Communications Security	2	2	3	4	5	6	7	8	9	10
87.	National Security	2	2	3	4	5	6	7	8	9	10
88.	Operations Security	2	2	3	4	5	6	7	8	9	10
89.	Peer-to-Peer Security	2	2	3	4	5	6	7	8	9	10
90.	Penetration Testing	2	2	3	4	5	6	7	8	9	10
91.	Perimeter Protection	2	2	3	4	5	6	7	8	9	10
92.	Personal Computer Security	2	2	3	4	5	6	7	8	9	10
93.	RFC-Request for Comments	2	2	3	4	5	6	7	8	9	10
94.	S/MIME	2	2	3	4	5	6	7	8	9	10
95.	Securing Code	2	2	3	4	5	6	7	8	9	10
96.	Security Architecture	2	2	3	4	5	6	7	8	9	10
97.	Software Engineering	2	2	3	4	5	6	7	8	9	10
98.	trust models and trust Management	2	2	3	4	5	6	7	8	9	10
99.	Watermarking	2	2	3	4	5	6	7	8	9	10

ภาคผนวก ข

ผลการจัดหมวดหมู่ย่อย

บทนี้จะแสดงผลของการจัดกลุ่มของหัวข้อย่อยทั้ง 14 ประเด็นของหมวดหมู่หลัก โดยใช้กรรมวิธีตามหัวข้อที่ 4.2 โดยมีรายละเอียดดังนี้

1) Access Control

ตารางที่ ข-1: แสดงการจัดกลุ่มของประเด็นย่อยต่อหัวข้อหลัก Access Control

ลำดับ	ประเด็น	ความถี่	Cluster								
			2	3	4	5	6	7	8	9	10
1	Access Control Lists	50	1	1	1	1	1	1	1	1	1
2	Camera & CCTV	25	2	2	2	2	2	2	2	2	2
3	Smart Card & Plastic Card	22	2	2	2	3	3	3	3	3	3
4	Detection	22	2	2	2	3	3	3	3	3	3
5	Fingerprint, Recognition	20	2	2	2	3	3	3	4	4	4
6	Role Based Access Control	11	2	3	3	4	4	4	5	5	5
7	XML	11	2	3	3	4	4	4	5	5	5
8	Authentication	9	2	3	3	4	4	5	6	6	6
9	Firewall	8	2	3	3	4	4	5	6	6	7
10	Htaccess	7	2	3	4	5	5	6	7	7	8
11	Barcode	6	2	3	4	5	5	6	7	7	8
12	Port	5	2	3	4	5	5	6	7	8	9
13	Network	5	2	3	4	5	5	6	7	8	9
14	Door entry	4	2	3	4	5	5	6	7	8	9
15	Java	3	2	3	4	5	6	7	8	9	10
16	Mandatory Access Control	2	2	3	4	5	6	7	8	9	10
17	Network Access Control	2	2	3	4	5	6	7	8	9	10
18	OpenLDAP	2	2	3	4	5	6	7	8	9	10
19	RSBAC	2	2	3	4	5	6	7	8	9	10
20	Internet Access Control	2	2	3	4	5	6	7	8	9	10

ได้เลือกเอาประเด็นที่1 ถึง 14 ที่ Cluster ที่ 6 เพราะทำให้แบ่งกลุ่มข้อมูลความถี่ที่น่าสนใจได้ไม่เกิน 16 ประเด็น ซึ่งสามารถแบ่งข้อมูลได้ 6 กลุ่มซึ่ง 5 กลุ่มแรกเป็นประเด็นที่เลือกเพื่อมาเป็นหมวดหมู่ย่อยของหมวดหมู่หลัก Access Control

2) Authentication

ตารางที่ ข-2: แสดงการจัดกลุ่มของประเด็นย่อยต่อหัวข้อหลัก Authentication

ลำดับ	ประเด็น	ความถี่	Cluster								
			2	3	4	5	6	7	8	9	10
1	Password	41	1	1	1	1	1	1	1	1	1

ลำดับ	ประเด็น	ความถี่	Cluster								
			2	3	4	5	6	7	8	9	10
2	Biometric	24	2	2	2	2	2	2	2	2	2
3	Network Authentication	24	2	2	2	2	2	2	2	2	2
4	Digital Signatures	18	2	2	3	3	3	3	3	3	3
5	RFC	18	2	2	3	3	3	3	3	3	3
6	Kerberos	15	2	2	3	3	4	4	4	4	4
7	Encryption	9	2	3	4	4	5	5	5	5	5
8	Fingerprint	8	2	3	4	4	5	5	5	6	6
9	Smart card	6	2	3	4	5	6	6	6	7	7
10	Access Controls	6	2	3	4	5	6	6	6	7	7
11	RADIUS	6	2	3	4	5	6	6	6	7	7
12	Single sign	5	2	3	4	5	6	6	7	8	8
13	Two-factor authentication	5	2	3	4	5	6	6	7	8	8
14	Java	5	2	3	4	5	6	6	7	8	8
15	NTLM Authentication	4	2	3	4	5	6	6	7	8	9
16	Privacy	4	2	3	4	5	6	6	7	8	9
17	Intrusion detection	3	2	3	4	5	6	7	8	9	10
18	PPP	2	2	3	4	5	6	7	8	9	10
19	Remote Acess Network	2	2	3	4	5	6	7	8	9	10

ได้เลือกเอาประเด็นที่ 1 ถึง 16 ที่ Cluster ที่ 7 เพราะทำให้แบ่งกลุ่มข้อมูลความถี่ที่น่าสนใจได้ไม่เกิน 16 ประเด็น ซึ่งสามารถแบ่งข้อมูลได้ 7 กลุ่มซึ่ง 6 กลุ่มแรกเป็นประเด็นที่เลือกเพื่อมาเป็นหมวดหมู่ย่อยของหมวดหมู่หลัก Authentication

3) Biometrics

ตารางที่ ข-3: แสดงการจัดกลุ่มของประเด็นย่อยต่อหัวข้อหลัก Biometrics

ลำดับ	ประเด็น	ความถี่	Cluster								
			2	3	4	5	6	7	8	9	10
1	Smart Cards	55	1	1	1	1	1	1	1	1	1
2	Finger Print	34	2	2	2	2	2	2	2	2	2
3	Access Control	27	2	2	2	3	3	3	3	3	3
4	Face, Recognition	26	2	2	2	3	3	3	3	4	4
5	Authentication	19	2	3	3	4	4	4	4	5	5
6	Voice biometrics	15	2	3	3	4	5	5	5	6	6
7	Privacy	14	2	3	3	4	5	5	6	7	7
8	Iris	13	2	3	3	4	5	5	6	7	8
9	CCTV & Cameras	6	2	3	4	5	6	6	7	8	9
10	Information security	3	2	3	4	5	6	7	8	9	10
11	XML	2	2	3	4	5	6	7	8	9	10
12	Hand Geometry	2	2	3	4	5	6	7	8	9	10
13	Crypto-Gram	2	2	3	4	5	6	7	8	9	10

ได้เลือกเอาทุกประเด็นเพราะมีข้อมูลน้อยมาก และไม่เกิน 10-16 ประเด็น

4) Cryptography

ตารางที่ ข-4: แสดงการจัดกลุ่มของประเด็นย่อยต่อหัวข้อหลัก Cryptography

ลำดับ	ประเด็น	ความถี่	Cluster								
			2	3	4	5	6	7	8	9	10
1	Key Cryptography	72	1	1	1	1	1	1	1	1	1
2	Privacy	37	2	2	2	2	2	2	2	2	2
3	Quantum	19	2	3	3	3	3	3	3	3	3
4	Java Cryptography	23	2	3	3	3	3	4	4	4	4
5	PGP	11	2	3	4	4	4	5	5	5	5
6	Policy	9	2	3	4	4	5	6	6	6	6
7	Network Security	8	2	3	4	4	5	6	6	7	7
8	Information Security	7	2	3	4	4	5	6	6	7	8
9	Digital Signatures	6	2	3	4	4	5	6	7	8	9
10	Steganography	5	2	3	4	4	5	6	7	8	9
11	Attacks	3	2	3	4	5	6	7	8	9	10
13	RSA	3	2	3	4	5	6	7	8	9	10
14	Internet Cryptography	3	2	3	4	5	6	7	8	9	10
15	Codebreakers	3	2	3	4	5	6	7	8	9	10
16	Legislation, Law	2	2	3	4	5	6	7	8	9	10

ได้เลือกเอาประเด็นที่ 1 ถึง 10 ที่ Cluster ที่ 5 เพราะทำให้แบ่งกลุ่มข้อมูลความถี่ที่น่าสนใจได้ไม่เกิน 16 ประเด็น ซึ่งสามารถแบ่งข้อมูลได้ 5 กลุ่มซึ่ง 4 กลุ่มแรกเป็นประเด็นที่เลือกเพื่อมาเป็นหมวดหมู่ย่อยของหมวดหมู่หลัก Cryptography

5) e-Commerce

ตารางที่ ข-5: แสดงการจัดกลุ่มของประเด็นย่อยต่อหัวข้อหลัก e-Commerce

ลำดับ	ประเด็น	ความถี่	Cluster								
			2	3	4	5	6	7	8	9	10
1	SSL	46	1	1	1	1	1	1	1	1	1
2	Hosting	43	1	1	1	1	2	2	2	2	2
3	Network Security	40	1	1	1	1	2	2	3	3	3
4	Internet Security	29	2	2	2	2	3	3	4	4	4
5	Certificates	21	2	2	3	3	4	4	5	5	5
6	Web Hosting	13	2	2	3	4	5	5	6	6	6
7	Law	7	2	3	4	5	6	6	7	7	7
8	Security Audit	6	2	3	4	5	6	6	7	7	8
9	Programming	5	2	3	4	5	6	6	7	8	9
10	Seal	4	2	3	4	5	6	6	7	8	9
11	PKI	4	2	3	4	5	6	6	7	8	9
13	Policy Framework for Interpreting Risk	2	2	3	4	5	6	7	8	9	10
14	Homeland Security	2	2	3	4	5	6	7	8	9	10
15	Commerce Security Information	2	2	3	4	5	6	7	8	9	10

ได้เลือกเอาประเด็นที่ 1 ถึง 11 ที่ Cluster ที่ 7 เพราะทำให้แบ่งกลุ่มข้อมูลความถี่ที่น่าสนใจได้ไม่เกิน 16 ประเด็น ซึ่งสามารถแบ่งข้อมูลได้ 7 กลุ่มซึ่ง 6 กลุ่มแรกเป็นประเด็นที่เลือกเพื่อมาเป็นหมวดหมู่ย่อยของหมวดหมู่หลัก e-Commerce

6) e-mail Security

ตารางที่ ข-6: แสดงการจัดกลุ่มของประเด็นย่อยต่อหัวข้อหลัก e-mail

ลำดับ	ประเด็น	ความถี่	Cluster								
			2	3	4	5	6	7	8	9	10
1	Privacy	69	1	1	1	1	1	1	1	1	1
2	Encryption	65	1	1	1	1	1	1	2	2	2
3	Network Security	47	2	2	2	2	2	2	3	3	3
4	Spam	36	2	2	3	3	3	3	4	4	4
5	Virus	28	2	2	3	3	4	4	5	5	5
6	Policy	24	2	2	3	3	4	4	5	6	6
7	PGP	20	2	3	4	4	5	5	6	7	7
8	Information Security	17	2	3	4	4	5	5	6	7	7
9	Anonymous	16	2	3	4	4	5	5	6	7	7
10	Filtering	14	2	3	4	4	5	6	7	8	8
11	Anti-Spam	13	2	3	4	4	5	6	7	8	8
13	Anti-Virus	12	2	3	4	4	5	6	7	8	8
14	MIME	10	2	3	4	4	5	6	7	8	8
15	Internet Security	8	2	3	4	5	6	7	8	9	9
16	Response	7	2	3	4	5	6	7	8	9	9
17	Auditing	6	2	3	4	5	6	7	8	9	9
18	Security Testing	6	2	3	4	5	6	7	8	9	9
19	Hoax Emails	5	2	3	4	5	6	7	8	9	10
20	Certificates	4	2	3	4	5	6	7	8	9	10
21	Administration	3	2	3	4	5	6	7	8	9	10
22	Security Management	3	2	3	4	5	6	7	8	9	10
23	Firewalls	2	2	3	4	5	6	7	8	9	10

ได้เลือกเอาประเด็นที่ 1 ถึง 14 ที่ Cluster ที่ 5 เพราะทำให้แบ่งกลุ่มข้อมูลความถี่ที่น่าสนใจได้ไม่เกิน 16 ประเด็น ซึ่งสามารถแบ่งข้อมูลได้ 5 กลุ่มซึ่ง 4 กลุ่มแรกเป็นประเด็นที่เลือกเพื่อมาเป็นหมวดหมู่ย่อยของหมวดหมู่หลัก e-mail Security

7) Firewalls

ตารางที่ ข-7: แสดงการจัดกลุ่มของประเด็นย่อยต่อหัวข้อหลัก Firewalls

ลำดับ	ประเด็น	ความถี่	Cluster								
			2	3	4	5	6	7	8	9	10
1	Network	83	1	1	1	1	1	1	1	1	1
2	VPN	48	2	2	2	2	2	2	2	2	2
3	Personal Firewalls	35	2	2	3	3	3	3	3	3	3
4	Internet Security	32	2	2	3	3	3	3	4	4	4
5	Filtering	18	2	3	4	4	4	4	5	5	5
6	Linux	16	2	3	4	4	4	5	6	6	6
7	Anti-Virus	15	2	3	4	4	4	5	6	6	7
8	Router	14	2	3	4	4	4	5	6	6	7
9	Windows	14	2	3	4	4	4	5	6	6	7
10	Information security	14	2	3	4	4	4	5	6	6	7
11	IDS	6	2	3	4	5	5	6	7	7	8
12	Scan Port	6	2	3	4	5	5	6	7	7	8

ลำดับ	ประเด็น	ความถี่	Cluster								
			2	3	4	5	6	7	8	9	10
13	SSL	4	2	3	4	5	6	7	8	8	9
14	Unix	2	2	3	4	5	6	7	8	9	10
15	Encryption	2	2	3	4	5	6	7	8	9	10
16	Penetration Testing	2	2	3	4	5	6	7	8	9	10

ได้เลือกเอาประเด็นที่ 1 ถึง 10 ที่ cluster ที่ 5 เพราะทำให้แบ่งกลุ่มข้อมูลความถี่ที่น่าสนใจได้ไม่เกิน 10 ประเด็น ซึ่งสามารถแบ่งข้อมูลได้ 5 กลุ่มซึ่ง 4 กลุ่มแรกเป็นประเด็นที่เลือกเพื่อมาเป็นหมวดหมู่ย่อยของหมวดหมู่หลัก Firewalls

8) Intrusion Detection Systems

ตารางที่ ข-8: แสดงการจัดกลุ่มของประเด็นย่อยต่อหัวข้อหลัก Intrusion Detection Systems

ลำดับ	ประเด็น	ความถี่	Cluster								
			2	3	4	5	6	7	8	9	10
1	Network security	28	1	1	1	1	1	1	1	1	1
2	Firewall	22	1	2	2	2	2	2	2	2	2
3	Audit	19	1	2	2	3	3	3	3	3	3
4	Hackers & Hacking	15	1	2	3	4	4	4	4	4	4
5	Snort	13	1	2	3	4	5	5	5	5	5
6	Vulnerability	4	2	3	4	5	6	6	6	6	6
7	Scanner	4	2	3	4	5	6	6	6	7	7
8	Honeypot	4	2	3	4	5	6	6	6	7	8
9	Internet Security	3	2	3	4	5	6	7	7	8	9
10	Information Systems	3	2	3	4	5	6	7	7	8	9
11	Detection signatures	3	2	3	4	5	6	7	7	8	9
12	VPN	2	2	3	4	5	6	7	8	9	10
13	Intelligent intrusion	2	2	3	4	5	6	7	8	9	10
14	File Integrity	2	2	3	4	5	6	7	8	9	10

ได้เลือกเอาประเด็นที่ 1 ถึง 11 ที่ cluster ที่ 8 เพราะทำให้แบ่งกลุ่มข้อมูลความถี่ที่น่าสนใจได้ไม่เกิน 10 ประเด็น ซึ่งสามารถแบ่งข้อมูลได้ 8 กลุ่มซึ่ง 7 กลุ่มแรกเป็นประเด็นที่เลือกเพื่อมาเป็นหมวดหมู่ย่อยของหมวดหมู่หลัก Inftrusion Detection Systems

9) Networking Security

ตารางที่ ข-9: แสดงการจัดกลุ่มของประเด็นย่อยต่อหัวข้อหลัก Network Security

ลำดับ	ประเด็น	ความถี่	Cluster								
			2	3	4	5	6	7	8	9	10
1	Intrusion detection	29	1	1	1	1	1	1	1	1	1
2	Scanning	23	1	1	1	2	2	2	2	2	2
3	Anti Virus & Virus	37	1	2	2	3	3	3	3	3	3
4	Policy	22	1	1	1	2	2	2	4	4	4
5	Hacking	21	1	1	1	2	2	2	4	4	5
6	Encryption	14	2	3	3	4	4	4	5	5	6
7	Wireless Network	14	2	3	3	4	4	4	5	5	6
8	Penetration Testing	13	2	3	3	4	4	4	5	5	6

9	Information security	9	2	3	3	4	5	5	6	6	7
10	Internet Security	9	2	3	3	4	5	5	6	6	7
11	Firewalls	8	2	3	3	4	5	5	6	6	7
12	Biometric	6	2	3	4	5	6	6	7	7	8
13	Smart Card	5	2	3	4	5	6	6	7	8	9
14	Information Systems Security	5	2	3	4	5	6	6	7	8	9
15	Privacy	4	2	3	4	5	6	6	7	8	9
16	VPN	4	2	3	4	5	6	6	7	8	9
17	Hotfix Checker	2	2	3	4	5	6	7	8	9	10
18	Vulnerability	2	2	3	4	5	6	7	8	9	10
19	Certificate Security	2	2	3	4	5	6	7	8	9	10
20	Cert Coordination Center	2	2	3	4	5	6	7	8	9	10

ได้เลือกเอาประเด็นที่ 1 ถึง 11 ที่ cluster ที่ 4 เพราะทำให้แบ่งกลุ่มข้อมูลความถี่ที่น่าสนใจได้ไม่เกิน 16 ประเด็น ซึ่งสามารถแบ่งข้อมูลได้ 4 กลุ่มซึ่ง 3 กลุ่มแรกเป็นประเด็นที่เลือกเพื่อมาเป็นหมวดหมู่ย่อยของหมวดหมู่หลัก Network Security

10) Operating System

ลำดับ	ประเด็น	ความถี่	Cluster								
			2	3	4	5	6	7	8	9	10
1	Linux	97	1	1	1	1	1	1	1	1	1
2	Windows	82	1	1	2	2	2	2	2	2	2
3	Unix	70	1	1	2	2	3	3	3	3	3
4	Network Security	46	2	2	3	3	4	4	4	4	4
5	FreeBSD	30	2	3	4	4	5	5	5	5	5
6	Patches	30	2	3	4	4	5	5	5	5	5
7	Mac	24	2	3	4	4	5	5	6	6	6
8	Information Security	23	2	3	4	4	5	5	6	6	6
9	Audit	23	2	3	4	4	5	5	6	6	6
10	Solaris	22	2	3	4	4	5	5	6	6	6
11	Access control	17	2	3	4	5	6	6	7	7	7
12	Exploits	14	2	3	4	5	6	6	7	7	8
13	Microsoft	14	2	3	4	5	6	6	7	7	8
14	Hackers & Hacking	10	2	3	4	5	6	6	7	8	9
15	Security Checklist	9	2	3	4	5	6	6	7	8	9
16	Smartcards	5	2	3	4	5	6	7	8	9	10
17	Application Security	5	2	3	4	5	6	7	8	9	10
18	Anti-virus	5	2	3	4	5	6	7	8	9	10
19	Oracle Security	4	2	3	4	5	6	7	8	9	10
20	OpenVMS	3	2	3	4	5	6	7	8	9	10
21	Network Operating System	3	2	3	4	5	6	7	8	9	10
22	Intrusion Detection System	2	2	3	4	5	6	7	8	9	10

ได้เลือกเอาประเด็นที่ 1 ถึง 10 ที่ clustet ที่ 5 พราะทำให้แบ่งกลุ่มข้อมูลความถี่ที่น่าสนใจได้ไม่เกิน 16 ประเด็น ซึ่งสามารถแบ่งข้อมูลได้ 5 กลุ่มซึ่ง 4 กลุ่มแรกเป็นประเด็นที่เลือกเพื่อมาเป็นหมวดหมู่ย่อยของหมวดหมู่หลัก Operating System

11) Policy

ตารางที่ ข-11: แสดงการจัดกลุ่มของประเด็นย่อยต่อหัวข้อหลัก Policy

ลำดับ	ประเด็น	ความถี่	Cluster					
			2	3	4	5	6	7
1	Privacy	134	1	1	1	1	1	1
2	Information security	99	1	2	2	2	2	2
3	Network Security	64	1	2	3	3	3	3
4	HIPAA	11	2	3	4	4	4	4
5	Windows	5	2	3	4	5	5	5
6	Law	4	2	3	4	5	5	6
7	Rfc 2196	2	2	3	4	5	6	7
8	Access Control	2	2	3	4	5	6	7

ได้เลือกเอาทุกประเด็นเพราะมีข้อมูลน้อยมาก และไม่เกิน 10-16 ประเด็น

12) Privacy

ตารางที่ ข-12: แสดงการจัดกลุ่มของประเด็นย่อยต่อหัวข้อหลัก Privacy

ลำดับ	ประเด็น	ความถี่	Cluster								
			2	3	4	5	6	7	8	9	10
1	Privacy Policy	243	1	1	1	1	1	1	1	1	1
2	Privacy Statement	99	2	2	2	2	2	2	2	2	2
3	Rights	37	2	3	3	3	3	3	3	3	3
4	Internet Privacy	31	2	3	3	3	4	4	4	4	4
5	Anonymous and Anomymity	29	2	3	3	3	4	4	4	4	5
6	P3P	20	2	3	3	4	5	5	5	5	6
7	HIPAA	11	2	3	4	5	6	6	6	6	7
8	Law	8	2	3	4	5	6	7	7	7	8
9	Personal privacy	6	2	3	4	5	6	7	7	8	9
10	PGP	6	2	3	4	5	6	7	7	8	9
11	Cookies	5	2	3	4	5	6	7	7	8	9
12	GNU Privacy	5	2	3	4	5	6	7	7	8	9
13	Digital Privacy	6	2	3	4	5	6	7	7	8	9
14	Biometrics	3	2	3	4	5	6	7	8	9	10
15	Privacy laws	3	2	3	4	5	6	7	8	9	10
16	Privacy Management	3	2	3	4	5	6	7	8	9	10
17	Printed Copy	2	2	3	4	5	6	7	8	9	10

ได้เลือกเอาประเด็นที่ 1 ถึง 13 ที่ cluster ที่ 8 เพราะทำให้แบ่งกลุ่มข้อมูลความถี่ที่น่าสนใจได้ไม่เกิน 10 ประเด็น ซึ่งสามารถแบ่งข้อมูลได้ 8 กลุ่มซึ่ง 7 กลุ่มแรกเป็นประเด็นที่เลือกเพื่อมาเป็นหมวดหมู่ย่อยของหมวดหมู่หลัก Privacy

13) Risk Assessment and Analysis

ตารางที่ ข-14: แสดงการจัดกลุ่มของประเด็นย่อยต่อหัวข้อหลัก Risk Assessment and Analysis

ลำดับ	ประเด็น	ความถี่	Cluster								
			2	3	4	5	6	7	8	9	10
1	Information Security	100	1	1	1	1	1	1	1	1	1
2	Network Security	62	1	2	2	2	2	2	2	2	2
3	HIPAA	30	2	3	3	3	3	3	3	3	3
4	Vulnerability	30	2	3	3	3	3	3	3	3	3
5	Security Audits	17	2	3	4	4	4	4	4	4	4
6	Privacy	12	2	3	4	5	5	5	5	5	5
7	Internet Security	11	2	3	4	5	5	5	5	5	6
8	Virus	8	2	3	4	5	5	6	6	6	7
9	Threat	6	2	3	4	5	6	7	7	7	8
10	Investigation	6	2	3	4	5	6	7	7	7	8
11	Business continuity	5	2	3	4	5	6	7	7	8	9
12	Methodology	5	2	3	4	5	6	7	7	8	9
13	Policy	5	2	3	4	5	6	7	7	8	9
14	Risk Assessment Process and Methodology	5	2	3	4	5	6	7	7	8	9
15	Security Plan	5	2	3	4	5	6	7	7	8	9
16	Intrusion detection	4	2	3	4	5	6	7	7	8	9
17	Security Survey And Risk Assessment	3	2	3	4	5	6	7	8	9	10
18	Assessment Checklist	2	2	3	4	5	6	7	8	9	10
19	Penetration Testing	2	2	3	4	5	6	7	8	9	10

ได้เลือกเอาประเด็นที่ 1 ถึง 10 cluster ที่ 9 เพราะทำให้แบ่งกลุ่มข้อมูลความถี่ที่น่าสนใจได้ไม่เกิน 16 ประเด็น ซึ่งสามารถแบ่งข้อมูลได้ 9 กลุ่มซึ่ง 8 กลุ่มแรกเป็นประเด็นที่เลือกเพื่อมาเป็นหมวดหมู่ย่อยของหมวดหมู่หลัก Risk Assessment and Analysis

14) Viruses Worms Trojans and Malicious Code

ตารางที่ ข-14: แสดงการจัดกลุ่มของประเด็นย่อยต่อหัวข้อหลัก Viruses Worms Trojans and Malicious Code

ลำดับ	ประเด็น	ความถี่	Cluster								
			2	3	4	5	6	7	8	9	10
1	Network Security	119	1	1	1	1	1	1	1	1	1
2	Anti-Virus	63	2	2	2	2	2	2	2	2	2
3	Information Security	57	2	2	2	2	3	3	3	3	3
4	Internet Security	54	2	2	2	2	3	3	3	3	3
5	Security Scan	47	2	2	2	3	4	4	4	4	4
6	Anti-Trojan	26	2	3	3	4	5	5	5	5	5
7	Firewall	22	2	3	3	4	5	5	6	6	6
8	Privacy	20	2	3	3	4	5	5	6	6	6
9	Vulnerabilities	18	2	3	3	4	5	5	6	6	7
10	Patch	17	2	3	3	4	5	5	6	6	7
11	Hacking	13	2	3	4	5	6	6	7	7	8
12	Virus Information	13	2	3	4	5	6	6	7	7	8
13	Hoaxes	11	2	3	4	5	6	6	7	7	8
14	CIAC, Computer Incident A	9	2	3	4	5	6	6	7	8	9
15	CERT	8	2	3	4	5	6	6	7	8	9
16	Attacks	7	2	3	4	5	6	6	7	8	9

ลำดับ	ประเด็น	ความถี่	Cluster								
			2	3	4	5	6	7	8	9	10
17	Threats	4	2	3	4	5	7	6	8	9	10
18	Exploits	4	2	3	4	5	7	6	8	9	10
19	Backdoor Trojan	4	2	3	4	5	7	6	8	9	10
20	PGP	3	2	3	4	5	7	6	8	9	10
21	Security incidents	3	2	3	4	5	7	6	8	9	10
22	Exploit	3	2	3	4	5	7	6	8	9	10
23	Content filtering	3	2	3	4	5	7	6	8	9	10
24	Malicious	2	2	3	4	5	7	6	8	9	10
25	Risk Management	2	2	3	4	5	7	6	8	9	10
26	Hacker	2	2	3	4	5	7	6	8	9	10

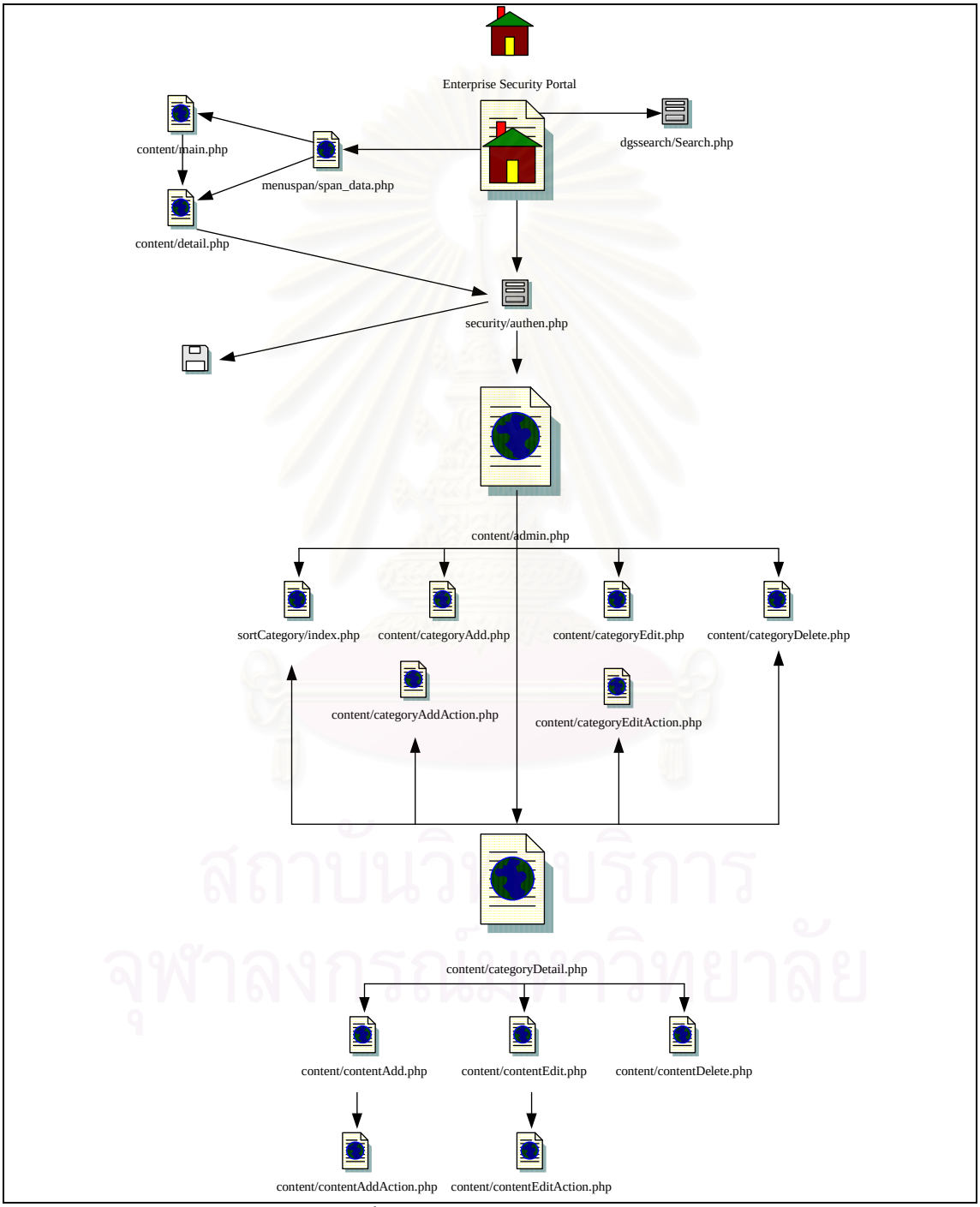
ได้เลือกเอาประเด็นที่ 1 ถึง 11 cluster ที่ 4 เพราะทำให้แบ่งกลุ่มข้อมูลความถี่ที่น่าสนใจได้ไม่เกิน 16 ประเด็น ซึ่งสามารถแบ่งข้อมูลได้ 4 กลุ่มซึ่ง 3 กลุ่มแรกเป็นประเด็นที่เลือกเพื่อมาเป็นหมวดหมู่ย่อยของหมวดหมู่หลัก Viruses Worms Trojans and Malicious Code

สถาบันวิทยบริการ
จุฬาลงกรณ์มหาวิทยาลัย

ภาคผนวก ค

การออกแบบระบบ

ค-1. ภาพรวมความสัมพันธ์ของหน้าจอในระบบ



รูปที่ ค-1: System Overview Design

ค-2. การออกแบบหน้าจอส่วนผู้ใช้งานระบบ (User Screen Design)

ตารางที่ ค-1: การออกแบบหน้าจอแสดงข้อมูลหลัก

หน้าจอ	หน้าจอแสดงข้อมูลหลัก
แฟ้มข้อมูล	/content/main.php
คำอธิบาย	หน้าจอแสดงผลหลัก โดยจะแสดงรายการข้อมูล / ประเภทข้อมูลย่อยภายใต้ประเภทข้อมูลที่กำหนด
ค่าที่รับเข้า	CategoryID = รหัสประเภทที่ต้องการดูข้อมูล

ตารางที่ ค-2: การออกแบบหน้าจอแสดงข้อมูลย่อย

หน้าจอ	หน้าจอแสดงข้อมูลย่อย
แฟ้มข้อมูล	/content/detail.php
คำอธิบาย	หน้าจอแสดงรายละเอียดข้อมูล
ค่าที่รับเข้า	categoryID = รหัสประเภทที่ต้องการดูข้อมูล contentID = รหัสข้อมูลที่ต้องการดูข้อมูล

ค-3. การออกแบบหน้าจอส่วนผู้ดูแลระบบ (Administrator Screen Design)

ตารางที่ ค-3: การออกแบบหน้าจอหลักผู้ดูแลระบบ

หน้าจอ	หน้าจอหลักผู้ดูแลระบบ
แฟ้มข้อมูล	/content/admin.php
คำอธิบาย	หน้าจอหลักของผู้ดูแลระบบ แสดงหมวดหมู่ของเนื้อหาหลัก สามารถเพิ่ม/แก้ไข/ลบหมวดหมู่ของเนื้อหาหลักได้

ตารางที่ ค-4: การออกแบบหน้าจอรายละเอียดข้อมูลภายใต้ประเภทใดๆ

หน้าจอ	หน้าจอรายละเอียดข้อมูลภายใต้ประเภทใดๆ
แฟ้มข้อมูล	/content/categoryDetail.php
คำอธิบาย	หน้าจอแก้ไขรายละเอียดของประเภทข้อมูลลำดับใดๆ (ระดับที่ 1 เป็นต้นไป) โดยสามารถเพิ่ม/แก้ไข/ลบข้อมูลเนื้อหา (ในกรณีที่ไม่มีประเภทข้อมูลย่อย) หรือเพิ่ม/แก้ไข/ลบประเภทข้อมูลย่อยในระดับต่อไป
ค่าที่รับเข้า	categoryID = รหัสของประเภทข้อมูลที่ต้องการแก้ไข

ตารางที่ ค-5: การออกแบบหน้าจอเพิ่มชื่อของประเภทข้อมูล

หน้าจอ	หน้าจอเพิ่มชื่อของประเภทข้อมูล
แฟ้มข้อมูล	/content/categoryAdd.php
คำอธิบาย	สำหรับกรอกชื่อของประเภทข้อมูล เพื่อไปเพิ่มข้อมูล ลักษณะเป็นการเปิดหน้าต่างใหม่ (popup) เมื่อเพิ่มข้อมูลเสร็จแล้วปิดหน้าต่าง พร้อม update ข้อมูลหน้าหลัก
ค่าที่รับเข้า	ParentCategoryID = รหัสของประเภทข้อมูลที่อยู่ก่อนหน้า 1 ระดับ (ถ้าไม่ส่งค่าแสดงว่าเป็น

	ข้อมูลระดับสูงสุด)

ตารางที่ ค-6: การออกแบบหน้าจอแก้ไขชื่อของประเภทข้อมูล

หน้าจอ	หน้าจอแก้ไขชื่อของประเภทข้อมูล
แฟ้มข้อมูล	/content/categoryEdit.php
คำอธิบาย	สำหรับแก้ไขชื่อของประเภทข้อมูล โดยจะแสดงข้อมูลเดิมใน textbox ก่อน ลักษณะเป็นการเปิดหน้าต่างใหม่ (popup) เมื่อเพิ่มข้อมูลเสร็จแล้วปิดหน้าต่าง พร้อม update ข้อมูลหน้าหลัก
ค่าที่รับเข้า	categoryID = รหัสของประเภทข้อมูลที่ต้องการแก้ไข

ตารางที่ ค-7: การออกแบบหน้าจอเพิ่มข้อมูลเนื้อหา

หน้าจอ	หน้าจอเพิ่มข้อมูลเนื้อหา
แฟ้มข้อมูล	/content/contentAdd.php
คำอธิบาย	รับรายละเอียดของข้อมูล โดยให้ใส่รายละเอียดเนื้อหาผ่านทาง Rich Text Edit Module แล้ว จัดเก็บเนื้อหาไว้ใน file HTML เพื่อความสะดวกและยืดหยุ่นในการแก้ไขเนื้อหาในภายหลัง
ค่าที่รับเข้า	categoryID = รหัสของประเภทข้อมูลที่อยู่เหนือข้อมูล

ตารางที่ ค-8: การออกแบบหน้าจอแก้ไขข้อมูลเนื้อหา

หน้าจอ	หน้าจอแก้ไขข้อมูลเนื้อหา
แฟ้มข้อมูล	/content/contentAdd.php
คำอธิบาย	แก้ไขข้อมูล โดยอ่าน file HTML แล้วมาแสดงใน Rich Text Edit Module
ค่าที่รับเข้า	contentID = รหัสของข้อมูลที่ต้องการแก้ไข

ตารางที่ ค-9: การออกแบบหน้าจอแนบเอกสาร

หน้าจอ	หน้าจอแนบเอกสาร
แฟ้มข้อมูล	/content/attach.php
คำอธิบาย	เพิ่ม ลบ เอกสารแนบ
ค่าที่รับเข้า	contentID = รหัสของข้อมูลที่ต้องการแนบเอกสาร

ค-4. การออกแบบหน้าจอสำหรับค้นหา (Search Design)

ตารางที่ ค-10: การออกแบบหน้าจอแสดงการรับข้อมูลสำหรับค้นหา

หน้าจอ	หน้าจอแสดงการรับข้อมูลสำหรับค้นหา
แฟ้มข้อมูล	/dgssearch/search.php
คำอธิบาย	หน้าจอที่ใช้สำหรับค้นหาโดยค้นหาจากคำสำคัญที่ผู้ใช้ป้อนเข้ามา จากนั้นระบบจะทำการ ค้นหาในฐานข้อมูลและไฟล์ข้อมูลที่จัดเก็บ
ค่าที่รับเข้า	keyword = คำที่ต้องการหา num = จำนวนที่ต้องการแสดงในแต่ละหน้าจอ

ภาคผนวก ง

การออกแบบโครงสร้างฐานข้อมูล

ตารางที่ ง-1: โครงสร้างฐานข้อมูล

ชื่อ Table	คำอธิบาย Table
CATEGORY	เก็บประเภทของข้อมูล
CONTENT	เนื้อหาของข้อมูล
FILE_STORAGE	ตารางสำหรับเก็บไฟล์ข้อมูล/รูปภาพ ของข้อมูลต่างๆ ภายใต้ประเภทข้อมูล
USERS	ตารางข้อมูลผู้ใช้งาน

รายละเอียดของโครงสร้างข้อมูล

ชื่อ Table	ชื่อ Field	ชนิดข้อมูล	คำอธิบาย	FK	PK	Null option
CATEGORY	CategoryID	Number(6)	รหัสประเภทข้อมูล		(pk)	Not Null
	CategoryName	Varchar(255)	ชื่อประเภทข้อมูล			Not Null
	ParentCategory	Number(6)	รหัสประเภทข้อมูลที่เหนือกว่า 1 ระดับ			Not Null
	Description	Memo	คำอธิบายประเภทข้อมูล			Not Null
	SortID	Number(5)	ลำดับความสำคัญ โดยเรียงลำดับความสำคัญจากมากไปน้อย			
	MasterID	Number(6)	รหัสประเภทข้อมูลหลัก			Not Null
CONTENT	ContentID	Number(6)	รหัสข้อมูล		(pk)	Not Null
	categoryID	Number(6)	รหัสประเภทข้อมูล		(fk)	Not Null
	title	varchar(255)	ชื่อหัวข้อเรื่อง			Not Null
	Author	varchar(50)	ผู้แต่งหรือเจ้าของผลงาน			Not Null
	OtherContributors	varchar(50)	ผู้ร่วมงานหรือหน่วยงานอื่นนอกจากผู้แต่งหรือ เจ้าของผลงานที่มีชื่อปรากฏในข้อผู้แต่ง			Null

ชื่อ Table	ชื่อ Field	ชนิดข้อมูล	คำอธิบาย	FK	PK	Null option
	DateRefer	datetime	วันที่อ้างอิง			Not Null
	DateCreate	datetime	วันที่-เวลานำเข้าข้อมูล			Not Null
	DateModified	datetime	วันที่-เวลาปรับปรุงข้อมูลล่าสุด			Not Null
	Visitor	Number(5)	จำนวนผู้เข้าชม			Null
	HtmlPath	varchar(255)	ชื่อ Path ที่เก็บไฟล์ HTML (contentID.txt) ซึ่งเป็นรายละเอียด (Description) ของรายการนี้			Not Null
	MasterID	Number(6)	รหัสประเภทข้อมูลหลัก			Not Null
	Publisher	varchar(120)	สำนักพิมพ์/แหล่งที่มา			Null
	ResourceType	varchar(2)	ประเภทเนื้อหา			Null
FILE_STORAGE	fileID	Number(6)	รหัสไฟล์ข้อมูล		(pk)	Not Null
	ContentID	Number(6)	รหัสจากตาราง CONTENT		(fk)	Not Null
	fileName	datetime	ชื่อไฟล์ข้อมูล (เดิม)			Not Null
	filePath	datetime	ชื่อ Path ไฟล์ข้อมูล (..+fileID+fileName)			Not Null
	fileType	varchar(50)	ประเภทไฟล์ข้อมูล			Null
	describe	Memo	คำอธิบายไฟล์ข้อมูล			Not Null
	dateLastUpdate	datetime	วันที่-เวลาปรับปรุงข้อมูลล่าสุด			Null
	datePost	datetime	วันที่-เวลานำเข้าข้อมูล			Null
	Confirm	varchar(1)	ยืนยันก่อนการเปิดไฟล์			Null
	Ref	varchar(120)	แหล่งที่มา			Null
USERS	Userid	Number(6)	หมายเลขผู้ใช้งาน		(pk)	Not Null
	Username	varchar(8)	รหัสผู้ใช้งาน			Not Null
	Password	varchar(8)	รหัสผ่าน			Not Null
	Name	varchar(50)	ชื่อ			Null
	Admin	varchar(1)	ประเภทผู้ใช้งาน			Null

ประวัติผู้เขียนวิทยานิพนธ์

นายสุรสิทธิ์ มัลลิกานิล เกิดเมื่อวันที่ 30 มกราคม พ.ศ.2519 ที่จังหวัดสกลนคร สำเร็จการศึกษาปริญญาตรีจากคณะวิทยาศาสตร์ มหาวิทยาลัยเชียงใหม่ สาขาวิชาวิทยาการคอมพิวเตอร์ เมื่อปี พ.ศ.2540 และเข้าศึกษาต่อหลักสูตรวิทยาศาสตร์มหาบัณฑิต (วท.ม.) ภาควิชาวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย ในปีการศึกษา 2544 ขณะทำวิทยานิพนธ์ (พ.ศ.2547) ได้ทำงานอยู่ที่ สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ โครงการส่งเสริมเครือข่ายวิสาหกิจคอมพิวเตอร์ ในตำแหน่งเจ้าหน้าที่ระบบคอมพิวเตอร์ 1 (นักพัฒนาระบบ)

สถาบันวิทยบริการ
จุฬาลงกรณ์มหาวิทยาลัย