PRINCE OF SONGKLA UNIVERSITY
FACULTY OF ENGINEERING

Midterm Examination: Semester 1 **Academic Year**: 2013

Date: 28 July 2013 **Time**: 13.30-15.30 (2 hours)

Subject Number: 242-500 **Room**: R201

Subject Title: Research and Development Methodologies

Exam Duration: 3 hours (180 minutes)

This paper has 15 pages (including a 4-page article), 9 questions 150 marks (25%).

Authorised Materials:

- Writing instruments (e.g. pens, pencils).
- Textbooks, a notebook, handouts, and dictionaries are permitted.

Instructions to Students:

- Scan all the questions before answering so that you can manage your time better.
- Write your answers in Thai only.
- Write your name and ID on every page.
- Any unreadable parts will be considered wrong.

Cheating in this examination

Lowest punishment: Failed in this subject and courses dropped for next semester.

Highest punishment: Expelled.

NO	Time (Min)	Marks	Collected	NO	Time (Min)	Marks	Collected
1		20		6		8	
2		20		7		7	
3		43		8		5	
4		7		9		8	
5		32		Raw		25%	
Total	120	150	Percentage				

Question 1 **(20 marks)**

From the attached paper, seek for the following items.

a) Motivation/Problem Statements (5 marks)

.....

.....

.....

.....

.....

b) Contribution (5 marks)

.....

.....

.....

.....

.....

c) Objectives (5 marks)

.....

.....

.....

.....

.....

d) Scopes (5 marks)

.....

.....

.....

.....

.....

Question 2 **(20 marks)**

Tell whether the following statements are right (T) or wrong (F).

_____a) An article in conference proceedings may present on-going research with some results.

_____b) An article in a journal must present a complete research.

_____c) Basic research is also called fundamental or pure research. It is exploratory and often driven by the researcher's curiosity, interest, and intuition. Therefore, it is sometimes conducted without any practical end in mind, although it may have unexpected results pointing to practical applications.

_____d) The supervisor is not responsible for the content and scope of your thesis.

_____e) If we do not want to repeat the mistakes of the others, we need to read the literature.

_____f) If we do something soon, it will tell us what to do next.

_____g) You can publish a paper that includes your supervisor's name without your supervisor's approval.

_____h) You should prepare the slide presentation on your own. You should not bother your supervisor about this.

_____i) The more pages for presentation, the better preparation you can show to the audience.

_____j) We should focus at the solution rather than the problem. How to build a solution is more important than understanding what the problem is.

_____k) A proposal is a technically feasible plan for solving a problem.

_____l) You should not make it clear when the words or ideas that you are using are your own and when they are taken from another writer.

_____m) The thesis is a formal document of which purpose is to prove that you have made an original contribution to knowledge.

_____n) A thesis usually follows the chronology of how the research is conducted.

_____o) Outlines can be used to help you prepare to write a single paragraph, a composition, a paper, or even a book.

_____p) Abstract, Contents, Introduction, and Conclusions are read first by the readers or referees and therefore give very first impressions which are important.

_____q) The key information in "Conclusions" is the list of claims to originality or new results

Question 3 **(43 marks)**

Answer the following questions about research documents.

a) What do successful proposals need? (4 marks)

.....

.....

.....

.....

.....

.....

.....

.....

Name_____ ID_____

b) What are the pitfalls about writing a proposal? (4 marks)

.....

.....

.....

.....

.....

.....

.....

c) What are to be in the Front Matter of a formal report? (5 marks)

.....

.....

.....

.....

.....

.....

.....

d) What are to be in the Back Matter of a formal report? (3 marks)

.....

.....

.....

.....

.....

e) What is plagiarism? (5 marks)

.....

.....

.....

.....

.....

f) List the ethics in writing a research article. (5 marks)

.....

.....

.....

.....

.....

.....

g) List at least 5 questions to be answered in order to check whether your research article is ready for submission. (5 marks)

.....

.....

.....

.....

.....

.....

.....

.....

h) What is Impact Factor? Explain how it is calculated and what its value means briefly. (5 marks)

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

i) How do we write a literature survey? (4 marks)

.....

.....

.....

.....

.....

.....

j) What will not normally contain in written academic English? (3 marks)

.....

.....

.....

.....

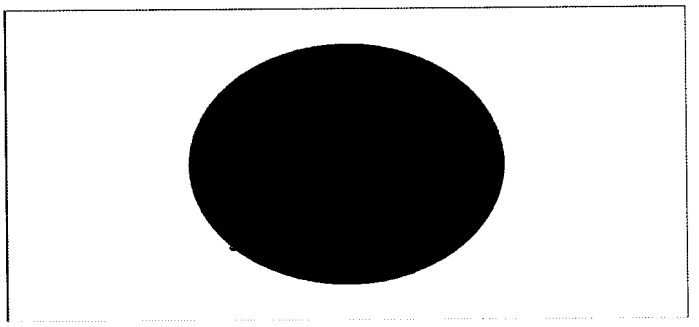
.....

.....

Question 4 **(7 marks)**

Spot what are wrong with the following data representations. Also inform what should be changed or added.

a)



.....

.....

.....

b)

Foods/Dishes	Quantity	Energy
Boned, sliced Hainan-style chicken with marinated rice (Thai: ข้าวมันไก่)	300	596
'Red' pork with rice (Thai: ข้าวหมูแดง)	320	540
Stewed pork leg with rice (Thai: ข้าวขาหมู)	289	438
Fried rice with pork/chicken/shrimp (Thai: ข้าวผัดหมู/ไก่/ไข่)	315	557
Rice topped with stir-fried chicken and basil (Thai: ข้าวผัดกะเพราไก่)	293	554

Table 1. Common Thai dishes and their energy expenditure

.....

.....

.....

c)

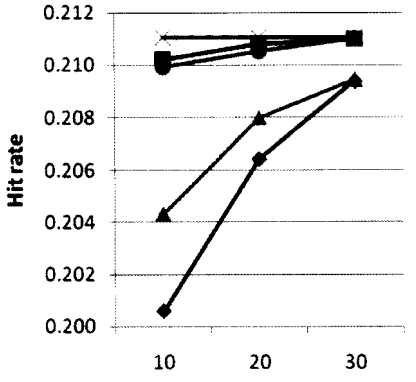


Figure 5. Performances of different policies using 15-day NY trace and uniform cost.

.....

.....

.....

e) What are the objectives in writing and publishing research articles? (3 marks)

.....

.....

.....

.....

.....

.....

f) Why do we need to do a literature survey? Give at least 3 reasons. (3 marks)

.....

.....

.....

.....

.....

g) What do you need to do at the meeting with your supervisor? (6 marks)

.....

.....

.....

.....

.....

.....

h) List code of conducts or work ethics of a researcher. (4 marks)

.....

.....

.....

.....

.....

.....

.....

Question 6 **(8 marks)**

What type of the presentation media to be used for the following requirements?

a) figures and graphs

.....

b) photos of complex objects

.....

c) dynamic material, e.g. animation

.....

d) words

.....

e) the agenda and important points, to be stayed up all the time or a long time

.....

.....

f) working through something, where the process is important

.....

g) complex tables, with lots of figures, equations,

.....

h) anything that can't be understood in 30 seconds

.....

Question 7 **(7 marks)**

List pitfalls and shortcomings of the following methods or media.

a) Copy and Paste (3 marks)

.....

.....

.....

.....

.....

.....

.....

b) Graphs (1 mark)

.....

.....

c) Diagrams (3 marks)

.....

.....

.....

.....

.....

.....

.....

.....

d) Result and Discussion (2 marks)

.....

.....

.....

.....

.....

.....

Pichaya Tandayya

Lecturer

"I have no special talents.
I am only passionately curious."

Albert Einstein

Name_____ID_____

การกำหนดวันหมดอายุของจุดอ่อนในซอฟต์แวร์ระบบ

Defining Expiration Date of System Software Vulnerability

ปุณธวัช ว่องธวัชชัย[1], ยรรยง เต็งอำนวย[2] และ ทรงพล ต่อนี[3]

[1] ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย

254 ถนนพญาไท แขวงวังใหม่ เขตปทุมวัน กทม. 10330 โทรศัพท์ : 0-2218-6991 E-mail: Puntawat.V@Student.chula.ac.th

[2] ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย

254 ถนนพญาไท แขวงวังใหม่ เขตปทุมวัน กทม. 10330 โทรศัพท์. 0-2218-6998 E-mail: yunyong.t@chula.ac.th

[3] ภาควิชาสุขศึกษา คณะพลศึกษา มหาวิทยาลัยศรีนครินทรวิโรฒ

114 สุขุมวิท 23 แขวงคลองเตยเหนือ เขตวัฒนา กทม. 10110 โทรศัพท์. 0-2649-5000 ต่อ 2567 E-mail: songpol@swu.ac.th

บทคัดย่อ

ในปัจจุบันจุดอ่อนที่เกิดขึ้นใหม่ในระบบคอมพิวเตอร์ยังคงก่อความเสียหายเป็นวงกว้าง ยากต่อการควบคุม และไม่สามารถระบุได้แน่ชัดว่าหายไปจากระบบอย่างถาวรแล้วหรือไม่ งานวิจัยนี้ได้ทำการวิเคราะห์การสาบสูญและการหมดอายุของจุดอ่อนเป็นกลุ่มและรายตัวด้วยวิธีการหาระยะเวลาสาบสูญที่เหมาะสมและวิเคราะห์ระยะปลอดเหตุการณ์ โดยอาศัยข้อมูลข่าวสาธารณะโดยใช้ค่าเฉลี่ยขอบเขตบนและค่ามัธยฐานของระยะเวลาที่จุดอ่อนยังคงมีอยู่ในระบบที่ระดับความเชื่อมั่น 95% ช่วยให้ทราบว่าจุดอ่อนยังมีอันตรายหรือก่อความเสียหายในระบบคอมพิวเตอร์ได้อีกหรือไม่ ก่อให้เกิดประโยชน์ต่อผู้ดูแลระบบในการจัดลำดับความสำคัญการเฝ้าระวังถูกโจมตีได้อย่างมีประสิทธิภาพ

คำสำคัญ: จุดอ่อน, การหมดอายุ, การสาบสูญ, ซอฟต์แวร์ระบบ

Abstract

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

Keywords: Vulnerability, Expiration, Disappearance, System software

1. บทนำ

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 ส่งผลให้เครื่องคอมพิวเตอร์ทั่วโลกอาจไม่ได้รับการแพทช์อย่างทั่วถึง ก่อให้เกิดการโจมตีและสร้างความเสียหายตามมาได้อีกสาเหตุหนึ่งคือ การขาดความเอาใจใส่ของผู้ดูแลระบบในการติดตามสถานะของจุดอ่อนและการแพทช์คอมพิวเตอร์ในระบบ

โดยทั่วไป ก่อนที่จุดอ่อนจะตายนั้น จะต้องมีการสาบสูญจากวงการข่าวเป็นระยะเวลาหนึ่ง ดังนั้น งานวิจัยนี้ทำการวิเคราะห์หาระยะเวลาสาบสูญ โดยใช้ค่าเฉลี่ยขอบเขตบนที่ระดับความเชื่อมั่น 95% ของระยะเวลาที่จุดอ่อนหายไปจากระบบ และกำหนดวันหมดอายุของจุดอ่อนจากการวิเคราะห์ระยะเวลาที่จุดอ่อนยังคงอยู่ในระบบ (Survival time) มาเป็นเกณฑ์ในการอ้างอิงอายุของจุดอ่อนโดยประมาณ ซึ่งทำให้สามารถชี้วัดได้ว่าจุดอ่อนยังมีอันตรายหรือก่อความเสียหายได้อีก หรือไม่

2. งานวิจัยที่เกี่ยวข้อง

2.1 Probability of Attack Based on System Vulnerability Life Cycle

Jumratjaroenvanit และ Teng-amnuay [1] 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

2.2 Windows of Vulnerability: A Case Study Analysis

Arbaugh และคณะ [2] ได้ทำการคิดค้นแบบจำลองวัฏจักรวงจรชีวิตสำหรับจุดอ่อนในระบบคอมพิวเตอร์ โดยมีช่วงชีวิตที่สำคัญ ได้แก่ การเกิด (birth) การถูกค้นพบ (discovery) การเปิดเผยข้อมูล (disclosure) การเปิดเผยข้อมูลในที่สาธารณะ (publicity) การทำสคริปท์ (scripting) การแก้ไขจุดอ่อน (correction) และการตาย (death) ซึ่งแบบจำลองนี้สามารถนำไปประยุกต์ใช้กับกรณีศึกษาจำนวนทั้งหมด 3 ตัวอย่าง ได้แก่ Phf incident, IMAP incident และ BIND incident เพื่อเปิดเผยให้เห็นว่าระบบนั้นยังคงมีจุดอ่อนให้พบเห็นได้อยู่บ่อยครั้งหลังจากมีแพทช์สำหรับแก้ไขซ่อมแซมจุดอ่อนให้นำไปใช้งานได้แล้ว

3. การเก็บข้อมูล

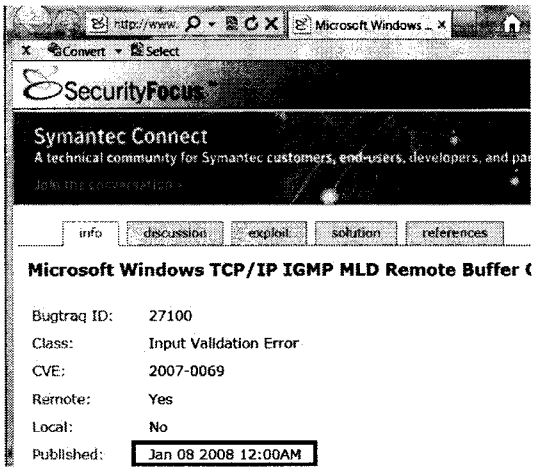
ในงานวิจัยชิ้นนี้ได้เลือกข้อมูลของจุดอ่อนจาก Windows XP จำนวน 258 ตัวขึ้นมาเป็นกรณีศึกษา เนื่องจากเป็นระบบปฏิบัติการที่หยุดการพัฒนาแล้ว มีวงจรชีวิตของจุดอ่อนที่ค่อนข้างสมบูรณ์

3.1 ฐานข้อมูลซีวีอี

งานวิจัยนี้อาศัยฐานข้อมูลของจุดอ่อนจากซีวีอี (CVE) [3] ซึ่งได้รวบรวมไว้เป็นหมวดหมู่โดยประกอบด้วยเขตข้อมูลที่สำคัญได้แก่ Name, Status, Description, References, Phase, Votes และ Comments ซึ่งข้อมูลที่นำมาใช้ในงานวิจัยคือ Name หรือชื่อของซีวีอีและ Reference ซึ่งเป็นแหล่งอ้างอิงในการเชื่อมโยงไปหาข่าวรายงานการโจมตี

3.2 การจัดเก็บข้อมูลข่าวการโจมตี

ในการจัดเก็บข้อมูล จะนำ Reference ของแต่ละซีวีอีมาตรวจสอบเพื่อเก็บวันที่ของข่าวตามรูปที่ 1 และนับจำนวนความถี่ที่เกิดขึ้นและนำไปคำนวณหาระยะเวลาสาบสูญและอายุของจุดอ่อนที่เหมาะสม นอกจากนั้น ยังใช้ฐานข้อมูลโอเอสวีดีบี (OSVDB) [4] และการค้นหาข่าวผ่าน Google จำนวน 30 ผลการค้นหาแรก [5] มาเพิ่มเติม



รูปที่ 1 การตรวจสอบวันที่ของข่าวการโจมตีจุดอ่อน

หลังจากได้วันที่ของข่าวแล้ว จะนำมาบันทึกลงตารางพร้อมทั้งนับความถี่ และคำนวณหาระยะห่างของข่าวซึ่งหมายถึงระยะเวลาที่จุดอ่อนว่างเว้นจากการเป็นข่าวโดยบันทึกข้อมูล 1 จุดอ่อน ต่อ 1 ตาราง

เมื่อได้ข้อมูลจนครบทุกจุดอ่อนแล้ว จะนำจุดอ่อนมาจัดกลุ่มเพื่อเตรียมการวิเคราะห์โดยแบ่งตามประเภท ได้แก่ ระดับความรุนแรง ผลกระทบต่อระบบ ประเภทของการโจมตี และบริเวณที่เกิด แต่ได้ตัดจุดอ่อน 4 ตัว เนื่องจากมีค่าระยะเวลาที่พบจุดอ่อนในระบบ (Active period) แตกต่างไปจากกลุ่มมาก (Extreme value) อาจทำให้เกิดความคลาดเคลื่อนของผลการทดลอง ทำให้เหลือจุดอ่อน 254 ตัว ดังตารางที่ 1

4. การกำหนดระยะเวลาสาบสูญของจุดอ่อน

หลังจากได้ค่าระยะเวลาที่ข่าวของจุดอ่อนหายไปจากระบบสูงสุดครบทุกจุดอ่อน จะนำค่าที่ได้มาหาระยะเวลาสาบสูญของจุดอ่อนที่เหมาะสมโดยใช้สมการช่วงความเชื่อมั่น 95% [6]

$$\bar{x} - t_{\frac{\alpha}{2},DF}\frac{s}{\sqrt{n}} < \mu < \bar{x} + t_{\frac{\alpha}{2},DF}\frac{s}{\sqrt{n}} \qquad (1)$$

จากสมการ (1) กำหนด α = 0.05 และ DF=253 สามารถคำนวณช่วงความเชื่อมั่น 95% ของระยะเวลาที่จุดอ่อนหายไปจากระบบสูงสุด มีค่าอยู่ในช่วง 235.79 ถึง 301.04 วัน ได้กราฟที่มีลักษณะเบ้ขวาดังรูปที่ 2 ในที่นี้จะใช้ค่าขอบเขตบนคือ 301.34 วัน เป็นจุดตัด (Cut point) ของการกำหนดระยะเวลาสาบสูญของจุดอ่อน ซึ่งคิดเป็น 77 จาก 254ตัว

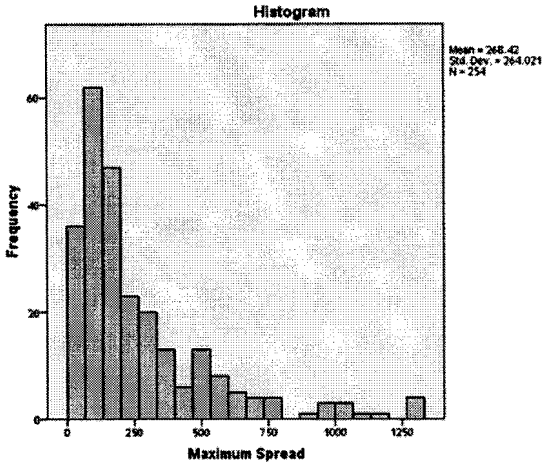
5. วิเคราะห์ระยะเวลาที่จุดอ่อนยังคงอยู่ในระบบ

ในการวิเคราะห์หาค่ามัธยฐานของระยะเวลาที่จุดอ่อนยังคงมีอยู่ในระบบ (Survival time) ที่ช่วงความเชื่อมั่น 95% ด้วยวิธีการของ

Kaplan-Meier [6] นั้น กำหนดช่วงระยะเวลาในการศึกษาข้อมูล คือ 7 ส.ค. 2544 – 1 เม.ย. 2555 เป็นเวลารวมทั้งสิ้น 3,890 วัน

วันที่	จำนวนข่าว	ระยะห่างของข่าว (วัน)
13/3/2010	1	-
13/4/2010	11	31
14/4/2010	3	1
16/4/2010	1	2
รวมเวลาที่พบในระบบ		34
หายไปจากระบบสูงสุด		31

ตารางที่ 1 ตัวอย่างข้อมูลการโจมตีในแต่ละจุดอ่อน



รูปที่ 2 ฮิสโทรแกรมของระยะเวลาสูงสุดที่จุดอ่อนหายไปจากระบบ

เหตุการณ์ที่สนใจ คือ การสาบสูญของจุดอ่อน ซึ่งนำไปสู่การหมดอายุของจุดอ่อน ถ้าจุดอ่อนใดมีถ้าจุดอ่อนใดมีค่าระยะเวลาที่หายไปจากระบบครั้งสุดท้ายไม่เกิน 301.34 วัน จะถือว่าไม่สาบสูญและจัดว่าเป็น Censored เนื่องจากจุดอ่อนยังคงมีนัยสำคัญ ในทางกลับกัน ถ้าจุดอ่อนใดมีค่าเวลาที่หายไปจากระบบครั้งสุดท้ายเกิน 301.34 วัน ถือว่าเกิดเหตุการณ์สาบสูญ (Failure) และมีตัวแปรที่เกี่ยวข้องกับการวิเคราะห์ได้แก่

ตัวแปรเวลา คือระยะเวลาที่จุดอ่อนยังคงมีนัยสำคัญ

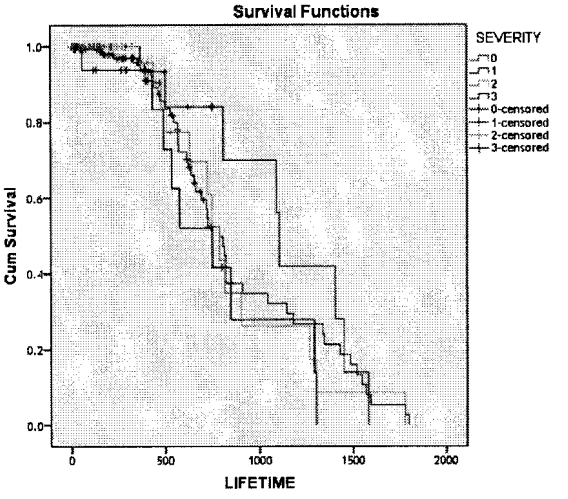
ตัวแปรสถานะ คือเหตุการณ์ที่สนใจแบ่งเป็น 2 กรณีคือ จุดอ่อนสาบสูญและไม่สาบสูญ

ตัวแปรปัจจัย ใช้ในการวิเคราะห์จุดอ่อนเชิงกลุ่ม ในงานวิจัยนี้ได้นำเสนอปัจจัยของระดับความรุนแรงของจุดอ่อน ซึ่งแบ่งออกเป็น 4 กลุ่ม ตามเกณฑ์ของซีวีเอสเอส (Common Vulnerability Scoring System) [7] ได้แก่ รุนแรงที่สุด มาก ปานกลาง และ ต่ำ

เครื่องมือที่ใช้ในการคำนวณคือ IBM SPSS เวอร์ชั่น 20 โดยมีผลการคำนวณค่ามัธยฐานของระยะเวลาที่จุดอ่อนยังคงมีอยู่ในระบบดังตารางที่ 2 และรูปที่ 3

SEVERITY	Median			
	Estimate	Std. Error	95% Confidence Interval	
			Lower Bound	Upper Bound
Highest (0)	1108.000	20.508	1067.805	1148.195
High (1)	787.000	55.316	678.581	895.419
Medium (2)	787.000	50.611	687.802	886.198
Low (3)	750.000	161.881	432.713	1067.287
Overall	810.000	32.010	747.261	872.739

ตารางที่ 2 มัธยฐานระยะเวลาที่จุดอ่อนยังคงมีนัยสำคัญ



รูปที่ 3 ระยะเวลาที่จุดอ่อนยังคงมีนัยสำคัญจำแนกตามความรุนแรง

จากตารางที่ 2 และรูปที่ 3 พบว่าจุดอ่อนที่มีระดับความรุนแรงที่สุด จะมีระยะเวลาที่จุดอ่อนยังคงมีนัยสำคัญมากที่สุด ในขณะที่จุดอ่อนที่มีระดับความรุนแรงต่ำ จะมีระยะเวลาที่จุดอ่อนยังคงมีนัยสำคัญน้อยที่สุด แต่อย่างไรก็ตามจากการทดสอบความแตกต่างของระยะเวลาที่จุดอ่อนยังคงมีนัยสำคัญจำแนกตามระดับความรุนแรงของจุดอ่อนโดยใช้ Log-rank พบว่า ในแต่ละระดับความรุนแรงของจุดอ่อนมีระยะเวลาที่จุดอ่อนยังคงมีนัยสำคัญไม่แตกต่างกัน (p=0.439)

6. การกำหนดวันหมดอายุของจุดอ่อน

จากจุดอ่อนที่สาบสูญ 77 ตัวจาก 254 ตัวในหัวข้อ 4 นั้น สามารถนำจุดอ่อนดังกล่าวมาตรวจสอบได้ว่า จุดอ่อนเหล่านั้นหมดอายุหรือไม่โดยการนำจุดอ่อนแต่ละตัวมาเปรียบเทียบค่าระยะเวลาที่พบข่าวของจุดอ่อนว่ามีค่ามากกว่าระยะเวลาที่จุดอ่อนยังคงมีนัยสำคัญหรือไม่ ถ้าหากมากกว่า จะถือว่าจุดอ่อนนั้นได้หมดอายุลงแล้ว เป็นอันตรายต่อระบบต่ำ ดังสรุปข้อมูลในตารางที่ 3

จากตารางที่ 3 สรุปได้ว่า มีจุดอ่อนที่สาบสูญ 77 ตัว คิดเป็น 30.31% ซึ่งหมายความว่าสามารถลดลำดับความสำคัญในงานเฝ้าระวังการ

ระดับความรุนแรง	จุดอ่อน (ตัว)	สาบสูญ (ตัว)	หมดอายุ (ตัว)	คิดเป็น (%)
Highest	25	8	4	16.00
High	154	47	20	12.98
Medium	58	13	6	10.34
Low	17	9	4	23.52
รวม	254	77	34	13.38

ตารางที่ 3 สรุปข้อมูลการสาบสูญและตายของจุดอ่อน

โจมตีของผู้ดูแลระบบลงไปได้มากถึง 30.31% จากภาระงานปกติ และหมดอายุ 34 ตัวจากจุดอ่อนที่สาบสูญ 77 ตัว คิดเป็น 44.15% และ คิดเป็น 13.38% ของจุดอ่อนทั้งหมด แสดงให้เห็นว่าจุดอ่อนที่เกิดขึ้นภายใน Windows XP ส่วนใหญ่ยังคงมีนัยสำคัญต่อระบบมาก และยังไม่ได้รับการแก้ไขได้อย่างทันท่วงทีเท่าที่ควร ถึงแม้ว่าทางผู้ผลิตจะมีการออกแพทช์เพื่อปรับปรุงแก้ไขช่องโหว่ของจุดอ่อนอย่างสม่ำเสมอแล้วก็ตาม

7. สรุป

จากหัวข้อ 4 หัวข้อ 5 และหัวข้อ 6 สามารถสรุปได้ว่า ถ้าจุดอ่อนใดที่มีระยะเวลาที่หายไปจากระบบในครั้งหลังสุดมากกว่าระยะเวลาสาบสูญของจุดอ่อน (Disappearance period) จะถือว่าจุดอ่อนนั้นได้สาบสูญลงและในจุดอ่อนที่สาบสูญแล้วนั้น ถ้ามีระยะเวลาที่พบจุดอ่อนมากกว่าค่ามัธยฐานของระยะเวลาที่จุดอ่อนยังคงมีอยู่ในระบบ (Survival time) จะถือว่าจุดอ่อนนั้นได้หมดอายุลงไปแล้ว ซึ่งสามารถกำหนดเป็นระดับการเฝ้าระวังได้ 3 ระดับคือ ระดับสูง สำหรับจุดอ่อนที่ยังไม่เข้าสู่สถานะสาบสูญ ระดับปานกลาง สำหรับจุดอ่อนที่อยู่ในสถานะสาบสูญ และระดับต่ำ สำหรับจุดอ่อนที่อยู่ในสถานะหมดอายุที่ผู้ดูแลระบบสามารถจัดลำดับความ สำคัญรองลงมา เพื่อเป็นประโยชน์ต่อผู้ดูแลระบบในการจัดลำดับความสำคัญของงานเฝ้าระวังดูแลระบบได้อย่างมีประสิทธิภาพ

เอกสารอ้างอิง

[1] Jumratjaroenvanit, A.; Teng-amnuay, Y.; , "Probability of Attack Based on System Vulnerability Life Cycle," Electronic Commerce and Security, 2008 International Symposium on , vol., no., pp.531-535, 3-5 August 2008.

[2] William A. Arbaugh, William L. Fithen, John McHugh, "Windows of Vulnerability: A Case Study Analysis," Computer, pp. 52-59, December, 2000.

[3] CVE, "Common Vulnerabilies and Exposures (CVE)," available at: http://cve.mitre.org, last access: June 7, 2012.

[4] OSVDB, "Open Source Vulnerability Database (OSVDB)," available at: http://osvdb.org, last access: June 7, 2012.

[5] 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

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

[7] CVSS, "Common Vulnerability Scoring System (CVSS)," available at: http://www.first.org/cvss, last access: June 7, 2012.