การกำหนดวันหมดอายุของจุดอ่อนในซอฟต์แวร์ระบบ

นายปุณธวัช ว่องธวัชชัย

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต
สาขาวิชาวิทยาศาสตร์คอมพิวเตอร์ ภาควิชาวิศวกรรมคอมพิวเตอร์
คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
ปีการศึกษา 2555

DEFINING EXPIRATION DATE OF SYSTEM SOFTWARE VULNERABILITY

Mr. Puntawat Vongthawatchai

A Thesis Submitted in Partial Fulfillment of the Requirements

for the Degree of Master of Science Program in Computer Science

Department of Computer Engineering

Faculty of Engineering

Chulalongkorn University

Academic Year 2012

หัวข้อวิทยานิพนธ์	การกำหนดวันหมดอายุของจุดอ่อนในซอฟต์แวร์ระบบ
โดย	นายปุณธวัช ว่องธวัชชัย
สาขาวิชา	วิทยาศาสตร์คอมพิวเตอร์
อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก	อาจารย์ ดร.ยรรยง เต็งอำนวย
อาจารย์ที่ปรึกษาวิทยานิพนธ์ร่วม	ผู้ช่วยศาสตราจารย์ ดร.ทรงพล ต่อนี

คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย อนุมัติให้นับวิทยานิพนธ์ฉบับนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญามหาบัณฑิต

…….. คณบดีคณะวิศวกรรมศาสตร์
(รองศาสตราจารย์ ดร.บุญสม เลิศหิรัญวงศ์)

คณะกรรมการสอบวิทยานิพนธ์

…….. ประธานกรรมการ
(รองศาสตราจารย์ ดร.ทวิตีย์ เสนีวงศ์ ณ อยุธยา)

……..อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก
(อาจารย์ ดร.ยรรยง เต็งอำนวย)

…….. อาจารย์ที่ปรึกษาวิทยานิพนธ์ร่วม
(ผู้ช่วยศาสตราจารย์ ดร.ทรงพล ต่อนี)

…….. กรรมการ
(ผู้ช่วยศาสตราจารย์ ดร.ชวลิต ศรีสถาพรพัฒน์)

ปุณธวัช ว่องธวัชชัย : การกำหนดวันหมดอายุของจุดอ่อนในซอฟต์แวร์ระบบ. (DEFINING EXPIRATION DATE OF SYSTEM SOFTWARE VULNERABILITY) อ. ที่ปรึกษาวิทยานิพนธ์หลัก: อ.ดร.ยรรยง เต็งอำนวย อ. ที่ปรึกษาวิทยานิพนธ์ร่วม: ผศ.ดร.ทรงพล ต่อนี, 52 หน้า.

ในปัจจุบันจุดอ่อนที่เกิดขึ้นใหม่ในระบบคอมพิวเตอร์ยังคงก่อความเสียหายเป็นวงกว้างยากต่อการควบคุม และไม่สามารถระบุได้แน่ชัดว่าหายไปจากระบบอย่างถาวรแล้วหรือไม่ งานวิจัยนี้ได้ทำการวิเคราะห์การสาบสูญและการหมดอายุของจุดอ่อนเป็นกลุ่มและรายตัวด้วยวิธีการหาระยะเวลาสาบสูญที่เหมาะสมและวิเคราะห์ระยะปลอดเหตุการณ์ โดยอาศัยข้อมูลข่าวการโจมตีระบบจากสื่อออนไลน์สาธารณะ และฐานข้อมูลซีวีอี นำมาประมวลผลและวิเคราะห์ข้อมูลโดยใช้โดยใช้ค่าเฉลี่ยขอบเขตบนและค่ามัธยฐานของระยะเวลาที่จุดอ่อนยังคงมีอยู่ในระบบที่ระดับความเชื่อมั่น 95% ซึ่งช่วยให้ทราบได้ว่าจุดอ่อนยังอันตรายหรือสามารถก่อความเสียหายในระบบคอมพิวเตอร์ได้อีกหรือไม่ ก่อให้เกิดประโยชน์ต่อผู้ดูแลระบบในการจัดลำดับความสำคัญของการเฝ้าระวังการถูกโจมตีได้อย่างมีประสิทธิภาพ

ภาควิชา...วิศวกรรมคอมพิวเตอร์..... ลายมือชื่อนิสิต……..
สาขาวิชา…วิทยาศาสตร์คอมพิวเตอร์.. ลายมือชื่อ อ. ที่ปรึกษาวิทยานิพนธ์หลัก.....
ปีการศึกษา…2555…… ลายมือชื่อ อ. ที่ปรึกษาวิทยานิพนธ์ร่วม.....

5270398921 : MAJOR COMPUTER SCIENCE

KEYWORDS: VULNERABILITY / EXPIRATION / DISAPPEARANCE / SYSTEM SOFTWARE

PUNTAWAT VONGTHAWATCHAI: DEFINING EXPIRATION DATE OF SYSTEM SOFTWARE VULNERABILITY, ADVISOR: YUNYONG TENG-AMNUAY, Ph.D., CO-ADVISOR: SONGPHOL TORNEE, Ph.D., 52 pp.

System software vulnerabilities still cause damage continuously and cannot be readily determined that they are all clear from the systems. This research analyzes disappearance period and expiration date of system software vulnerabilities based on public news and CVE database by defining appropriate disappearance period using 95% confidence interval upper bound limit for mean of dormant time and 95% confidence interval median of survival time. This can indicate whether a particular vulnerability is still dangerous and can help administrators in prioritizing their tasks.

Department: …Computer Engineering.. Student's Signature……..……

Field of Study: ..Computer Science..… Advisor's Signature……..……..

Academic Year: ..2012……. Co-advisor's Signature……

กิตติกรรมประกาศ

วิทยานิพนธ์ฉบับนี้สามารถสำเร็จลงไปได้ด้วยดีจากการให้คำปรึกษาอันเป็นประโยชน์ยิ่งของ อ.ดร.ยรรยง เต็งอำนวย และ ผศ.ดร.ทรงพล ต่อนี ที่ได้ให้คำปรึกษาทางด้านสถิติเพื่อการวิจัย ก่อให้เกิดแนวคิดที่ชัดเจนและสามารถนำไปประยุกต์ใช้งานได้จริง

ขอขอบคุณ คณาจารย์ เพื่อนๆ พี่ๆ น้องๆ ที่ห้องปฏิบัติการ ISEL จุฬาลงกรณ์มหาวิทยาลัย สำหรับกำลังใจและบรรยากาศที่ดี ในการทำวิจัย และ นิสิตปริญญาตรีชั้นปีที่ 3 ห้องปฏิบัติการ WICOS มหาวิทยาลัยเกษตรศาสตร์ จำนวน 4 คน สำหรับความช่วยเหลือระหว่างการวิจัย รวมไปถึง คุณพ่อ คุณแม่ และ น้องสาว ที่คอยช่วยเหลือ สนับสนุน และให้กำลังใจจนกระทั่งงานวิจัยสำเร็จได้ด้วยดี

สารบัญ

หน้า

หน้า

หน้า

สารบัญตาราง

ตารางที่ หน้า

สารบัญรูป

รูปที่ หน้า

บทที่ 1

บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

ในปัจจุบันจุดอ่อนในระบบคอมพิวเตอร์ส่วนใหญ่สืบเนื่องมาจากกระบวนการพัฒนาซอฟต์แวร์เกือบทุกชนิดทั้งโดยเจตนาและไม่เจตนา โดยจุดอ่อนที่เกิดขึ้นนั้นนำไปสู่ปัญหาต่างๆ ระหว่างการใช้งานซึ่งก่อให้เกิดความเสียหายแก่ระบบได้เป็นอย่างมาก เช่น การถูกโจรกรรมข้อมูล การทำลายล้างระบบ เป็นต้น เหตุการณ์ต่างๆ เหล่านี้นำไปสู่การศึกษาค้นคว้าวิจัยเกี่ยวกับวัฏจักรวงจรชีวิตของจุดอ่อนอย่างเป็นระบบตั้งแต่การเกิดจนตายลง เพื่อช่วยให้ผู้ดูแลระบบทราบสถานการณ์ปัจจุบันของจุดอ่อนได้อย่างชัดเจน สามารถรับมือกับภัยคุกคามและเฝ้าระวังความปลอดภัยให้กับระบบคอมพิวเตอร์ได้อย่างรัดกุม ช่วยให้ระบบนั้นรอดพ้นจากการถูกบุกรุก ก่อกวน หรือ ทำลาย ได้อย่างมีประสิทธิภาพ

หนึ่งในสถานะของจุดอ่อนที่ผู้วิจัยให้ความสนใจเป็นพิเศษ คือ การตาย หรือ การหมดอายุของจุดอ่อน ซึ่งจุดอ่อนจะเข้าสู่สถานะดังกล่าวได้ก็ต่อเมื่อมีการแก้ไขซอฟต์แวร์ที่ยังมีจุดอ่อนให้สามารถรับมือจากการถูกโจมตีได้โดยการแพทช์ (Patch) ถ้าคอมพิวเตอร์ภายในองค์กรทุกเครื่องที่ใช้ซอฟต์แวร์ดังกล่าวได้ทำการแพทช์อย่างครบถ้วนแล้วนั้น ในทางทฤษฎีจะถือว่าจุดอ่อนนั้นได้ตายลงและไม่เป็นอันตรายใดๆ ต่อระบบอีก แต่ยังมีความเป็นไปได้ที่ยังมีจุดอ่อนนั้นคงเหลืออยู่ในระบบ เนื่องจากสาเหตุหลายประการ เช่น การกระจายข่าวสารเกี่ยวกับจุดอ่อนที่เกิดขึ้นนั้นอาจไม่ทั่วถึงพอ ส่งผลให้เครื่องคอมพิวเตอร์ทั่วโลกอาจไม่ได้รับการแพทช์อย่างทั่วถึงก่อให้เกิดการโจมตีและสร้างความเสียหายตามมาได้อีกสาเหตุหนึ่งคือการขาดความเอาใจใส่ของผู้ดูแลระบบในการติดตามสถานะของจุดอ่อนและการแพทช์คอมพิวเตอร์ในระบบ

โดยทั่วไป ก่อนจะถือว่าจุดอ่อนนั้นตาย ควรต้องมีการสาบสูญจากวงการข่าวเป็นระยะเวลาหนึ่ง ดังนั้น งานวิจัยนี้ทำการวิเคราะห์หาระยะเวลาสาบสูญ โดยใช้ค่าเฉลี่ยขอบเขตบนที่ระดับความเชื่อมั่น 95% ของระยะเวลาที่จุดอ่อนหายไปจากระบบ และกำหนดวันหมดอายุของจุดอ่อนจากการวิเคราะห์ระยะเวลาที่จุดอ่อนยังคงอยู่ในระบบ (Survival time) มาเป็นเกณฑ์ในการอ้างอิงอายุของจุดอ่อนโดยประมาณ ซึ่งทำให้สามารถชี้วัดได้ว่าจุดอ่อนยังมีอันตรายหรือก่อความเสียหายได้อีกหรือไม่

1.2 วัตถุประสงค์ของการวิจัย

ในงานวิจัยนี้มีวัตถุประสงค์เพื่อกำหนดวันหมดอายุของจุดอ่อนในซอฟต์แวร์ระบบสำหรับการจัดลำดับความสำคัญในการเฝ้าระวังการถูกโจมตี

1.3 ขอบเขตของการวิจัย

1. เก็บข้อมูลข่าวการโจมตีจากฐานข้อมูลโอเอสวีดีบี [1] ฐานข้อมูลซีวีอี [2] และสื่อออนไลน์สาธารณะ
2. ใช้ข้อมูลของ Windows XP เป็นกรณีศึกษา
3. กำหนดระยะเวลาการสาบสูญของจุดอ่อนโดยใช้ทฤษฎีช่วงความเชื่อมั่น [15]
4. กำหนดวันหมดอายุของจุดอ่อนโดยอาศัยหลักการของ Survival analysis [3]
5. เครื่องมือที่ใช้ในการวิเคราะห์ข้อมูลคือ โปรแกรม IBM SPSS เวอร์ชัน 20

1.4 ขั้นตอนของการทำวิจัย

1. ศึกษางานวิจัยที่เกี่ยวข้องกับวงจรชีวิตของจุดอ่อน และ หลักการของ Survival analysis
2. ศึกษาการใช้งานฐานข้อมูลโอเอสวีดีบี และ ซีวีอี โปรแกรม IBM SPSS
3. เก็บข้อมูลข่าวการโจมตีและรวบรวมไว้ในรูปแบบของตาราง
4. คำนวณหาระยะห่างของการเกิดข่าว พร้อมทั้งคำนวณหาค่าสูงสุด
5. คำนวณหาระยะเวลาของข่าวที่ยังคงมีนัยสำคัญในระบบ
6. แบ่งจุดอ่อนออกเป็นกลุ่มตามคุณสมบัติที่กำหนดเพื่อเตรียมการวิเคราะห์ข้อมูล
7. คำนวณหาระยะเวลาสาบสูญ และกำหนดวันหมดอายุของจุดอ่อน
8. วิเคราะห์และสรุปผล พร้อมข้อเสนอแนะ
9. จัดทำรายงานวิทยานิพนธ์ฉบับสมบูรณ์

1.5 ประโยชน์ที่คาดว่าจะได้รับ

1. สามารถใช้เป็นแนวทางในการกำหนดหลักเกณฑ์เพื่อการประกาศอย่างเป็นทางการถึงการสิ้นสุดอายุขัยของจุดอ่อนในซอฟต์แวร์ระบบ
2. สามารถช่วยให้ผู้ดูแลระบบในการจัดลำดับความสำคัญของการเฝ้าระวังการถูกโจมตีได้อย่างมีประสิทธิภาพ

บทที่ 2

ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

2.1 วัฏจักรวงจรชีวิตของจุดอ่อน

จุดอ่อนที่เกิดขึ้นมาในระบบคอมพิวเตอร์นั้น เพื่อให้ง่ายต่อการรับมือและจัดการกับจุดอ่อนที่เกิดขึ้นจึงมีการคิดค้นวัฏจักรวงจรชีวิตของจุดอ่อน [4], [5] ขึ้นโดยแบ่งออกเป็นช่วงเวลาต่างๆ ดังนี้

1. การเกิดของจุดอ่อน (Birth) จุดอ่อนที่เกิดขึ้นมาใหม่นั้น มักเกิดขึ้นจากการพัฒนาหรือปรับปรุงแก้ไขระบบซอฟต์แวร์ขนาดใหญ่โดยเจตนาและไม่เจตนาจากผู้พัฒนาโปรแกรม

2. การค้นพบจุดอ่อน (Discovery) ถ้าหากจุดอ่อนเกิดขึ้นโดยเจตนาแล้วนั้นส่วนใหญ่ผู้พัฒนามักจะตรวจพบและสามารถแก้ไขจุดอ่อนดังกล่าวได้ทันทีระหว่างการพัฒนาหรือทดสอบซอฟต์แวร์ และถ้าจุดอ่อนดังกล่าวนั้นเกิดขึ้นโดยไม่เจตนา การค้นพบจุดอ่อนอาจตกไปอยู่ในมือของผู้เจาะระบบ ซึ่งถ้าเป็นผู้เจาะระบบที่มีความประสงค์ดี (White hat hacker) [6] ก็จะช่วยให้ผู้พัฒนาสามารถแก้ไขจุดอ่อนนั้นได้อย่างปลอดภัย แต่ถ้าหากว่าจุดอ่อนถูกค้นพบโดยผู้เจาะระบบที่ประสงค์ร้าย (Black hat hacker) [7] อาจก่อให้เกิดความเสี่ยงต่อการถูกโจมตีแบบ Zero day attack ได้ถ้าหากว่าไม่สามารถแก้ไขจุดอ่อนนั้นได้ทันเวลา

3. การเปิดเผยรายละเอียดจุดอ่อน (Disclosure) เมื่อมีการค้นพบจุดอ่อนที่เกิดขึ้นได้แล้ว (ยกเว้นการถูกค้นพบโดย Black hat hacker) จะเกิดการรวบรวมข้อมูลและแนวทางการรับมือขึ้นมาโดยละเอียดและมีการเปิดเผยในวงจำกัดเฉพาะผู้พัฒนาซอฟต์แวร์หรือกลุ่มของ White hat hacker ผ่านเว็บไซต์ในรูปแบบของจดหมายแบบ mailing list หรือ กระดานข่าว เช่น bugtraq โดยทั้งหมดนี้มีจุดประสงค์เพื่อแลกเปลี่ยนข้อมูลในการระดมความคิดเพื่อช่วยแก้ไขจุดอ่อนที่เกิดขึ้นนั้นโดยเร็วที่สุดก่อนที่ Black hat hacker จะทราบจุดอ่อนและก่อความเสียหายต่อระบบตามมาทีหลังได้

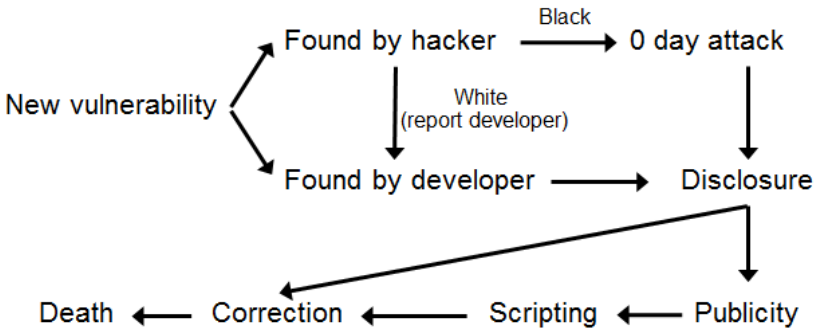
4. การเปิดเผยรายละเอียดจุดอ่อนสู่สาธารณะ (Publicity) หลังจากจุดอ่อนถูกเปิดเผยรายละเอียดภายในวงจำกัดได้ระยะหนึ่ง จะมีข่าวเปิดเผยสู่สาธารณะเป็นวงกว้างในหลายๆ สื่อ โดยมีจุดประสงค์หลักเพื่อให้ผู้ใช้งานได้ทราบถึงความเสี่ยงที่อาจเกิดขึ้น รวมถึงการรับมือ เพื่อช่วยป้องกันความเสียหายที่อาจเกิดขึ้นได้ในเบื้องต้น อย่างไรก็ตามในช่วงเวลานี้ผู้พัฒนายังคงคิดค้นหาวิธีแก้ไขจุดอ่อนที่เกิดขึ้นต่อไป

5. การทำสคริปท์สำหรับการโจมตี (Scripting) ในช่วงแรกของการค้นพบจุดอ่อนโดย Black hat hacker นั้น การโจมตีจุดอ่อนจะต้องอาศัยเทคนิคและทักษะเฉพาะตัวของผู้โจมตีเอง แต่เมื่อวันเวลาผ่านไป ผู้โจมตีมักจะมีการรวบรวมขั้นตอนการโจมตีจุดอ่อนออกมาเป็นโปรแกรมขนาดเล็กหรือสคริปท์เพื่อให้ผู้ใช้งานทั่วไปที่ต้องการโจมตีระบบเพื่อผลประโยชน์อย่างใดอย่างหนึ่งสามารถนำไปใช้งานได้อย่างง่าย

และสะดวกมากยิ่งขึ้น ซึ่งช่วงเวลานี้มักเกิดการโจมตีและเกิดความเสียหายขึ้นเป็นวงกว้างเพราะสคริปท์ส่วนใหญ่มักจะทำงานอย่างต่อเนื่องแบบอัตโนมัติ

6. การแก้ไขจุดอ่อน (Correction) เมื่อผู้พัฒนาซอฟต์แวร์สามารถแก้ไขจุดอ่อนที่เกิดขึ้นได้แล้วนั้น จะมีการสรุปรวบรวมรายละเอียดและวิธีการแก้ไขโดยส่วนใหญ่มักใช้วิธีดัดแปลงซอฟต์แวร์เพิ่มเติมผ่านแพทช์ (patch) ดัดแปลงการตั้งค่า (configuration) ของซอฟต์แวร์ หรือเปลี่ยนซอฟต์แวร์เป็นเวอร์ชันใหม่ซึ่งเสมือนเป็นการแพทช์รวบยอดโดยอัตโนมัติ ทั้งหมดนี้เพื่อให้ระบบสามารถรับมือกับการโจมตีได้อย่างมีประสิทธิภาพ อย่างไรก็ตามสถานะ Correction อาจเกิดขึ้นก่อนข้อที่ 4 และ 5 ได้

7. การตายของจุดอ่อน (Death) เมื่อผู้ใช้งานหรือผู้ดูแลระบบโดยภาพรวมนั้นได้ทำการแก้ไขตามข้อ 2.1.6 มาเป็นระยะเวลาหนึ่งแล้วนั้นในทางทฤษฎีจะถือว่าจุดอ่อนได้ตายลงเนื่องจากบรรดาผู้โจมตีส่วนใหญ่เลิกให้ความสนใจต่อจุดอ่อนนั้นๆ หรือสคริปท์สำหรับการโจมตีไม่สามารถทำงานอย่างได้ผลอีกต่อไป โดยในปัจจุบันยังไม่มีผู้ใดสามารถกำหนดลักษณะการตายหรือระยะเวลาการตายของจุดอ่อนได้อย่างชัดเจนเนื่องจากสาเหตุหลายประการ เช่น อาจจะมีคอมพิวเตอร์ที่ปิดการใช้งานอยู่เป็นเวลานานได้กลับมาใช้งานใหม่ซึ่งอาจจะยังไม่ได้รับการแก้ไขจุดอ่อนนั้นๆ หรือ ผู้ดูแลระบบอาจขาดความเอาใจใส่ยังไม่ได้ทำการแก้ไขจุดอ่อนที่มีอยู่ในองค์กรแต่ในขณะเดียวกันการโจมตีจุดอ่อนก็อาจยังเข้าไม่ถึงในส่วนดังกล่าว



รูปที่ 2.1 วัฏจักรวงจรชีวิตของจุดอ่อน

2.2 วัฏจักรวงจรชีวิตของระบบ

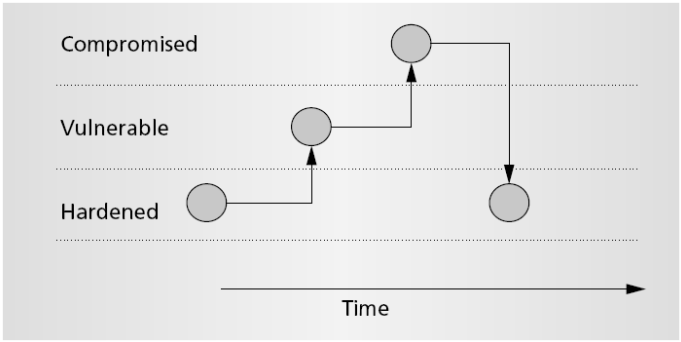
จากข้อ 2.1 จะขอกล่าวในอีกมุมมองหนึ่งซึ่งเป็นมุมมองของตัวระบบที่ได้รับผลกระทบจากการโจมตีจุดอ่อนโดยจะแบ่งออกเป็น 3 สถานะ [4] ดังนี้

1. ระบบที่แข็งแกร่ง (Hardened) จัดเป็นสถานะปรกติของระบบซึ่งสามารถทำงานได้ตามปรกติและมีความปลอดภัยรวมถึงสามารถต้านทานการโจมตีในรูปแบบต่างๆ ได้เป็นส่วนใหญ่

2. มีจุดอ่อนเกิดขึ้นในระบบ (Vulnerable) โดยการที่ระบบจะเข้าสู่สถานะนี้ได้อาจเกิดจากสาเหตุบางประการ เช่น มีการโจมตีรูปแบบใหม่ๆ เกิดขึ้นและผู้ดูแลระบบยังไม่ได้ทำการแก้ไข หรือ อาจเกิดจาก

การเปลี่ยนแปลงซอฟต์แวร์ระบบจนเกิด bug และกลายเป็นจุดอ่อนเสียเอง ณ จุดนี้ ถ้าหากผู้ดูแลระบบหรือผู้ใช้สามารถแก้ไขได้ทัน ก็จะทำให้ระบบกลับเข้าสู่สถานะ Hardened ในข้อ 2.1 ดังเดิม

3. ระบบถูกโจมตีและยึดครอง (Compromised) เมื่อใดก็ตามที่ระบบมีความหละหลวมและไม่สามารถต้านทานต่อการโจมตีได้ ผู้โจมตีจะทำการเจาะระบบและเข้ายึดครองในที่สุด ซึ่งอาจก่อให้เกิดความเสียหายได้ อย่างไรก็ตามถ้ามีการแก้ไขจุดอ่อนที่เกิดขึ้นตามข้อ 2.1.6 ได้แล้วนั้น ระบบก็สามารถกลับเข้าสู่สถานะ Hardened ตามข้อ 2.1 ได้ดังเดิม



รูปที่ 2.2 วัฏจักรวงจรชีวิตของระบบ [4]

2.3 ฐานข้อมูลซีวีอี

ในปัจจุบันมีจุดอ่อนที่เกิดขึ้นในซอฟต์แวร์เป็นจำนวนมากจนทำให้มีความคิดที่จะรวบรวมข้อมูลจุดอ่อนที่เกิดขึ้นจากทุกภาคส่วน เพื่อเป็นศูนย์กลางในการแลกเปลี่ยนข้อมูลของจุดอ่อน เป็นการช่วยจัดระเบียบและสามารถนำไปใช้ในการอ้างอิงกับงานต่างๆ ทางด้านความปลอดภัยของคอมพิวเตอร์ โดยบริษัท MITRE [1] ได้เข้ามาเป็นผู้ดูแลระบบฐานข้อมูลนี้โดยได้รับทุนสนับสนุนจาก National Cyber Security Division ซึ่งอยู่ภายใต้การกำกับดูแลของ United States Department of Homeland Security

ฐานข้อมูลซีวีอีนั้นประกอบไปด้วยเขตข้อมูลที่สำคัญต่างๆ ดังต่อไปนี้

1. Name หรือ CVE Name เป็นหมายเลขประจำตัวของข้อมูลจุดอ่อนที่ได้รับรายงานเข้ามา จะมีรูปแบบโดย CVE-yyyy-ID เช่น CVE-2005-0088 หมายถึง ข้อมูลจุดอ่อนลำดับที่ 88 ของปี 2005

2. Status หรือสถานะของจุดอ่อนที่ได้รับรายงานเข้ามาซึ่งจะแบ่งออกเป็น 2 สถานะ ได้แก่ Entry และ Candidate โดยเมื่อมีการรายงานจุดอ่อนเข้ามาใหม่นั้น ข้อมูลซีวีอีดังกล่าวจะมีสถานะเป็น Entry และเมื่อผ่านการตรวจสอบ พิสูจน์ และปรับปรุงแก้ไขให้ตรงกับความเป็นจริงจากทีมผู้ตรวจสอบซีวีอีแล้วนั้น สถานะจึงจะมีการเปลี่ยนเป็น Candidate ซึ่งอาจไม่ได้หมายความว่าซีวีอีทุกรายการจะสามารถเปลี่ยนเป็น Candidate ได้ เนื่องจากถ้าหากว่ารายงานที่ได้รับเข้ามาดังกล่าวไม่เป็นความจริง ก็จะมีการลบรายการนั้นออกจากฐานข้อมูลซีวีอีต่อไป

3. Description หรือรายละเอียดเชิงลึกของจุดอ่อนที่เกิดขึ้นในซอฟต์แวร์รวมถึงลักษณะอาการที่เกิดขึ้นถ้าหากระบบที่ใช้ซอฟต์แวร์ดังกล่าวนั้นถูกโจมตี

4. References หรือแหล่งอ้างอิงข้อมูลจุดอ่อนที่เชื่อถือได้ โดยส่วนใหญ่จะมาจากหน่วยงานที่คอยเฝ้าระวังรักษาความปลอดภัย เช่น CERT [8], BUGTRAQ [9], OSVDB [2] , SECUNIA [10] หรือหน่วยงานที่พัฒนาซอฟต์แวร์เหล่านั้นขึ้นมา เช่น REDHAT [11], DEBIAN [12], SUN [13] โดยจุดอ่อน 1 จุด อาจอ้างอิงมาจากหลายแหล่งได้ ซึ่งทั่วไปนั้นมีรูปแบบการอ้างอิงโดย “Reference ID 1 | URL 1 | Reference ID 2 | URL 2 | …” โดย URL อาจไม่มีหรือจะใช้เป็นหัวข้อของ Mailing list แทนก็ได้ เช่น

“SGI:19970301-01-P	URL:ftp://patches.sgi.com/support/free/security/advisories/19970301-01-P	XF:sgi-fsdump”

.

หมายเหตุ ในข้อ 5-7 เป็นเขตข้อมูลเฉพาะรายการซีวีอีที่มีสถานะเป็น candidate แล้วเท่านั้น

5. Phase หรือช่วงเวลาระหว่างการตรวจสอบรายการซีวีอี เพื่อเปลี่ยนสถานะจาก entry เป็น candidate โดยเริ่มจากช่วงแรกคือ assigned จนถึงช่วงสุดท้ายที่จะได้เป็น candidate โดยสมบูรณ์คือช่วง final โดยมีรายละเอียดเพิ่มเติมใน [14]

6. Votes หรือผลการโหวตของคณะกรรมการระหว่างการตรวจสอบรายการซีวีอีในระหว่างขั้นตอนการตรวจสอบและคัดเลือกซีวีอีก่อนที่จะเปลี่ยนสถานะสู่ candidate ต่อไป

7. Comments หรือข้อเสนอแนะเพิ่มเติมของคณะกรรมการระหว่างตรวจสอบและคัดเลือกรายการซีวีอี

2.4 ทฤษฎีช่วงความเชื่อมั่น

ในการประมาณค่าพารามิเตอร์ในประชากรนั้น โดยปรกติแล้วสามารถประมาณค่าได้ 2 ลักษณะ คือ การประมาณค่าแบบค่าเดียว และ การประมาณค่าแบบช่วง ซึ่งในงานวิจัยนี้จะใช้การประมาณค่าแบบช่วง [15] เนื่องจากการประมาณค่าแบบค่าเดียวไม่สามารถให้รายละเอียดของผลการสุ่มตัวอย่างได้ชัดเจน ดังนั้น การประมาณค่าแบบช่วง จะช่วยในการยืนยันว่าช่วงที่กำหนดขึ้นมานั้นมีความครอบคลุมค่าพารามิเตอร์ไว้ได้ด้วยความน่าจะเป็นที่ถูกกำหนดขึ้นซึ่งในที่นี้เรียกว่า ระดับความเชื่อมั่น (Level of Confidence) ซึ่งโดยปรกติแล้วนั้น ค่าที่นิยมใช้ในงานวิจัยมักกำหนดไว้ที่ 0.9,0.95 หรือ 0.99 นั่นหมายความว่า ยอมให้ค่าประมาณที่ได้มีโอกาสผิดพลาด 10%, 5% หรือ 1% ตามลำดับ หรือในอีกมุมมองหนึ่งคือ มีความมั่นใจในค่าประมาณที่ได้จะมีความถูกต้องด้วยระดับความเชื่อมั่น 90%, 95% หรือ 99% ตามลำดับในสมการช่วงความเชื่อมั่น ดังสมการที่ 2.1

$$\bar{x} - t_{\frac{\alpha}{2},DF}\frac{s}{\sqrt{n}} < \mu < \bar{x} + t_{\frac{\alpha}{2},DF}\frac{s}{\sqrt{n}} \qquad (2.1)$$

จากสมการที่ 2.1 ค่า μ หมายถึงค่าเฉลี่ยของประชากร ซึ่งถูกกำหนดเป็นการประมาณแบบช่วง โดยมีขอบเขตล่างคือ $\bar{x} - t_{\frac{\alpha}{2},DF}\frac{s}{\sqrt{n}}$ และ ขอบเขตบนคือ $\bar{x} + t_{\frac{\alpha}{2},DF}\frac{s}{\sqrt{n}}$ เมื่อ $\bar{x}$ แทนค่าเฉลี่ยเลขคณิตของระยะห่างของการเกิดข่าวสูงสุด s แทนส่วนเบี่ยงเบนมาตรฐานของระยะห่างของการเกิดข่าวสูงสุด t แทนการแจกแจงแบบ t และ n แทนจำนวนประชากร โดยมีระดับความเชื่อมั่นที่ถูกกำหนดโดยค่า α ดังสมการที่ 2.2 และค่า DF (Degree of freedom) ถูกกำหนดโดยสมการที่ 2.3

$$\alpha = 1 - \text{Level of confidence} \tag{2.2}$$

$$DF = n - 1 \tag{2.3}$$

จากสมการที่ 2.2 และ 2.3 ถ้าหากต้องการประมาณค่าเฉลี่ย μ แบบช่วงที่ระดับความเชื่อมั่น 95% ให้กำหนดค่า α=0.05 และ DF=257 จะทำให้ได้ค่า $t_{\frac{\alpha}{2},DF}$ มีค่าเป็น $t_{0.025,257}$ ซึ่งมีค่าเท่ากับ 1.96 จะได้สมการสำหรับการคำนวณหาระยะเวลาการสาบสูญของจุดอ่อนสำหรับงานวิจัยนี้ ดังสมการที่ 2.4

$$\bar{x} - 1.96\frac{s}{\sqrt{n}} < \mu < \bar{x} + 1.96\frac{s}{\sqrt{n}} \tag{2.4}$$

2.5 การวิเคราะห์ระยะเวลาการอยู่รอด

การค้นคว้าและวิจัยโดยทั่วไปนั้นมักให้ความสนใจต่อเหตุการณ์ต่างๆ ที่เกิดขึ้นระหว่างการทดลอง ยกตัวอย่างจากการทดลองเกี่ยวกับวงจรชีวิตของจุดอ่อนจะมีเหตุการณ์ที่น่าสนใจเช่น การเกิด การสาบสูญ หรือการหมดอายุ เป็นต้น การวิเคราะห์อย่างง่ายนั้นจะใช้ค่าร้อยละหรืออัตราของการเกิดเหตุการณ์มาเป็นตัวชี้วัด แต่บ่อยครั้งพบว่าระยะเวลาตั้งแต่เริ่มศึกษาจนกระทั่งเกิดเหตุการณ์ หรืออีกมุมมองหนึ่งคือระยะปลอดเหตุการณ์นั้นหรือระยะเวลาการอยู่รอดนั้นมีความสำคัญมากกว่า เช่น แทนที่จะมาตรวจสอบว่าการแพทช์ทำให้จุดอ่อนหมดอายุลงหรือไม่ ก็มาดูว่าจุดอ่อนสามารถอยู่รอดต่อไปในระบบได้อีกนานเท่าใด กรณีนี้ข้อมูลอาจไม่สมบูรณ์ได้เช่นกัน (เกิด Censored observation) เนื่องจากหลายสาเหตุเช่น ระยะเวลาวิจัยที่มีจำกัด ทำให้บางจุดอ่อนอาจเกิดเหตุการณ์ (เช่น เกิดรายงานข่าว เกิดการสาบสูญ หรือ หมดอายุ) หลังจากวันที่หยุดเก็บข้อมูล (วันสิ้นสุดการศึกษา)

ข้อมูลที่ได้เหล่านี้ แม้เป็นข้อมูลต่อเนื่องโดยธรรมชาติ แต่การวิเคราะห์ด้วยวิธีทางสถิติธรรมดา เช่น การหาค่าเฉลี่ย การทดสอบโดยใช้ค่า t หรือ การวิเคราะห์การถดถอยแบบเชิงเส้นนั้นยังไม่ถูกต้องเหมาะสม เนื่องจากข้อมูลไม่สมบูรณ์ แม้จะเลือกวิเคราะห์โดยใช้ค่าร้อยละหรืออัตราของการเกิดเหตุการณ์ก็จะด้อยประสิทธิภาพเพราะไม่ได้ใช้ข้อมูลเกี่ยวกับระยะเวลา รูปแบบการวิเคราะห์ที่เหมาะสมเฉพาะกับข้อมูลประเภทนี้เรียกว่า Survival analysis ซึ่งมีวิธีการทางสถิติหลายวิธี เป็นวิธีการวิเคราะห์ที่กำลังทวีความสำคัญขึ้นเป็นลำดับ และมีการใช้ในงานวิจัยมากเป็นอันดับสองรองจาก Logistic regression โดยใน

งานวิจัยนี้จะเลือกใช้วิธีการของ Kaplan-Meier [3] ในการวิเคราะห์และกำหนดวันหมดอายุของจุดอ่อน และผลลัพธ์สุดท้ายที่ได้จากการวิเคราะห์คือ ระยะเวลาในการอยู่รอด (Survival time) รวมกับผลการทดสอบค่าที่ได้โดยใช้ Log-rank เพื่อตรวจสอบหาความแตกต่างของข้อมูลว่าแตกต่างกันอย่างมีนัยสำคัญหรือไม่

นิยามต่างๆ ที่จำเป็นต้องกำหนดขึ้นก่อนการวิเคราะห์ Survival analysis ประกอบด้วย

1. วันเริ่มต้นศึกษาข้อมูล (Begin date) เป็นจุดเริ่มต้นจริงของกระบวนการที่นำไปสู่การเกิดเหตุการณ์ที่ศึกษา

2. เหตุการณ์ (Event) เป็นเหตุการณ์ที่สนใจระหว่างศึกษาข้อมูล

3. การวัดการเกิดเหตุการณ์ เมื่อเกิดเหตุการณ์ที่สนใจขึ้นจะเรียกว่า Failure และเมื่อสิ้นสุดระยะเวลาการศึกษาแล้วนั้นไม่เกิดเหตุการณ์ที่สนใจขึ้นเลย จะเรียกว่า Censored

4. วันสิ้นสุดการศึกษาข้อมูล (End date) คือจุดตัดของช่วงเวลาเพื่อใช้ในการกำหนดขอบเขตของระยะเวลาที่ชัดเจนในการวิเคราะห์ข้อมูล

5. การกำหนดกลุ่มตัวอย่าง โดยแบ่งข้อมูลที่ได้ออกเป็นกลุ่มตามคุณสมบัติของกลุ่มประชากรที่นำมาวิเคราะห์ เช่น แบ่งกลุ่มตามตำแหน่งที่เกิดการโจมตี หรือ แบ่งกลุ่มตามระดับความรุนแรง เป็นต้น

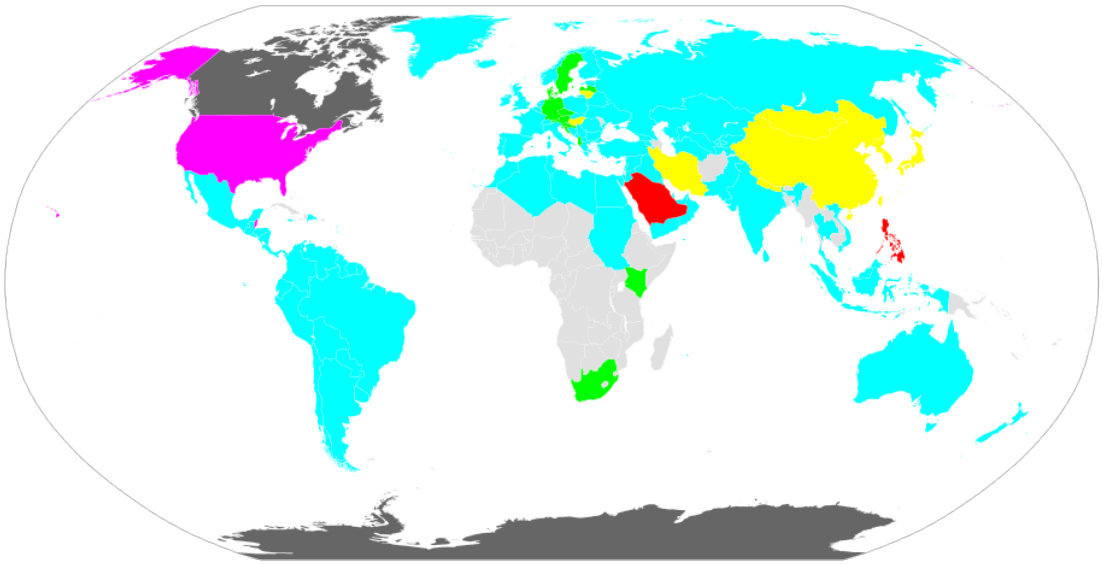
วิธีการของ Kaplan-Meier นั้น ถูกกำหนดด้วย Survival function ($\hat{S}(t)$) ดังสมการที่ 2.5

$$\hat{S}(t) = \prod_{t_i \le t} \left(1 - \frac{d_i}{n_i}\right) \tag{2.5}$$

จากสมการที่ 1 ค่า t_i คือระยะเวลาที่ศึกษาข้อมูล ณ จุดของเวลาสิ้นสุดการศึกษา i และ d_i คือจำนวนของจุดอ่อนที่สาบสูญรวม ณ จุดของเวลาสิ้นสุดการศึกษา i และ n_i คือจำนวนของจุดอ่อนที่ยังไม่สาบสูญเทียบกับเวลา t_i สมการนี้จะนำไปสู่การหาค่ามัธยฐานของระยะเวลาในการอยู่รอดโดยประมาณ (Estimate median survival time) โดยการคำนวณหาระยะเวลาในการอยู่รอดน้อยที่สุดที่มีค่า S(t) (Survival probability) น้อยกว่าหรือเท่ากับ 0.5 ซึ่งกลุ่มข้อมูลโดยส่วนน้อยที่จะไม่สามารถคำนวณค่าออกมาได้ และ ช่วงความเชื่อมั่น 95% ของค่ามัธยฐานของระยะเวลาในการอยู่รอด (Confidence interval for the median survival time) สามารถคำนวณออกมาได้ 2 แบบตามวิธีการของ Brookmeyer and Crowley หรือ Andersen ซึ่งในงานวิจัยนี้จะใช้โปรแกรม IBM SPSS เวอร์ชัน 20 ในการคำนวณ

2.6 มาตรฐานรูปแบบวันที่สากล

ในปัจจุบันการเขียนวันที่ตามแบบสากลนั้น นิยมใช้กันหลากหลายรูปแบบ ซึ่งในงานวิจัยนี้จำเป็นต้องมีการตรวจสอบวันที่ของข่าว ดังนั้นเพื่อเป็นการป้องกันความผิดพลาดในระหว่างการดำเนินงานวิจัยในส่วนของการตรวจสอบวันที่ของข่าว จึงสรุปเป็นแผนภาพได้ดังรูปที่ 2.3 [16]



สี	รูปแบบ	พื้นที่ที่มีการใช้งาน
ฟ้า	L	อินเดีย อเมริกาใต้ เอเชีย (เอเชียกลาง เอเชียตะวันออกเฉียงใต้ และเอเชียตะวันตก) ทวีปยุโรปเกือบทั้งหมด แอฟริกาเหนือ และ ทวีปออสเตรเลีย
เหลือง	B	จีน เกาหลี อิหร่าน ญี่ปุ่น ฮังการี และ ลิทัวเนีย
ม่วง	M	สหรัฐอเมริกา เบลีซ
เขียว	B, L	เนปาล แอฟริกาใต้ ออสเตรีย โปรตุเกส สวีเดน นอร์เวย์ และ เดนมาร์ค
แดง	L, M	ฟิลิปปินส์ และ ซาอุดิอาระเบีย
เทา	B, L, M	แคนาดา

รูปที่ 2.3 รูปแบบวันที่ตามแบบสากล

จากรูปที่ 2.3 สามารถสรุปเป็นรูปแบบของวันที่ได้ดังนี้ [16]

1. แบบ L หรือ Gregorian little-endian จะขึ้นต้นด้วยวัน คือ “วัน เดือน ปี” เช่น 30/10/2009, 30 November 2009 หรือ 30/10/09 เป็นต้น
2. แบบ B หรือ Gregorian big-endian จะขึ้นต้นด้วยปี คือ “ปี เดือน วัน” เช่น 2011/11/12, 11/11/12 หรือ 2011 November, 12 เป็นต้น
3. แบบ M หรือ Middle-endian จะขึ้นต้นด้วยเดือน คือ “เดือน วัน ปี” เช่น 11/12/2007, November 12, 2007 หรือ 11/12/07 เป็นต้น
4. แบบที่ใช้ในระบบคอมพิวเตอร์ คือ “วัน เดือน ปี มาตรฐานเวลา” เช่น 12 January 2000 GMT, 30 March 2005 JST หรือ 15 May 2008 ICT เป็นต้น

2.7 งานวิจัยที่เกี่ยวข้อง

ผู้วิจัยได้ศึกษางานวิจัยของ William A. Arbaugh และคณะ [4] ซึ่งได้ทำการคิดค้นแบบจำลองวัฏจักรวงจรชีวิตสำหรับจุดอ่อนในระบบคอมพิวเตอร์ และได้นำไปประยุกต์ใช้กับกรณีศึกษาจำนวนทั้งหมด 3 ตัวอย่าง ได้แก่ Phf incident, IMAP incident และ BIND incident เพื่อเปิดเผยให้เห็นว่าระบบนั้นยังคงมีจุดอ่อนให้พบเห็นได้อยู่บ่อยครั้งหลังจากมีแพทช์สำหรับแก้ไขซ่อมแซมจุดอ่อนให้นำไปใช้งานได้แล้ว งานวิจัยของ Jeffrey R Jones และคณะ [17] ได้ทำการคาดคะเนปริมาณของจุดอ่อนโดยการวิเคราะห์ข้อมูลจำนวนของจุดอ่อนที่ได้รับการเปิดเผยสู่สาธารณะแต่ยังไม่ได้รับการแก้ไขจากผู้พัฒนาซอฟต์แวร์ออกมาในรูปของดีวีอี (Daily Vulnerability Exposure) และ ทีทีเอฟ (Vendor Time To Fix) เพื่อช่วยผู้พัฒนาซอฟต์แวร์ในการตรวจสอบกระบวนการเฝ้าระวังรักษาความปลอดภัยที่มีต่อกลุ่มนักวิจัยทางด้านความปลอดภัยในระบบคอมพิวเตอร์ซึ่งคอยค้นหาและเปิดเผยจุดอ่อนของซอฟต์แวร์สู่สาธารณะ นอกจากนี้ยังช่วยวางแผนการใช้ทรัพยากรให้แก่ผู้พัฒนาซอฟต์แวร์อีกด้วย งานวิจัยของ Amontip Jumratjaroenvanit และ Yunyong Teng-Amnuay [5] ได้กำหนดช่วงเวลาสำคัญของจุดอ่อนจากหลายๆ แหล่งข้อมูลออกมาได้ 5 รูปแบบ ได้แก่ การโจมตีแบบซีโร่เดย์ (Zero-day attack) การโจมตีแบบซีโร่เดย์แบบเทียม (Pseudo zero-day attack) ภาวะเสี่ยงต่อการเกิดการโจมตีแบบซีโร่เดย์แบบเทียม (Potential of pseudo zero-day attack) ภาวะเสี่ยงต่อการเกิดการโจมตี (Potential of attack) และ การโจมตีแบบพาสซีฟ (Passive attack) โดยเฉพาะการโจมตีแบบซีโร่เดย์แบบเทียมซึ่งเป็นผลมาจากความหละหลวมในการปฏิบัติงานของผู้ดูแลระบบนั้นมีปริมาณเพิ่มมากขึ้นทุกวันอย่างเห็นได้ชัด ปัจจัยต่างๆ เช่น สภาพความพร้อมของแพทช์และโค้ต (code) ในการเจาะระบบได้ช่วยให้นำไปสู่การวิเคราะห์ความน่าจะเป็นที่จะเกิดการโจมตีจุดอ่อน (Probability of attack) ผ่านแผนภูมิเรดาร์ ทั้งหมดนี้ เพื่อช่วยให้ผู้ดูแลระบบสามารถจัดลำดับความสำคัญในการจัดการกับจุดอ่อนที่เกิดขึ้นในระบบคอมพิวเตอร์ได้เป็นอย่างมาก งานวิจัยของ Ratsameetip Wita และ Yunyong Teng-Amnuay [18] เห็นว่าระบบคอมพิวเตอร์ที่มีเครื่องมือช่วยรักษาความปลอดภัยที่มีประสิทธิภาพนั้นไม่ได้ช่วยให้ระบบมีความปลอดภัยได้เลยถ้าหากระบบปฏิบัติการที่ใช้อยู่นั้นยังคงมีจุดอ่อนตกค้างอยู่ในระบบ ด้วยเหตุนี้จึงนำไปสู่คิดค้น Profiling scheme บนพื้นฐานระดับความร้ายแรงของการโจมตีตามรายการในฐานข้อมูลซีวีอี (Common Vulnerabilities and Exposures) เพื่อใช้ในการวัดระดับของจุดอ่อนสำหรับระบบปฏิบัติการโดยใช้ 3 ระบบเป็นกรณีศึกษา ได้แก่ ลินุกซ์วานิลลา (Vanilla Linux) ลินุกซ์ที่ผ่านการเพิ่มความแข็งแกร่ง (Linux with hardening) และ ลินุกซ์แอลเอสเอ็ม (Linux with LSM) ซึ่งมีการเปรียบเทียบประสิทธิภาพทางด้านความปลอดภัยด้วยระบบการให้คะแนน เพื่อพิสูจน์ให้เห็นว่าลินุกซ์ที่ผ่านการเสริมความแข็งแกร่งทางด้านความปลอดภัยนั้นสามารถต้านทานการโจมตีได้ดีกว่าลินุกซ์วานิลลาอย่างเห็นได้ชัด และงานวิจัยของ Ashish Arora และคณะ [19] กล่าวไว้ว่า ซอฟต์-

แวร์ใดๆ ก็ตามที่ออกสู่สาธารณะแล้วนั้นจะมีจำนวนของการถูกเปิดเผยจุดอ่อนเกิดขึ้นได้ทุกเวลาถ้าหากปล่อยระบบให้เกิดภาวะที่จะถูกโจมตีเอาไว้ ดังนั้น ผู้วิจัยจึงได้มีการนำเสนอวิธีในการระบุและวิเคราะห์จุดอ่อนเหล่านี้โดยใช้ข้อมูลสาธารณะจากแหล่งข้อมูลที่เข้าถึงได้ง่าย เช่น ข้อมูลจากหน่วยงานเฝ้าระวังรักษาความปลอดภัย (CERT) หรือ ข้อมูลจากฐานข้อมูลซีวีอีเพื่อสังเกตความรับผิดชอบของผู้พัฒนาในการตอบสนองต่อจุดอ่อนที่เกิดขึ้นเพื่อเป็นประโยชน์ต่อผู้บริโภคต่อไป

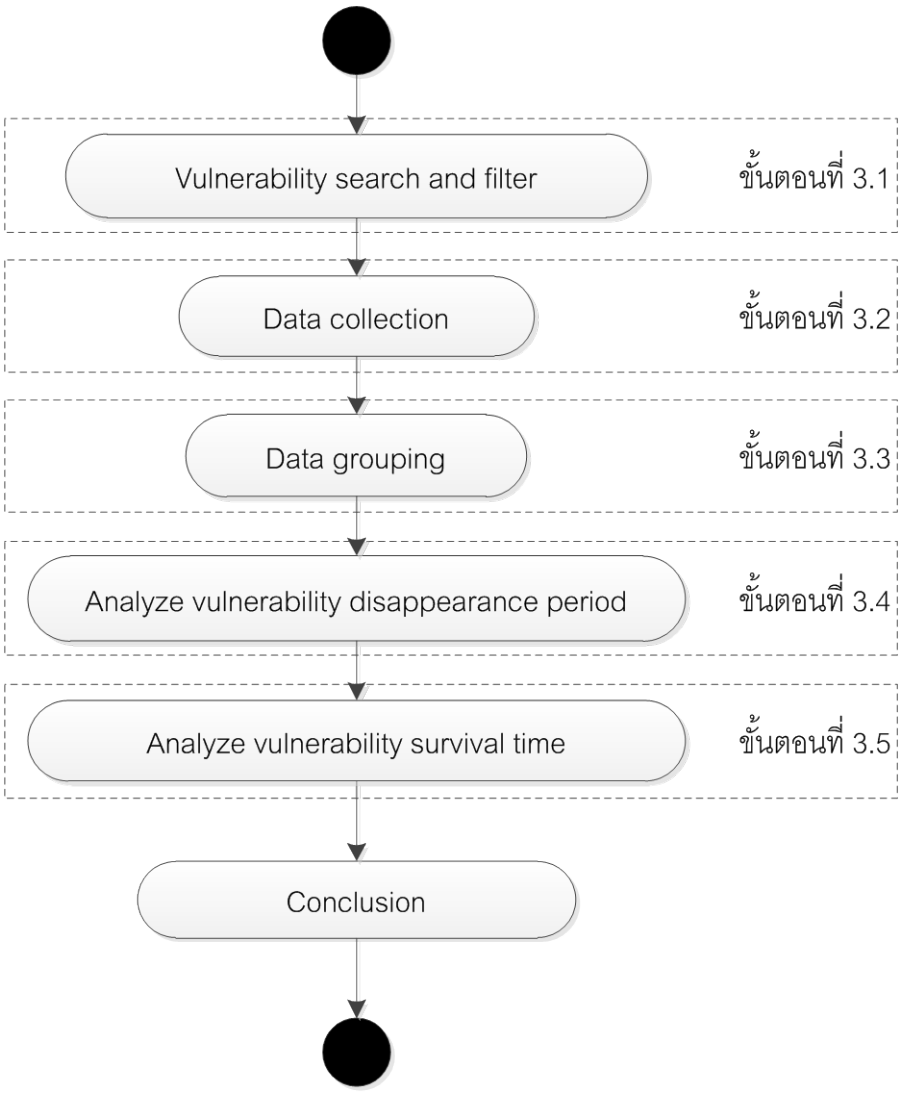
บทที่ 3

วิธีดำเนินงานวิจัย

ในบทนี้จะกล่าวถึง การดำเนินงานวิจัยซึ่งแบ่งออกเป็น 5 หัวข้อหลักๆ ประกอบด้วย

1. การค้นหาและคัดกรองจุดอ่อน
2. การเก็บข้อมูลข่าว
3. การจัดกลุ่มของจุดอ่อน
4. การวิเคราะห์ระยะเวลาสาบสูญของจุดอ่อน
5. การวิเคราะห์ระยะเวลาที่จุดอ่อนยังคงอยู่ในระบบ

ซึ่งขั้นตอนการดำเนินงานวิจัยสามารถเขียนเป็นแผนภาพแอคทิวิตี ดังรูปที่ 3.1



รูปที่ 3.1 แผนภาพขั้นตอนการดำเนินงานวิจัย

3.1 การค้นหาและคัดกรองจุดอ่อน

ในขั้นตอนแรกของการดำเนินงานวิจัยคือการค้นหาจุดอ่อนที่ต้องการนำมาทดลอง ซึ่งในงานวิจัยนี้ได้เลือกจุดอ่อนจากระบบปฏิบัติการ Windows XP จำนวน 258 ตัว (ณ วันที่ 11 กันยายน 2554) ซึ่งเป็นระบบปฏิบัติการที่ไม่เก่าและไม่ได้ใหม่จนเกินไปและมีวงจรชีวิตที่ค่อนข้างสมบูรณ์ การรวบรวมจุดอ่อนทำได้โดยการกรองจุดอ่อนจากฐานข้อมูลโอเอสวีดีบีดังตัวอย่างจากรูปที่ 3.2 ซึ่งเป็นฐานข้อมูลที่รวบรวมข้อมูลจุดอ่อนทั้งหมดที่เกิดขึ้นในระบบคอมพิวเตอร์ที่อ้างอิงฐานข้อมูลซีวีอีเป็นหลัก จุดอ่อนที่ผ่านการคัดกรองมานั้น เป็นจุดอ่อนที่เกิดขึ้นภายในระบบปฏิบัติการ และ เกิดจากโปรแกรมสนับสนุนการทำงานของระบบปฏิบัติการ โดยรายละเอียดของจุดอ่อนทั้งหมดที่เกิดขึ้นในระบบ Windows XP ได้แสดงไว้ในส่วนของภาคผนวก ก

CVE Name	Description
CVE-2011-0032	Microsoft Windows DirectShow Path Subversion Arbitrary DLL Injection Code Execution
CVE-2011-0042	Microsoft Windows Media Player / Center .dvr-ms File Handling Arbitrary Code Execution
CVE-2011-0654	Microsoft Windows Common Internet File System (CIFS) Malformed Browser Message Handling Overflow
CVE-2011-0039	Microsoft Windows LSASS Authentication Request Privilege Escalation
CVE-2010-3970	Microsoft Windows Bitmap Thumbnail shimgvw.dll CreateSizedDIBSECTION() Function biClrUsed Parameter Overflow

รูปที่ 3.2 ตัวอย่างจุดอ่อนของ Windows XP จากฐานข้อมูลโอเอสวีดีบี

จากผลการค้นหาจะทำการรวบรวมรายการจุดอ่อนโดยใช้ CVE Name เป็นตัวระบุชื่อของจุดอ่อนและบันทึกข้อมูลในรูปแบบตาราง เพื่อง่ายต่อการนำไปวิเคราะห์ข้อมูล ดังรูปที่ 3.3

	A	B	C	D
1	CVE ID			
2	CVE-1999-0504			
3	CVE-2003-0528			
4	CVE-2003-0715			
5	CVE-2004-0209			
6	CVE-2004-0214			
7	CVE-2004-0420			
8	CVE-2004-0571			
9	CVE-2004-0572			
10	CVE-2004-0574			
11	CVE-2004-0575			
12	CVE-2004-0840			

รูปที่ 3.3 รายการจุดอ่อนที่ใช้ในการทดลอง

3.2 การเก็บข้อมูลข่าว

การเก็บข้อมูลข่าวที่เกี่ยวข้องกับจุดอ่อนนั้นส่วนใหญ่จะเป็นข่าวเกี่ยวกับรายงานการโจมตีระบบ โดยจะแบ่งการเก็บข้อมูลจาก 3 แหล่งได้แก่ ฐานข้อมูลซีวีอี ฐานข้อมูลโอเอสวีดีบี และผลการค้นหาจากกูเกิ้ลจำนวน 30 ผลการค้นหาแรก [20] โดยข้อมูลสำคัญที่จะนำไปใช้การทดลองคือ วันที่ของข่าวในระบบ วัน-เดือน-ปี แบบแจกแจงความถี่ ระยะเวลาที่ข่าวยังคงมีนัยสำคัญในระบบ และระยะห่างของการเกิดข่าว โดยแยกบันทึกข้อมูล 1 จุดอ่อนต่อ 1 ตาราง เช่นตัวอย่างของ CVE-2005-0060 ดังตารางที่ 3.1

ตารางที่ 3.1 วันที่ของข่าวที่เกิดขึ้นแบบแจกแจงความถี่ของ CVE-2005-0060

วันที่	จำนวนข่าว (ชิ้น)	ระยะห่าง(วัน)
12/4/2005	7	
13/4/2005	3	1
2/5/2005	5	19
4/5/2005	4	2
1/6/2005	4	28
2/6/2005	4	1
21/11/2005	1	172
15/5/2006	1	175
รวมเวลา	398	วัน

อนึ่ง การรวบรวมข้อมูลข่าวในงานวิจัยนี้ ทำด้วยมือโดยการตรวจสอบเว็บไซต์ทีละหน้าและบันทึกขึ้นมูลทีละรายการซึ่งมีปริมาณมาก ดังนั้นอาจมีความคลาดเคลื่อนของข้อมูลบางส่วน

3.2.1 วิธีการตรวจสอบวันที่ของข่าว

ในการเก็บข้อมูลของแต่ละข่าวนั้น ส่วนที่สำคัญที่สุดในการทดลองคือ วันที่ของข่าว ซึ่งในหัวข้อนี้จะกล่าวถึงลักษณะการลงวันที่ของข่าวในทุกรูปแบบที่เกิดขึ้นระหว่างการทดลอง รวมถึงวิธีคัดกรองวันที่ของข่าวที่ถูกต้องเพื่อให้เกิดความคลาดเคลื่อนของผลการทดลองน้อยที่สุด

เมื่อเปิดข่าวแต่ละข่าวขึ้นมาตรวจสอบนั้น ในแต่ละเว็บเพจจะมีคำสำคัญที่ช่วยระบุตำแหน่งของวันที่ข่าว เช่น Date, Posted on, Last update, Last revised, Reported on, Release date, Publish date, Last review, Updated, Published, ฯลฯ ซึ่งเมื่อพบคำสำคัญเหล่านี้ โดยส่วนใหญ่จะเป็นจุดที่ระบุวันที่ของข่าวนั้น ดังตัวอย่างของ CVE-2011-0654 จากรูปที่ 3.4 แต่บางข่าวอาจมีวันที่ระบุมากกว่า 1 จุด

ดังนั้นเพื่อความถูกต้อง จำเป็นต้องมีการตรวจสอบเนื้อหาของข่าวนั้นด้วยมืออีกครั้งหนึ่งว่าเป็นข่าวที่เกี่ยวข้องกับซีวีอีตัวนั้นๆ จริงหรือไม่

รูปที่ 3.4 ตัวอย่างวันที่ของข่าวที่ถูกต้องของ CVE-2011-0654

จากรูปที่ 3.4 สังเกตได้ว่า มีวันที่ระบุอยู่ถึง 2 จุด ซึ่งในกรณีนี้ถือว่าเป็นความเคลื่อนไหวของข่าวตั้งแต่เริ่มรายงานและมีการติดตามผล ทำให้สามารถนำไปใช้ได้ทั้ง 2 วันที่

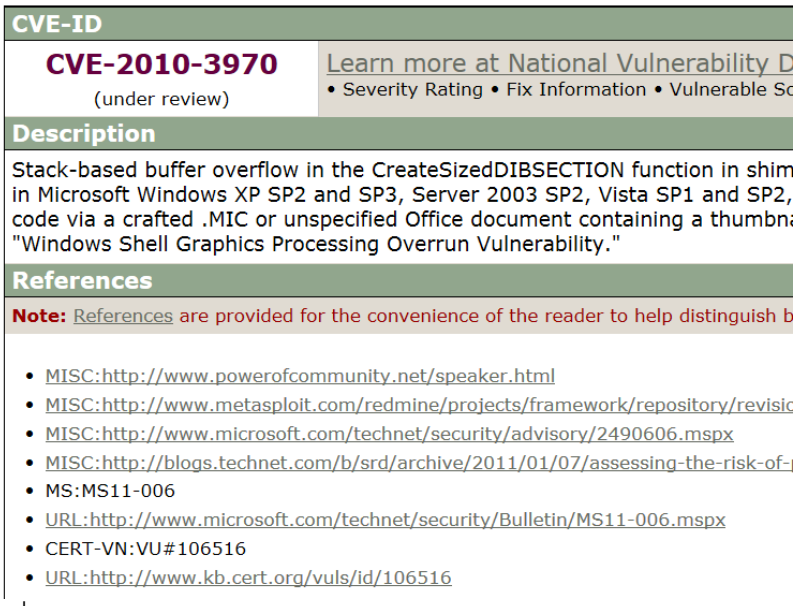
อนึ่ง รูปแบบของวันที่ของ Gregorian little-endian, Middle-endian และ Gregorian big-endian มีความคล้ายกันอยู่มาก มักอาจทำให้เกิดความสับสนในการตรวจสอบอยู่บ่อยครั้งตัวอย่างเช่น 10/05/11 อาจหมายถึง 10 พฤษภาคม 2011 หรือ 5 ตุลาคม 2011 หรือ 11 พฤษภาคม 2010 ก็ได้ ดังนั้นเพื่อเป็นการป้องกันความสับสนที่อาจเกิดขึ้นจำเป็นที่จะต้องตรวจสอบแหล่งที่มาของข่าวนั้นให้ชัดเจนว่าเป็นของประเทศใดตามรูปที่ 2.3 ในส่วนของบทที่ 2 เพื่อจะได้บันทึกข้อมูลลงในตารางได้อย่างถูกต้อง

3.2.2 การเก็บข้อมูลข่าวจากฐานข้อมูลซีวีอี

การเก็บข้อมูลข่าวจากฐานข้อมูลซีวีอีนั้น แบ่งออกเป็นขั้นตอนสำคัญได้ดังนี้

1. ในแต่ละจุดอ่อนที่ถูกเก็บอยู่ในฐานข้อมูลซีวีอีจะมีเว็บลิงค์อยู่ที่ http://cve.mitre.org/cgi-bin/cvename.cgi?name=<ปี-เลขที่> เช่น http://cve.mitre.org/cgi-bin/cvename.cgi?name=2010-3970 หมายถึงข้อมูลของจุดอ่อนที่มี CVE Name คือ CVE-2010-3970

2. ภายในหน้าเว็บเพจ ให้ทำการตรวจสอบเว็บลิงค์ในส่วนของแหล่งอ้างอิงข้อมูล (References) ทุกลิงค์ ดังรูปที่ 3.5 ซึ่งภายในนั้นเป็นรายงานข่าวการโจมตีที่เกี่ยวข้องกับจุดอ่อนตัวนั้นๆ ทั้งหมด



รูปที่ 3.5 รายการอ้างอิงของจุดอ่อน CVE-2010-3970 จากฐานข้อมูลซีวีอี

3. จากรูปที่ 3.5 จะขอยกตัวอย่างรายงานข่าวการโจมตีของจุดอ่อน CVE-2010-3970 จากเว็บลิงค์ http://www.kb.cert.org/vuls/id/106516 ดังรูปที่ 3.6

รูปที่ 3.6 ตัวอย่างรายงานข่าวการโจมตีของจุดอ่อน CVE-2010-3970 จาก US-CERT

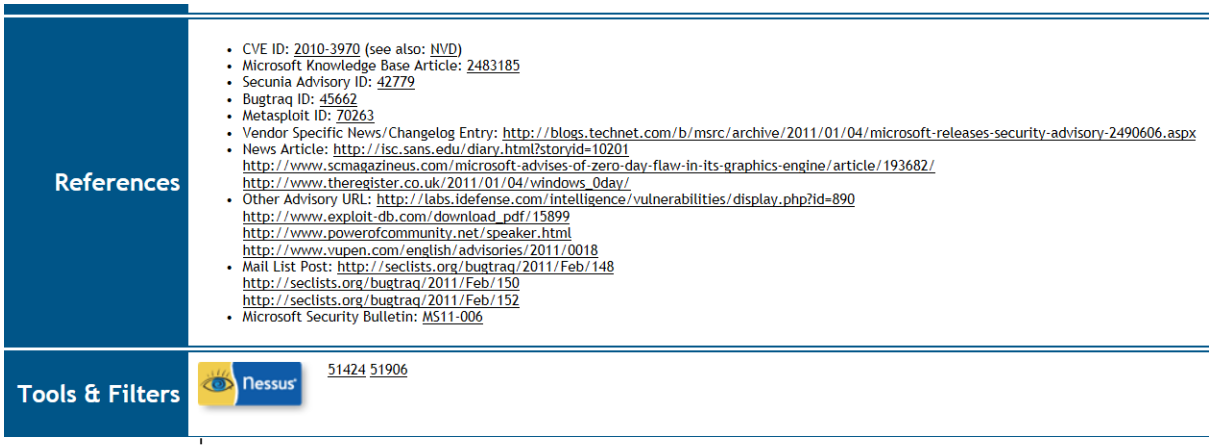
4. จากรูปที่ 3.6 ทำให้ได้ข้อมูลวันที่ 2 จุด คือ วันที่รายงานข่าว คือ 05/01/2011 และ วันที่มีการปรับปรุงและติดตามผล คือ 08/02/2011 ให้ทำการบันทึกวันที่ทั้ง 2 พร้อมทั้งความถี่ ลงในตารางเก็บข้อมูลของจุดอ่อน CVE-2010-3970

5. ทำซ้ำในข้อ 1-4 เพื่อตรวจสอบข้อมูลวันที่กับเว็บลิงค์ที่เหลือทั้งหมดที่อยู่ในส่วนของ References และในจุดอ่อนที่เหลือทั้งหมด

3.2.3 การเก็บข้อมูลข่าวจากฐานข้อมูลโอเอสวีดีบี

การเก็บข้อมูลข่าวจากฐานข้อมูลซีวีอีนั้น แบ่งออกเป็นขั้นตอนสำคัญได้ดังนี้

1. ภายในฐานข้อมูลโอเอสวีดีบี จะมีการจัดเก็บข้อมูลของจุดอ่อนเรียงตาม OSVDB ID เป็นหลัก แต่การตรวจสอบข้อมูลจุดอ่อนโดยใช้ CVE Name ก็สามารถทำได้เช่นกัน โดยเมื่อเปิดเว็บเพจของแต่ละจุดอ่อนขึ้นมานั้น (ในที่นี้ขอยกตัวอย่างของจุดอ่อน CVE-2010-3970) ให้ทำการตรวจสอบในส่วนของแหล่งอ้างอิงข้อมูล (References) แบบเดียวกันกับฐานข้อมูลซีวีอี ดังรูปที่ 3.7



รูปที่ 3.7 รายการอ้างอิงของจุดอ่อน CVE-2010-3970 จากฐานข้อมูลโอเอสวีดีบี

2. จากรูปที่ 3.7 ให้ทำการตรวจสอบเว็บลิงค์ทุกตัว โดยตรวจสอบวันที่ของข่าวที่เกิดขึ้นเช่นเดียวกันกับขั้นตอนที่ 3-4 ในหัวข้อ 3.2.3 ดังแสดงในรูปที่ 3.8 ในที่นี้ขอยกตัวอย่างจาก http://seclists.org/bugtraq/2011/Feb/148

VUPEN Security Research - Microsoft Windows Shell Graphics BMP "width" Integer Overflow Vulnerability

From: "VUPEN Security Research" <advisories () vupen com>
Date: Thu, 10 Feb 2011 17:56:03 +0100

```
VUPEN Security Research - Microsoft Windows Shell Graphics BMP "width" Integer Overflow Vulnerability

http://www.vupen.com/english/research.php


I. BACKGROUND
---------------------

"Microsoft Windows is a series of software operating systems and graphical
user interfaces produced by Microsoft. Windows had approximately 90% of
```

รูปที่ 3.8 ตัวอย่างรายงานข่าวการโจมตีของจุดอ่อน CVE-2010-3970 จาก VUPEN

3. จากรูปที่ 3.8 ทำให้ได้ข้อมูลวันที่รายงานของข่าวคือ 10/02/2011 ให้ทำการบันทึกวันที่พร้อมทั้งความถี่ ลงในตารางเก็บข้อมูลของจุดอ่อน CVE-2010-3970

4. ทำซ้ำในข้อ 1-3 เพื่อตรวจสอบข้อมูลวันที่กับเว็บลิงค์ที่เหลือทั้งหมดที่อยู่ในส่วนของ References และในจุดอ่อนที่เหลือทั้งหมด และถ้าหากมีรายงานข่าวใดซ้ำกับข่าวที่มีอยู่ใน References ของฐานข้อมูลซีวีอี ให้ทำการข้ามไปไม่ต้องนำมาตรวจสอบอีก

3.2.4 การเก็บข้อมูลข่าวจากกูเกิ้ล

การเก็บข้อมูลข่าวจากกูเกิ้ลนั้นจะใช้เครื่องมือในการช่วยค้นหาและบันทึกรายงานข่าวในรูปแบบของ html จากงานวิจัยของ Ratsmeetip Wita และ Yunyong Teng-Amnuay [20] โดยแบ่งออกเป็นขั้นตอนสำคัญได้ดังนี้

1. สร้างรายการของซีวีอีที่จะใช้ในการตรวจหาวันที่ของข่าว โดยบันทึกเป็นไฟล์ในรูปแบบของไฟล์ตาราง (spreadsheet)

2. เริ่มการทำงานของโปรแกรมโดยมีข้อมูลนำเข้าเป็นไฟล์ตารางจากข้อที่ 1 หลังจากนั้นโปรแกรมจะทำการค้นหาข่าวโดยใช้กูเกิ้ลเป็นเครื่องมือในการค้นหาหลัก และบันทึกผลลัพธ์ที่ได้ในรูปแบบของเว็บเพจ html จำนวน 30 ผลการค้นหาแรก

3. ทำการตรวจสอบวันที่ของข่าวจากเว็บเพจที่ได้ ในที่นี้ขอยกตัวอย่างของจุดอ่อน CVE-2010-3970 จากรายงานข่าว http://www.securityfocus.com/bid/45662/ ดังรูปที่ 3.9

Microsoft Windows 'CreateSizedDIBSECTION()' Vulnerability

Bugtraq ID:	45662
Class:	Boundary Condition Error
CVE:	CVE-2010-3970
Remote:	Yes
Local:	No
Published:	Jan 04 2011 12:00AM
Updated:	Feb 15 2011 02:39PM
Credit:	Moti & Xu Hao

รูปที่ 3.9 ตัวอย่างรายงานข่าวการโจมตีของจุดอ่อน CVE-2010-3970 จาก Securityfocus

4. จากรูปที่ 3.9 ทำให้ได้ข้อมูลวันที่ 2 จุด คือ วันที่รายงานข่าว คือ 04/01/2011 และ วันที่มีการปรับปรุงและติดตามผล คือ 15/02/2011 ให้ทำการบันทึกวันที่ทั้ง 2 พร้อมทั้งความถี่ ลงในตารางเก็บข้อมูลของจุดอ่อน CVE-2010-3970

5. ทำซ้ำกับผลลัพธ์จากการค้นหาที่เหลือ ถ้าหากรายงานข่าวใดซ้ำกับข่าวที่อยู่ในฐานข้อมูลซีวีอีและโอเอสวีดีบีไปแล้ว ให้ทำการข้ามการตรวจสอบข่าวนั้นๆ ไป และมีข้อควรระวังคือ ผลการค้นหาจากกูเกิ้ลนั้น อาจไม่ตรงกับคำค้นที่ได้ 100% ซึ่งส่งผลให้มีรายงานข่าวที่ไม่เกี่ยวข้องปะปนเข้ามาด้วยบางส่วน ดังนั้นเพื่อเป็นการป้องกันความผิดพลาดที่อาจเกิดขึ้นควรให้ความระมัดระวังในการตรวจสอบเป็นพิเศษ

หลังจากตรวจสอบวันที่ของข่าวตามขั้นตอนในหัวข้อที่ 3.2.2 – 3.2.4 แล้ว สามารถสรุปออกมาเป็นตารางเก็บข้อมูลแบบแจกแจงความถี่ทั้งหมด 258 ตาราง ในที่นี้ขอยกตัวอย่างจาก CVE-2010-3970 ดังตารางที่ 3.2

ตารางที่ 3.2 วันที่ของข่าวที่เกิดขึ้นแบบแจกแจงความถี่ของ CVE-2010-3970

วันที่	จำนวนข่าว (ชิ้น)	ระยะห่าง (วัน)
14/10/2010	1	
15/12/2010	1	62
22/12/2010	2	7
30/12/2010	1	8
4/1/2011	10	5
5/1/2011	7	1
6/1/2011	1	1
7/1/2011	1	1
9/1/2011	1	2
11/1/2011	1	2
12/1/2011	1	1
24/1/2011	1	12
8/2/2011	5	15
9/2/2011	2	1
10/2/2011	1	1
14/2/2011	1	4
15/2/2011	1	1
23/2/2011	1	8
25/2/2011	1	2
8/3/2011	1	11
25/3/2011	1	17
17/4/2011	1	23
18/7/2011	2	92
รวม	277	วัน

อนึ่ง ภายหลังจากการรวบรวมข้อมูลเสร็จสิ้นพบว่า มีจุดอ่อนอยู่จำนวน 4 ตัว ได้แก่ CVE-1999-0504, CVE-2003-0528, CVE-2003-0715 และ CVE-2004-0209 มีค่าระยะเวลาที่ยังคงมีนัยสำคัญในระบบสูงกว่าค่าปรกติมาก (Extreme value) จึงทำการตัด 4 จุดอ่อนนี้ออกจากการทดลองเพื่อลดความคลาดเคลื่อนของผลการทดลองให้มากที่สุด ทำให้คงเหลือจุดอ่อนที่ใช้ในการทดลองจำนวน 254 ตัว

3.3 การจัดกลุ่มของจุดอ่อน

เพื่อให้การวิเคราะห์วันหมดอายุของจุดอ่อนมีประสิทธิภาพ จึงมีการจัดกลุ่มของจุดอ่อน ซึ่งรายละเอียดของจุดอ่อนทั้งหมดได้แสดงไว้ที่ภาคผนวก ก โดยแบ่งออกเป็น 5 ลักษณะ ดังนี้

3.3.1 การจำแนกประเภทตามระดับความรุนแรงของจุดอ่อน

การจัดกลุ่มของจุดอ่อนตามระดับความรุนแรงได้มีการใช้ระบบคะแนนของซีวีเอสเอส (Common Vulnerability Scoring System) [21] เป็นเกณฑ์ในการแบ่งกลุ่ม (0-10 คะแนน) ซึ่งในแต่ละระดับคะแนนสามารถจำแนกจุดอ่อนได้ 4 กลุ่ม ได้แก่

1. จุดอ่อนที่มีระดับความรุนแรงสูงสุด มีคะแนน CVSS เท่ากับ 10 คะแนน
2. จุดอ่อนที่มีระดับความรุนแรงสูง มีคะแนน CVSS อยู่ในช่วง 7-9.9 คะแนน
3. จุดอ่อนที่มีระดับความรุนแรงปานกลาง มีคะแนน CVSS อยู่ในช่วง 4-6.9 คะแนน
4. จุดอ่อนที่มีระดับความรุนแรงต่ำ มีคะแนน CVSS อยู่ในช่วง 0-3.9 คะแนน

3.3.2 การจำแนกประเภทตามตำแหน่งที่เกิดของจุดอ่อน

การแบ่งกลุ่มของจุดอ่อนตามตำแหน่งที่เกิดที่ใช้ในงานวิจัยนี้ แบ่งตามตำแหน่งที่จุดอ่อนเกิดว่าอยู่ ณ ส่วนใดของระบบ โดยสามารถจำแนกจุดอ่อนได้ 5 กลุ่ม ได้แก่

1. ส่วนการเข้าถึงเชิงกายภาพ (Physical Access)
2. ส่วนการเข้าถึงระยะไกลและระบบเครือข่าย (Remote / Network Access)
3. ส่วนการเข้าถึงระดับท้องถิ่น (Local Access)
4. ส่วนการเข้าถึงระดับท้องถิ่นและระยะไกล (Local and Remote Access)
5. ส่วนที่ขึ้นกับชุดข้อมูลป้องกัน (Context Dependent)

3.3.3 การจำแนกประเภทตามรูปแบบการโจมตี

สามารถจำแนกจุดอ่อนได้ 4 กลุ่ม ได้แก่

1. การจัดการพิสูจน์ตัวจริง (Authentication Management)
2. การดำเนินการข้อมูลนำเข้า (Input Manipulation)
3. การเปิดเผยข้อมูล (Information Disclosure)
4. การขัดขวางการให้บริการ (Denial of Service)

3.3.4 การจำแนกประเภทตามลักษณะความเสียหาย

การจัดกลุ่มของจุดอ่อนในลักษณะนี้ อาศัยหลักการอ้างอิงจากพื้นฐานทางด้านความปลอดภัยของระบบคอมพิวเตอร์ ได้แก่ การรักษาความลับ การรักษาสภาพบูรณภาพ และการรักษาสภาพพร้อมใช้งาน ซึ่งสามารถจำแนกจุดอ่อนได้ 4 กลุ่มได้แก่

1. เสียความเป็นความลับ (Loss of Confidentiality) เกิดขึ้นจากการโจมตีเข้าไปในส่วนของข้อมูลที่เป็นความลับ ทำให้การทำงานและข้อมูลที่เป็นความลับถูกเปิดเผย และถูกขโมยไปจากระบบ

2. เสียสภาพบูรณภาพ (Loss of Integrity) เกิดขึ้นจากการโจมตีเพื่อเข้าไปเปลี่ยนแปลงข้อมูลต่างๆ ที่อยู่ในระบบคอมพิวเตอร์

3. เสียสภาพพร้อมใช้งาน (Loss of Availability) เกิดขึ้นจากการเข้าไปขัดขวางการทำงาน การประมวลผล การเรียกใช้ข้อมูล หรือ การเรียกใช้ทรัพยากรต่างๆ ภายในระบบคอมพิวเตอร์

4. เสียหายทั้งความเป็นความลับ สภาพบูรณภาพ และ สภาพพร้อมใช้งาน เกิดขึ้นจากการโจมตีที่ก่อให้เกิดความเสียหายครบทั้ง 3 อย่างตามหัวข้อที่ 1-3

3.3.5 การจำแนกประเภทของจุดอ่อนตามสถานะแพทช์

การจัดกลุ่มของจุดอ่อนในลักษณะนี้ จะช่วยในการทดอบประสิทธิภาพของการแพทช์ว่ามีประสิทธิภาพมากเพียงใด ทั้งในด้านของซอฟต์แวร์แพทช์ และ ผู้ให้บริการ ซึ่งสามารถจำแนกจุดอ่อนได้ 2 กลุ่มได้แก่

1. จุดอ่อนที่ยังไม่ได้รับการแพทช์
2. จุดอ่อนที่ได้รับการแพทช์แล้ว

3.4 การวิเคราะห์ระยะเวลาสาบสูญของจุดอ่อน

ในการวิเคราะห์เพื่อกำหนดระยะเวลาสาบสูญของจุดอ่อนในงานวิจัยนี้ได้อาศัยหลักการของทฤษฎีช่วงความเชื่อมั่นจากหัวข้อที่ 2.4 ซึ่งมีข้อมูลนำเข้าคือ ระยะห่างของการเกิดข่าวสูงสุดของแต่ละจุดอ่อน โดยใช้สมการช่วงความเชื่อมั่นจากสมการที่ 2.4 ในการคำนวณดังสมการที่ 3.1

$$\bar{x} - 1.96\frac{s}{\sqrt{n}} < \mu < \bar{x} + 1.96\frac{s}{\sqrt{n}} \qquad (3.1)$$

จากสมการที่ 3.1 เมื่อ $\bar{x}$ แทนค่าเฉลี่ยเลขคณิตของระยะห่างของการเกิดข่าวสูงสุด s แทนส่วนเบี่ยงเบนมาตรฐานของระยะห่างของการเกิดข่าวสูงสุด กำหนด α = 0.05 และ DF=253 และ μ แทนช่วงความเชื่อมั่น 95% ของระยะเวลาที่จุดอ่อนหายไปจากระบบสูงสุด และผลลัพธ์ที่ได้จะเป็นระยะเวลาการสาบสูญแบบเป็นช่วงซึ่งจะใช้ค่าขอบเขตบนเป็นจุดตัด (Cut point) ของการกำหนดระยะเวลาสาบสูญของ

จุดอ่อน และเครื่องมือที่ใช้ในการคำนวณคือ โปรแกรม IBM SPSS เวอร์ชัน 20 โดยผลการคำนวณได้กล่าวไว้ในบทที่ 4

3.5 การวิเคราะห์ระยะเวลาที่จุดอ่อนยังคงอยู่ในระบบ

ในการวิเคราะห์หาค่ามัธยฐานของระยะเวลาที่จุดอ่อนยังคงมีอยู่ในระบบหรือระยะเวลาที่จุดอ่อนยังคงมีนัยสำคัญ (Survival time) ที่ช่วงความเชื่อมั่น 95% ด้วยวิธีการของ Kaplan-Meier [3] นั้น กำหนดช่วงระยะเวลาในการศึกษาข้อมูล คือ 7 ส.ค. 2544 – 1 เม.ย. 2555 เป็นเวลารวมทั้งสิ้น 3,890 วัน

เหตุการณ์ที่สนใจ คือ การสาบสูญของจุดอ่อน ซึ่งนำไปสู่การหมดอายุของจุดอ่อน ถ้าจุดอ่อนใดมีค่าระยะเวลาที่หายไปจากระบบสูงสุดไม่เกินระยะเวลาสาบสูญ จะถือว่าจุดอ่อนยังไม่สาบสูญ (Censored) เนื่องจากจุดอ่อนยังคงมีนัยสำคัญ ในทางกลับกัน ถ้าจุดอ่อนใดมีค่าเวลาที่หายไปจากระบบครั้งสุดท้ายเกิน 301.34 วัน ถือว่าเกิดเหตุการณ์สาบสูญ (Failure) ซึ่งนำไปสู่การหมดอายุของจุดอ่อน และมีตัวแปรที่เกี่ยวข้องกับการวิเคราะห์ ได้แก่

ตัวแปรเวลา คือระยะเวลาที่พบข่าวของจุดอ่อน

ตัวแปรสถานะ คือเหตุการณ์ที่สนใจแบ่งเป็น 2 กรณีคือ จุดอ่อนสาบสูญและไม่สาบสูญ

ตัวแปรปัจจัย ใช้ในการวิเคราะห์จุดอ่อนเชิงกลุ่ม ในงานวิจัยนี้ได้นำเสนอการแบ่งกลุ่มตามหัวข้อที่ 3.3 และจุดอ่อนทั้งหมดโดยไม่แบ่งกลุ่ม เพื่อเปรียบเทียบความแตกต่างและดูคุณสมบัติที่ใช้ในการจัดกลุ่มจุดอ่อนว่าส่งผลต่ออายุของจุดอ่อนอย่างไรบ้าง โดยจัดเป็นกลุ่มได้ 6 กลุ่มดังนี้

1. จุดอ่อนทั้งหมดแบบไม่แบ่งกลุ่ม
2. จุดอ่อนแบ่งกลุ่มตามระดับความรุนแรง
3. จุดอ่อนแบ่งกลุ่มตามตำแหน่งที่เกิด
4. จุดอ่อนแบ่งกลุ่มตามรูปแบบการโจมตี
5. จุดอ่อนแบ่งกลุ่มตามลักษณะความเสียหาย
6. จุดอ่อนแบ่งกลุ่มตามสถานะแพทช์ของจุดอ่อน

เครื่องมือที่ใช้ในการคำนวณคือ โปรแกรม IBM SPSS เวอร์ชัน 20 ซึ่งผลลัพธ์ที่ได้สามารถนำมาตรวจสอบได้ว่า จุดอ่อนเหล่านั้นหมดอายุหรือไม่โดยการนำจุดอ่อนแต่ละตัวมาเปรียบเทียบค่าระยะเวลาที่พบข่าวของจุดอ่อนว่ามีค่ามากกว่าระยะเวลาที่จุดอ่อนยังคงมีนัยสำคัญหรือไม่ ถ้าหากมากกว่า จะถือว่าจุดอ่อนนั้นได้หมดอายุลงแล้ว เป็นอันตรายต่อระบบต่ำ โดยผลการทดลองได้กล่าวไว้ในบทที่ 4

บทที่ 4

ผลการวิจัย

จากการศึกษาและรวบรวมข้อมูลข่าวจากสื่อออนไลน์สาธารณะและการวิเคราะห์ระยะเวลาการสาบสูญรวมถึงวันหมดอายุของจุดอ่อน ทำให้ได้ผลการวิจัยดังนี้

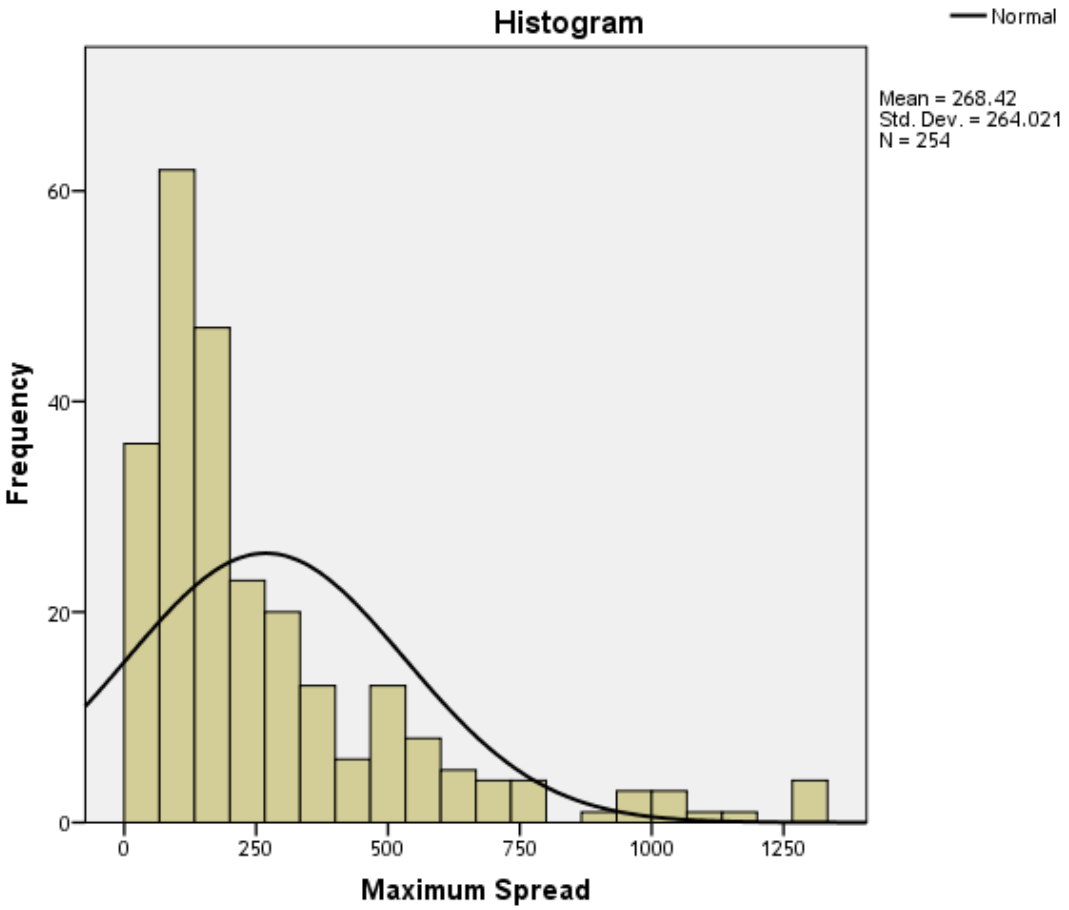
4.1 การกำหนดระยะเวลาสาบสูญของจุดอ่อน

ผลการวิเคราะห์ระยะเวลาสาบสูญของจุดอ่อนโดยใช้วิธีที่ได้กล่าวไว้แล้วในหัวข้อที่ 3.4 นั้น ได้นำจุดอ่อนทั้งหมด 254 ตัวมาทำการคำนวณหาช่วงความเชื่อมั่น 95% ของระยะเวลาที่จุดอ่อนหายไปจากระบบสูงสุด ซึ่งมีผลการคำนวณจากโปรแกรม IBM SPSS เวอร์ชัน 20 ดังตารางที่ 4.1

ตารางที่ 4.1 ผลการคำนวณระยะเวลาที่จุดอ่อนหายไปจากระบบสูงสุด

			Statistic
Maximum spread	Mean		268.42
	95% Confidence Interval for Mean	Lower Bound	235.79
		Upper Bound	301.04
	Std. Deviation		264.021
	Minimum		3
	Maximum		1325
	Range		1322

จากตารางที่ 3.3 ผลการคำนวณระยะเวลาที่จุดอ่อนหายไปจากระบบสูงสุด (Maximum spread) มีค่าอยู่ในช่วง 235.79 ถึง 301.04 วัน ได้กราฟที่มีลักษณะเบ้ขวาดังรูปที่ 4.1 ในที่นี้จะใช้ค่าขอบเขตบนคือ 301.34 วัน เป็นจุดตัด (Cut point) ของการกำหนดระยะเวลาสาบสูญของจุดอ่อน โดยนำไปเปรียบเทียบกับ ผลต่างของวันสุดท้ายที่ศึกษาข้อมูลกับวันสุดท้ายที่พบข่าว ถ้าหากว่ามากกว่า 301.34 วัน ให้ถือว่าจุดอ่อนนั้นอยู่ในสถานะสาบสูญ ซึ่งได้จุดอ่อนที่อยู่ในสถานะสาบสูญคิดเป็น 177 จาก 254 ตัว หรือ 69.68% ของจุดอ่อนทั้งหมดที่ใช้ในการทดลอง



รูปที่ 4.1 ฮิสโทรแกรมของระยะเวลาที่จุดอ่อนหายไปจากระบบสูงสุด

นอกจากนี้ยังสามารถสรุปผลการตรวจสอบจุดอ่อนที่มีสถานะสาบสูญ แยกตามประเภทของจุดอ่อนที่ได้กำหนดไว้ตามหัวข้อที่ 3.3 ดังตารางที่ 4.2

ตารางที่ 4.2 จำแนกรายละเอียดของจุดอ่อนที่มีสถานะสาบสูญแบบจำแนกประเภท

ประเภท	กลุ่ม	จำนวนจุดอ่อน	สาบสูญ	ไม่สาบสูญ	สาบสูญคิดเป็น
Severity	Highest	25	22	3	88.00%
	High	154	81	73	52.59%
	Medium	58	57	1	98.27%
	Low	17	17	0	100%
Location	Physical Access	3	3	0	100%
	Remote / Network Access	108	99	9	91.67%
	Local Access	69	43	26	62.31%
	Local and Remote Access	34	6	28	17.64%
	Context Dependent	20	7	13	35.00%
	Unknown Location	20	19	1	95.00%
Attack Type	Authentication Management	4	1	3	25.00%
	Input Manipulation	197	120	77	60.91%
	Information Disclosure	7	2	5	28.57%
	Denial of Service	27	26	1	96.29%
	Unknown Attack Type	19	17	2	89.47%
Impact	Loss of Confidentiality	7	7	0	100%
	Loss of Integrity	208	131	77	62.98%
	Loss of Availability	28	28	0	100%
	Loss all C, I and A	3	3	0	100%
	Unknown Impact	8	8	0	100%
Solution	Patched	119	113	6	94.95%
	Not Patched	135	64	71	47.40%
Total	Overall	254	177	77	69.68%

4.2 ผลการวิเคราะห์ระยะเวลาที่จุดอ่อนยังคงอยู่ในระบบ

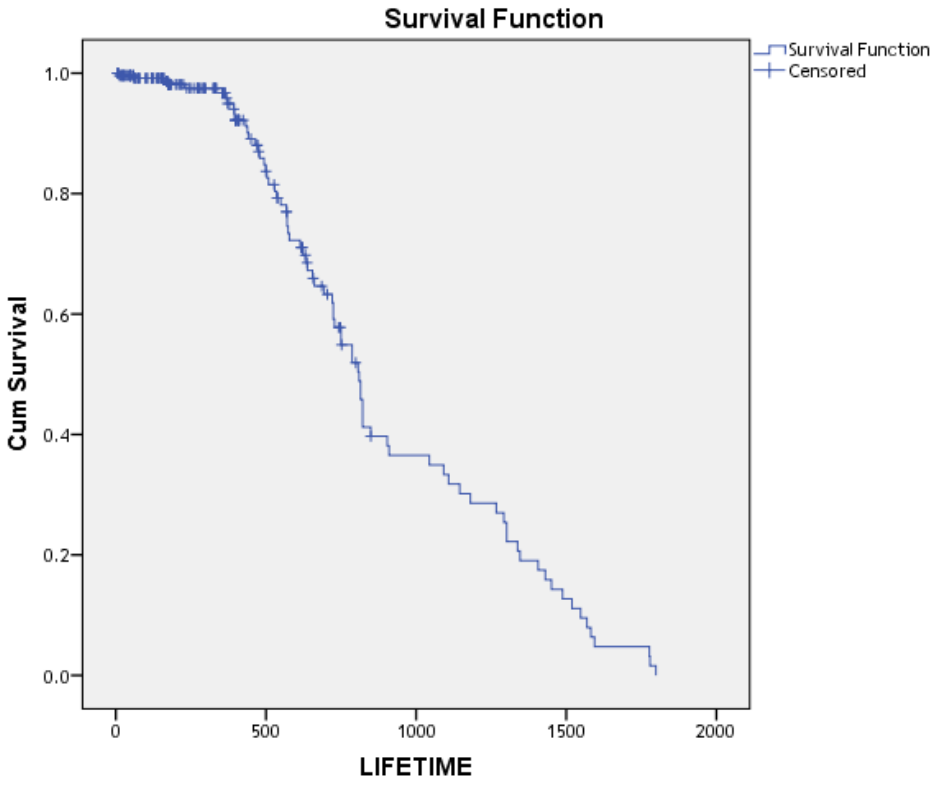
ผลการวิเคราะห์ระยะเวลาที่จุดอ่อนยังคงอยู่ในระบบโดยใช้วิธีที่ได้กล่าวไว้แล้วในหัวข้อที่ 3.5 นั้น ได้นำจุดอ่อนทั้งหมด 254 ตัวมาทำการคำนวณหาค่ามัธยฐานของระยะเวลาที่จุดอ่อนยังคงมีอยู่ในระบบ (Survival time) ที่ช่วงความเชื่อมั่น 95% ซึ่งผลการคำนวณที่ได้จะแบ่งออกเป็น 6 กลุ่มดังนี้

4.2.1 จุดอ่อนทั้งหมดโดยไม่แบ่งกลุ่ม

ในหัวข้อนี้จะแสดงผลการคำนวณค่ามัธยฐานระยะเวลาที่จุดอ่อนยังคงอยู่ในระบบของจุดอ่อนทั้งหมดแบบไม่แบ่งกลุ่ม เพื่อดูภาพรวมทั้งหมด ซึ่งมีผลการคำนวณดังตารางที่ 4.3 และรูปที่ 4.2

ตารางที่ 4.3 ผลการคำนวณค่ามัธยฐานระยะเวลาที่จุดอ่อนยังคงอยู่ในระบบของจุดอ่อนทั้งหมด

Estimate	Standard	95% Confidence Interval	
Median	Error	Lower Bound	Upper Bound
810.000	32.010	747.261	872.739



รูปที่ 4.2 ระยะเวลาที่จุดอ่อนยังคงอยู่ในระบบในภาพรวม

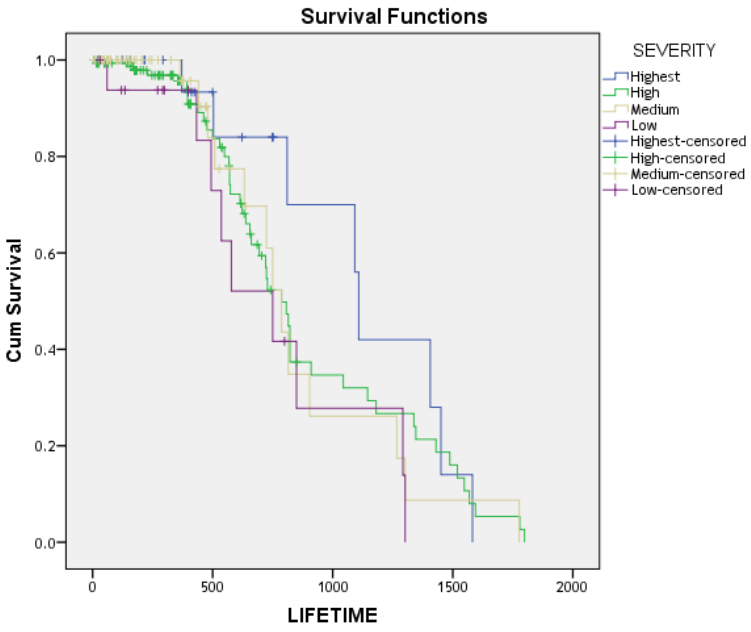
จากตารางที่ 4.3 และรูปที่ 4.2 พบว่าจุดอ่อนใดก็ตามที่อยู่ในสถานะสาบสูญและมีค่ามัธยฐานระยะเวลาที่จุดอ่อนยังคงอยู่ในระบบเกิน 810 วันจะถือว่าจุดอ่อนนั้นได้หมดอายุลง

4.2.2 จุดอ่อนแบ่งกลุ่มตามระดับความรุนแรง

ในหัวข้อนี้จะแสดงผลการคำนวณค่ามัธยฐานระยะเวลาที่จุดอ่อนยังคงอยู่ในระบบของจุดอ่อนโดยแบ่งกลุ่มตามระดับความรุนแรงเพื่อนำไปใช้เปรียบเทียบว่าระดับความรุนแรงของจุดอ่อนส่งผลต่อระยะเวลาที่จุดอ่อนยังคงอยู่ในระบบในระบบมากน้อยเพียงใด ซึ่งมีผลการคำนวณดังตารางที่ 4.4 และรูปที่ 4.3

ตารางที่ 4.4 ผลการคำนวณค่ามัธยฐานระยะเวลาที่จุดอ่อนยังคงอยู่ในระบบแบ่งตามระดับความรุนแรง

SEVERITY	Median			
	Estimate Median	Standard Error	95% Confidence Interval	
			Lower Bound	Upper Bound
Highest	1108.000	20.508	1067.805	1148.195
High	787.000	55.316	678.581	895.419
Medium	787.000	50.611	687.802	886.198
Low	750.000	161.881	432.713	1067.287
Overall	810.000	32.010	747.261	872.739



รูปที่ 4.3 ระยะเวลาที่จุดอ่อนยังคงอยู่ในระบบจำแนกตามระดับความรุนแรง

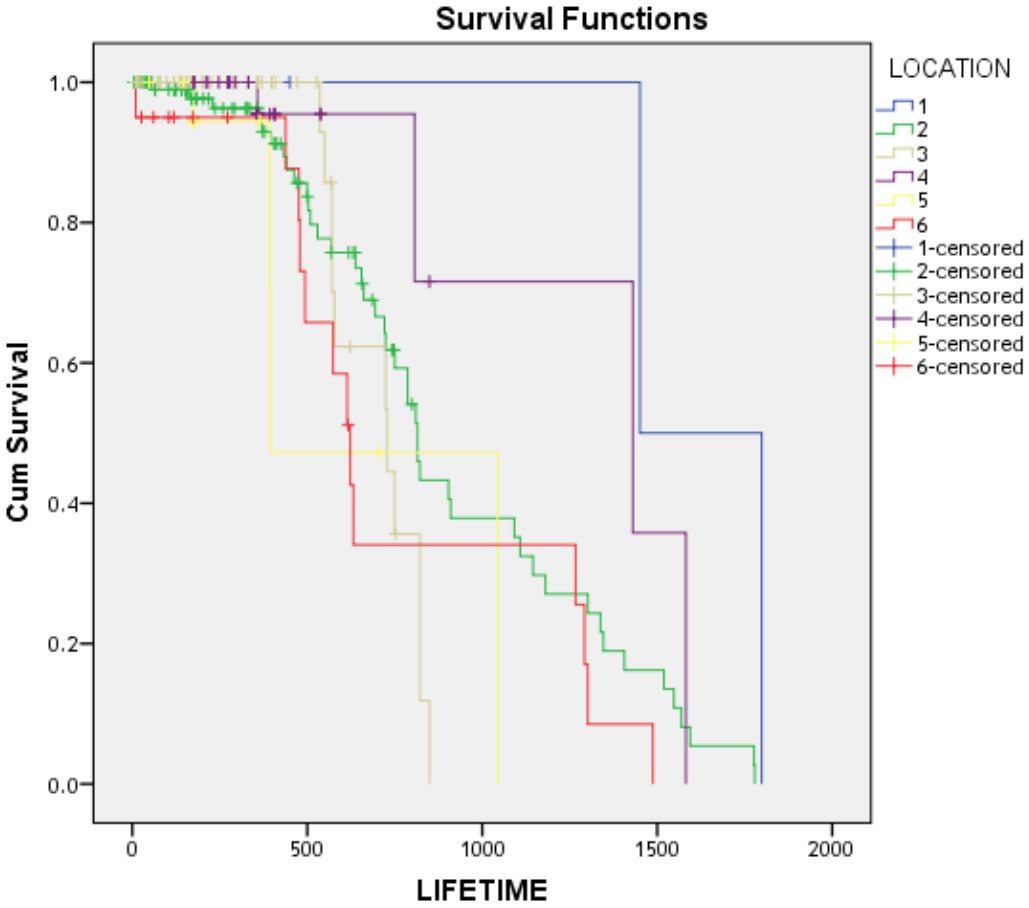
จากตารางที่ 4.4 และ รูปที่ 4.3 พบว่าจุดอ่อนที่มีระดับความรุนแรงที่สุด จะมีระยะเวลาที่จุดอ่อนยังคงอยู่ในระบบมากที่สุด ในขณะที่จุดอ่อนที่มีระดับความรุนแรงต่ำ จะมีระยะเวลาที่จุดอ่อนยังคงอยู่ในระบบน้อยที่สุด แต่อย่างไรก็ตามจากการทดสอบความแตกต่างของระยะเวลาที่จุดอ่อนยังคงอยู่ในระบบจำแนกตามระดับความรุนแรงของจุดอ่อนโดยใช้ Log-rank พบว่า ในแต่ละระดับความรุนแรงของจุดอ่อนมีระยะเวลาที่จุดอ่อนยังคงอยู่ในระบบไม่แตกต่างกัน (p=0.439)

4.2.3 **จุดอ่อนแบ่งกลุ่มตามตำแหน่งที่เกิด**

ในหัวข้อนี้จะแสดงผลการคำนวณค่ามัธยฐานระยะเวลาที่จุดอ่อนยังคงอยู่ในระบบของจุดอ่อนโดยแบ่งกลุ่มตามตามตำแหน่งที่เกิดเพื่อนำไปใช้เปรียบเทียบว่าจุดอ่อนที่มีตำแหน่งที่เกิดแต่ละที่ต่างกันนั้นส่งผลต่อระยะเวลาที่จุดอ่อนยังคงอยู่ในระบบในระบบมากน้อยเพียงใด ซึ่งมีผลการคำนวณดังตารางที่ 4.5 และรูปที่ 4.4

ตารางที่ 4.5 ผลการคำนวณค่ามัธยฐานระยะเวลาที่จุดอ่อนยังคงอยู่ในระบบแบ่งตามตำแหน่งที่เกิด

LOCATION	Median			
	Estimate Median	Standard Error	95% Confidence Interval	
			Lower Bound	Upper Bound
1. Physical access	1451.000	-	-	-
2. Remote / Network Access	815.000	34.367	747.640	882.360
3. Local Access	728.000	120.432	491.953	964.047
4. Local and Remote Access	1430.000	476.706	495.656	2364.344
5. Context Dependent	395.000	218.414	0.000	823.091
6. Location not specified	623.000	42.112	540.461	705.539
Overall	810.000	32.010	747.261	872.739



รูปที่ 4.4 ระยะเวลาที่จุดอ่อนยังคงอยู่ในระบบจำแนกตามตำแหน่งที่เกิด

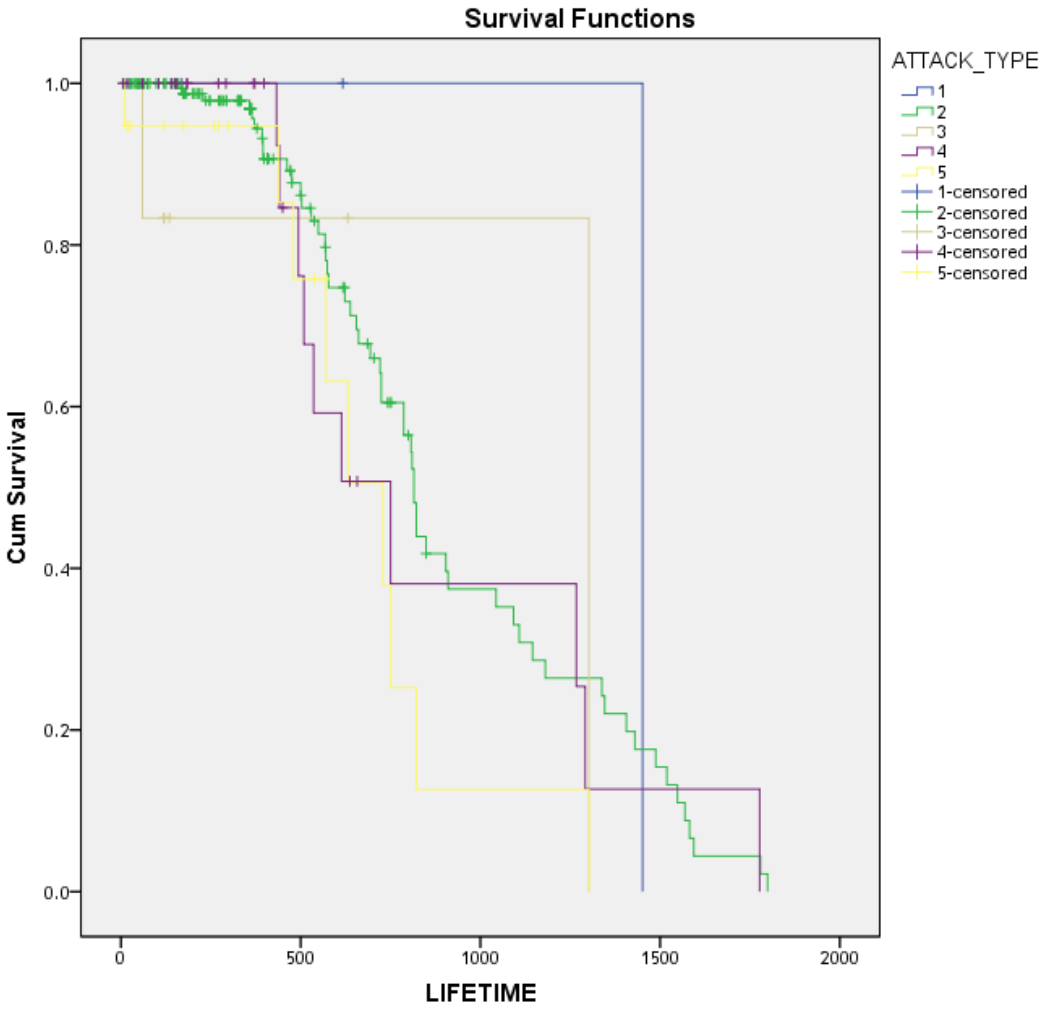
จากตารางที่ 4.5 และ รูปที่ 4.4 พบว่าจุดอ่อนที่เกิดขึ้นในส่วนของการเข้าถึงเชิงกายภาพ จะมีระยะเวลาที่จุดอ่อนยังคงอยู่ในระบบมากที่สุด ในขณะที่จุดอ่อนที่ไม่ทราบตำแหน่งที่เกิด จะมีระยะเวลาที่จุดอ่อนยังคงอยู่ในระบบน้อยที่สุด นอกจากนี้จากการทดสอบความแตกต่างของระยะเวลาที่จุดอ่อนยังคงอยู่ในระบบจำแนกตามตำแหน่งที่เกิดของจุดอ่อนโดยใช้ Log-rank พบว่า ในแต่กลุ่มมีระยะเวลาที่จุดอ่อนยังคงอยู่ในระบบแตกต่างกันอย่างมีนัยสำคัญอีกด้วย (p=0.030)

4.2.4 จุดอ่อนแบ่งกลุ่มตามรูปแบบการโจมตี

ในหัวข้อนี้จะแสดงผลการคำนวณค่ามัธยฐานระยะเวลาที่จุดอ่อนยังคงอยู่ในระบบของจุดอ่อนโดยแบ่งกลุ่มตามตามรูปแบบการโจมตีเพื่อนำไปใช้เปรียบเทียบว่าจุดอ่อนที่มีรูปแบบการโจมตีต่างกันไปนั้นส่งผลต่อระยะเวลาที่จุดอ่อนยังคงอยู่ในระบบในระบบมากน้อยเพียงใด ซึ่งมีผลการคำนวณดังตารางที่ 4.6 และรูปที่ 4.5

ตารางที่ 4.6 ผลการคำนวณค่ามัธยฐานระยะเวลาที่จุดอ่อนยังคงอยู่ในระบบแบ่งตามรูปแบบการโจมตี

ATTACK TYPE	Median			
	Estimate	Standard	95% Confidence Interval	
	Median	Error	Lower Bound	Upper Bound
1. Authentication Management	1451.000	-	-	-
2. Input Manipulation	815.000	18.661	778.424	851.576
3. Information Disclosure	1302.000	0.000	-	-
4. Denial of Service	750.000	155.987	444.265	1,055.735
5. Unknown Attack type	728.000	104.546	523.089	932.911
6. Overall	810.000	32.010	747.261	872.739



รูปที่ 4.5 ระยะเวลาที่จุดอ่อนยังคงอยู่ในระบบจำแนกตามรูปแบบการโจมตี

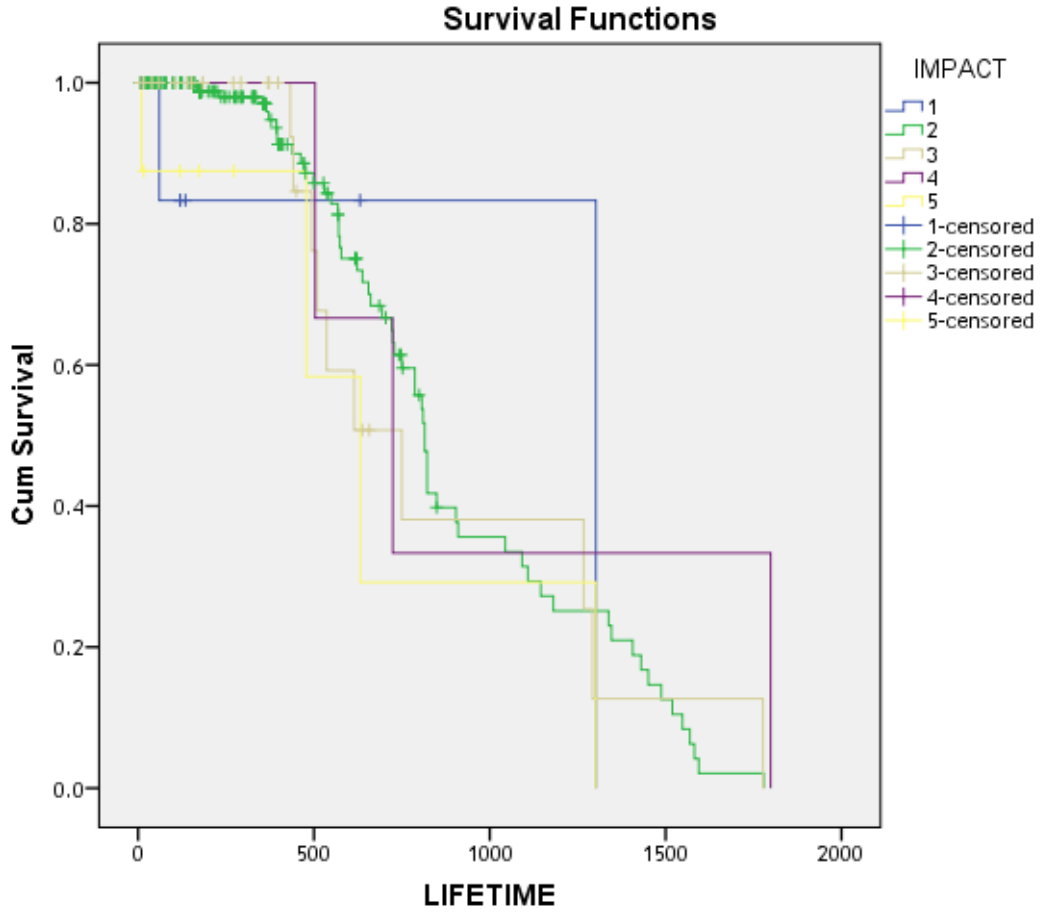
จากตารางที่ 4.6 และ รูปที่ 4.5 พบว่าจุดอ่อนที่มีรูปแบบการโจมตีการจัดการพิสูจน์ตัวจริง จะมีระยะเวลาที่จุดอ่อนยังคงอยู่ในระบบมากที่สุด ในขณะที่จุดอ่อนที่ไม่ทราบรูปแบบการโจมตีจะมีระยะเวลาที่จุดอ่อนยังคงอยู่ในระบบน้อยที่สุด แต่อย่างไรก็ตามจากการทดสอบความแตกต่างของระยะเวลาที่จุดอ่อนยังคงอยู่ในระบบจำแนกตามรูปแบบการโจมตีโดยใช้ Log-rank พบว่า ในจุดอ่อนที่มีรูปแบบการโจมตีต่างๆ กันมีระยะเวลาที่จุดอ่อนยังคงอยู่ในระบบไม่แตกต่างกัน (p=0.343)

4.2.5 **จุดอ่อนแบ่งกลุ่มตามลักษณะความเสียหาย**

ในหัวข้อนี้จะแสดงผลการคำนวณค่ามัธยฐานระยะเวลาที่จุดอ่อนยังคงอยู่ในระบบของจุดอ่อนโดยแบ่งกลุ่มตามตามลักษณะความเสียหายเพื่อนำไปใช้เปรียบเทียบว่าจุดอ่อนที่มีลักษณะความเสียหายต่างกันไปนั้นส่งผลต่อระยะเวลาที่จุดอ่อนยังคงอยู่ในระบบในระบบมากน้อยเพียงใด ซึ่งมีผลการคำนวณดังตารางที่ 4.7 และรูปที่ 4.6

ตารางที่ 4.7 ผลการคำนวณค่ามัธยฐานระยะเวลาที่จุดอ่อนยังคงอยู่ในระบบตามลักษณะความเสียหาย

IMPACT	Median			
	Estimate Median	Standard Error	95% Confidence Interval	
			Lower Bound	Upper Bound
1. Loss of Confidentiality	1302.000	.000	.	.
2. Loss of Integrity	815.000	16.406	782.844	847.156
3. Loss of Availability	750.000	155.987	444.265	1055.735
4. Loss all of C, I and A	724.000	180.446	370.326	1077.674
5. Unknown Impcat	632.000	126.586	383.891	880.109
Overall	810.000	32.010	747.261	872.739



รูปที่ 4.6 ระยะเวลาที่จุดอ่อนยังคงอยู่ในระบบจำแนกตามลักษณะความเสียหาย

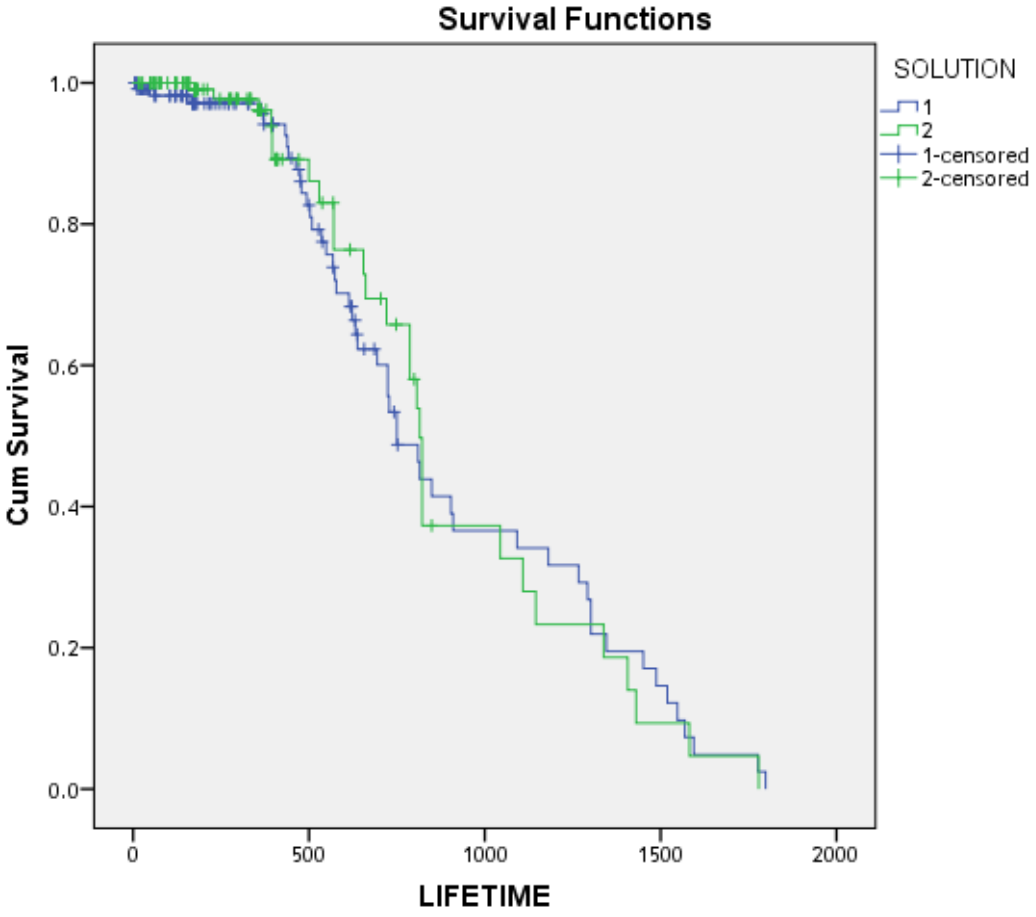
จากตารางที่ 4.7 และ รูปที่ 4.6 พบว่าจุดอ่อนที่ส่งผลให้เสียเป็นความลับจะมีระยะเวลาที่จุดอ่อนยังคงอยู่ในระบบมากที่สุด ในขณะที่จุดอ่อนที่ส่งผลให้เสียทั้งความเป็นความลับ สภาพบูรณภาพและสภาพร้อมใช้งาน จะมีระยะเวลาที่จุดอ่อนยังคงอยู่ในระบบน้อยที่สุด แต่อย่างไรก็ตามจากการทดสอบความแตกต่างของระยะเวลาที่จุดอ่อนยังคงอยู่ในระบบจำแนกตามรูปแบบการโจมตีโดยใช้ Log-rank พบว่า ในจุดอ่อนแต่ละกลุ่มที่ส่งผลกระทบในแต่ละด้านมีระยะเวลาที่จุดอ่อนยังคงอยู่ในระบบไม่แตกต่างกัน (p=0.462)

4.2.6 **จุดอ่อนแบ่งกลุ่มตามสถานะแพทช์**

ในหัวข้อนี้จะแสดงผลการคำนวณค่ามัธยฐานระยะเวลาที่จุดอ่อนยังคงอยู่ในระบบของจุดอ่อนโดยแบ่งกลุ่มตามตามสถานะแพทช์เพื่อนำไปใช้เปรียบเทียบว่าจุดอ่อนที่ได้รับการแพทช์แล้วกับจุดอ่อนที่ยังไม่ได้รับการแพทช์มีระยะเวลาที่จุดอ่อนยังคงอยู่ในระบบในระบบต่างกันมากน้อยเพียงใด ซึ่งมีผลการคำนวณดังตารางที่ 4.8 และรูปที่ 4.7

ตารางที่ 4.8 ผลการคำนวณค่ามัธยฐานระยะเวลาที่จุดอ่อนยังคงอยู่ในระบบตามสถานะแพทช์

SOLUTION	Median			
	Estimate Median	Standard Error	95% Confidence Interval	
			Lower Bound	Upper Bound
1. Patched	750.000	54.368	643.438	856.562
2. Not Patched	815.000	15.868	783.899	846.101
Overall	810.000	32.010	747.261	872.739



รูปที่ 4.7 ระยะเวลาที่จุดอ่อนยังคงอยู่ในระบบจำแนกตามสถานะแพทช์

จากตารางที่ 4.8 และ รูปที่ 4.7 พบว่าจุดอ่อนที่ยังไม่ได้รับการแพทช์มีระยะเวลาที่จุดอ่อนยังคงอยู่ในระบบมากกว่าจุดอ่อนที่ได้รับการแพทช์แล้วเล็กน้อย แต่อย่างไรก็ตามจากการทดสอบความแตกต่างของระยะเวลาที่จุดอ่อนยังคงอยู่ในระบบจำแนกตามรูปแบบการโจมตีโดยใช้ Log-rank พบว่า จุดอ่อนที่ได้รับการแพทช์และยังไม่ได้รับการแพทช์มีระยะเวลาที่จุดอ่อนยังคงอยู่ในระบบไม่แตกต่างกัน ($p=0.888$)

ผลการทดลองจากหัวข้อที่ 4.2.1-4.2.6 สามารถนำมาสรุปเป็นตารางแสดงระยะเวลาที่จุดอ่อนยังคงอยู่ในระบบจำแนกตามกลุ่มได้ดังตารางที่ 4.9

ตารางที่ 4.9 สรุประยะเวลาที่จุดอ่อนยังคงอยู่ในระบบจำแนกตามกลุ่ม

ประเภท	กลุ่ม	ระยะเวลาที่จุดอ่อนยังคงอยู่ในระบบ (วัน)
Severity	Highest	1108
	High	757
	Medium	757
	Low	750
Location	Physical Access	1451
	Remote / Network Access	815
	Local Access	728
	Local and Remote Access	1430
	Context Dependent	395
	Unknown Location	623
Attack Type	Authentication Management	1451
	Input Manipulation	815
	Information Disclosure	1302
	Denial of Service	750
	Unknown Attack Type	728
Impact	Loss of Confidentiality	1302
	Loss of Integrity	815
	Loss of Availability	750
	Loss all C, I and A	724
	Unknown Impact	632
Solution	Patched	750
	Not Patched	815
Total	Overall	810

4.3 การกำหนดวันหมดอายุของจุดอ่อน

จากผลการทดลองในหัวข้อที่ 4.1-4.2 นำไปสู่การกำหนดวันหมดอายุของจุดอ่อนโดยนำจุดอ่อนที่มีสถานะสาบสูญแต่ละตัวมาเปรียบเทียบค่าระยะเวลาที่พบข่าวของจุดอ่อนว่ามีค่ามากกว่าระยะเวลาที่จุดอ่อนยังคงอยู่ในระบบหรือไม่ ถ้าหากมากกว่า จะถือว่าจุดอ่อนนั้นได้หมดอายุลงแล้ว เป็นอันตรายต่อระบบต่ำ ซึ่งมีจุดอ่อนที่ใช้ในการทดลองทั้งหมด 77 ตัวจากจุดอ่อนทั้งหมด 254 ตัว ซึ่งผลการกำหนดวันหมดอายุของจุดอ่อนได้แบ่งออกเป็น 6 กลุ่มดังนี้

4.3.1 การกำหนดวันหมดอายุของจุดอ่อนทั้งหมดแบบไม่แบ่งกลุ่ม

ในหัวข้อนี้จะแสดงผลการกำหนดวันหมดอายุของจุดอ่อนแบบไม่แบ่งกลุ่ม เพื่อดูภาพรวมทั้งหมด ซึ่งมีผลการคำนวณดังตารางที่ 4.10

ตารางที่ 4.10 จุดอ่อนที่หมดอายุทั้งหมดแบบไม่แบ่งกลุ่ม

ระยะเวลาสาบสูญ (วัน)	ระยะเวลาที่ยังคงอยู่ในระบบ (วัน)	จุดอ่อนทั้งหมด (ตัว)	สาบสูญ (ตัว)	หมดอายุ (ตัว)
301.34	810.00	254	177	29

จากตารางที่ 4.10 จุดอ่อนทั้งหมดที่ใช้ในการทดลอง 254 ตัวมีจุดอ่อนสาบสูญ 177 ตัว คิดเป็น 69.68% และ จุดอ่อนที่หมดอายุลงแล้ว 29 ตัวคิดเป็น 11.41% ของจุดอ่อนทั้งหมด หรือ คิดเป็น 16.38% ของจุดอ่อนที่อยู่ในสถานะสาบสูญ ซึ่งแสดงให้เห็นว่าจุดอ่อนที่เกิดขึ้นภายใน Windows XP ส่วนใหญ่ยังคงมีอยู่ในระบบมาก และยังไม่ได้รับการแก้ไขได้อย่างทันท่วงทีเท่าที่ควร ถึงแม้ว่าทางผู้ผลิตจะมีการออกแพทช์เพื่อปรับปรุงแก้ไขช่องโหว่ของจุดอ่อนอย่างสม่ำเสมอแล้วก็ตาม

4.3.2 การกำหนดวันหมดอายุของจุดอ่อนแบ่งกลุ่มตามระดับความรุนแรง

ในหัวข้อนี้จะแสดงผลการกำหนดวันหมดอายุของจุดอ่อนแบ่งกลุ่มตามระดับความรุนแรงเพื่อเปรียบเทียบว่าระดับความรุนแรงของจุดอ่อนส่งผลต่ออายุของจุดอ่อนมากน้อยเพียงใด ซึ่งมีผลการคำนวณดังตารางที่ 4.11

ตารางที่ 4.11 จุดอ่อนที่หมดอายุแบ่งกลุ่มตามระดับความรุนแรง

ระดับความรุนแรง	ระยะเวลาสาบสูญ (วัน)	ระยะเวลาที่ยังคงอยู่ในระบบ (วัน)	จุดอ่อน (ตัว)	สาบสูญ (ตัว)	หมดอายุ (ตัว)	คิดเป็น (%)
Highest	301.34	1108.00	25	22	4	16.00
High		787.00	154	81	21	13.63
Medium		787.00	58	57	6	10.34
Low		750.00	17	17	5	29.41

จากตารางที่ 4.11 จุดอ่อนที่มีระดับความรุนแรงต่ำสุดมีสัดส่วนของจุดอ่อนที่หมดอายุลงแล้วสูงที่สุดถึง 29.41% ของจุดอ่อนในกลุ่ม ในขณะเดียวกันจุดอ่อนที่มีระดับความรุนแรงปานกลางกลับมีสัดส่วนของจุดอ่อนที่หมดอายุลงแล้วต่ำที่สุดที่ 10.34% ของจุดอ่อนในกลุ่ม

4.3.3 การกำหนดวันหมดอายุของจุดอ่อนแบ่งกลุ่มตามตำแหน่งที่เกิด

ในหัวข้อนี้จะแสดงผลการกำหนดวันหมดอายุของจุดอ่อนแบ่งกลุ่มตามตำแหน่งที่เกิดเพื่อเปรียบเทียบจุดอ่อนที่มีตำแหน่งที่เกิดแตกต่างกันนั้นส่งผลต่ออายุของจุดอ่อนมากน้อยเพียงใด ซึ่งมีผลการคำนวณดังตารางที่ 4.12

ตารางที่ 4.12 จุดอ่อนที่หมดอายุแบ่งกลุ่มตามตำแหน่งที่เกิด

ตำแหน่งที่เกิด	ระยะเวลาสาบสูญ (วัน)	ระยะเวลาที่ยังคงอยู่ในระบบ (วัน)	จุดอ่อน (ตัว)	สาบสูญ (ตัว)	หมดอายุ (ตัว)	คิดเป็น (%)
Physical Access	301.34	1451.00	3	3	2	66.67
Remote / Network Access		815.00	108	99	16	14.81
Local Access		728.00	69	43	4	6.34
Local and Remote Access		1430.00	34	6	2	5.88
Context Dependent		395.00	20	7	2	10.00
Unknown Location		623.00	20	19	6	30.00

จากตารางที่ 4.12 จุดอ่อนที่เกิดขึ้นจากส่วนการเข้าถึงเชิงกายภาพมีสัดส่วนของจุดอ่อนที่หมดอายุลงแล้วสูงที่สุดถึง 66.67% ของจุดอ่อนในกลุ่ม ในขณะเดียวกันจุดอ่อนที่เกิดขึ้นจากส่วนการเข้าถึงระดับท้องถิ่นและระยะไกลมีสัดส่วนของจุดอ่อนที่หมดอายุลงแล้วต่ำที่สุดที่ 5.88% ของจุดอ่อนในกลุ่ม แสดงให้เห็นว่าจุดอ่อนที่เกิดขึ้นจากส่วนการเข้าถึงเชิงกายภาพจะมีการเฝ้าระวังและรีบติดตามแก้ไขจุดอ่อนมากเป็นพิเศษกว่าจุดอ่อนกลุ่มอื่นๆ

4.3.4 การกำหนดวันหมดอายุของจุดอ่อนแบ่งกลุ่มตามรูปแบบการโจมตี

ในหัวข้อนี้จะแสดงผลการกำหนดวันหมดอายุของจุดอ่อนแบ่งกลุ่มตามรูปแบบการโมตีเพื่อเปรียบเทียบจุดอ่อนที่มีรูปแบบการโจมตีที่แตกต่างกันนั้นส่งผลต่ออายุของจุดอ่อนมากน้อยเพียงใด ซึ่งมีผลการคำนวณดังตารางที่ 4.13

ตารางที่ 4.13 จุดอ่อนที่หมดอายุแบ่งกลุ่มตามรูปแบบการโจมตี

รูปแบบการโจมตี	ระยะเวลาสาบสูญ (วัน)	ระยะเวลาที่ยังคงอยู่ในระบบ (วัน)	จุดอ่อน (ตัว)	สาบสูญ (ตัว)	หมดอายุ (ตัว)	คิดเป็น (%)
Authentication Management	301.34	1451.00	4	1	1	25.00
Input Manipulation		815.00	197	120	25	12.69
Information Disclosure		1302.00	7	2	1	14.28
Denial of Service		750.00	27	26	3	11.11
Unknown Attack Type		728.00	19	17	4	21.05

จากตารางที่ 4.13 จุดอ่อนที่มีการโจมตีการจัดการพิสูจน์ตัวจริงมีสัดส่วนของจุดอ่อนที่หมดอายุลงแล้วสูงที่สุดถึง 25.00% ของจุดอ่อนในกลุ่ม ในขณะเดียวกันจุดอ่อนที่มีการโจมตีการขัดขวางการให้บริการมีสัดส่วนของจุดอ่อนที่หมดอายุลงแล้วต่ำที่สุดที่ 11.11% ของจุดอ่อนในกลุ่ม แสดงให้เห็นว่าจุดอ่อนที่มีการโจมตีการจัดการพิสูจน์ตัวจริงจะมีการเฝ้าระวังและรีบติดตามแก้ไขจุดอ่อนมากเป็นพิเศษกว่าจุดอ่อนกลุ่มอื่นๆ

4.3.5 การกำหนดวันหมดอายุของจุดอ่อนแบ่งกลุ่มตามลักษณะความเสียหาย

ในหัวข้อนี้จะแสดงผลการกำหนดวันหมดอายุของจุดอ่อนแบ่งกลุ่มตามลักษณะความเสียหาย เพื่อเปรียบเทียบจุดอ่อนที่มีลักษณะความเสียหายที่แตกต่างกันนั้นส่งผลต่ออายุของจุดอ่อนมากน้อยเพียงใด ซึ่งมีผลการคำนวณดังตารางที่ 4.14

ตารางที่ 4.14 จุดอ่อนที่หมดอายุแบ่งกลุ่มตามลักษณะความเสียหาย

ลักษณะความเสียหาย	ระยะเวลาสาบสูญ (วัน)	ระยะเวลาที่ยังคงอยู่ในระบบ (วัน)	จุดอ่อน (ตัว)	สาบสูญ (ตัว)	หมดอายุ (ตัว)	คิดเป็น (%)
Loss of Confidentiality	301.34	1302.00	7	7	0	0
Loss of Integrity		815.00	208	131	6	2.88
Loss of Availability		750.00	28	28	3	10.71
Loss all of C, I and A		724.00	3	3	1	33.33
Unknown Impact		632.00	8	8	1	12.50

จากตารางที่ 4.14 จุดอ่อนที่ก่อให้เกิดทั้งการเสียความเป็นความลับ เสียสภาพบูรณภาพและสภาพพร้อมใช้งาน มีสัดส่วนของจุดอ่อนที่หมดอายุลงแล้วสูงที่สุดถึง 33.33% ของจุดอ่อนในกลุ่ม ในขณะเดียวกันจุดอ่อนที่ก่อให้เกิดการเสียความเป็นความลับมีสัดส่วนของจุดอ่อนที่หมดอายุลงแล้วต่ำที่สุดที่ 0% ของจุดอ่อนในกลุ่ม แสดงให้เห็นว่าจุดอ่อนที่ก่อให้เกิดทั้งการเสียความเป็นความลับ เสียสภาพบูรณภาพและสภาพพร้อมใช้งาน จะมีการเฝ้าระวังและรีบติดตามแก้ไขจุดอ่อนมากเป็นพิเศษกว่าจุดอ่อนกลุ่มอื่นๆ

4.3.6 การกำหนดวันหมดอายุของจุดอ่อนแบ่งกลุ่มตามสถานะแพทช์

ในหัวข้อนี้จะแสดงผลการกำหนดวันหมดอายุของจุดอ่อนแบ่งกลุ่มตามสถานะแพทช์เพื่อเปรียบเทียบจุดอ่อนที่ได้รับการแพทช์และยังไม่ได้รับการแพทช์ว่าส่งผลต่ออายุของจุดอ่อนมากน้อยเพียงใด ซึ่งมีผลการคำนวณดังตารางที่ 4.15

ตารางที่ 4.15 จุดอ่อนที่หมดอายุแบ่งกลุ่มตามสถานะแพทช์

สถานะ	ระยะเวลาสาบสูญ (วัน)	ระยะเวลาที่ยังคงอยู่ในระบบ (วัน)	จุดอ่อน (ตัว)	สาบสูญ (ตัว)	หมดอายุ (ตัว)	คิดเป็น (%)
Patched	301.34	750.00	119	113	23	19.32
Not Patched		815.00	135	64	9	6.67

จากตารางที่ 4.15 สังเกตได้ว่าจุดอ่อนที่ได้รับการแพทช์แล้วจะมีสัดส่วนของจุดอ่อนที่หมดอายุลงคิดเป็น 19.32% ซึ่งมากกว่าสัดส่วนของจุดอ่อนที่ยังไม่ได้รับการแพทช์อย่างเห็นได้ชัดเจน ซึ่งมีสัดส่วนของจุดอ่อนที่หมดอายุลงแล้วคิดเป็น 6.67% ซึ่งตรงตามหลักการของ [4] [19] คือ จุดอ่อนที่ได้รับการแพทช์แล้วจะเข้าสู่สถานะหมดอายุหรือตายในที่สุด

บทที่ 5

สรุปผลการวิจัยและข้อเสนอแนะ

จากการดำเนินงานวิจัยตั้งแต่การเก็บข้อมูลข่าวจนกระทั่งการวิเคราะห์วันหมดอายุของจุดอ่อนในแบบต่างๆ ทำให้สามารถระบุได้ว่า จุดอ่อนแต่ละตัวที่เกิดขึ้นมานั้นปัจจุบันยังคงมีนัยสำคัญต่อระบบมากน้อยเพียงใด ทำให้สามารถสรุปผลการวิจัย และเสนอแนะแนวทางต่างๆ เพื่อการทำวิจัยในอนาคตต่อไปได้ดังนี้

5.1 สรุปผลการวิจัย

ในปัจจุบันสาเหตุสำคัญที่ทำให้มีการศึกษาค้นคว้าเพื่อหาแนวทางในการวิเคราะห์และการกำหนดวันหมดอายุของจุดอ่อนสืบเนื่องมาจาก การที่ไม่สามารถระบุได้อย่างแน่ชัดว่า หลังจากสถานะแพทช์ของจุดอ่อนแล้วนั้น จุดอ่อนจะมีนัยสำคัญต่อระบบมากเพียงใด หมดอายุลงเมื่อใด หรือไม่เป็นอันตรายต่อระบบอีกต่อไป ทำให้มีการออกสำรวจข้อมูลจุดอ่อนของซอฟต์แวร์ระบบซึ่งงานวิจัยนี้ได้นำเสนอการกำหนดวันหมดอายุของจุดอ่อนที่เกิดขึ้นในระบบปฏิบัติการ Windows XP โดยอาศัยข้อมูลข่าวการโจมตีจากสื่อออนไลน์สาธารณะ ฐานข้อมูลซีวีอี และ ฐานข้อมูลโอเอสวีดีบี โดยใช้ข้อมูลวันที่ของข่าวเป็นข้อมูลนำเข้า และมีผลลัพธ์ที่ได้คือ ระยะห่างของข่าวที่เกิดขึ้น สามารถนำไปวิเคราะห์ระยะเวลาสาบสูญของจุดอ่อนโดยอาศัยทฤษฎีช่วงความเชื่อมั่น และ ข้อมูลระยะเวลาที่จุดอ่อนยังคงอยู่ในระบบ สามารถนำไปใช้ในการกำหนดวันหมดอายุของจุดอ่อนโดยอาศัยหลักในการวิเคราะห์ระยะเวลาที่จุดอ่อนยังคงอยู่ในระบบ (Survival analysis) โดยมีผลสรุปดังต่อไปนี้

จากจุดอ่อนที่ใช้ในการทดลองทั้งหมด 254 ตัว อยู่ในสถานะสาบสูญ 177 ตัว คิดเป็น 69.68% ของจุดอ่อนทั้งหมด และมีจุดอ่อนที่หมดอายุแล้ว 29 ตัว คิดเป็น 11.41% ของจุดอ่อนทั้งหมด หรือ 16.38% ของจุดอ่อนที่อยู่ในสถานะสาบสูญ

นอกจากนี้ยังมีการนำจุดอ่อนมาแยกวิเคราะห์ตามประเภท โดยแบ่งออกเป็น 5 กลุ่มได้ดังนี้

1. จุดอ่อนแบ่งกลุ่มตามระดับความรุนแรง มีสัดส่วนของจุดอ่อนที่หมดอายุแล้วสูงสุดคือ จุดอ่อนที่มีระดับความรุนแรงต่ำ มีสัดส่วนอยู่ที่ 29.41% ของจุดอ่อนในกลุ่ม และต่ำสุดคือ จุดอ่อนที่มีระดับความรุนแรงปานกลางมีสัดส่วนอยู่ที่ 10.34% ของจุดอ่อนในกลุ่ม
2. จุดอ่อนแบ่งกลุ่มตามตำแหน่งที่เกิด มีสัดส่วนของจุดอ่อนที่หมดอายุแล้วสูงสุดคือ จุดอ่อนที่เกิดขึ้นในส่วนของการเข้าถึงเชิงกายภาพ มีสัดส่วนอยู่ที่ 66.67% ของจุดอ่อนในกลุ่ม และต่ำสุดคือ จุดอ่อนที่เกิดขึ้นจากส่วนการเข้าถึงระดับท้องถิ่นและระยะไกลมีสัดส่วนอยู่ที่ 5.88% ของจุดอ่อนในกลุ่ม

3. จุดอ่อนแบ่งกลุ่มตามประเภทของการโจมตี มีสัดส่วนของจุดอ่อนที่หมดอายุแล้วสูงสุดคือ จุดอ่อนที่โจมตีการจัดการพิสูจน์ตัวจริง มีสัดส่วนอยู่ที่ 25% ของจุดอ่อนในกลุ่ม และต่ำสุดคือ จุดอ่อนที่โจมตีการการขัดขวางการให้บริการ มีสัดส่วนอยู่ที่ 11.11% ของจุดอ่อนในกลุ่ม

4. จุดอ่อนแบ่งกลุ่มตามลักษณะความเสียหาย มีสัดส่วนของจุดอ่อนที่หมดอายุแล้วสูงสุดคือ จุดอ่อนที่ก่อให้เกิดทั้งการเสียความเป็นความลับ เสียสภาพบูรณภาพและสภาพพร้อมใช้งาน มีสัดส่วนอยู่ที่ 33.33% ของจุดอ่อนในกลุ่ม และต่ำสุดคือ จุดอ่อนที่ก่อให้เกิดการเสียความเป็นความลับ มีสัดส่วนอยู่ที่ 0% ของจุดอ่อนในกลุ่ม

5. จุดอ่อนแบ่งกลุ่มตามสถานะแพทช์ มีสัดส่วนของจุดอ่อนที่หมดอายุแล้วสูงสุดคือ จุดอ่อนที่ได้รับการแพทช์แล้ว มีสัดส่วนอยู่ที่ 19.32% ของจุดอ่อนในกลุ่ม และต่ำสุดคือ จุดอ่อนที่ยังไม่ได้รับการแพทช์ มีสัดส่วนอยู่ที่ 6.67% ของจุดอ่อนในกลุ่ม

5.2 ปัญหาที่พบจากการวิจัย

ระหว่างการดำเนินงานวิจัยได้พบปัญหา อุปสรรคและข้อจำกัดต่างๆ ระหว่างการทำวิจัย ดังนี้

เนื่องด้วยข้อมูลนำเข้าที่ใช้ในงานวิจัยนี้เป็นข้อมูลจากสื่อออนไลน์สาธารณะ ดังนั้นในช่วงแรกของการดำเนินงานวิจัยการคัดกรองข้อมูลจึงเป็นไปด้วยความยากลำบากและเสียเวลามากเพราะต้องทำด้วยมือ และอาจมีความคลาดเคลื่อนของข้อมูลที่ได้อยู่บ้าง แต่ในช่วงหลังผู้วิจัยได้จัดตั้งทีมผู้ช่วยวิจัยขึ้นมาช่วยรวบรวมข้อมูลทำให้ย่นระยะเวลาไปได้มาก

นอกจากนี้ยังพบปัญหาปริมาณข้อมูลลักษณะเฉพาะบางอย่างของจุดอ่อนมีไม่เพียงพอต่อการนำไปวิเคราะห์ข้อมูลได้แก่ รายละเอียดการ Exploit ของจุดอ่อน ซึ่งทำให้การวิเคราะห์แบบเชิงกลุ่มไม่ได้ลงไปวิเคราะห์ข้อมูลในแบบดังกล่าว

5.3 ข้อเสนอแนะ

ถ้าหากมีการนำขั้นตอนวิจัยไปประยุกต์ใช้ในการตรวจสอบวันหมดอายุของจุดอ่อนในซอฟต์แวร์ตัวอื่น และในซอฟต์แวร์ดังกล่าวนั้นมีปริมาณจุดอ่อนเป็นจำนวนมาก เพื่อให้การวิเคราะห์ดำเนินไปด้วยความรวดเร็วก่อนที่ซอฟต์แวร์ดังกล่าวจะเก่าเกินไปและทำให้งานวิจัยดูไม่น่าสนใจ ควรจัดตั้งทีมผู้ช่วยวิจัยในการรวบรวมและประมวลผลข้อมูลให้เสร็จภายใน 1 เดือน และไม่ควรให้ภาระงานของแต่ละคนในทีมหนักจนเกินไป เนื่องจากข้อมูลมีความละเอียดอ่อนและง่ายต่อการผิดพลาด

ข้อมูลจากสื่อออนไลน์สาธารณะบางส่วนเป็นแหล่งข้อมูลในลักษณะของข้อมูลที่ไม่เป็นทางการจึงมีอาจมีความคลาดเคลื่อนและมีความน่าเชื่อถือได้ในระดับหนึ่งเท่านั้น ทำให้ผลการทดลองที่ได้นั้นเป็นเพียงการคาดเดาสถานะของจุดอ่อนที่มีความน่าเชื่อถือได้ดีในระดับหนึ่ง ผู้ที่นำไปประยุกต์ใช้ควรหาแหล่ง

อ้างอิงของข้อมูลอื่นๆ ประกอบการตัดสินใจเพิ่มเติมว่าจุดอ่อนที่ท่านให้ความสนใจอยู่นั้น ควรอยู่ในสถานะใดและควรที่จะเฝ้าระวังมากน้อยเพียงใด

5.4 งานวิจัยในอนาคต

จากงานวิจัยนี้ยังมีประเด็นที่สามารถนำไปทำวิจัยต่อได้อีกดังนี้

1. การกำหนดวันหมดอายุของจุดอ่อนในซอฟต์แวร์ตัวอื่นๆ เช่น Linux, Internet Browser, Windows เวอร์ชั่นอื่นๆ และทำการเปรียบเทียบผลที่ได้ร่วมกัน

2. การคิดค้นวิธีใหม่ๆ ในการกำหนดวันหมดอายุของจุดอ่อน พร้อมทั้งเปรียบเทียบและประเมินประสิทธิภาพที่ได้กับวิธีดั้งเดิม

รายการอ้างอิง

[1] CVE, Common Vulnerabilies and Exposures [Online]. Available from: http://cve.mitre.org [2012, June 7]

[2] OSVDB, Open Source Vulnerability Database [Online]. Available from: http://osvdb.org [2012, June 7]

[3] วีระศักดิ์ จงสู่วิวัฒน์วงศ์. (2550). กราฟ ตาราง และสมการสำหรับการวิจัยทางสุขภาพ. พิมพ์ครั้งที่ 1. กรุงเทพฯ : สำนักพิมพ์แห่งจุฬาลงกรณ์มหาวิทยาลัย.

[4] William A. Arbaugh, William L. Fithen, and John McHugh. Windows of Vulnerability: A Case Study Analysis. Computer 33, 12 (December 2000), 52-59.

[5] Amontip Jumratjaroenvanit and Yunyong Teng-amnuay. 2008. Probability of Attack Based on System Vulnerability Life Cycle. In Proceedings of the 2008 International Symposium on Electronic Commerce and Security (ISECS '08). IEEE Computer Society, Washington, DC, USA, 531-535.

[6] Wilhelm, Douglas. Professional Penetration Testing. Syngress Press : 503.

[7] Andress, Mandy; Cox, Phil; Tittel, Ed. CIW Security Professional. New York, NY: Hungry Minds, Inc.. p. 10.

[8] CERT, Computer Emergency Response Team [Online]. Available from: http://www.cert.org, [2011,Jan 25]

[9] Bugtraq mailing list [Online]. Available from: http://seclists.org/bugtraq/ [2011,Jan 25]

[10] Secunia [Online]. Available from: http://secunia.com [2010,Jan 7]

[11] redhat.com | The World's Open Source Leader [Online]. Available from: http://www.redhat.com [2011,Jan 25]

[12] Debian -- The Universal Operating System [Online]. Available from: http://www.debian.org [2011,Jan 25]

[13] Oracle and Sun [Online]. Available from: http://www.oracle.com/us/sun/index.html [2011,Jan 25]

[14] CVE - How We Build the CVE List [Online]. Available from: http://cve.mitre.org/cve/identifiers/build.html [2011,Jan 25]

[15] ภาควิชาสถิติ. (2549). หลักสถิติ 1. พิมพ์ครั้งที่ 4. กรุงเทพฯ : สำนักส่งเสริมและฝึกอบรม มก.

[16] Date format by country [Online]. Available from: http://en.wikipedia.org/wiki/Date_format_by_country [2012,July 25]

[17] Jeffrey R. Jones. 2007. Estimating Software Vulnerabilities. IEEE Security and Privacy 5, 4 (July 2007) : 28-32.

[18] Ratsameetip Wita and Yunyong Teng-Amnuay. 2005. Vulnerability Profile for Linux. In Proceedings of the 19th International Conference on Advanced Information Networking and Applications - Volume 1 (AINA '05), Vol. 1. IEEE Computer Society, Washington, DC, USA, 953-958.

[19] Ashish Arora and Rahul Telang. 2005. Economics of Software Vulnerability Disclosure. IEEE Security and Privacy 3, 1 (January 2005) : 20-25.

[20] Wita, R.; Jiamnapanon, N.; Teng-amnuay, Y.; , "An Ontology for Vulnerability Lifecycle," Intelligent Information Technology and Security Informatics (IITSI), 2010 Third International Symposium on , vol., no., pp.553-557, 2-4 April 2010

[21] CVSS, Common Vulnerability Scoring System [Online]. Available from: http://www.first.org/cvss [2012,June 7]

ภาคผนวก

ภาคผนวก ก

รายละเอียดของจุดอ่อนที่พบบนระบบปฏิบัติการ Windows XP ที่คัดกรองมาจากรายการซีวีอี

ในส่วนนี้จะแสดงรายการของจุดอ่อนที่พบบนระบบปฏิบัติการ Windows XP ที่คัดกรองมาจากรายการซีวีอีที่ใช้ในงานวิจัยนี้ จำนวนทั้งสิ้น 258 ตัว โดยแสดงรายละเอียดของแต่ละประเภทไว้ในตารางที่ ก.1 และข้อมูลรายละเอียดของจุดอ่อนในตารางที่ ก.2 ดังนี้

CVE Name	หมายเลขอ้างอิงจากรายการซีวีอี
Severity	ระดับความรุนแรงของจุดอ่อน
Location	ตำแหน่งที่เกิดจุดอ่อน
Attack Type	รูปแบบการโจมตี
Impact	ผลกระทบที่เกิดขึ้น
Solution	สถานะแพทช์ของจุดอ่อน

ตารางที่ ก.1 ประเภทของรายละเอียดของจุดอ่อน

Value	Severity	Location	Attack Type	Impact	Solution
0	Highest	Physical Access Required	Authentication Management	Loss of Confidentiality	No
1	High	Remote / Network Access	Input Manipulation	Loss of Integrity	Yes
2	Medium	Local Access Required	Information Disclosure	Loss of Availability	
3	Low	Local Access / Remote	Denial of Service	Loss of C.I.A.	
4		Context Dependent	Unknown Attack Type	Unknown Impact	
5		Unknown Location			

ในตารางที่ ก.2 มีการย่อคอลัมน์ของตารางโดยมีการแทนเป็นสัญลักษณ์ตัวอักษรเดียว คือ Severity แทนด้วย Se, Location แทนด้วย L, Attack Type แทนด้วย A, Impact แทนด้วย M และ Solution แทนด้วย So

ตารางที่ ก.2 รายละเอียดของจุดอ่อนที่พบบนระบบปฏิบัติการ Windows XP ที่คัดกรองมาจากรายการซีวีอี

CVE Name	Se	L	A	I	So
CVE-2004-0214	0	2	1	1	0
CVE-2004-0420	0	1	1	3	0
CVE-2004-0571	0	1	1	1	0
CVE-2004-0572	0	2	1	1	0
CVE-2004-0574	0	1	1	1	1
CVE-2004-0575	0	1	1	1	1
CVE-2004-0840	0	1	1	1	1
CVE-2004-0897	0	1	1	1	0
CVE-2004-0901	0	1	1	1	0
CVE-2004-0985	0	1	1	1	0
CVE-2004-2289	0	2	1	1	0
CVE-2005-0059	0	1	1	1	1
CVE-2005-0551	0	2	1	1	0
CVE-2005-1983	0	3	1	1	1
CVE-2005-3595	0	0	0	1	0
CVE-2006-2372	0	1	1	1	0
CVE-2006-2373	0	2	1	1	0
CVE-2006-3439	0	1	1	1	1
CVE-2008-4250	0	1	1	1	1
CVE-2010-0269	0	1	1	1	1
CVE-2010-2550	0	1	1	1	1
CVE-2010-2568	0	3	1	1	1
CVE-2010-3970	0	3	1	1	0
CVE-2011-0654	0	1	1	1	1
CVE-2011-0661	0	1	1	1	1
CVE-2001-0719	1	1	1	1	0

CVE Name	Se	L	A	I	So
CVE-2010-3222	1	2	1	1	1
CVE-2010-3227	1	3	1	1	1
CVE-2010-3230	1	3	1	1	1
CVE-2010-3231	1	3	1	1	1
CVE-2010-3232	1	3	1	1	1
CVE-2010-3233	1	3	1	1	1
CVE-2010-3234	1	3	1	1	1
CVE-2010-3235	1	3	1	1	1
CVE-2010-3236	1	3	1	1	1
CVE-2010-3237	1	3	1	1	1
CVE-2010-3239	1	3	1	1	1
CVE-2010-3240	1	3	1	1	1
CVE-2010-3241	1	3	1	1	1
CVE-2010-3242	1	3	1	1	1
CVE-2010-3974	1	3	1	1	1
CVE-2011-0028	1	3	1	1	1
CVE-2011-0032	1	3	1	1	1
CVE-2011-0034	1	3	1	1	1
CVE-2011-0039	1	2	1	1	1
CVE-2011-0041	1	3	1	1	0
CVE-2011-0042	1	3	1	1	1
CVE-2011-0660	1	1	1	1	1
CVE-2011-0662	1	2	1	1	1
CVE-2011-0665	1	2	1	1	1
CVE-2011-0666	1	2	1	1	1
CVE-2011-0667	1	2	1	1	1

CVE Name	Se	L	A	I	So
CVE-2001-0876	1	1	1	1	0
CVE-2001-0909	1	5	1	1	0
CVE-2001-1200	1	0	1	3	0
CVE-2002-1327	1	5	1	1	0
CVE-2003-0003	1	1	1	1	0
CVE-2003-0004	1	5	1	1	0
CVE-2003-0109	1	1	1	1	1
CVE-2003-0306	1	5	1	1	0
CVE-2003-0533	1	1	1	1	1
CVE-2003-0806	1	1	1	1	0
CVE-2003-0906	1	1	1	1	0
CVE-2003-0909	1	2	0	1	0
CVE-2003-1027	1	1	1	1	0
CVE-2004-0117	1	1	1	1	0
CVE-2004-0119	1	1	1	1	0
CVE-2004-0197	1	1	1	3	0
CVE-2004-0206	1	1	1	1	1
CVE-2004-0208	1	2	0	1	0
CVE-2004-0893	1	2	1	1	0
CVE-2004-1173	1	1	4	1	0
CVE-2004-2290	1	5	4	1	0
CVE-2004-2339	1	2	1	1	0
CVE-2005-0044	1	1	1	1	0
CVE-2005-0045	1	1	1	1	0
CVE-2005-0047	1	2	4	1	0
CVE-2005-0048	1	1	1	1	0
CVE-2005-0051	1	1	2	0	0

CVE Name	Se	L	A	I	So
CVE-2011-0670	1	2	1	1	1
CVE-2011-0671	1	2	1	1	1
CVE-2011-0672	1	2	1	1	1
CVE-2011-0673	1	4	1	1	1
CVE-2011-0674	1	4	1	1	1
CVE-2011-0675	1	4	1	1	0
CVE-2011-0676	1	4	1	1	0
CVE-2011-0677	1	4	1	1	0
CVE-2011-1225	1	2	1	1	1
CVE-2011-1226	1	2	1	1	1
CVE-2011-1227	1	2	1	1	1
CVE-2011-1228	1	2	1	1	1
CVE-2011-1229	1	2	1	1	1
CVE-2011-1230	1	2	1	1	1
CVE-2011-1231	1	2	1	1	1
CVE-2011-1232	1	2	1	1	1
CVE-2011-1233	1	4	1	1	1
CVE-2011-1234	1	4	1	1	1
CVE-2011-1235	1	4	1	1	1
CVE-2011-1236	1	4	1	1	1
CVE-2011-1237	1	4	1	1	1
CVE-2011-1238	1	4	1	1	1
CVE-2011-1239	1	2	1	1	1
CVE-2011-1240	1	2	1	1	1
CVE-2011-1241	1	2	1	1	1
CVE-2011-1242	1	2	1	1	1
CVE-2010-1891	2	2	1	1	1

CVE Name	Se	L	A	I	So
CVE-2005-0053	1	1	1	1	0
CVE-2005-0055	1	1	1	1	0
CVE-2005-0057	1	1	1	1	0
CVE-2005-0058	1	3	1	1	1
CVE-2005-0060	1	2	1	1	0
CVE-2005-0061	1	2	4	1	0
CVE-2005-0063	1	1	1	1	0
CVE-2005-0554	1	1	1	1	0
CVE-2005-1206	1	1	1	1	1
CVE-2005-1207	1	3	1	1	0
CVE-2005-1984	1	1	1	1	0
CVE-2005-1989	1	1	4	1	0
CVE-2005-2123	1	1	1	1	0
CVE-2005-2124	1	1	1	1	1
CVE-2005-4560	1	3	1	1	1
CVE-2006-0025	1	1	1	1	1
CVE-2006-1303	1	1	1	1	0
CVE-2006-1314	1	1	1	1	1
CVE-2006-2370	1	1	1	1	1
CVE-2006-2371	1	1	1	1	1
CVE-2006-2379	1	1	1	1	0
CVE-2006-3086	1	1	1	1	0
CVE-2006-3209	1	2	4	4	1
CVE-2006-3942	1	1	3	2	0
CVE-2006-4688	1	1	1	1	1
CVE-2007-0025	1	3	1	1	1
CVE-2007-0069	1	1	1	1	1

CVE Name	Se	L	A	I	So
CVE-2010-1888	2	2	1	1	1
CVE-2010-1887	2	2	1	1	1
CVE-2010-1894	2	2	1	1	1
CVE-2010-1895	2	2	1	1	1
CVE-2010-1896	2	2	1	1	0
CVE-2010-1897	2	2	1	1	1
CVE-2010-1886	2	2	2	0	0
CVE-2010-2265	2	1	1	1	1
CVE-2010-0484	2	2	1	1	1
CVE-2010-0485	2	2	1	1	1
CVE-2010-1255	2	2	1	1	1
CVE-2009-2653	2	2	1	1	0
CVE-2007-1204	2	1	1	1	0
CVE-2006-6579	2	5	4	4	0
CVE-2006-1315	2	1	2	0	1
CVE-2006-0026	2	1	1	1	1
CVE-2006-1313	2	1	1	1	0
CVE-2006-1184	2	1	3	2	1
CVE-2006-2297	2	1	1	1	0
CVE-2006-0012	2	1	1	1	1
CVE-2005-0803	2	1	3	2	0
CVE-2005-2120	2	2	1	1	0
CVE-2005-1218	2	1	3	2	0
CVE-2005-2303	2	1	3	2	0
CVE-2005-1988	2	1	1	1	0
CVE-2005-2308	2	1	1	1	0
CVE-2005-1990	2	1	1	1	1

CVE Name	Se	L	A	I	So
CVE-2007-0210	1	2	1	1	1
CVE-2007-0211	1	2	4	1	1
CVE-2007-0214	1	4	1	1	1
CVE-2007-0942	1	1	1	1	1
CVE-2007-1492	1	5	3	2	0
CVE-2007-3039	1	1	1	1	1
CVE-2007-5348	1	1	1	1	1
CVE-2008-0015	1	4	1	1	1
CVE-2008-0083	1	4	1	1	1
CVE-2008-0322	1	2	1	1	1
CVE-2008-1083	1	4	1	1	1
CVE-2008-1087	1	4	1	1	1
CVE-2008-1453	1	1	1	1	1
CVE-2008-2253	1	4	1	1	1
CVE-2008-3008	1	4	1	1	1
CVE-2008-3464	1	2	1	1	1
CVE-2008-2010	1	1	1	1	0
CVE-2009-0081	1	1	1	1	1
CVE-2009-0082	1	2	1	1	1
CVE-2009-0083	1	2	4	1	1
CVE-2009-0085	1	1	1	1	1
CVE-2009-1511	1	1	3	2	0
CVE-2009-3548	1	5	0	1	1
CVE-2010-0483	1	4	1	1	1
CVE-2010-0818	1	3	1	1	1
CVE-2010-0819	1	2	1	1	1
CVE-2010-0820	1	1	1	1	1

CVE Name	Se	L	A	I	So
CVE-2005-2307	2	1	3	2	0
CVE-2005-1211	2	1	1	1	0
CVE-2005-1433	2	1	3	2	0
CVE-2005-0553	2	1	1	1	1
CVE-2005-0054	2	1	1	1	0
CVE-2005-0056	2	1	1	1	0
CVE-2004-1049	2	2	1	1	1
CVE-2004-1305	2	2	3	2	0
CVE-2004-1319	2	1	1	1	0
CVE-2005-1792	2	5	4	4	0
CVE-2004-1623	2	1	1	1	0
CVE-2004-2176	2	5	4	4	0
CVE-2003-0718	2	1	3	2	0
CVE-2004-0839	2	1	1	1	0
CVE-2004-2527	2	0	3	2	0
CVE-2004-0199	2	1	1	1	0
CVE-2003-0907	2	5	4	4	0
CVE-2004-0120	2	1	3	2	0
CVE-2004-0474	2	1	1	1	0
CVE-2003-0897	2	5	4	1	0
CVE-2003-0813	2	1	3	2	0
CVE-2003-0505	2	1	1	1	0
CVE-2002-1230	2	2	1	1	0
CVE-2002-0864	2	5	3	2	0
CVE-2002-0974	2	1	1	2	0
CVE-2002-2117	2	5	3	2	0
CVE-2002-0283	2	5	3	2	0

CVE Name	Se	L	A	I	So
CVE-2010-1175	1	5	4	4	0
CVE-2010-1882	1	4	1	1	1
CVE-2010-1883	1	3	1	1	1
CVE-2010-1885	1	3	1	1	1
CVE-2010-2551	1	1	3	2	1
CVE-2010-2552	1	1	3	2	1
CVE-2010-2553	1	1	1	1	1
CVE-2010-2563	1	3	1	1	1
CVE-2010-2564	1	1	1	1	1
CVE-2010-2566	1	1	1	1	1
CVE-2010-2567	1	1	1	1	1
CVE-2010-2738	1	3	1	1	1
CVE-2010-2739	1	2	1	1	0
CVE-2010-2740	1	1	1	1	1
CVE-2010-2741	1	1	1	1	1
CVE-2010-2743	1	2	1	1	1
CVE-2010-2744	1	2	1	1	1
CVE-2010-2746	1	3	1	1	1
CVE-2010-3140	1	3	4	1	0
CVE-2010-3144	1	3	1	1	1

CVE Name	Se	L	A	I	So
CVE-2002-1670	2	5	4	4	0
CVE-2001-1571	2	1	2	0	0
CVE-2001-0877	2	1	3	2	0
CVE-2007-3724	3	5	3	2	0
CVE-2007-1537	3	2	3	2	0
CVE-2006-2374	3	1	3	2	0
CVE-2006-2334	3	2	1	1	0
CVE-2005-4697	3	2	2	0	0
CVE-2005-4696	3	2	2	0	0
CVE-2005-2765	3	2	1	1	0
CVE-2005-1982	3	1	2	0	0
CVE-2005-0550	3	2	3	2	0
CVE-2005-0555	3	1	1	1	1
CVE-2005-0904	3	1	3	2	0
CVE-2005-0852	3	2	3	2	0
CVE-2004-1331	3	1	1	1	0
CVE-2004-0207	3	2	4	1	0
CVE-2002-2324	3	2	4	1	1
CVE-2002-2105	3	5	3	2	0
CVE-2001-1570	3	5	4	4	0

ประวัติผู้เขียนวิทยานิพนธ์

นาย ปุณธวัช ว่องธวัชชัย เกิดเมื่อวันที่ 7 มกราคม 2528 ที่จังหวัดกรุงเทพมหานคร สำเร็จการศึกษาปริญญาตรี วิทยาศาสตร์บัณฑิต จากภาควิชาวิทยาการคอมพิวเตอร์ คณะวิทยาศาสตร์ มหาวิทยาลัยเกษตรศาสตร์ ในปีการศึกษา 2551 และเข้าศึกษาต่อในหลักสูตร วิทยาศาสตร์มหาบัณฑิต ที่ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย เมื่อ พ.ศ.2552