รายการอ้างอิง

ภาษาอังกฤษ

Bach, Maurice J. The design of the UNIX operating system , Prentice-Hall , 1986.

Brand, Russell L., Copying with the Threat of Computer Security Incidents Aprimer from Prevention through Recovery , Berkeley , CA., 1990.

Cameron Debra, Unix Standard. Computer Technology Research Corp.,1991.

d i g i t a l. DEC MLS+, Trusted UNIX Operating System , SPD 46.21.02 ,Digital Department Cooperation, 1996.

d i g i t a l. Enhanced Security DEC OSF/1 , Order Number : AA-Q0R2AA-TE. Digital Department Cooperation., 1994.

d i g i t a l. OSF/1 Technical Seminar Student Guide. EY-G999E-SG.0002 , Digital Department Cooperation., 1994.

d i g i t a l. System Administration DEC OSF/1 , Order Number : AA-PS2RB-TE . Digital Department Cooperation., 1994.

Curry, David A. Improving the security of your UNIX system , Information and telecommunications Sciences and Technology Division: SRI International, 1990.

Curry, David A. UNIX System Security : A guide for Users and System Administrators , Addison-Wesley, 1992.

DOD (U.S. Dept of Defense). Orange book: Trusted Computing System Evaluation Criteria , DoD5200.28-STD,1983.

Eugen Mate Bacic. UNIX & Security, Sr. InfoSec Research Scientist., Canadian System Security Centre., Communications Security Establishment, CANADA.

Farrow Rik. UNIX security : How to protect your data and prevent intruders , Addison wesly, 1991.

Garfinkel Simson, and Gene Spafford. Practical Unix Security. Computer Security, O'Reilly & Associates, Inc.,1992.

Grampp, F.T. and Moris, R.H. "UNIX Operating System Security," UNIX System Readings and Applications Volume II , Prentice-Hall, 1987.

NCSC (National Computer Security Center). Tan Book: A Guide to understanding Audit in Trusted Systems, NCSC-TG-001, 1987.

NCSC (National Computer Security Center). Salamon Book: A Guide to understanding Discretionary Access Control in Trusted Systems, NCSC-TG-003, 1987.

NCSC (National Computer Security Center). Coral Book: A Guide to understanding Configuration Management in Trusted Systems, NCSC-TG-006-88, 1988.

NCSC (National Computer Security Center). Burgundy Book: A Guide to understanding Design Documentation in Trusted Systems, NCSC-TG-007, 1988.

NCSC (National Computer Security Center). Brown Book: A Guide to understanding Trusted Facility Management in Trusted Systems, NCSC-TG-015, 1989.

NCSC (National Computer Security Center). A Guide to Writing Trusted Facility Manuals in Trusted Systems, NCSC-TG-016, 1992.

NCSC (National Computer Security Center). A Guide to understanding Identification and Authentication in Trusted Systems, NCSC-TG-017, 1991.

NCSC (National Computer Security Center). A Guide to Writing the Security Features User's Guide for Trusted Systems, NCSC-TG-026, 1991.

Pfleeger, Charles P. Security in computing , Prentice-Hall, 1989.

Russell Deborah, and G.T.Gangemi Sr. Computer Security Basics. Computer Security, O'Reilly & Associates, Inc., 1991.

Wang Federal. Wang's XTS-300 Computer System Receives B3 Security Rating from the U.S. National Security Agency (NSA) , Wang Federal, Inc., 1995.

ภาคผนวก

ภาคผนวก ก

อภิธานศัพท์ (GLOSSARY)

Access	-เป็นการกระทำระหว่างตัวกระทำ และตัวถูกกระทำ ที่มีผลทำให้ข้อมูลไหลจากที่หนึ่งไปอีกที่หนึ่ง
Audit Trail	-เป็นเซตของระเบียน ที่เก็บหลักฐาน ของการประมวลผลหรือการกระทำต่าง ๆ ใช้ช่วยในการตรวจดูข้อมูลจากแหล่งที่มา และการเปลี่ยนแปลง
Authenticate	- การแสดงความถูกต้องของสิทธิในการพิสูจน์ตน
Bell-LaPadula Model	-เป็นรูปแบบ การเปลี่ยนสภาวะของนโยบายด้านความมั่นคง ในระบบคอมพิวเตอร์ ซึ่งอธิบายถึงกฎในการควบคุมการเข้าถึง โดยแบ่งสมาชิกเป็น 2 พวกคือ ตัวกระทำ และตัวถูกกระทำ แนวคิดด้าน สภาวะความมั่นคงนี้ ถูกกำหนดและพิสูจน์ได้ว่า แต่ละสภาวะการเปลี่ยนแปลง จะสามารถรักษาระดับความมั่นคงของระบบไว้ได้
Certification	-เป็นเทคนิคในการประเมินคุณสมบัติด้านความมั่นคงของระบบ
Covert Channel	-เป็นช่องทางการสื่อสาร ที่ยอมให้บางโปรเซสส่งผ่านข้อมูลที่สามารถไประเมิดนโยบายความมั่นคงของระบบ
Covert Storage Channel	-เป็นช่องทางลับที่เกี่ยวข้องการเขียนที่ตั้งของที่เก็บ โดยโปรเซสหนึ่ง และมีการอ่านที่ตั้งของที่เก็บนี้ โดยอีกโปรเซสหนึ่งไม่ว่าจะโดยทางตรง หรือทางอ้อมก็ตาม โดยที่ช่องเก็บลับนี้ จะเกี่ยวข้องกับ ทรัพยากรที่เห็นเป็นรูปร่างได้ของระบบ เช่น เซกเตอร์บนดิสต์ ซึ่งจะเป็นการแบ่ง หรือร่วมกันใช้งาน โดยตัวกระทำ 2 ตัวที่มีระดับ ความมั่นคง ต่างกัน
Covert Timing Channel	-เป็นช่องทางลับที่โปรเซสหนึ่งให้สัญญาณข้อมูลไปที่โปรเซสอื่นโดยการแทรกซ้อนตัวเองเข้ากับทรัพยากรของระบบ เช่น เวลาของ CPU ด้วยวิธีการถ่ายเทนี้ มีผลทำให้เวลาตอบสนองที่แท้จริงของระบบ ถูกสังเกตได้จากโปรเซลที่สอง
Data Integrity	-เป็นสภาวะที่ข้อมูลรักษาความเป็นบูรณภาพไว้ได้

Discretionary Access Control (DAC)	-เป็นวิธีหนึ่งในการจำกัดการเข้าถึงตัวถูกกระทำ โดยอาศัยการแสดงตนของตัวกระทำหรือกลุ่มของตัวกระทำ การควบคุมจะอาศัยดุลยพินิจ ที่ตัวกระทำนั้น ได้รับอนุญาตในการเข้าถึง และสามารถที่จะถ่ายทอดสิทธิไปยังตัวกระทำตัวอื่นได้
Flaw	-เป็นข้อผิดพลาด หรือช่องโหว่ที่ถูกมองข้ามไป ในระบบ โดยไม่มีการผ่านการตรวจจับจากกลไกการป้องกันของระบบ
Mandatory Access Control (MAC)	-การควบคุมการเข้าถึงภายใต้อาณัติ เป็นวิธีในการจำกัดการเข้าถึงตัวถูกกระทำ โดยอาศัยความไหวของข้อมูล (มักแสดงในรูปของป้ายชื่อ) ที่อยู่ในตัวถูกกระทำ และการแสดงตนอย่างเป็นทางการของตัวกระทำ (อย่างเช่น ความกระจ่าง) ที่สามารถใช้เข้าถึงข้อมูลที่มีความไหวนั้น ๆ
Multilevel Device	-เป็นอุปกรณ์ที่ยอมให้โปรเซส 2 โปรเซส หรือมากกว่า ที่มีระดับความมั่นคงต่างกัน เข้ามาใช้งานในเวลาเดียวกันได้ โดยปราศจากการเสี่ยง ซึ่งการที่กระทำได้ดังนี้จะอาศัยป้ายชื่อความไหว (เช่น เครื่องสามารถอ่านได้ หรือ คนสามารถอ่านได้) ที่เก็บอยู่ที่สื่อทางกายภาพ และยังคงสภาพเมื่อถูกนำมาใช้ในการประมวลผล
Multilevel Secure	-เป็นการจำแนกการเก็บข้อมูลที่มีความไหวต่างกัน และยอมให้ตัวกระทำที่มีความมั่นคงต่างกันมาใช้งานได้ในเวลาเดียวกัน โดยสามารถป้องกันผู้ใช้เข้าถึงข้อมูลที่ตนไม่มีสิทธิได้
Object	-หมายถึงตัวถูกกระทำ ตัวอย่างเช่น เรคคอร์ด บอล์ค เพจ เซกเมนต์ ไฟล์ ไดเรกทอรี ทรี และโปรแกรม และยังรวมถึงบิต ไบต์ เวิร์ด ฟิลด์ เครื่องประมวลผล จอแสดงวิดีโอ คีย์บอร์ด นาฬิกา เครื่องพิมพ์ และ อื่น ๆ
Object Reuse	-เป็นการนำตัวถูกกระทำ มาใช้ใหม่ คือ มีการกำหนดค่า ให้กับตัวถูกกระทำบางตัวที่เป็นสื่อ เช่น เพจเฟรม เซกเตอร์ของดิสต์ เทปแม่เหล็ก ด้วยค่าที่มากกว่า1 ครั้งซึ่งถ้าเป็นระบบที่มีความมั่นคง การกำหนดค่าใหม่ให้กับสื่อเหล่านี้ จะต้องไม่มีข้อมูลเดิมของเก่า ค้างอยู่บนตัวถูกกระทำเหล่านี้
Password	-รหัสผ่าน หรือชุดของตัวอักขระ ที่ใช้สำหรับในการแสดงตนและพิสูจน์ตน
Penetration Testing	-เป็นส่วนในการ ทดสอบการเจาะระบบ โดยที่พยายามกำจัดคุณสมบัติด้านความมั่นคงของระบบ

Process	-เป็นโปรแกรมในขณะที่กำลังทำงาน
Reference Monitor Concept	-เป็นแนวคิดในเรื่องการควบคุมการเข้าถึง โดยอ้างจากสื่อที่ตัวกระทำ มีการเข้าถึงตัวถูกกระทำทั้งหมด เป็นการเฝ้าดูการทำงานในระบบ
Security Kernel	-เป็นส่วนประกอบพื้นฐานของคอมพิวเตอร์ที่ไว้ใจได้ ทั้งทางด้านฮาร์ดแวร์ เฟิร์มแวร์และซอฟต์แวร์ ที่ใช้สนับสนุนแนวคิดในการเฝ้าดูการทำงานของระบบ โดยต้องมีการป้องกันสื่อที่มีการเข้าถึงทุกชนิด จากการถูกดัดแปลง และสามารถตรวจสอบได้ว่าถูกต้อง
Security Level	-การจำแนกและการแบ่งระดับขั้นความมั่นคงของความไหวของข้อมูล
Security Policy	-เป็นกฎหรือนโยบายด้านความมั่นคง ที่ใช้จัดการกับข้อมูล ที่กระจายในหน่วยงาน
Security Relevant Event	-เป็นเหตุการณ์ที่เกี่ยวข้องหรือพยายามเปลี่ยนสภาวะความมั่นคงในระบบ เช่น เปลี่ยนดีเอซี เปลี่ยนระดับความมั่นคงของตัวกระทำ หรือเปลี่ยนรหัสผ่านของผู้ใช้ เป็นต้น หรือเป็นเหตุการณ์ ที่พยายามสร้างความเสียหายที่มีผลต่อความมั่นคงของระบบ เช่นพยายามเข้าสู่ระบบ พยายามทำการล้ำสิทธิที่ได้รับ หรือพยายามทำลายไฟล์ เป็นต้น
Sensitive Information	-เป็นข้อมูลที่มีความไหว มักถูกตรวจสอบ โดยผู้ที่มีอำนาจในการบริหารและต้องได้รับการปกป้อง จากการเปิดเผยหรือป้องกันจากผู้ที่ไม่ได้รับสิทธิ ในการปลอมแปลงแก้ไขหรือทำลาย
Sensitivity Label	-ป้ายความไหว ใช้สำหรับเป็นข้อมูลในการบอกอธิบายระดับความมั่นคงของตัวถูกกระทำ ซึ่งระบบคอมพิวเตอร์ที่ไว้ใจได้ (ทีซีบี) จะอาศัยป้ายความไหวนี้ ในการตัดสินใจการควบคุมการเข้าถึงภายใต้อาณัติ
Single-Level Device	- เป็นอุปกรณ์ที่ใช้ในการประมวลผลข้อมูลที่มีระดับความมั่นคงในระดับหนึ่งในเวลาหนึ่ง ๆ ถ้าอุปกรณ์นี้ไม่จำเป็นที่จะได้รับความไว้วางใจ ในการแยกข้อมูลที่มีระดับความมั่นคงต่างกันออกจากกัน ข้อมูลที่มีป้ายความไหว ก็จะไม่ถูกนำมาเก็บหรือประมวลผลพร้อมกับข้อมูลอื่น ๆ ที่ประมวลผลอยู่
Storage object	-เป็นตัวถูกกระทำหนึ่งที่สนับสนุนการเข้าถึงทั้งการอ่านและเขียน
Subject	-เป็นตัวผู้กระทำในระบบ โดยทั่วไปมักเป็นบุคคล โปรเซส หรืออุปกรณ์ที่มีผลทำให้ข้อมูลไหลระหว่างตัวถูกกระทำ หรือการเปลี่ยนสถานะของระบบ

Trap Door	-เป็นกลไกทางซอฟต์แวร์ หรือฮาร์ดแวร์ที่ซ่อนอยู่ ที่สามารถผ่านหรือกำจัดกลไกการป้องกัน ของระบบได้ โดยมากมักจะทำงานในที่ที่ไม่ปรากฏ ให้เห็น เช่น การสุ่มลำดับคีย์ที่เทอร์มินอล เป็นต้น
Trojan Horse	-เป็นโปรแกรมที่ทำงานอย่างหนึ่งแล้วมีโปรแกรมการทำงานอีกอย่างแอบแฝงอยู่
Trusted Computer	-เป็นระบบที่รวมเอาทั้งฮาร์ดแวร์ และซอฟต์แวร์ที่เชื่อถือได้ มาใช้ระบบประมวลผลข้อมูลที่มีความไหวต่างกันได้ในขณะเวลาเดียวกัน
Trusted Computing Base (TCB)	-เป็นการรวมกลไกในการปกป้องระบบคอมพิวเตอร์ ซึ่งจะประกอบด้วยฮาร์ดแวร์ ซอฟต์แวร์ และเฟิร์มแวร์ ซึ่งการประสานกันในการทำงานนี้จะเป็นไปในบังคับตามนโยบายด้านความมั่นคง โดยมีการสร้างสภาวะการปกป้องพื้นฐาน และเตรียมรับระบบคอมพิวเตอร์ที่ไว้ใจได้ ที่เพิ่มเข้ามาตามความต้องการของผู้ใช้
Trusted Path	-เส้นทางการไว้ใจได้ หมายถึง กลไกที่ผู้ใช้ที่เทอร์มินอลสามารถติดต่อโดยตรงกับทีซีบี
User	-หมายถึงผู้ใช้ใด ๆ ก็ตามที่ติดต่อโดยตรงเข้าสู่ระบบคอมพิวเตอร์

ภาคผนวก ข

แบบจำลองของ Bell-LaPadula

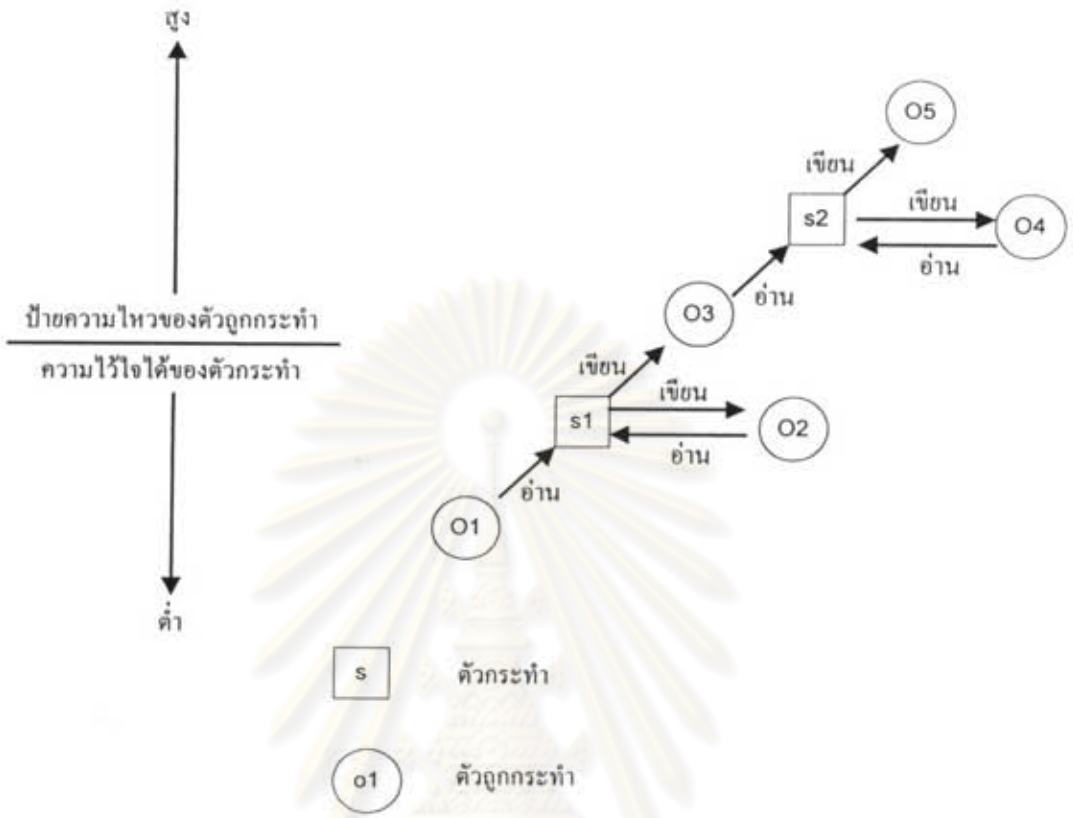
จุดมุ่งหมายของแบบจำลองนี้ ใช้จำแนกการสื่อสาร ตามระดับความลับหรือความสำคัญของข้อมูล โดยคำนึงถึงการไหลของข้อมูลที่เป็นความลับ ซึ่งจะอธิบายถึงการเชื่อมต่อของตัวถูกกระทำและตัวกระทำ ในระดับความไหวของข้อมูลที่แตกต่างกัน โดยยึดหลักการว่าในขณะใดขณะหนึ่ง เครื่องสามารถที่จะทำการประมวลผลข้อมูลที่มีระดับความลับ ความสำคัญต่างกันได้ในเวลาเดียวกัน คือในขณะที่โปรแกรมหนึ่งทำการประมวลผลข้อมูลที่มีความสำคัญสูงหรือลับสุดยอด จะต้องสามารถป้องกันไม่ให้ข้อมูลรั่ว ในขณะที่อีกโปรแกรมหนึ่ง กำลังประมวลผลข้อมูลที่มีระดับความสำคัญรองลงมา เช่นในระดับความลับธรรมดา ต้องมีการป้องกันผู้ใช้ที่กำลังใช้ข้อมูลระดับความลับธรรมดา ไม่สามารถเข้าถึงข้อมูลในระดับลับสุดยอดได้

โดยกำหนดคุณสมบัติของแบบจำลองดังนี้ ให้

S	เป็นเซตของตัวกระทำ และ
O	เป็นเซตของตัวถูกกระทำ
s	เป็นตัวกระทำที่เป็นสมาชิกของ S และ
o	เป็นตัวถูกกระทำที่เป็นสมาชิกของ O
c(s) และ c(o)	เป็นการระบุขั้นความมั่นคง
$\leq$	เป็นความสัมพันธ์ของระดับขั้นความมั่นคง

ซึ่งจะทำให้เกิดคุณสมบัติของการไหลของข้อมูลที่เป็นความลับอยู่ 2 ประการคือ

1. คุณสมบัติทั่วไป ตัวกระทำ s สามารถเข้าถึงโดยใช้สิทธิการอ่านตัวถูกกระทำ o ได้ถ้า $c(o) \leq c(s)$
2. คุณสมบัติสตาร์ (*-property) ถ้าตัวกระทำ s สามารถที่จะอ่านตัวถูกกระทำ o ได้ ก็จะสามารถเข้าถึงโดยการเขียนตัวถูกกระทำ p ได้ ถ้า $c(o) \leq c(p)$ ดังรูปแสดงการไหลของข้อมูล



รูปแสดงการไหลของข้อมูล

ประวัติผู้เขียน

นางสาว เบญจพร ลิ้มธรรมาภรณ์ เกิดเมื่อวันที่ 7 พฤษภาคม พ.ศ. 2514 ที่จังหวัดกรุงเทพฯ สำเร็จการศึกษาวิทยาศาสตรบัณฑิต สาขาวิทยาการคอมพิวเตอร์ ที่สถาบันเทคโนโลยีพระจอมเกล้าพระนครเหนือ ในปีการศึกษา 2534 และเข้าศึกษาต่อในหลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิทยาศาสตร์คอมพิวเตอร์ ที่จุฬาลงกรณ์มหาวิทยาลัย ในปีการศึกษา 2536 ระหว่างที่กำลังศึกษา รับราชการในตำแหน่งนักวิชาการคอมพิวเตอร์ สำนักคอมพิวเตอร์และเทคโนโลยีสารสนเทศ สถาบันเทคโนโลยีพระจอมเกล้าพระนครเหนือ ตั้งแต่ปี พ.ศ. 2535 จนถึงปัจจุบัน