(ร่าง)

รายงานการวิจัยฉบับสมบูรณ์
การพัฒนาบทเรียนวิดีโอสตรีมมิ่งแบบปฏิสัมพันธ์
เรื่อง ความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และการสื่อสารข้อมูล
คณะวิทยาการสื่อสาร มหาวิทยาลัยสงขลานครินทร์
Development of an Interaction Video Streaming Lesson on Security of Computer Systems and Data Communication the Faculty of Communication Sciences, Prince of Songkla University

จรุงวิทย์ บุญเพิ่ม

อำนาจ สุคนเขตร์

ได้รับทุนอุดหนุนการวิจัยจากกองทุนวิจัยวิทยาเขตปัตตานี

มหาวิทยาลัยสงขลานครินทร์ วิทยาเขตปัตตานี

ประจำปีงบประมาณ 2563 สัญญาเลขที่ ACA6203015S-0

การพัฒนาบทเรียนวิดีโอสตรีมมิ่งแบบปฏิสัมพันธ์ เรื่อง ความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และการสื่อสารข้อมูล คณะวิทยาการสื่อสาร มหาวิทยาลัยสงขลานครินทร์

จรุงวิทย์ บุญเพิ่ม
วท.ม.(วิทยาการคอมพิวเตอร์), อาจารย์
คณะวิทยาการสื่อสาร มหาวิทยาลัยสงขลานครินทร์ วิทยาเขตปัตตานี
E-mail : jarungwit.b@g.psu.ac.th

อำนาจ สุคนเขตร์
วท.บ.(วิทยาการคอมพิวเตอร์) , นักวิชาการคอมพิวเตอร์ ชำนาญการ
ฝ่ายเทคโนโลยีและนวัตกรรมการเรียนรู้
สำนักวิทยบริการ มหาวิทยาลัยสงขลานครินทร์ วิทยาเขตปัตตานี
E-mail : amnat.s@g.psu.ac.th

บทคัดย่อ

การศึกษาวิจัยครั้งนี้มีวัตถุประสงค์เพื่อเพื่อพัฒนาวิดีโอปฏิสัมพันธ์ เรื่อง ความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และการสื่อสารข้อมูล เพื่อเปรียบเทียบผลสัมฤทธิ์ทางการเรียนก่อนเรียนกับหลังเรียนของนักศึกษาที่เรียนด้วยวิดีโอปฏิสัมพันธ์ เรื่อง ความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และการสื่อสารข้อมูล และศึกษาความพึงพอใจของนักศึกษาที่มีต่อวิดีโอปฏิสัมพันธ์ เรื่อง ความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และการสื่อสารข้อมูล ในปีการศึกษา 2563 จำนวน 60 คน เครื่องมือที่ใช้ในการวิจัยครั้งนี้ ได้แก่ วิดีโอสตรีมมิ่งแบบปฏิสัมพันธ์ เรื่อง ความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และการสื่อสารข้อมูล แบบทดสอบความรู้ก่อนเรียน แบบทดสอบความรู้หลังเรียน และแบบประเมินความพึงพอใจที่มีต่อวิดีโอสตรีมมิ่งแบบปฏิสัมพันธ์ เรื่อง ความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และการสื่อสารข้อมูล การวิเคราะห์ข้อมูลโดยใช้การหาค่าร้อยละ ค่าเฉลี่ย และส่วนเบี่ยงเบนมาตรฐาน ผลการวิจัย พบว่า วิดีโอสตรีมมิ่งแบบปฏิสัมพันธ์มีประสิทธิภาพตามเกณฑ์ที่กำหนด 80/80 มีค่าประสิทธิภาพเฉลี่ยเท่ากับ 81.33/83.67 ผลสัมฤทธิ์การเรียนของนักศึกษาหลังเรียนสูงกว่าก่อนเรียน ได้คะแนนเฉลี่ยร้อยละ 83.67 และนักศึกษามีความพึงพอใจต่อการเรียนระดับดีมาก

คำสำคัญ

การพัฒนา, วิดีโอ, สตรีมมิ่ง, ปฏิสัมพันธ์, ความมั่นคง, ระบบ, คอมพิวเตอร์

Development of an Interaction Video Streaming Lesson on Security of Computer Systems and Data Communication the Faculty of Communication Sciences, Prince of Songkla University

Jarungwit Boonperm
M.Sc.(Computer Science), Lecturer
Faculty of Communication Sciences
E-mail : jarungwit.b@g.psu.ac.th

Amnat Suconkhet
B.Sc.(Computer Science), Computer Technical Officer, Professional Level
Division of Technology and Learning Innovation
Office of Acadimic Services
Prince of Songkla University, Pattani Campus
E-mail : amnat.s@g.psu.ac.th

Abstract

Development of an Interactive Video Streaming Lesson on Security of Computer Systems and Data Communication aims to develop an interactive video on security of computer systems and data communication. To compare pre-study and post-study achievement of students who studied with interactive video on security of computer systems and data communication. In addition to studying the satisfaction of 60 students with an interactive video on security of computer systems and information communication of the academic year 2020. The tools were used in this research were an interactive video streaming security of computer systems and data communication, pre-test, post-test and an interactive video streaming satisfaction assessment. Data analysis used percentage, mean and standard deviation. The results showed an interactive video streaming was effective according to the specified criteria 80/80. The mean efficiency was 81.33/83.67. The average score was 83.67% means the results of students after learning are better than before learning and the students were satisfied with their studies at an excellent level.

Keyword

development, video, streaming, interaction, stability, system, computer

บทที่ 1
บทนำ

1.1 ความสำคัญและที่มาของหัวข้อการวิจัย

สื่อการสอนหลักที่นำพาความรู้จากผู้สอนสู่การถ่ายทอดให้กับผู้เรียนทั้งภาพและเสียงและสนับสนุนความสำเร็จของผู้เรียน คือ การใช้สื่อวิดีโอ เน้นการใช้วิดีโอในการเรียนเป็นหลัก(video-based learning) โดยเฉพาะวิดีโอที่มีปฏิสัมพันธ์กับผู้เรียน หรือการออกแบบกิจกรรมการเรียนการสอนที่ให้ผู้เรียนที่เข้ามาศึกษาได้เรียนรู้ร่วมกัน เกิดปฏิสัมพันธ์ในการเรียนโดยทั่วไปปฏิสัมพันธ์ในการเรียนแบ่งออกเป็น ปฏิสัมพันธ์ระหว่างผู้สอนกับผู้เรียน ปฏิสัมพันธ์ระหว่างเนื้อหากับผู้เรียน และปฏิสัมพันธ์ระหว่างผู้เรียนกับผู้เรียน อีกหนึ่งแนวคิด คือ ปฏิสัมพันธ์ระหว่างผู้สอนกับผู้สอน ปฏิสัมพันธ์ระหว่างเนื้อหากับเนื้อหา ปฏิสัมพันธ์ผู้สอนกับเนื้อหา อีกทั้งผู้สอนควรคำนึงถึงการนำไปใช้ คือ เทคโนโลยีที่เกี่ยวข้องกับการแบ่งช่องทางการเผยแพร่วิดีโอ คือ OTT (over-the-top content) ซึ่งเป็นการบริการแพร่วิดีโอผ่านอินเทอร์เน็ต โดยที่ผู้สอนไม่ต้องพัฒนาโครงข่ายสัญญาณเอง อีกทั้งผู้สอนอาจจะเลือกใช้ OTT จากผู้ให้บริการที่มีอยู่เพื่อความสะดวกในการใช้งานวิดีโอในการเรียนการสอนประโยชน์หรือจุดเด่นของวิดีโอมีหลายหลายซึ่งสามารถสรุปออกมาได้ คือ วิดีโอสามารถถ่ายทอดเหตุการณ์ที่กำลังเกิดขึ้น (see something happen) สามารถเล่าเรื่องราวที่เกิดขึ้นได้มากกว่าภาพถ่าย (tell a story) และวิดีโอสามารถทำให้ผู้เรียนได้รับรู้ถึงความรู้สึกที่ผู้สอนต้องการถ่ายทอดออกมาในเนื้อเรื่อง (emotional engagement) และในลักษณะของการเรียนแบบเปิดและในรูปแบบของ MOOC นั้น สื่อหลักที่ใช้คือ วิดีโอ(Video-based) ในที่นี้หมายถึงการให้ผู้เรียนเรียนจากวิดีโอ ไม่ใช้การใช้วิดีโอในรูปแบบของการสื่อสารแบบผสานเวลาและไม่ผสานเวลา คำว่า วิดีโอ นับว่าเป็นสื่อชนิดหนึ่งในการเรียนการสอน คำว่า สื่อ เป็นคำมาจากภาษาลาตินว่า “medium” แปลว่า “ระหว่าง” หมายถึงสิ่งใดก็ตามที่บรรจุข้อมูลเพื่อให้ผู้รับส่งและผู้รับสามารถสื่อสารกันได้ตรงตามวัตถุประสงค์ปกติแล้วคำว่า สื่อ จะใช้เป็นพหูพจน์เสมอ ซึ่งตรงกับกับว่า “media” ในภาษาอังกฤษ (กิดานันท์ มลิทอง, 2548) วีดิทัศน์หรือวิดีโอ ในปัจจุบันเป็นที่นิยมในวงการศึกษาเนื่องจากวิดีโอเป็นสื่อการสอน วิดีโอสามารถแบ่งออกตามระบบ คือ analog video และ digital video(Weise & Weynand, 2012) วิดีโอแอนะล็อกเป็นวิดีโอที่ทำการบันทึกข้อมูลภาพและเสียงให้อยู่ในรูปแบบของสัญญาณแอนะล็อก ส่วนวิดีโอดิจิทัล (digital video) เป็นวิดีโอที่ทำการบันทึกข้อมูลภาพและเสียงที่ได้มาจากกล้องวิดีโอดิจิทัลให้อยู่ในรูปแบบสัญญาณดิจิทัล

ในการจัดการเรียนการสอนมีการนำวิดีโอมาใช้กันอย่างแพร่หลาย โดยรูปแบบของวิดีโอออกเป็น 3 กลุ่ม คือ (1) วิดีโอออนดีมานด์ (on-demand video) (2) วิดีโอสื่อสารทางเดียวเวลาจริงทันที (one-way real time video) (3) วิดีโอสื่อสารสองทางเวลาจริงทันที(two-way real time video) (Greenberg & Zanetis, 2012) ซึ่งรายละเอียดต่าง ๆ ของแต่ละประเภทของวิดีโอสามารถสรุปตามตาราง ดังนี้

On-demand Video	One-way Real Time Video	Two-way Real Time Video
- วิดีโอดิจิทัล ตัวอย่างของเนื้อหาที่ส่งด้วยวิธีนี้รวมถึงภาพยนตร์ โปรแกรมการศึกษาและเนื้อหาการออกอากาศ on-demand - รูปแบบของวิดีโอที่มีระยะเวลาสั้น รวมถึงคลิป YouTube, Podcasting, video on demand ส่งผ่านความสามารถในเทคโนโลยีสตรีมมิ่ง - การบันทึกภาพการบรรยายในห้องเรียนรวมทั้งการเก็บบรรยากาศผ่านเทคโนโลยีสตรีมมิ่ง - วิดีโอเกมที่สามารถให้บริการได้ตามความต้องการหรือในเวลาจริง	- การออกอากาศเนื้อหา รวมถึงโปรแกรมการศึกษา - สตรีมมิ่งวิดีโอ (streaming video) รวมทั้งเรียนแบบถ่ายทอดสดหรือกิจกรรมต่าง ๆ - การจับภาพการบรรยายรูปแบบของการสตรีมมิ่งวิดีโอเพื่อให้บริการรับชมตามความต้องการ - การจัดผ่านดาวเทียมซึ่งรวมถึงการเรียนการสอนแบบถ่ายทอดสด	- การส่งผ่านดาวเทียมรวมถึงการสื่อสารสองทางหรือหลายวิธีการในการเรียนการสอนแบบถ่ายทอดสด - การมีปฏิสัมพันธ์ในการประชุมทางไกล และเทคโนโลยีทางไกลเสมือนจริง ซึ่งประกอบด้วยสองสถานที่หรือมากกว่าสองสถานที่ ที่เชื่อมต่อกับการเรียนการสอนแบบถ่ายทอดสด การนำเสนอผลงานและการทำงานร่วมกัน

ผู้สอนสามารถเลือกใช้วิดีโอให้เหมาะสมกับกิจกรรมการเรียน-การสอน ตามลักษณะของวิดีโอแต่ละประเภท ได้แก่ (1) วิดีโอออนดีมานด์ และวิดีโอถ่ายทอด-สด เป็นสื่อการสอนและช่องทางการสื่อสารแบบทางเดียวทั้งในเวลาเดียวกันและต่างเวลากันเหมาะสมสำหรับฝึกหัดผู้เรียนให้ปฏิบัติตาม สั่งสมจนเกิดเป็นความชำนาญ และตกผลึกเป็นความรู้ใหม่ที่ได้จากการปฏิบัติ โดยเฉพาะวิดีโอถ่ายทอดสด ทำให้ผู้เรียนรู้สึกว่าตนเองเสมือนว่าอยู่ในเหตุการณ์ แล้วเกิดอารมณ์ที่จะเข้ากิจกรรม อีกทั้งผู้เรียนสามารถแสดงความคิดเห็นผ่านเครื่องมือสนับสนุนอื่น ๆ (2) วิดีโอคอนเฟอเรนซ์ เหมาะกับการเป็นสื่อกลางที่จะเชื่อมความสัมพันธ์ระหว่างผู้เรียน สร้างปฏิสัมพันธ์ทางสังคม

ประโยชน์ของการใช้วิดีโอเป็นสื่อการสอนหรือทรัพยากรในการเรียนรู้ ช่วยพัฒนาการทางด้านการเรียนรู้ของผู้เรียนแบ่งออกเป็น (1) ด้านพุทธิพิสัย (cognitive domain) ผู้เรียนสามารถทำความเข้าใจและรับสาร เกิดเป็นความจำได้โดยการใช้ เสียง สี ภาพเคลื่อนไหวทำให้ผู้เรียนมีความสนใจในการเรียน รวมไปถึงการแสดงกระบวนการ ขั้นตอนการทำงานต่าง ๆ ในแต่ละเนื้อหาได้ง่าย อีกทั้งวิดีโอสามารถนำเสนอข้อมูลภาพที่เป็นเรื่องยากที่จะถ่ายทอดในรูปแบบอื่น ๆ เช่น การให้ผู้เรียนได้มองเห็นถึงการเดินบนดวงจันทร์ การเยี่ยมชมภูเขาไฟระเบิด (2) ด้านจิตพิสัย (affective domain) วิดีโอสร้างแรงจูงใจให้ผู้เรียนเกิดความอยากเรียน หากผู้เรียนมีแรงจูงใจในการเรียนแล้ว จะส่งผลต่อผลสัมฤทธิ์ทางการเรียน รวมถึงช่วยลดข้อจำกัดทางความสามารถในการอ่านของผู้เรียน หมายถึง ถ้าหากเป็นการเรียนโดยใช้สื่อสิ่งพิมพ์ อาจมีผู้เรียนจำนวนมากที่มีความยากลำบากในการอ่าน และพลาดโอกาสทางการเรียนรู้ แต่ในมุมมองของวิดีโอผู้เรียนสามารถเรียนรู้ได้เปรียบเสมือนเป็นภาษาที่สอง โดยขึ้นอยู่กับความสามารถของนักออกแบบการสอนและเนื้อหาที่สอน(3) ด้านทักษะพิสัย (psychomotor domain) วิดีโอช่วยแสดงขั้นตอนและรายละเอียดต่าง ๆ ในการเคลื่อนไหว

เป็นตัวอย่างให้ผู้เรียนทำตาม รวมไปถึงการบันทึกการเรียนการสอนหน้าชั้นหรืองานนำเสนอหน้าชั้นของผู้เรียนแล้วมาศึกษาเพื่อพัฒนาทักษะในการนำเสนอหน้าชั้นเรียน และสร้างรูปแบบพฤติกรรมเชิงบวกและเพื่อกระตุ้นให้ผู้เรียนในการเรียน เช่น การใช้วิดีโอเพื่อนำเข้าสู่บทเรียน แนะนำการเรียน แสดงให้เห็นขั้นตอนของการเรียนทั้งหมดเพื่อสร้างแรงจูงใจให้ผู้เรียนเกิดการมีส่วนร่วมของผู้เรียนในแต่ละลำดับขั้นการเรียนรู้ อีกทั้งการใช้ Video Call แสดงการโต้ตอบของผู้เรียนและผู้สอนแบบ real time ในการสาธิตการทำงานต่าง ๆ (4)ด้านความสัมพันธ์ระหว่างบุคคลและความรับผิดชอบ (interpersonal domain) เป็นการนำวิดีโอมาเป็นตัวอย่างหรือเหตุการณ์ต่าง ๆ ให้ผู้เรียนวิเคราะห์ เพื่อให้ผู้เรียนมีการแลกเปลี่ยนความคิดเห็นระหว่างชั้นเรียน และช่วยสร้างความสัมพันธ์ทางการเรียน อีกทั้งวิดีโอยังยังช่วยในการส่งเสริมการอภิปรายและการสะท้อนความคิดเกี่ยวข้องแต่ละบุคคล หรือการสื่อสารในเรื่องใดเรื่องหนึ่งหรือเรื่องเดียวกันได้ (Denning, 1992;Smaldno, Lowther, & Russell, 2012)

การออกแบบวิดีโอในการเรียนการสอนถือว่าเป็นขั้นตอนที่สำคัญ เนื่องจากการที่จะส่งสาร หรือข้อมูลไปให้ผู้เรียน ให้ได้รับข้อมูลหรือสารตรงตามวัตถุประสงค์ของผู้สอนนั้นจะทำให้การเรียนการสอนมีประสิทธิภาพ โดยขั้นของการสร้างความรู้ของผู้เรียนนั้น ผู้เรียนจะรับข้อมูลที่หลากหลายแล้วเปลี่ยนเป็นความรู้ โดยการออกแบบให้วิดีโอมีการปฏิสัมพันธ์กับผู้เรียนที่ผ่านมามีวิธีการต่าง ๆ เช่น การใช้วิดีโอเล่าเรื่องราวโดยใช้วิดีโอที่เสนอปัญหา(problem-based video) หรือ วิดีโอที่ให้ตัวให้ผู้เรียน แล้วให้ผู้เรียนตัดสิ้นใจว่าจะดำเนินเรื่องไปทางใด สามารถทำได้โดยใช้ YouTube ในการสร้างปฏิสัมพันธ์ โดยเมื่อเล่นคลิปวิดีโอจบแล้วสามารถสร้างข้อความขึ้นเพื่อเป็นตัวเลือก เพื่อเชื่อมโยงไปยังวิดีโอต่อไปตามสถานการณ์ซึ่งเรียงร้อยกันเป็นเรื่องราว ที่มีการออกแบบเป็นอย่างดีจนสุดท้ายผู้เรียนสามารถเรียนรู้วิดีโอปฏิสัมพันธ์ในการเรียนแบบเปิดในศตวรรษที่ 21 ในการตัดสินใจของตนเองว่าผลที่ตามมาคืออะไร เมื่อตัดสินใจแบบนั้นไปแล้วจะได้รับผลออกมาในรูปแบบใด

การที่จะให้ผู้เรียน เรียนรู้จากวิดีโอที่ผู้สอนต้องการถ่ายทอดมา ระยะเวลาของคลิปวิดีโอ มุมกล้อง การจัดตำแหน่งภาพ กราฟิก การจัดแสง เทคนิควิธีการต่าง รูปแบบการเล่าเรื่องสิ่งเหล่านี้ถือว่าเป็นสิ่งที่สำคัญมากที่ผู้สอนต้องมีการออกแบบอย่างชัดเจน ที่จะสร้างแรงจูงใจให้ผู้เรียนให้มีความตั้งใจ และสนใจอยู่กับเนื้อหาตลอดเวลา โดยอีกหนึ่งวิธีการ คือการแทรกเทคนิคการตั้งคำถามเข้ามาในวิดีโอบรรยาย โดยวิธีการแทรก จะแทรกเมื่อใด แทรกโดยใช้คำถามประเภทใด และเมื่อไรควรจะแทรก คำถามเหล่านี้สามารถอธิบายได้โดยวิธีการแทรกอาจแทรกโดยใช้คำถามในลักษณะของข้อความ ประเภทของคำถามนั้นสามารถนำเทคนิค5W1H คือ Who What Where When Why และ How เข้ามาช่วยในการตั้งคำถามโดยดูผลลัพธ์ที่ผู้สอนต้องการให้ผู้เรียน เช่น คำถามที่เน้นการคิดขั้นสูง (high order thinking skill) ควรใช้คำถาม When Why และ How เพื่อกระตุ้นให้ผู้เรียนเกิดการวิเคราะห์หาคำตอบส่วนคำถามที่เน้นการคิดขั้นพื้นฐาน (lower order thinking skill) ควรใช้คำถาม WhoWhat Where เพื่อ กระตุ้นให้ผู้เรียนเกิดการเรียนรู้หรือหากผู้สอนต้องการพัฒนาความสามารถในการแก้ปัญหา ความคิดสร้างสรรค์ให้ผู้เรียน ผู้สอนควรศึกษาขั้นตอนของความสามารถในการแก้ปัญหา ขั้นตอนของความคิดสร้างสรรค์ แล้วออกแบบคำถามตามขั้นตอนต่าง ๆ โดยตำแหน่งของคำถามควรแทรกก่อนหน้าวิดีโอแต่ละตอน แทรกระหว่างเนื้อหาใจความสำคัญและแทรกท้ายวิดีโอแต่ละตอน (นรินธน์

นนทมาลย์, 2554) ทั้งหมดนี้เป็นหน้าที่หลักของผู้สอนที่จะต้องมีการวิเคราะห์ ออกแบบ แล้วจึงนำไปสู่ขั้นของการผลิตให้ครอบคลุมกับเนื้อหา เพื่อดึงดูดให้ผู้เรียนมีความตั้งใจในการเรียน และสามารถนำคำถามที่แทรกในวิดีโอมาจัดกิจกรรมการเรียนการสอนเพิ่มเติมได้ เช่น ให้ผู้เรียนศึกษาจากวิดีโอแล้วตอบคำถามจากวิดีโอโดยการให้ผู้เรียนเขียนคำตอบใน Blog ส่วนตัวของผู้เรียน หรืออาจจะใช้คำถามนำ ถามสรุปหรือระหว่างวิดีโอ เพื่อเปิดการอภิปราย แลกเปลี่ยนความคิดเห็นของผู้เรียน อีกทั้งยังนำคำถามที่แทรกในวิดีโอนำมาประเมินผลในการเรียนการสอน รวมไปถึงการสร้างวิดีโอปฏิสัมพันธ์ที่ใช้ HTML 5 ช่วยให้ผู้สอนสามารถเพิ่มคำถาม โดยคำถามจะแสดงเป็นข้อความและการโต้ตอบประเภทอื่น ๆ ในวิดีโอผ่านเว็บไซต์ เพื่อให้ผู้เรียนได้แสดงความคิดเห็นได้หลายรูปแบบในระบบการจัดการเรียนการสอน เช่น WordPress, Moodle และ Drupal โดยการใช้ plugin ของ H5P (Joubel, 2017) ที่สามารถใช้บริการได้ที่ https://h5p.org/interactive-video หรือ Edpuzzle ที่สามารถใช้บริการได้ที่ https://edpuzzle.com/โดยใช้หลักการเดียวกันคือ ผู้สอนสามารถอัพโหลดวิดีโอบน Youtube หรือ Vimeo แล้วนำลิงค์วิดีโอที่ผู้สอนอัพโหลดแล้วมาสร้างวิดีโอปฏิสัมพันธ์

การประเมินวิดีโอเพื่อใช้ในการเรียนการสอน การใช้งานที่มีประสิทธิภาพของวิดีโอควรเริ่มต้นด้วยการที่ผู้สอนเลือกวิดีโอ ในการตัดสินใจ สร้างแรงจูงใจให้ผู้เรียน และแจ้งให้ผู้เรียนทราบและปฏิบัติตามควรจะเป็นวิดีโอที่เกี่ยวข้องกับผู้เรียนและกระตุ้นให้ผู้เรียนต้องการที่จะเรียนรู้เพิ่มเติมเกี่ยวกับหัวข้อ ให้มีประสิทธิภาพด้านการศึกษา วิดีโอต้องสื่อสารอย่างมีประสิทธิภาพให้กับนักเรียนและช่วยให้ผู้เรียนสร้างความรู้ขึ้นมาใหม่ มีแนวทาง ดังนี้

1. การตั้งชื่อวิดีโอควรจะเกี่ยวข้องกับกลุ่มบุคคลมากกว่าการตัดสินใจเพียงคนเดียวเนื่องจากจะช่วยเพิ่มมุมมองของผู้เรียนหรือเพื่อขยายฐานประสบการณ์ในการกำหนดวิดีโอที่มีประสิทธิภาพทางการศึกษา

2. มุมมองของผู้เรียนเมื่อได้ดูวิดีโอที่ผู้สอนเตรียมไว้ให้ อาจได้รับความรู้หรือมุมมองที่แตกต่างจากการที่ผู้สอนเลือก วิดีโอที่ดึงดูดความสนใจของผู้สอนอาจไม่ดึงดูดความสนใจของผู้เรียน

3. บางครั้งผู้สอนมีการประเมินคัดเลือกวิดีโออยู่แล้ว มันจะมีประโยชน์เพื่อใช้ในการหารือเกี่ยวกับเกณฑ์การประเมินก่อนที่จะดาเนินการขั้นตอนการคัดเลือกและใช้เกณฑ์การประเมินตลอดการคัดเลือกและการอภิปราย

วิดีโอสตรีมมิ่งแบบปฏิสัมพันธ์นี้สามารถแทรกคำถามระหว่างวิดีโอ ทำให้สามารถเร้าความสนใจและทำให้ผู้เรียนได้เรียนรู้ตามรูปแบบการเรียนของตนเอง เกิดความเข้าใจในเนื้อหาตามที่ผู้สอนต้องการนำเสนอและสามารถกลับมาศึกษาได้ด้วยตนเอง หากผู้สอนมีการออกแบบการสร้างปฏิสัมพันธ์ระหว่างเนื้อหากับผู้เรียนโดยการใช้คำถาม เพื่อกระตุ้นให้ผู้เรียนเกิดการเรียนรู้ตามวัตถุประสงค์ที่กำหนดไว้หรือใช้คำถามเพื่อการประเมินระหว่างเรียนรู้ด้วยจากวิดีโอ ซึ่งเป็นลักษณะของการประเมิน เพื่อการพัฒนาการเรียนรู้ของผู้เรียน รวมถึงคำถามที่แสดงระหว่างผู้เรียนได้เรียนรู้จากวิดีโอแล้วผู้เรียนได้ตอบคำถาม คำตอบของผู้เรียนจะถูกบันทึกในระบบการจัดการเรียนการสอน เพื่อเป็นการประเมินผู้เรียนระหว่างเรียนได้

ปัจจุบันมีภัยคุกคามและการโจมตีในรูปแบบต่างๆ บนอินเทอร์เน็ตมากขึ้น คณะผู้วิจัยได้ตระหนักถึงเรื่อง ความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และการสื่อสารข้อมูล ที่นักศึกษาหรือสาธารณชนทั่วไปควรตระหนักรู้ถึงความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และการสื่อสารข้อมูล จึงได้จัดทำโครงการวิจัยนี้ขึ้นมา

1.2 วัตถุประสงค์ของโครงการวิจัย

1. เพื่อพัฒนาวิดีโอปฏิสัมพันธ์ เรื่อง ความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และการสื่อสารข้อมูล

2. เพื่อเปรียบเทียบผลสัมฤทธิ์ทางการเรียน ก่อนเรียนกับหลังเรียน ของนักศึกษาที่เรียนด้วยวิดีโอปฏิสัมพันธ์ เรื่อง ความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และการสื่อสารข้อมูล

3. ศึกษาความพึงพอใจของนักศึกษาที่มีต่อวิดีโอปฏิสัมพันธ์ เรื่อง ความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และการสื่อสารข้อมูล

1.3 สมมุติฐานการวิจัย

1. สื่อวิดีโอปฏิสัมพันธ์ เรื่อง ความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และการสื่อสารข้อมูล มีคุณภาพในระดับดีมาก

2. นักศึกษามีผลสัมฤทธิ์ทางการเรียนสูงขึ้น เมื่อเรียนผ่านสื่อวิดีโอปฏิสัมพันธ์ เรื่อง ความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และการสื่อสาร หลังเรียนสูงกว่าก่อนเรียน อย่างมีนัยสำคัญทางสถิติที่ระดับ .05

3. ความพึงพอใจของผู้เรียนที่มีต่อสื่อวิดีโอปฏิสัมพันธ์ เรื่อง ความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และการสื่อสาร มีความพึงพอใจอยู่ในระดับดีมาก

1.4 ขอบเขตของการวิจัย

ประชากร

ประชากรที่ในการศึกษาวิจัยครั้งนี้ ได้แก่ นักศึกษาระดับปริญญาตรี คณะวิทยาการสื่อสาร มหาวิทยาลัยสงขลานครินทร์ วิทยาเขตปัตตานี ภาคเรียนที่ 1 ปีการศึกษา 2562

กลุ่มตัวอย่าง

กลุ่มตัวอย่างที่ใช้ในการศึกษาวิจัยครั้งนี้ ได้แก่ นักศึกษาระดับปริญญาตรี คณะวิทยาการสื่อสาร มหาวิทยาลัยสงขลานครินทร์ วิทยาเขตปัตตานี ที่ลงทะเบียนเรียนในวิชา 871-310 การปฏิสัมพันธ์ระหว่างมนุษย์และคอมพิวเตอร์ (Human Computer Interaction) และ 871-411 ความมั่นคงของระบบคอมพิวเตอร์และการสื่อสารข้อมูล (Computer System and Data Communication Security) จำนวน 60 คน ได้มาจากการเลือกแบบเฉพาะเจาะจง (Purposive Sampling)

ตัวแปรต้น

1. วิดีโอปฏิสัมพันธ์ เรื่อง ความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และการสื่อสารข้อมูล

2. การเรียนด้วยวิดีโอปฏิสัมพันธ์ เรื่อง ความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และการสื่อสารข้อมูล

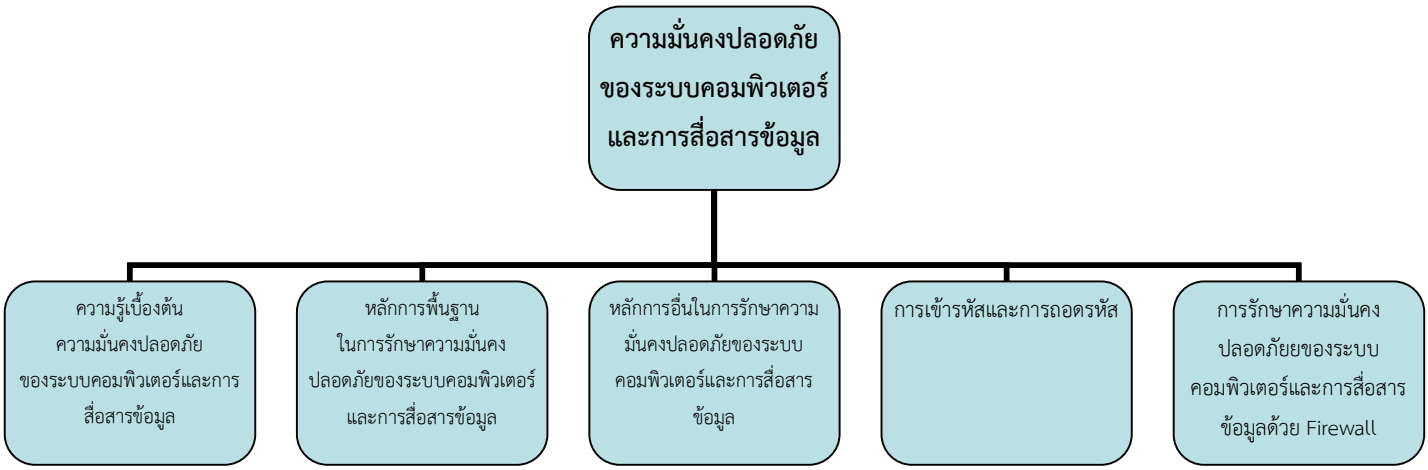
ตัวแปรตาม ได้แก่

1. ประสิทธิภาพของวิดีโอปฏิสัมพันธ์ เรื่อง ความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และการสื่อสารข้อมูล

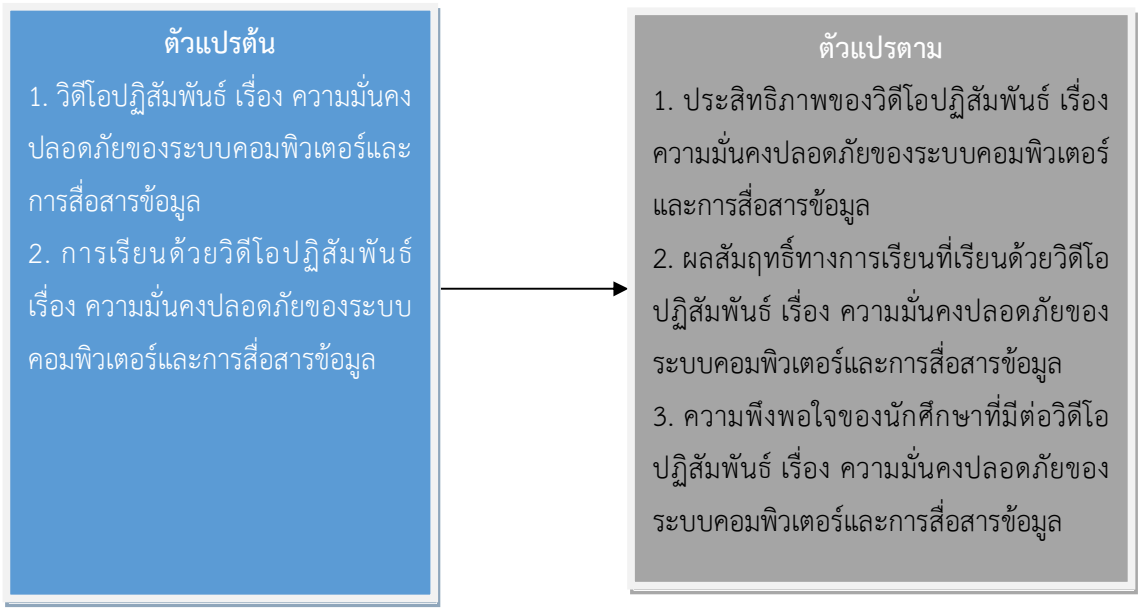
2. ผลสัมฤทธิ์ทางการเรียนที่เรียนด้วยวิดีโอปฏิสัมพันธ์ เรื่อง ความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และการสื่อสารข้อมูล

3. ความพึงพอใจของนักศึกษาที่มีต่อวิดีโอปฏิสัมพันธ์ เรื่อง ความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และการสื่อสารข้อมูล

ขอบเขตเนื้อหา



1.5 กรอบแนวคิดในการวิจัย



1.6 ประโยชน์ที่คาดว่าจะได้รับ

1. ได้สื่อวิดีโอปฏิสัมพันธ์ เรื่อง ความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และการสื่อสารข้อมูล ที่มีคุณภาพสามารถสื่อความหมายสามารถสื่อความหมายระหว่างผู้เรียนกับผู้สอนได้อย่างชัดเจน

2. นักศึกษามีความรู้ ความเข้าใจหลังเรียนจากสื่อวิดีโอปฏิสัมพันธ์ เรื่อง ความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และการสื่อสารข้อมูล มากขึ้น

3. นักศึกษามีความพึงพอใจเมื่อเรียนผ่านสื่อวิดีโอปฏิสัมพันธ์ เรื่อง ความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และการสื่อสารข้อมูล

4. เป็นแนวทางในการพัฒนาสื่อวิดีโอปฏิสัมพันธ์ในเรื่องและรายวิชาอื่นๆ ต่อไป

บทที่ 2
เอกสารและงานวิจัยที่เกี่ยวข้อง

ในการพัฒนาสื่อวิดีโอปฏิสัมพันธ์ เรื่อง ความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และการสื่อสารข้อมูล คณะวิทยาการสื่อสาร มหาวิทยาลัยสงขลานครินทร์ ผู้วิจัยได้ศึกษาเอกสารและงานวิจัยที่เกี่ยวข้องดังนี้

2.1 ความรู้เกี่ยวกับสื่อวิดีโอปฏิสัมพันธ์

2.1.1 ความหมายของวิดีโอสตรีมมิ่งแบบปฏิสัมพันธ์

2.1.2 องค์ประกอบของวิดีโอสตรีมมิ่งแบบปฏิสัมพันธ์

2.1.3 รูปแบบการมีปฏิสัมพันธ์

2.1.4 วิดีโอปฏิสัมพันธ์

2.2 ความรู้เกี่ยวกับความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และการสื่อสารข้อมูล

2.2.1 ความหมายและหลักการความมั่นคงปลอดภัย

2.2.2 การรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์

2.2.3 หลักการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์

2.2.4 การเข้ารหัสและการถอดรหัส

2.2.5 ไฟร์วอลล์

2.1 ความรู้เกี่ยวกับสื่อวิดีโอปฏิสัมพันธ์

2.1.1 ความหมายของวิดีโอสตรีมมิ่งแบบปฏิสัมพันธ์

มีนักวิชาการต่างๆ ได้ให้ความหมายของวิดีโอสตรีมมิ่งไว้ดังนี้

พรสุข ตันตระรุ่งโรจน์ (2557) กล่าวไว้ในหนังสือรวมบทความ เรื่อง เทคโนโลยีและสื่อสารการศึกษา : นวัตกรรมการเรียนรู้แบบผสมผสาน ว่า การสตรีมมิ่งวิดีโอเป็นการเพิ่มขีดความสามารถในการเข้าถึงข้อมูลและรูปแบบการนำเสนอข้อมูลข่าวสาร ผ่านเว็บบราวเซอร์โดยเฉพาะอย่างยิ่งการสตรีมมิ่งวิดีโอเพื่อการสื่อสารและความบันเทิง สตรีมมิ่งวิดีโอเป็นการส่งภาพและเสียงผ่านเว็บบราวเซอร์ได้โดยไม่ต้องรอการดาวน์โหลดไฟล์ให้เสร็จก่อน

กฤช พลไพรสรรพ์ (2554) ได้ระบุว่า วิดีโอสตรีมมิ่ง เป็นการให้บริการข้อมูลวิดีโอดิจิทัล ผ่านเครือข่ายอินเทอร์เน็ต ทำให้สามารถให้บริการแก่ผู้ใช้จำนวนมากเมื่อเทียบกับระบบวิดีโอคอนเฟอเรนท์ตามปกติ แต่มีการลงทุนน้อยกว่า นอกจากนี้ยังมีความยืดหยุ่นในการใช้งานสามารถให้บริการได้ทุกที่ที่มีระบบอินเทอร์เน็ต โดยระบบวิดีโอสตรีมมิ่งสามารถที่จะปรับขนาดของการส่งข้อมูลให้เหมาะสมกับความเร็วอินเทอร์เน็ตของผู้ใช้ได้

นรินธน์ นนทมาลย์ (2554) ได้ระบุถึงเทคโนโลยีการนำเสนอสื่อแบบสตรีมมิ่งเกิดขึ้นจากความต้องการนำเสนอภาพเคลื่อนไหวเสียง วิดีโอ ผ่านเครือข่ายอินเทอร์เน็ต การนำเสนอรูปแบบเดิมนั้นจำเป็นต้องดาวน์โหลดข้อมูลดังกล่าวมาที่เครื่องลูกข่ายจนครบก่อนจึงจะนำเสนอได้ ทำให้การนำเสนอต้องเสียเวลารอคอบด้วยเทคโนโลยีสตรีมมิ่งช่วยให้การนำเสนอสื่อต่างๆ เป็นไปอย่างราบรื่น ไม่รู้สึกว่าต้องรอคอย

นานเกินไป โดยเครื่องแม่ข่ายจะทยอยส่งข้อมูลคล้ายการไหลของกระแสน้ำ (Streaming) อย่างต่อเนื่อง ทำให้ข้อมูลไม่สะดุด ซึ่งเป็นเทคโนโลยีที่นำมาใช้กันอย่างแพร่หลายในปัจจุบัน

ลักษณะการส่งสตรีมมิ่งมีเดียที่ได้รับความนิยมในปัจจุบันนี้ คือ โปรเกรสซีฟดาวน์โหลด (Progressive Download) ออนดีมานด์ (On-Demand Files) และการถ่ายทอดสด (Live Broadcasting)

1. โปรเกรสซีฟดาวน์โหลด (Progressive Download) เป็นเทคโนโลยีที่เกิดจากการผสมผสานวิธีการส่งข้อมูลแบบสตรีม และการดาวน์โหลดเข้าด้วยกัน วิธีการนี้เป็นการดาวน์โหลดข้อมูลลงบนเครื่องคอมพิวเตอร์ของผู้ชม ซึ่งในระหว่างดาวน์โหลดอยู่นั้น ผู้ชมสามารถที่จะเล่นหรือแสดงผลได้ก่อนที่การดาวน์โหลดจะเสร็จสิ้นสมบูรณ์ เนื่องจากระบบได้มีการนำพื้นที่บางส่วนภายในหน่วยความจำชั่วคราวของเครื่องคอมพิวเตอร์ที่เรียกว่า Buffer มาใช้งานเพื่อเก็บพักข้อมูล แต่วิธีการนี้มักนิยมใช้กับไฟล์มัลติมีเดียที่มีขนาดไม่ใหญ่มากนัก ซึ่งเหมาะสำหรับผู้ที่ต้องการถ่ายทอดและเผยแพร่ไฟล์ข้อมูลที่มีคุณภาพสูงกว่าไฟล์สตรีมมิ่งมีเดียทั่วไป โดยผ่านทางช่องสัญญาณ (Bandwidth) ที่มีขนาดจำกัด

2. ออนดีมานด์ (On-Demand Files) เป็นวิธีการที่สามารถเรียกใช้งานได้ทันทีเมื่อต้องการ โดยไฟล์เหล่านี้จะถูกเข้ารหัสในรูปแบบที่เหมาะสมต่อการแสดงผลแบบสตรีมมิ่งแล้วนำไปจัดเก็บไว้บนเซิร์ฟเวอร์ เพื่อให้ทุกคนสามารถเรียกใช้งานพร้อมกันหลายคนในเวลาเดียวกัน โดยแต่ละคนสามารถควบคุมฟังก์ชั่นการทำงานได้อิสระ ไม่ว่าจะเป็นหยุดการแสดงผลชั่วคราว แสดงผลย้อนกลับ หรือแม้กระทั่งแต่การแสดงผลซ้ำ ซึ่งได้รับความนิยมใช้งานกันอย่างแพร่หลาย

3. การถ่ายทอดสด (Live Broadcasting) การถ่ายทอดสดบนอินเทอร์เน็ตเป็นการถ่ายทอดเหตุการณ์ที่เกิดขึ้น ณ ขณะนั้น โดยที่ผู้ชมได้รับชมและฟังเหตุการณ์ต่างๆ ได้เป็นปัจจุบันและทันท่วงที ด้วยวิธีการแปลงสัญญาณนำเข้าข้อมูลจากกล้องวิดีโอไปเป็นข้อมูลดิจิตอล แล้วส่งผ่านข้อมูลเหล่านี้ในรูปแบบของสตรีมมิ่งไปยังเครื่องเซิร์ฟเวอร์ ซึ่งได้ทำการติดตั้งระบบบริหารจัดการไว้แล้ว จากนั้นเครื่องเซิร์ฟเวอร์จะทำการถ่ายทอดสดไปยังเครื่องผู้ชมปลายทางได้คราวละพร้อมๆ กันเป็นจำนวน (นรินธน์ นนทมาลย์, 2554)

วรพจน์ นวลสกุล (2540) ระบุว่า วีดิทัศน์ตามประสงค์เป็นระบบสื่อประสมปฏิสัมพันธ์ (Multimedia Interactive) บนเครือข่ายคอมพิวเตอร์ที่ทำงานเหมือนกับเคเบิลทีวี แตกต่างตรงที่มีจำนวนเรื่องให้ผู้ชมได้มีโอกาสได้เลือกเองมากกว่า โดยไม่คำนึงกำลังให้บริการรายการใดกับใครอยู่ในขณะนั้น และไม่ต้องเสียเวลารอชมต่อจากผู้อื่น อีกทั้งผู้ชมเองก็สามารถควบคุมการเล่นหรือศึกษาได้ด้วยตนเองบนเครื่องส่วนบุคคลที่ต่อเชื่อมระบบเครือข่าย จากที่ได้กล่าวมาข้างต้นเป็นการสรุปความหมายของวีดิทัศน์ตามประสงค์

ศิรินทิพย์ นันทวาศ (2555) ได้กล่าวถึง วิดีโอแบบปฏิสัมพันธ์เป็นการผสมผสานกันระหว่างวิดีโอและบทเรียนอิเล็กทรอนิกส์ในรูปของสื่อประสมที่ให้ทั้งภาพเคลื่อนไหวแบบวิดีโอภาพนิ่งเสียง ตัวอักษร และกิจกรรมการสอนแบบสื่ออิเล็กทรอนิกส์โดยมีการเรียกใช้ข้อมูลในลักษณะสื่อหลายมิติเพื่อใช้เป็นสื่อในการจัดกิจกรรมการเรียนการสอนโดยเฉพาะอย่างยิ่งในการศึกษารายบุคคลและการศึกษาแบบอิสระ

จากความหมายของวิดีโอสตรีมมิ่งและวีดิทัศน์ตามประสงค์ ที่ได้กล่าวโดยนักวิชาการศึกษาข้างต้นสรุปความหมายของวิดีโอสตรีมมิ่งแบบปฏิสัมพันธ์ ได้ว่า เป็นบทเรียนอิเล็กทรอนิกส์ที่นำเสนอใน

รูปแบบอิเล็กทรอนิกส์ หรืออีกนัยนึงเรียกได้ว่า วิดีโอคอร์สแวร์ เป็นลักษณะของสื่อประสมที่สามารถควบคุมการแสดงผลในรูปแบบของภาพ เสียง ภาพเคลื่อนไหว ข้อความ

2.1.2 องค์ประกอบของวิดีโอสตรีมมิ่งแบบปฏิสัมพันธ์

สมจิต จันทร์ฉาย (2557) ได้กล่าวถึงระบบการเรียนการสอนว่า หมายถึง องค์ประกอบของการเรียนการสอนที่ได้รับการจัดให้มีความสัมพันธ์และส่วนเสริมกันอย่างเป็นระบบ โดยมีจุดมุ่งหมายเพื่อนำไปใช้เป็นแนวทางการดำเนินการจัดการเรียนการสอนให้ผู้เรียนบรรลุเป้าหมายการเรียนการสอนที่ต้องการ ระบบการเรียนการสอนยังช่วยในการวางแผนการเรียนการสอน การประเมิน แผนการเรียนการสอน และการออกแบบการเรียนการสอน เป็นต้น ระบบการเรียนการสอนจึงประกอบด้วยองค์ประกอบเชิงระบบ คือ ปัจจัยนำเข้า (Input) กระบวน (Process) ผลผลิต (Output) การควบคุม (Control) และการให้ข้อมูลป้อนกลับ (Feedback) มีรายละเอียดของแต่ละองค์ประกอบดังนี้

1. ปัจจัยนำเข้า (Input) ประกอบด้วย พื้นฐานความรู้เดิมของผู้เรียน จุดประสงค์การเรียนรู้ เนื้อหา สื่อ-อุปกรณ์ แหล่งเรียนรู้ และเวลา

2. กระบวน (Process) ประกอบด้วย การจัดการเรียนการสอน การพัฒนาทักษะการเรียนรู้แก่ผู้เรียน และการบริหารจัดการชั้นเรียน

3. ผลผลิต (Output) ประกอบด้วย ผลการเรียนรู้ ได้แก่ ความรู้ ทักษะ เจตคติและคุณลักษณะของผู้เรียน

4. การควบคุม (Control) ประกอบด้วย การวัดประเมินผลผู้เรียนและการวัดประเมินผลการเรียนการสอน

5. การให้ข้อมูลป้อนกลับ (Feedback) หมายถึง องค์ประกอบการเรียนการสอนต่างๆ ซึ่งได้รับการบันทึกไว้ภายหลังการดำเนินการการเรียนการสอน เพื่อนำไปใช้ในการปรับปรุงและพัฒนาการเรียนการสอนต่อไป (สมจิต จันทร์ฉาย, 2557)

จินตวีร์ คล้ายสังข์ และประกอบ กรณีกิจ (2552) ได้กล่าวถึงองค์ประกอบของบทเรียนอีเลิร์นนิ่งว่ามีองค์ประกอบที่สำคัญ 4 ส่วน คือ (1) บทเรียนอิเล็กทรอนิกส์ (2) ระบบการจัดการเรียนรู้ (3) การติดต่อสื่อสาร และ (4) การประเมินผลการเรียน ซึ่งเมื่อนำองค์ประกอบทั้ง 4 มาประกอบเข้ากันแล้ว ระบบจะทำงานประสานกันได้อย่างลงตัว โดยแต่ละองค์ประกอบมีรายละเอียดดังนี้

1. บทเรียนอิเล็กทรอนิกส์ เป็นเนื้อหาสาระที่นำเสนอในรูปแบบอิเล็กทรอนิกส์ เช่น วิดีโอคอร์สแวร์

2. ระบบบริหารจัดการ คือโปรแกรมบริหารจัดการการเรียนรู้ที่ทำหน้าที่เป็นศูนย์กลางจัดการและสนับสนุนการจัดการเรียนรู้ ซึ่งใช้เทคโนโลยีอินเตอร์เน็ตเข้ามาจัดการให้เกิดปฏิสัมพันธ์ ระหว่างผู้สอนและผู้เรียน ผู้เรียนกับผู้เรียน และผู้เรียนกับแหล่งข้อมูล ทั้งนี้ จะช่วยให้ผู้เรียนและผู้สอนสามารถเข้าถึงเนื้อหาและใช้งานได้ง่าย โดยมีเครื่องมือทางด้านการจัดการ การปรับปรุง การควบคุม การสำรองข้อมูล การสนับสนุนข้อมูล การบันทึกสถิติผู้เรียน และการประเมินผล ตลอดจนการตรวจให้คะแนนผู้เรียน ซึ่งผู้ใช้สามารถเรียกเครื่องมือนี้ผ่านโปรแกรมเว็บบราวเซอร์ และแบ่งเครื่องมือของระบบจัดการเรียนรู้เป็น 6 กลุ่ม ดังนี้

2.1 เครื่องมือสื่อสาร ได้แก่ การอภิปราย การแลกเปลี่ยนไฟล์ อีเมล์ วารสาร/บันทึกออนไลน์ การสนทนา การบริการวิดีโอ และไวด์บอร์ด

2.2 เครื่องมืออำนวยความสะดวก ได้แก่ บุ๊กมาร์ค ปฏิทินการเรียน การสืบค้นภายในรายวิชา และการแนะนำการเรียน

2.3 เครื่องมือสนับสนุนผู้เรียน ได้แก่ การจัดกลุ่ม การประเมินตนเอง การสร้างชุมชน และแฟ้มสะสมผลงานผู้เรียน

2.4 เครื่องมือบริหารรายวิชา ได้แก่ การระบุตัวตนของผู้เรียนการกำหนดสิทธิ์ การเข้าใช้รายวิชา และการลงทะเบียน

2.5 เครื่องมือส่งผ่านรายวิชา ได้แก่ การจัดการรายวิชา การช่วยเหลือผู้สอน การประเมินออนไลน์ การติดตามผู้เรียน และการทดสอบและให้คะแนนอัตโนมัติ

2.6 การออกแบบหลักสูตร ได้แก่ การเข้าถึงระบบ เทมเพลตรายวิชา การจัดการหลักสูตร การปรับแต่งมุมมองของหน้าจอ การออกแบบการสอน การยินยอมมาตรฐานการสอน และการใช้เนื้อหาร่วมและการใช้ซ้ำ

3. การติดต่อสื่อสาร เป็นเครื่องมือที่ช่วยผู้เรียนได้ติดต่อสอบถาม ปรึกษาหารือและแลกเปลี่ยนความคิดเห็น โดยเครื่องมือที่ช่วยในการติดต่อสื่อสารในการจัดการเรียนรู้ออนไลน์สามารถแบ่งได้ 2 ประเภท คือแบบประสานเวลาและแบบไม่ประสานเวลา ตัวอย่างเครื่องมือที่ใช้ ได้แก่ แชท อีเมล์ กลุ่มข่าว ห้องสนทนา กระดานอภิปราย กระดานประกาศ บล็อก วิกิ เป็นต้น

4. การประเมินผลการเรียน ในบทเรียนบางวิชาจำเป็นต้องมีการวัดระดับความรู้ก่อนเรียน การทดสอบย่อยท้ายบท การสอบใหญ่ก่อนจบหลักสูตร สามารถจัดการผ่านระบบการจัดการเรียนรู้ เช่น แบบเลือกตอบ แบบถูกผิด แบบเติมคำตอบ และแบบจับคู่ การประเมินอีกรูปแบบหนึ่งจากการทำกิจกรรมออนไลน์ของผู้เรียนเพื่อนำมาประกอบการพิจารราผลการเรียนรู้ของผู้เรียนด้วย เช่น จำนวนครั้งการเข้าเรียนในห้องเรียนออนไลน์ การเข้าร่วมทำกิจกรรมออนไลน์ เวลาที่เข้าใช้ในแต่ละบทเรียน ความถี่ในการแสดงความคิดเห็นหรืออภิปราย ตลอดจนคุณภาพของการแสดงความคิดเห็นหรือการอภิปราย งานที่ได้รับมอบหมาย การเขียนบันทึกการเรียนรู้ประจำวัน และแฟ้มสะสมงานอิเล็กทรอนิกส์ เป็นต้น (จินตวีร์ คล้ายสังข์ และประกอบกรณีกิจ, 2552)

ถนอมพร เลาหจรัสแสง (2545) ได้นำองค์ประกอบของสื่อแบบอิเล็กทรอนิกส์มาประยุกต์ใช้ ซึ่งองค์ประกอบมีดังต่อไปนี้ ได้จัดองค์ประกอบของสื่ออิเล็กทรอนิกส์ไว้ 4 องค์ประกอบหลัก ได้แก่

1.เนื้อหา องค์ประกอบที่สำคัญที่สุดของสื่อแบบอิเล็กทรอนิกส์ก็คือการที่ผู้เรียนจะบรรลุวัตถุประสงค์ของการเรียนในลักษณะนี้อย่างไร ผู้สอนจะจัดเนื้อหาให้แก่ผู้เรียนอย่างไร เพราะผู้เรียนต้องใช้เวลาส่วนใหญ่ศึกษาเนื้อหาด้วยตนเอง ต้องคิดค้นหาวิธี ปรับเปลี่ยน วิเคราะห์อย่างมีหลักการและเหตุผล ซึ่งองค์ประกอบอันดับแรกของ e-Learning ไม่ได้จำกัดเฉพาะบทเรียนคอมพิวเตอร์หรือคอร์สแวร์เท่านั้น ยังรวมถึงส่วนประกอบสำคัญอื่นๆ ที่สื่อแบบอิเล็กทรอนิกส์จำเป็นต้องมีเพื่อให้เนื้อหามีความสมบูรณ์ องค์ประกอบที่สำคัญของเนื้อหาได้แก่

1.1 โอมเพจ หรือเว็บหน้าแรกเป็นองค์ประกอบแรกของเนื้อหาการออกแบบให้เกิดความสวยงามจึงเป็นปัจจัยสำคัญที่ส่งผลต่อผู้เรียนให้เกิดความสนใจและกลับเข้ามาเรียนมากขึ้น ซึ่งจะประกอบไปด้วยองค์ประกอบที่จำเป็น ดังนี้

1.1.1 คำประกาศแนะนำการเรียนทางสื่อแบบอิเล็กทรอนิกส์โดยรวมอาจจะยังไม่ใช่คำประกาศหรือคำแนะนำในการเรียนที่เฉพาะเจาะจงของวิชาใดๆ อาจจะเป็นสิ่งที่ผู้สอนสามารถไปกำหนดข้อตกลง ประกาศหรือคำแนะนำที่สำคัญต่างๆ ด้วยตนเอง ไว้ในส่วนรายวิชาที่รับผิดชอบ ซึ่งเรียนจะมองเห็นได้หลังจากที่ผู้เรียนเข้าใช้ระบบแล้ว และสามารถเข้าไปยังส่วนต่างๆ ของรายวิชานั้นๆ อาจจะเพิ่มข้อความทักทายต้อนรับผู้เรียน เพื่อนำเข้าสู่การเรียนทางสื่อแบบอิเล็กทรอนิกส์ก็ได้

1.1.2 ระบบเข้าสู่บทเรียนและรหัสผ่าน (ระบบ login) ต้องอยู่หรือแสดงอยู่ในส่วนบนที่มองเห็นได้ชัดเจน ทำให้ง่ายต่อการเข้าใช้ระบบของผู้เรียน

1.1.3 ควรมีการแจ้งผู้เรียนให้มีการทราบล่วงหน้าเกี่ยวกับโปรแกรมต่างๆ รายละเอียดของโปรแกรมที่จำเป็นสำหรับการเรียกดูเนื้อหาอย่างสมบูรณ์ และสิ่งที่จำเป็น (Requirements) อื่นๆ เช่น การปรับขนาดหน้าจอหรือคุณสมบัติต่างๆ ของหน้าจอ เป็นต้น

1.1.4 การติดต่อกับหน่วยงานที่รับผิดชอบควรมีการแสดงชื่อผู้รับผิดชอบ รวมทั้งวิธีในการติดต่อกลับมายังผู้รับผิดชอบ เช่น ผู้เยี่ยมชมสามารถที่จะส่งข้อความคำติชมรวมทั้งผลป้อนกลับต่างๆ ที่อาจมีส่งมายังหน่วยงานที่รับผิดชอบได้

1.1.5 วันที่และเวลาที่ทำการปรับปรุงแก้ไขเว็บไซต์ล่าสุด เพื่อประโยชน์สำหรับผู้เรียนในการอ้างอิง

1.1.6 ระบบนับจำนวนผู้เรียน ที่เข้ามาเรียน หรือการนับจำนวนผู้เข้ามาเยี่ยมชมเว็บไซต์ ซึ่งเป็นองค์ประกอบที่ผู้ออกแบบสามารถเลือกมาใส่หรือไม่ใส่ก็ได้ ข้อดีของการมีระบบนับจำนวนผู้เข้ามาเว็บไซต์อาจจะช่วยกระตุ้นให้ผู้เรียน อายากกลับเข้ามาเรียนอีกและเพิ่มผู้เรียนมาเรียนร่วมกันจำนวนมากๆ

1.2 ส่วนแสดงรายชื่อวิชา เมื่อผู้เรียนเข้าสู่ระบบแล้ว ระบบจะแสดงชื่อรายวิชาทั้งหมดที่ผู้เรียนมีสิทธิ์เข้าเรียนได้ ในลักษณะสื่อแบบอิเล็กทรอนิกส์

1.3 เว็บหน้าแรกของแต่ละวิชา

1.3.1 คำประกาศ/คำแนะนำการเรียนทางสื่ออิเล็กทรอนิกส์หมายถึง คำประกาศหรือคำนะนำการเรียนที่เฉพาะเจาะจงสำหรับวิชาใดวิชาหนึ่ง นอกจากนี้ควรใส่ข้อความทักทายต้อนรับผู้เรียนเข้าสู่การเรียนในรายวิชาด้วย

1.3.2 รายละเอียดของผู้สอน ได้แก่ ชื่อผู้สอนและรายละเอียดวิธีการติดต่อผู้สอน เช่น e-mail address หรือโอมเพจส่วนตัวของผู้สอน

1.3.3 ประมวลรายวิชา (Syllabus) หมายถึง ส่วนที่แสดงสังเขปรายวิชา จะมีคำอธิบายลักษณะรายวิชาสั้นๆ เกี่ยวกับหน่วยเรียน วิธีการเรียน วัตถุประสงค์ และเป้าหมายของ

รายวิชา สิ่งคาดหวังจากผู้เรียนจะได้รับในการเรียน การมอบหมายงานและกำหนดส่งงาน เกณฑ์การประเมินกิจกรรมหรืองานให้ผู้เรียนทำ อาจจะเป็นในลักษณะของรายบุคคลหรือกลุ่มย่อย

1.3.4 ห้องเรียน (Classroom) ประกอบด้วยบทเรียน หรือคอร์สแวร์ที่ผู้สอนได้เตรียมไว้ให้กับผู้เรียน ซึ่งเนื้อหาสามารถแบ่งออกได้ตามลักษณะของสื่อที่ใช้นำเสนอเนื้อหา ได้แก่ เนื้อหาในรูปแบบตัวอักษร เนื้อในรูปแบบตัวอักษร ภาพ วิดีโอ หรือสื่อประสมอื่นๆ ที่ผลิตขึ้นมาอย่างง่ายๆ และเสียค่าใช้จ่ายน้อยๆ ซึ่งเนื้อหาจะเป็นมัลติมีเดียที่มีการออกแบบอย่างมีระบบ

1.3.5 หน้าเว็บสนับสนุนการเรียน (Resources) การจัดแหล่งเรียนรู้อื่นๆ เพิ่มเติมแต่ละหัวข้อสำหรับผู้เรียนให้ผู้เรียนเข้าไปศึกษา รวมทั้งเอกสารวิชาการอื่นๆ ที่เหมะสมกับรายวิชา ได้แก่ วิดีโอ วารสารวิชาการ หนังสือพิมพ์ รายการวิทยุ เป็นต้น หรืออาจเชื่อมโยงไปยังห้องสมุดหรือฐานข้อมูลงานวิจัยอื่นๆ ด้วย

1.3.6 ความช่วยเหลือ (Help) แสดงรายละเอียดวิธีการขอความช่วยเหลือไม่ว่าจะเป็นทางด้านเทคนิคแก่ผู้เรียน แสดงวิธีการหาเครื่องมือสืบค้น (Search) ส่วนต่างๆ ของเว็บ ส่วนแสดงแผนที่ไซต์ (site map) เพื่อแสดงภาพรวมโดยรวมของเว็บให้ผู้เรียนเข้าถึงข้อมูลได้สะดวกขึ้น

1.3.7 รายวิชาอื่นๆ (Other Courses) หากมีรายวิชาหลายวิชาควรมีลิงค์เพื่อกลับมายังเมนูรวมวิชาเรียนเพื่อให้ผู้เรียนเข้าไปยังห้องเรียนอื่นๆ ได้ทันทีโดยไม่ต้องออกจากระบบ และเข้าสู้ระบบใหม่

1.3.8 หน้าเว็บแสดงคำตอบที่พบบ่อย (FAQs) เมื่อมีการใช้งานเว็บจริงได้ระยะเวลาหนึ่ง จะพบว่าผู้ใช้ระบบ อาจจะเป็นผู้เรียนหรือผู้สอนจะมีคำถามเกี่ยวกับเนื้อหาการเรียนหรือปัญหาที่พบในขณะทำงาน คำถามเกี่ยวกับด้านเทคนิค สามารถนำมารวบรวมเพื่อนำแสดงในรูปแบบของคำตอบและคำถามที่พบบ่อย เพื่อลดเวลาในการตอบคำถามซ้ำๆ เป็นการสนับสนุนให้ผู้ใช้สามารถแก้ปัญหาได้ด้วยตนเอง

1.3.9 ลิงค์เชื่อมโยงการจัดการสอนด้านอื่นๆ (Management) ได้แก่ หน้าของ แบบสอบถาม แบบทดสอบ ผลการทดสอบ รวมถึงสถิติต่างๆ สามารถแสดงให้ผู้เรียนเข้าไปดูได้ ซึ่งในส่วนที่กล่าวมานี้จะเป็นส่วนหนึ่งของการบริหารจัดการรายวิชา

1.3.10 ลิงค์แสดงส่วนของการติดต่อสื่อสารกับผู้อื่น (Discussion) เพื่อบริการให้ผู้เรียนสามารถติดต่อสื่อสารกับอาจารย์ผู้สอนและเพื่อร่วมชั้นเรียนได้

1.3.11 การเข้าสู่ระบบและออกจากระบบ (Login/Logout) ควรแสดงปุ่มไว้เพื่อความปลอดภัย (Security) ของผู้เรียน และป้องกันผู้ที่ไม่มีสิทธิ์เข้าใช้แอบมาใช้ระบบด้วย

2. ระบบบริหารจัดการรายวิชา (Course Management System) เป็นองค์ประกอบ ที่สำคัญมากสำหรับ e-Learning ที่รวบรวมเครื่องมือซึ่งออกแบบให้เกิดความสะดวกแก่ผู้ใช้ในการจัดการกับการเรียนการสอนออนไลน์ ซึ่งอาจแบ่งได้ 3 กลุ่ม ได้แก่ (1) ผู้สอน (Instructors) (2) ผู้เรียน (Students) และ (3) ผู้บริหารระบบเครือข่าย (Network Administrator) เครื่องมือจะแบ่งตามระดับในการเข้าใช้งานของแต่ละกลุ่ม ได้แก่ พื้นที่และเครื่องมือช่วยในการเตรียมเนื้อหาบทเรียน พื้นที่และเครื่องมือ

สำหรับการทำแบบทดสอบ แบบสอบถาม การจัดการแฟ้มข้อมูลต่างๆ รวมถึงเครื่องมือในการติดต่อสื่อสาร ได้แก่ อีเมล์ กระดานสนทนาแบบไม่ใช่ในเวลาจริง (Web Board) หรือกระดานสนทนาในเวลาจริง (Chat) อาจจะมีระบบพิเศษอื่นๆ เพื่ออำนวยความสะดวกให้แก่ผู้ใช้อีก เช่น ระบบแสดงคะแนนให้ผู้เรียนเข้าดูคะแนนสอบ แสดงสถิติการเข้าใช้งานในระบบ ระบบที่ให้ผู้เรียนสามารถสร้างตารางการเรียนหรือปฏิทินการเรียนได้ เป็นต้น

3. โหมดการติดต่อสื่อสาร (Modes of Communication) เป็นองค์ประกอบของ e-Learning และขาดไม่ได้ก็คือการจัดให้ผู้เรียนสามารถติดต่อสื่อสารกับผู้สอน หรือวิทยากร ผู้เชี่ยวชาญอื่นๆ ฯ รวมถึงผู้เรียนด้วยกันเอง ในรูปแบบที่หลากหลายและต้องสะดวกต่อผู้ใช้งาน คือต้องมีเครื่องมือที่จัดหาให้ผู้เรียนมีใช้ได้มากกว่า 1 รูปแบบ รวมถึงเครื่องมือจะต้องใช้ง่ายต่อผู้ใช้งาน (User-Friendly) เครื่องที่สื่อแบบอิเล็กทรอนิกส์ที่สำคัญได้แก่

3.1 การประชุมทางคอมพิวเตอร์ หมายถึง การประชุมผ่านระบบคอมพิวเตอร์ในรูปแบบของการติดต่อสื่อสารแบบต่างเวลา เช่น การแลกเปลี่ยนข้อความผ่านกระดานสนทนาอิเล็กทรอนิกส์ หรือเว็บบอร์ด เป็นต้น หรือในลักษณะการติดต่อสื่อสารแบบเวลาเดียวกัน เช่น การสนทนาออนไลน์ (Chat) หรืออาจจัดให้มีการถ่ายทอดสัญญาณภาพและเสียงสด ผ่านทางเว็บหรือวิดีโอคอนเฟอเรนต์ เป็นต้น สามารถนำไปใช้ดำเนินกิจกรรมการเรียนการสอน สำหรับผู้สอนสามารถเปิดการพูดคุยในหัวข้อที่เกี่ยวข้องกับเนื้อหาในรายวิชา ซึ่งอาจจะอยู่ในรูปแบบการเปิดอภิปรายออนไลน์ การบรรยาย การสัมภาษณ์ผู้เชี่ยวชาญ เป็นต้น

3.2 ไปรษณีย์อิเล็กทรอนิกส์เป็นการติดต่อสื่อสารรูปแบบหนึ่งมีความสำคัญมากเพื่อให้ผู้เรียนติดต่อสื่อสารกับผู้สอนได้อย่างต่อเนื่อง หรือผู้เรียนอื่นๆ ในลักษณะรายบุคคล เช่น การส่งงานและผู้สอนสามารถให้ผลป้อนกลับ ให้คำแนะนำและปรึกษากับผู้เรียน เพื่อกระตุ้นให้ผู้เรียนเข้าร่วมกิจกรรมการเรียน

4. แบบฝึกหัด/แบบทดสอบ เป็นองค์ประกอบสุดท้ายของสื่อแบบอิเล็กทรอนิกส์ ได้แก่ การจัดให้ผู้เรียนได้มีโอกาสในการโต้ตอบกับเนื้อหา ในรูปแบบของการทำแบบฝึกหัดหรือแบบทดสอบความรู้ ซึ่งมีรายละเอียด ดังนี้

4.1 การจัดให้มีแบบฝึกสำหรับผู้เรียนตามเนื้อหาที่นำเสนอ จำเป็นอย่างยิ่งที่ต้องมีแบบฝึกเพื่อตรวจสอบความเข้าใจ ความรอบรู้ว่าเพียงพอหรือยัง ทั้งนี้เพราะสื่อแบบอิเล็กทรอนิกส์ เป็นระบบการเรียนการสอนที่เน้นการเรียนรู้ด้วยตนเองของผู้เรียนเป็นสำคัญ รวมถึงการทำให้ผู้เรียนทราบได้ว่าตนนั้นพร้อมสำหรับการทดสอบ การประเมินผลหรือไม่

4.2 การจัดให้มีแบบทดสอบผู้เรียน สามารถทำเป็นแบบทดสอบก่อนเรียน หรือระหว่างเรียน หรือหลังเรียน สำหรับสื่อแบบอิเล็กทรอนิกส์แล้ว ระบบบริหารจัดการรายวิชาสามารถสนับสนุนผู้สอนในการออกข้อสอบในหลายรูปแบบ ได้แก่ การประเมินผลในรูปแบบของอัตนัย ปรนัย ถูกผิด จับคู่ การส่งข้อความให้ครูผู้สอนตรวจ การส่งข้อความให้เพื่อนช่วยตรวจ ฯลฯ นอกจากนี้ยังทำให้ผู้สอนเกิดความสะดวกในการจัดการสอบ ในการทำคลังข้อสอบไว้เพื่อเลือกในการนำกลับมาใช้หรือปรับปรุง แก้ไขใหม่ได้

อย่างง่ายดาย ช่วยในเรื่องของการคำนวณ ตัดเกรดการประเมินผลผู้เรียน เช่น การเลือกประเมินผลผู้เรียนแบบระบบอิงกลุ่มหรืออิงเกณฑ์ การใช้สถิติในการคิดคำนวณ เช่น การใช้ค่าเฉลี่ย ค่า T-Score และแสดงผลในรูปแบบกราฟได้

ศิรินทิพย์ นันทวาศ (2555) ได้กล่าวถึงองค์ประกอบของสื่อแบบอิเล็กทรอนิกส์ในรูปแบบวิดีโอแบบปฏิสัมพันธ์ประกอบด้วยองค์ประกอบดังนี้

1. เนื้อหาของบทเรียน
2. ระบบบริหารการเรียนรู้
3. การติดต่อสื่อสาร
4. การสอบและการวัดผลการเรียน

2.1.3 รูปแบบการมีปฏิสัมพันธ์

แนวคิดการออกแบบวิดีโอสตรีมมิ่งแบบมีปฏิสัมพันธ์ผู้วิจัยได้สรุปรูปแบบการมีปฏิสัมพันธ์ระหว่างผู้เรียน ดังรายละเอียดต่อไปนี้

1. การมีปฏิสัมพันธ์กับข้อมูลประเภทตัวอักษร

1.1 การย่อขยายตัวอักษร ผู้เรียนสามารถทำได้โดยการใช้นิ้งกางออกบนหน้าจอ เพื่อขยายตัวอักษร หรือใช้สอบนิ้วที่กางออกหุบเนื้อหาเพื่อลดขนาดอักษร

1.2 การโต้ตอบแบบสอบถาม หรือแบบทดสอบ ผู้เรียนสามารถตอบคำถามเพื่อทบทวนจากตัวเลือกที่สามารถกำหนดให้เป็น ตัวเลือกประเภทข้อความ หรือตัวเลือกประเภทรูปภาพได้ ซึ่งจะมีการประเมินค่าย้อนกลับให้ผู้อ่านได้ทราบทันที

1.3 การป้ายสีให้กับข้อความเพื่อเน้นคำสำคัญ หรือส่วนสำคัญของเนื้อหา

1.4 การบันทึกข้อความเพิ่มเติมในส่วนของคำสำคัญ หรือเนื้อหาที่สำคัญ

2. การมีปฏิสัมพันธ์กับข้อมูลประเภทมัลติมีเดีย

2.1 ข้อมูลประเภทรูปภาพ ผู้เรียนสามารถย่อขยาย และเลื่อนดูส่วนประกอบของรูปภาพได้ โดยการสัมผัสบนรูปภาพทุกรูปภาพ เพื่อขยายมุมมองรูปภาพนั้นให้มีขนาดใหญ่ขึ้น สามารถใช้การแตะและลากนิ้ว ดูรายละเอียดต่างๆ ที่ปรากฏบนภาพนั้นได้ นอกจากนั้นหากเรียงในรูปแบบสมุดภาพ สามารถใช้นิ้วแตะและลากเพื่อเลื่อนไปดูภาพถัดไปได้ทันที

2.2 ข้อมูลประเภทภาพสามมิติ รูปแบบการมีปฏิสัมพันธ์ลักษณะคล้ายกับข้อมูลประเภทรูปภาพทั่วไป แต่สามารถขยาย และดูวัตถุได้โดยรอบแบบ 360 องศา

2.3 ข้อมูลประเภทวิดีโอ สามารถสัมผัสเพื่อเล่นภาพ ขยายมุมมองหน้าจอให้ขยายเต็มจอ ปรับเพิ่มความดังของเสียง หยุด กรอกลับ หรือเล่นต่อได้ผ่านเครื่องควบคุมการนำเสนอวิดีโอ

3. การมีปฏิสัมพันธ์กับข้อมูลประเภทภาษาที่ใช้ในการเขียนเว็บไซต์ การมีปฏิสัมพันธ์ในลักษณะนี้จะขึ้นอยู่กับจุดมุ่งหมายของข้อมูลที่ถูกเขียนขึ้น เช่น การกดปุ่มเพื่อแสดงรายละเอียดที่ซ่อนอยู่ หรือลากวางเพื่อให้เกิดเสียง เป็นต้น

2.1.4 วิดีโอปฏิสัมพันธ์

สุรพล โฉมฉายแสง (2550) วิดีโอปฏิสัมพันธ์ หมายถึง ระบบสื่อประสมชนิดหนึ่งที่ประกอบด้วยระบบของวีดิทัศน์ทำงานร่วมกับระบบไมโครคอมพิวเตอร์ โดยมีอุปกรณ์เชื่อมโยงระบบทั้งสองเข้าด้วยกัน การดำเนินไปของบทเรียนขึ้นอยู่กับการเลือกตอบสนองของผู้เรียนเป็นสำคัญ

พลากร ขุริมนต์ (2550) วิดีโอปฏิสัมพันธ์ หมายถึง บทเรียนที่ใช้คอมพิวเตอร์เป็นสื่อในการนำเสนอโดย การผสมผสานระหว่างเสียงกับภาพนิ่งและภาพเคลื่อนไหว ซึ่งผู้เรียนสามารถโต้ตอบกับบทเรียนได้โดยใช้เม้าส์เลือกรายการที่ปรากฏบนหน้าจอ

วิดีโอปฏิสัมพันธ์ หมายถึง ระบบสื่อประสมประกอบด้วยภาพเคลื่อนไหว ตัวอักษรและเสียงในรูปแบบการนำเสนอโดยการผสมผสานระหว่างเสียงกับภาพนิ่งและภาพเคลื่อนไหว ซึ่งผู้เรียนสามารถตอบโต้กับสื่อภาพเคลื่อนไหวได้ โดยผ่านอุปกรณ์อิเล็กทรอนิกส์

1. ประเภทของวิดีโอปฏิสัมพันธ์

Beardalee และคณะ (Beardalee, Edward C., and Davis, Geoffrey L. 1989 อ้างถึงใน สุรพล โฉมฉายแสง. 2550) ได้จำแนกประเภทของวิดีโอปฏิสัมพันธ์ออกเป็น 4 ระดับ โดยพิจารณาอุปกรณ์ที่ใช้และลักษณะของการปฏิสัมพันธ์ของผู้เรียนต่อระบบเป็นหลักสำคัญ ดังนี้

1.1 วิดีโอปฏิสัมพันธ์ระดับ 0 ระบบนี้ผู้เรียนจะไม่มีปฏิสัมพันธ์หรือการตอบสนองใดๆ กับระบบเลย แผ่นวีดิทัศน์เพียงแต่แสดงภาพไปเรื่อยๆ เป็นเส้นตรงตั้งแต่ต้นจนจบ

1.2 วิดีโอปฏิสัมพันธ์ระดับ 1 การมีปฏิสัมพันธ์ของผู้เรียนค่อนข้างจะถูกจำกัดในการเรียกภาพเดี่ยวให้ปรากฏขึ้นมาอย่างรวดเร็ว แม้กระทั้งการสั่งให้ภาพเคลื่อนไหวไปข้างหน้าหรือถอยหลังทั้งช้าหรือเร็ว เพราะไม่มีโปรแกรมภายในระบบหรือไม่มีคอมพิวเตอร์ควบคุมการทำงานของระบบ

1.3 วิดีโอปฏิสัมพันธ์ระดับที่ 2 โปรแกรมที่คอยควบคุมแผ่นวิดีโอที่ใช้เล่นนั้นจะถูกบันทึกลงในร่องเสียงของแผ่นวิดีโอแล้ว และจะถูกสั่งงานด้วยไมโครโพรเซสเซอร์ที่สร้างไว้ในเครื่องเล่นแผ่นวิดีโอนั้นเองจะไม่มีโปรแกรมหรือคอมพิวเตอร์จากภายนอกมาคอยควบคุมระบบแผ่นวิดีโอ

1.4 วิดีโอปฏิสัมพันธ์ระดับ 3 เป็นระดับที่ได้รับความนิยมมากที่สุดเป็นระดับที่ผู้เรียนมีปฏิสัมพันธ์สูงสุดของระบบ เนื่องด้วยมีโปรแกรมควบคุมจากระบบคอมพิวเตอร์ภายนอกตัวระบบวิดีโอ

จากการศึกษาวิดีโอปฏิสัมพันธ์ผู้วิจัยเลือกรูปแบบของวิดีโอปฏิสัมพันธ์ในระดับที่ให้ผู้เรียนสามารถควบคุมวิดีโอได้อย่างสมบูรณ์ สามารถควบคุมการรับชมวิดีโอ และสามารถปฏิสัมพันธ์กับแบบฝึกหัดแบบทดสอบในแต่ละช่วงของวิดีโอได้อย่างมีประสิทธิภาพ

2.2 ความรู้เกี่ยวกับความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และการสื่อสารข้อมูล

2.2.1 ความหมายและหลักการความมั่นคงปลอดภัย

กรกช วิไลลักษณ์ (2558) ได้กล่าวว่า เมื่อกล่าวถึงการรักษาความมั่นคงปลอดภัย สิ่งที่ผู้คนโดยทั่วไปคำนึงถึงเป็นสิ่งแรกคือการค้นหาการบุกรุกของผู้ไม่ประสงค์ดีกับระบบคอมพิวเตอร์ซึ่งนิยมเรียกว่า “ แฮกเกอร์ ” รวมถึงการกำจัดโปรแกรมที่ถูกพัฒนาขึ้นเพื่อทำลายความมั่นคงปลอดภัยของคอมพิวเตอร์หรือมัลแวร์ประเภทต่าง ๆ โดยไม่ตระหนักรู้ถึงความหมายที่แท้จริงของ ” ความมั่นคงปลอดภัย “ ของระบบ

คอมพิวเตอร์ซึ่งแท้จริงแล้วมีความหมายครอบคลุมถึง การรักษาความลับ การรักษาความครบถ้วนสมบูรณ์และการรักษาความพร้อมใช้ของทรัพยากรในระบบคอมพิวเตอร์ในทุก ๆ ระดับ เริ่มต้นตั้งแต่อุปกรณ์ฮาร์ดแวร์ ระบบปฏิบัติการซอฟต์แวร์ต่าง ๆ ที่ถูกติดตั้ง และการเชื่อมต่อกันเป็นเครือข่าย และรวมถึงข้อมูลหรือสารสนเทศซึ่งถูกจัดเก็บและประมวลผลโดยอุปกรณ์และซอฟต์แวร์ที่เชื่อมต่อเป็นระบบ ความหมายของการรักษาความมั่นคงปลอดภัยในระบบคอมพิวเตอร์จึงมีขอบเขตมากกว่าการรักษาความมั่นคงปลอดภัยให้กับคอมพิวเตอร์หรืออุปกรณ์เพียงอย่างเดียว

1. ทรัพยากรสารสนเทศ

ทรัพยากรสารสนเทศ มีความหมายครอบคลุมถึงเครื่องคอมพิวเตอร์และอุปกรณ์เชื่อมต่อต่าง ๆและครอบคลุมถึงองค์ประกอบอื่น ๆ ดังต่อไปนี้

1.1 มนุษย์ (people) ได้แก่ ผู้ที่เกี่ยวข้องกับระบบคอมพิวเตอร์เช่น ผู้ใช้งาน ผู้ดูแลระบบ ทั้งนี้โดยปกติแล้วมนุษย์จะถูกประเมินเป็นภัยคุกคามหลักต่อทรัพยากรสารสนเทศเนื่องจากมีเป็นทรัพยากรที่เป็นมีจุดอ่อนมากที่สุดในการรักษาความมั่นคงปลอดภัย แม้ว่าทรัพยากรอื่น ๆ จะถูกปกป้องและกำหนดมาตรการอย่างรัดกุมที่สุดแล้ว หากผู้คนที่เกี่ยวข้องกับทรัพยากรนั้นละเลย หรือขาดความตระหนักรู้ก็จะส่งผลให้ทรัพยากรนั้นถูกโจมตีสำเร็จ เช่น การให้บริการรับฝากไฟล์ผ่านอินเทอร์เน็ตซึ่งเลือกใช้เทคโนโลยีการรักษาความมั่นคงปลอดภัยที่เข้มแข็งมาก แต่ผู้ใช้งานบันทึกข้อมูลสำหรับใช้พิสูจน์ตัวจริงและกำหนดสิทธิ์โดยเขียนลงบนกระดาษแปะไว้ที่หน้าจอมอินเตอร์ย่อมเป็นการเพิ่มความเสี่ยงที่จะมีผู้ไม่ประสงค์ดีใช้ข้อมูลดังกล่าวเข้าถึงข้อมูลที่ถูกจัดเก็บในระบบนั้น โดยอาจเปลี่ยนแปลง แก้ไข หรือลบข้อมูลนั้นโดยไม่ได้รับอนุญาต เป็นต้น นอกจากนี้มนุษย์ยังเป็นองค์ประกอบสำคัญของการโจมตีความมั่นคงปลอดภัยของระบบคอมพิวเตอร์ด้วยเหตุจูงใจที่หลากหลาย เช่น ความต้องการชื่อเสียง ความโลภ แนวทางทางการเมืองโดยเมื่อโจมตีสำเร็จอาจได้รับค่าจ้างหรือการยอมรับจากสังคมที่เขาต้องการ เป็นต้น

1.2 ฮาร์ดแวร์และอุปกรณ์ต่อเชื่อมต่าง ๆ (hardware and its peripheral) ในที่นี้มีความหมายรวมถึงเครื่องคอมพิวเตอร์แท็บเล็ต และสมาร์ทโฟนซึ่งมีความสามารถในการรับข้อมูล ประมวลผล แสดงผลและเชื่อมต่อกับเครือข่ายคอมพิวเตอร์ได้ ความไม่มั่นคงปลอดภัยของอุปกรณ์เหล่านี้อาจเกิดขึ้นเนื่องจากมีภัยคุกคามเกิดขึ้นกับอุปกรณ์โดยตรง เช่น การขโมย ซึ่งส่งผลให้เจ้าของไม่สามารถใช้งานได้หรือนำข้อมูลส่วนบุคคลในอุปกรณ์นั้นไปเปิดเผยทำให้ความลับของข้อมูลนั้นถูกทำลายลงหรืออาจเกิดจากไฟฟ้ากระชากและทำให้ข้อมูลที่จัดเก็บในอุปกรณ์นั้น ๆ เสียหาย นอกจากนี้ยังรวมถึงการที่ฮาร์ดแวร์ นั้น ๆ ถูกทำลาย หรือทำให้ใช้การไม่ได้โดยมีสาเหตุจากธรรมชาติเช่น น้าท่วม ฟ้าผ่าอุปกรณ์ เป็นต้น

1.3 ซอฟต์แวร์ (software) ที่ถูกพัฒนาขึ้นมักมีข้อบกพร่องที่เกี่ยวข้องกับความมั่นคงปลอดภัยเนื่องจากคุณสมบัตินี้มักถูกละเลยในระหว่างขั้นตอนการวิเคราะห์และพัฒนาซอฟต์แวร์นั้น ๆ ทำให้เมื่อมีการนำมาใช้งานมักจะมีช่องโหว่ที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัย เช่น อุปกรณ์เร้าเตอร์สำหรับใช้งานอินเทอร์เน็ตสำหรับเชื่อมต่อผ่านระบบเอดีเอสแอลบางรุ่นมีข้อบกพร่องเกี่ยวกับความมั่นคงปลอดภัยและเมื่อผู้ไม่ประสงค์ดีโจมตีระบบสำเร็จจะสามารถปลอมแปลงกระบวนการสอบถามโดเมนได้ เป็นต้นดังนั้นผู้ใช้งาน หรือผู้ดูแลระบบจะต้องดำเนินการการปรับปรุงคุณสมบัติซอฟต์แวร์ตามหลังอยู่เสมอ ๆ ทั้งนี้

การปรับปรุงคุณสมบัติดังกล่าว ผู้พัฒนาซอฟต์แวร์อาจสร้างช่องโหว่ที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยเพิ่มมากขึ้นโดยไม่ได้ตั้งใจก็เป็นได้

1.4 ข้อมูลและสารสนเทศ (data and information) เป็นทรัพยากรที่สำคัญต่อบุคคลหรือองค์กรที่เป็นผู้สร้าง ประมวลผล และรับส่งข้อมูลสารสนเทศนั้น ๆ ด้วยเหตุนี้ทรัพยากรนี้จึงเป็นเป้าหมายหลักของการโจมตีของผู้ไม่ประสงค์ดีโดยผลเสียหายที่เกิดขึ้นมักจะเกิดขึ้นในสามลักษณะสำคัญคือ การเปิดเผยความลับการแก้ไขข้อมูลโดยไม่มีสิทธิ์และการทำให้ข้อมูลนั้น ๆ ไม่สามารถเข้าถึงได้เช่น ถูกลบ เปลี่ยนแปลงสิทธิ์ หรือถูกเข้ารหัสลับเพื่อเรียกค่าไถ่ เป็นต้น

1.5 ขั้นตอนระเบียบวิธีปฏิบัติ (procedure) ขั้นตอนการดำเนินการกับข้อมูลมักถูกละเลยจากผู้ที่เกี่ยวข้องทำให้มีช่องโหว่ที่อาจทำให้เกิดการละเมิดความมั่นคงปลอดภัยได้เช่น องค์กรต่าง ๆ มักมีการฝึกอบรมพนักงานให้ดำเนินการอย่างใดอย่างหนึ่งกับซอฟต์แวร์ที่ใช้ในองค์กรในรูปแบบของคู่มือการทำงานทำให้พนักงานที่มีหน้าที่คล้ายคลึงกันสามารถใช้งานซอฟต์แวร์ได้เหมือน ๆ กัน โดยมักละเลยการสร้างความตระหนักรู้เกี่ยวกับการใช้งานซอฟต์แวร์อย่างมั่นคงปลอดภัยเป็นผลให้เกิดช่องโหว่ของการรักษาความมั่นคงปลอดภัยได้เช่น พนักงานบัญชีคนหนึ่งอาจเข้าใช้งานระบบเงินเดือนค้างไว้โดยไม่ได้ล็อกหน้าจอขณะพักรับประทานอาหารกลางวัน ผู้ไม่ประสงค์ดีอาจเข้าใช้งานซอฟต์แวร์และปรับเปลี่ยนข้อมูลในระบบบัญชีได้ เป็นต้น

1.6 เครือข่าย (network) ระบบสารสนเทศในปัจจุบันถูกเชื่อมต่อเข้าด้วยกันผ่านเครือข่ายการรับส่งข้อมูลไม่ว่าจะเป็นเครือข่ายส่วนตัว เครือข่ายเฉพาะบริเวณ และมักเชื่อมต่อกับเครือข่ายอินเทอร์เน็ตแม้ว่าการเชื่อมต่อกันดังที่ได้กล่าวมาจะสร้างความสามารถในการใช้งานทรัพยากรสารสนเทศร่วมกันจากระยะทางไกล และทำให้เกิดการใช้งานทรัพยากรอย่างมีประสิทธิภาพมากยิ่งขึ้น การเชื่อมต่อกันเป็นเครือข่ายยิ่งมีขนาดมากเท่าไรย่อมเป็นการเพิ่มความเสี่ยงที่ทรัพยากรจะถูกโจมตีและเพิ่มความยากในการรักษาความมั่นคงปลอดภัยมากยิ่งขึ้นเมื่อกล่าวโดยนัยแล้วจะเห็นว่า ทรัพยากรสารสนเทศมีองค์ประกอบสำคัญๆ ดังที่ได้กล่าวมาอย่างไรก็ดีทรัพยากรสารสนเทศอาจถูกินยามได้ในความหมายที่ใกล้เคียงกันแต่ถูกินยามขึ้นมาในระยะเริ่มต้นคือระบบคอมพิวเตอร์ซึ่งประกอบด้วย ฮาร์ดแวร์ซอฟต์แวร์มนุษย์และข้อมูล ซึ่งจะขาดองค์ประกอบสำคัญคือเครือข่ายและขั้นตอนวิธีปฏิบัติซึ่งเป็นองค์ประกอบที่สำคัญในปัจจุบันเนื่องจากการประยุกต์ใช้งานเทคโนโลยีสารสนเทศและการสื่อสารในปัจจุบันมีการแลกเปลี่ยนทรัพยากรกันผ่านช่องทางการสื่อสารและระบบเครือข่าย ตลอดจนการประมวลผลข้อมูลในปัจจุบันมีความซับซ้อนมากขึ้นกว่าในอดีต ดังนั้นเมื่อกล่าวถึงระบบคอมพิวเตอร์ในปัจจุบันจึงนิยมใช้คำว่าทรัพยากรสารสนเทศซึ่งมีความหมายครอบคลุมถึงทรัพยากรเครือข่ายและขั้นตอนวิธีปฏิบัติที่เกี่ยวข้อง

2.2.2 การรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์

การรักษาความมั่นคงปลอดภัย หมายถึง การทำให้มั่นใจได้ว่าทรัพยากรสารสนเทศที่มีอยู่มีความถูกต้องสมบูรณ์และพร้อมใช้งานสำหรับผู้ใช้งานที่ได้รับสิทธิ์ในการเข้าถึงทรัพยากรนั้น ๆ ในที่นี้จะยกตัวอย่างการรักษาความมั่นคงปลอดภัยของเครื่องคอมพิวเตอร์ส่วนบุคคลซึ่งจัดเก็บข้อมูลซึ่งอาจมีข้อมูลที่ไม่ต้องการให้ผู้อื่นล่วงรู้ ตลอดจนต้องการรักษาความครบถ้วนสมบูรณ์ของไฟล์ต่าง ๆ ที่ถูกจัดเก็บไว้ใน

คอมพิวเตอร์ไม่ให้ถูกทำลายโดยมัลแวร์และป้องกันการแพร่ระบาดของหนอนอินเทอร์เน็ต ซึ่งอาจทำให้เครื่องคอมพิวเตอร์ไม่สามารถใช้งานได้ นักศึกษาอาจพิจารณาตั้งพาสเวิร์ดเพื่อควบคุมการเข้าถึงเข้าถึงเครื่องคอมพิวเตอร์จัดการเข้ารหัสลับฮาร์ดดิสก์ติดตั้งซอฟต์แวร์ตรวจจับคอมพิวเตอร์ไวรัส และเปิดการใช้งานไฟร์วอลส่วนบุคคล 3 เป็นต้น โดยทั่วไปการจัดการความมั่นคงปลอดภัยของทรัพยากรสารสนเทศสามารถจำแนกตามเป้าหมายของการรักษาความมั่นคงปลอดภัยได้ดังต่อไปนี้

2.2.2.1 ความมั่นคงปลอดภัยเชิงกายภาพ (physical security) เพื่อป้องกันอุปกรณ์สิ่งของหรือบริเวณให้ปราศจากการเข้าถึงโดยไม่ได้รับอนุญาต และการใช้งานที่ไม่ถูกต้อง เช่น การตั้งรหัสผ่านเพื่อเข้าใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล สร้างห้องปฏิบัติการสำหรับระบบคอมพิวเตอร์และเครือข่าย การจัดให้มีระบบไฟสำรอง การจัดให้มีระบบดับเพลิง การจัดให้มีการพิสูจน์ตัวจริงก่อนเข้าถึงฮาร์ดแวร์หรือห้องที่ใช้จัดเก็บฮาร์ดแวร์ตลอดจนทรัพยากรเครือข่ายที่เกี่ยวข้อง เป็นต้น

2.2.2.2 ความมั่นคงปลอดภัยส่วนบุคคล (personnel security) เพื่อรักษาบุคลากรหรือกลุ่มของผู้ใช้งานที่ได้รับสิทธิ์ให้เข้าถึงและดำเนินงานได้อย่างมั่นคงปลอดภัย เช่น การกำหนดสิทธิ์ให้กับเจ้าหน้าที่ตามความรู้รับผิดชอบ โดยกำหนดให้เจ้าหน้าที่ทั่วไปไม่สามารถอ่านข้อมูลที่ถูกสร้างขึ้นโดยหัวหน้างานของตนเอง แต่สามารถแก้ไขและตรวจสอบผู้ทำการแก้ไขทรัพยากรนั้น ๆ ได้การบังคับให้ผู้ใช้งานเปลี่ยนรหัสผ่านเมื่อเข้าสู่ระบบในครั้งแรกและทุก ๆ สามเดือน เป็นต้น

2.2.2.3 ความมั่นคงปลอดภัยของการดำเนินงาน (operation security) เพื่อปกป้องหรือป้องกันกระบวนการทำงาน ตลอดจนกิจกรรมอื่น ๆ ที่เกี่ยวข้อง

2.2.2.4 ความมั่นคงปลอดภัยของการสื่อสาร (communication security) เพื่อป้องกันสื่อนำสัญญาณข้อมูลต่าง ๆ ที่รับส่งผ่านช่องทางการสื่อสาร โดยมุ่งเน้นการรักษาความมั่นคงปลอดภัยของอุปกรณ์ต่าง ๆที่เชื่อมต่อกันเป็นระบบสื่อสาร รวมถึงการแพร่สัญญาณให้มีความมั่นคงปลอดภัย เช่น การกำหนดมาตรการเฝ้าตรวจการดักรับข้อมูล การเข้ารหัสข้อมูลที่มีการรับส่งกันในเครือข่ายหรือระหว่างเครือข่าย การใช้บริการวีพีเอ็นในการเชื่อมต่อระบบคอมพิวเตอร์ระหว่างสาขาซึ่งทำให้มั่นใจได้ว่าการรับส่งข้อมูลระหว่างจุดจะถูกเข้ารหัสทำให้ผู้ไม่ประสงค์ดีที่ดักรับข้อมูลได้ไม่สามารถวิเคราะห์หรือแปลความหมายข้อมูลที่ดักรับได้ เป็นต้น

2.2.2.5 ความมั่นคงปลอดภัยของเครือข่าย (network security) เพื่อป้องกันการเข้าถึงอุปกรณ์ เครือข่ายต่าง ๆ และอุปกรณ์ที่นำมาเชื่อมต่อเข้ากับเครือข่าย เช่น การแบ่งเครือข่ายออกเป็นเครือข่ายย่อย ๆ เพื่อจำแนกกลุ่มผู้ใช้งานและระบบบริการต่าง ๆ รวมถึงการจัดให้มีการเฝ้าตรวจความมั่นคงปลอดภัย และการจัดให้มีการพิสูจน์ตัวจริงของผู้ใช้งานก่อนจึงจะสามารถใช้งานเครือข่ายได้จะเห็นได้ว่ามีความแตกต่างจากความมั่นคงปลอดภัยของการสื่อสารโดยมีขอบเขตที่แคบกว่าและพิจารณาทุกการเชื่อมต่อในบริเวณที่เกี่ยวข้อง เช่น ระบบเครือข่ายภายในบ้าน ระบบเครือข่ายภายในบริษัท เป็นต้น

2.2.2.6 ความมั่นคงปลอดภัยของข้อมูลข่าวสาร (information security) เพื่อรักษาความลับ ความครบถ้วนสมบูรณ์และความพร้อมใช้ขององค์ประกอบต่าง ๆ ที่ถูกผนวกรวมเข้าเป็นระบบสารสนเทศ นับตั้งแต่กระบวนการสร้าง ประมวลผล และการรับส่งสารสนเทศนั้น ๆ

2.2.3 หลักการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์

ในการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประกอบด้วย 2 หลักการได้แก่ หลักการพื้นฐาน และหลักการอื่น ๆ ที่เกี่ยวข้องกับความมั่นคงปลอดภัย

2.2.3.1 หลักการพื้นฐาน การรักษาความมั่นคงปลอดภัยจะสำเร็จได้ก็ต่อเมื่อองค์กรหรือบุคคลนั้น ๆ ได้มีการจัดการกำหนดนโยบายที่เกี่ยวข้อง การควบคุมการดำเนินการให้เป็นไปตามนโยบาย การเสริมสร้างความรู้ความเข้าใจที่เกี่ยวข้อง การฝึกอบรม การสร้างความตระหนักรู้และการประยุกต์ใช้เทคโนโลยีที่เกี่ยวข้องอย่างเหมาะสม

1. การรักษาความลับ (confidentiality) หมายถึง กระบวนการ มาตรการและการจัดการที่เกี่ยวข้องกับการรักษาความลับของสารสนเทศที่ถูกประมวลผลส่งต่อและจัดเก็บให้สามารถเข้าถึงและเข้าใจความหมายได้เฉพาะผู้ที่มีสิทธิ์เข้าถึงทรัพยากรนั้น ๆ ตัวอย่างข้อมูลที่ควรมีการจัดเก็บและมีการกำหนดมาตรการควบคุมการเข้าถึงเพื่อรักษาความลับของข้อมูลที่สำคัญ

2. การรักษาความครบถ้วนสมบูรณ์ (integrity) หมายถึง กระบวนการมาตรการและการจัดการที่เกี่ยวข้องกับการตรวจสอบความครบถ้วนสมบูรณ์ของสารสนเทศที่ถูกประมวลผลส่งต่อและจัดเก็บให้มีความถูกต้องสมบูรณ์และสามารถตรวจสอบความครบถ้วนสมบูรณ์นั้นได้

3. การรักษาความพร้อมใช้ (availability) หมายถึง กระบวนการมาตรการและการจัดการที่เกี่ยวข้องกับการรักษาความพร้อมใช้ของสารสนเทศที่ถูกประมวลผล ส่งต่อและจัดเก็บให้มีความพร้อมใช้อยู่เสมอ ทำให้ผู้ใช้ที่มีสิทธิ์เข้าถึงและใช้งานทรัพยากรสารสนเทศนั้น ๆ สามารถเข้าใช้งานได้เช่น เมื่อกล่าวถึงความพร้อมใช้ของระบบบริการธนาคารอิเล็กทรอนิกส์อาจหมายถึงลูกค้าสามารถเข้าถึงและใช้งานบริการนั้นได้เสมอตลอด 24 ชั่วโมง และอาจหมายรวมถึงเจ้าหน้าที่ๆเกี่ยวข้องสามารถเข้าถึงและบริหารจัดการซอฟต์แวร์นั้นได้ เป็นต้น

2.2.3.2 หลักการอื่น ๆ ที่เกี่ยวข้องกับความมั่นคงปลอดภัย การรักษาความมั่นคงปลอดภัยทรัพยากรสารสนเทศจึงเป็นกระบวนการเชิงบริหารที่นำเอานโยบาย การดำเนินงาน และการประยุกต์ใช้เทคโนโลยีที่เกี่ยวข้องเพื่อป้องกันและจำกัดผลเสียหายต่อการรักษาความลับ ความครบถ้วนสมบูรณ์และความพร้อมใช้ของทรัพยากรสารสนเทศนั้น ๆ

1. ช่องโหว่ (vulnerability) คือความบกพร่องหรือจุดอ่อนที่มีอยู่ในทรัพยากรสารสนเทศโดยเป็นผลมาจากการออกแบบ การพัฒนาซอฟต์แวร์การจัดการกระบวนการทำงาน หรือการบำรุงรักษาระบบนั้น ๆ เช่น ช่องโหว่ของระบบปฏิบัติการช่องโหว่ของซอฟต์แวร์เว็บบราวเซอร์การอนุญาตให้ผู้ไม่มีบัตรเข้าถึงห้องสำคัญๆ ที่เกี่ยวข้องกับกระบวนการทำงานโดยไม่มีการตรวจสอบหรือการไม่ควบคุมให้มีการตรวจสอบเอกสารลับก่อนการทิ้งขยะ เป็นต้น เมื่อพิจารณาตามกลุ่มของทรัพยากรจะสามารถจำแนกประเภทของช่องโหว่ได้ 3 ลักษณะ ดังต่อไปนี้

1.1 ช่องโหว่ที่เกี่ยวข้องกับฮาร์ดแวร์หมายถึง ข้อบกพร่องที่เกี่ยวข้องกับความมั่นคงปลอดภัยของฮาร์ดแวร์เช่น ช่องโหว่ของการเข้ารหัสของระบบขายปลีกครบวงจร (Point of Sale; POS)ซึ่งส่งผลให้ผู้โจมตีสามารถขโมยข้อมูลบัตรเครดิตของผู้ใช้บริการ4 หรือช่องโหว่ของ

ระบบสมองกลที่ใช้ควบคุมรถยนต์ ที่เมื่อถูกโจมตีผ่านเครือข่ายแล้วจะทำให้ผู้โจมตีสามารถควบคุมการระบบควบคุมภายในรถยนต์ คันนั้น ๆ ได้ 5 เป็นต้น

1.2 ช่องโหว่ที่เกี่ยวข้องกับซอฟต์แวร์หมายถึง ข้อบกพร่องที่เกี่ยวข้องกับซอฟต์แวร์ต่าง ๆ ที่เมื่อเกิดการโจมตีต่อซอฟต์แวร์นั้น ๆ แล้วจะส่งผลกระทบต่อความมั่นคงปลอดภัยของซอฟต์แวร์ และซอฟต์แวร์ระบบอื่น ๆ ที่เกี่ยวข้อง เช่น ช่องโหว่ของระบบปฏิบัติการที่เกี่ยวข้องกับการแชร์ไฟล์ผ่านระบบเครือข่ายคอมพิวเตอร์ที่หากผู้ไม่ประสงค์ดีโจมตีตอบริการแชร์ไฟล์สำเร็จอาจทำการลบโฟลเดอร์หรือไฟล์ต่าง ๆ โดยไม่ได้รับอนุญาต เป็นต้น

1.3 ช่องโหว่ที่เกี่ยวข้องกับการบริหารจัดการข้อมูล หมายถึง ข้อบกพร่องที่เกี่ยวข้องกับการจัดการข้อมูลต่าง ๆ ทั้งที่เป็นข้อมูลที่ไม่ได้จัดเก็บในรูปแบบดิจิทัล และข้อมูลในรูปแบบดิจิทัล เช่น หากองค์กรหรือบุคคลจัดเก็บข้อมูลซึ่งใช้ในการพิสูจน์ตัวจริงอย่างไม่เหมาะสม เมื่อข้อมูลนั้นรั่วไหลออกไปอาจส่งผลให้เกิดการโจมตีต่อองค์กรนั้น ๆ ได้หรือเปิดโอกาสให้มีการโจมตีต่อทรัพยากรอื่น ๆ เป็นต้น

2. ภัยคุกคาม (threat) คือบุคคลหรือผู้ใดก็ตามที่สามารถใช้ประโยชน์จากช่องโหว่ที่มีเข้าถึงและทำลายความมั่นคงปลอดภัยของทรัพยากรสารสนเทศได้ ภัยคุกคามต่อทรัพยากรสารสนเทศจำแนกได้ 4 ลักษณะ คือ

2.1 การดักรับ (interception) หมายถึง เหตุการณ์ที่ผู้ไม่ประสงค์ดีเข้าถึงหรือดักรับข้อมูลโดยปราศจากสิทธิ์โดยถูกต้อง เช่น การดักรับที่รับส่งกันระหว่างผู้รับและผู้ส่งในระบบเครือข่ายคอมพิวเตอร์ (sniffing) การแอบอ่านข้อมูลจากหน้าจอของผู้อื่น การแอบฟังผู้อื่นพูดคุยกันเพื่อให้ได้ข้อมูลที่ตนเองไม่มีสิทธิ์เข้าถึง

2.2 การขัดจังหวะ (interruption) หมายถึง เหตุการณ์ที่ผู้ไม่ประสงค์ดีกระทำแล้วส่งผลให้ผู้ใช้งานที่มีสิทธิ์ไม่สามารถเข้าถึงหรือใช้งานทรัพยากรนั้น ๆ ได้เช่น การตัดสายสัญญาณเครือข่ายการลบไฟล์ข้อมูล การทำลายคอมพิวเตอร์ หรือการนำเข้าข้อความที่ระบบประมวลผลแล้วทำให้ระบบปฏิเสธการให้บริการ เป็นต้น

2.3 การดัดแปลงแก้ไข (modification) หมายถึง การเข้าถึงและแก้ไขทรัพยากรสารสนเทศโดยไม่มีสิทธิ์เช่น การเปลี่ยนแปลงการปรับตั้งค่าต่าง ๆ ของระบบปฏิบัติการการอนุญาตให้มีการเข้าถึงจากระยะไกลโดยไม่มีการพิสูจน์ตัวจริง ซึ่งอาจส่งผลกระทบต่อความมั่นคงปลอดภัย การดักรับโดยการเปลี่ยนเส้นทางและการเปลี่ยนแปลงข้อมูลที่ถูกรับส่งผ่านเครือข่าย เป็นต้นโดยการดัดแปลงแก้ไขดังกล่าวอาจกระทำได้ในกรณีอื่น ๆ เช่น เพื่อนของนักศึกษาอาจแก้ไขไฟล์รายงานของนักศึกษาที่ถูกบันทึกไว้ในสื่อจัดเก็บข้อมูล เช่น แฟลชไดร์ฟโดยที่นักศึกษาไม่ทราบ เมื่อนักศึกษาส่งรายงานไปยังอาจารย์จึงพบว่าข้อมูลนั้นไม่ใช้ข้อมูลที่ถูกต้อง เป็นต้น

2.4 การปลอมแปลง (fabrication) หมายถึง การสร้างข้อมูลหรือสิ่งแปลกปลอมเข้าสู่ระบบสารสนเทศ เช่น การเพิ่มข้อมูลลงในระบบจัดการฐานข้อมูล การตั้งเครือข่ายไร้สายที่มีชื่อสถานีเหมือนกับเครือข่ายเป้าหมาย เพื่อดักรับข้อมูลต่าง ๆ และการปลอมแปลงหมายเลขไอพีเพื่อหลบ

เลี่ยงกลไกพิสูจน์ ตัวจริงเพื่อเข้าใช้งานเครือข่าย การปลอมแปลงตนเองเป็นบุคคลอื่นเพื่อหลอกถามข้อมูล เป็นต้น วัตถุประสงค์หลักของการปลอมแปลงจึงเกี่ยวข้องกับการล่อลวงให้เหยื่อเข้าใจผิดว่าข้อมูลหรือสารสนเทศนั้นเป็นข้อมูลหรือตัวตนจริง ๆ ของผู้นั้น หากเหยื่อตายใจและให้ข้อมูลหรือเปิดเผยข้อมูลสำคัญจะทำให้เกิดการละเมิดความมั่นคงปลอดภัยต่อเหยื่อนั้น ๆ เช่น การส่งจดหมายโดยอ้างว่าผู้ส่งเป็นหัวหน้างานและให้ส่งความลับขององค์กรไปยังอีเมล หรือให้จัดพิมพ์เอกสารแล้วส่งไปยังผู้โจมตี เป็นต้น

2.2.3.3 การโจมตี (attack) คือการกระทำหรือผลที่เกิดขึ้นเมื่อเกิดภัยคุกคามต่อช่องโหว่ต่าง ๆ ที่มีอยู่ในทรัพยากรสารสนเทศ ทั้งนี้การโจมตีอาจไม่ได้มีต้นกำเนิดจากผู้ไม่ประสงค์ดีแต่เพียงอย่างเดียวก็เป็นได้เช่น ทรัพยากรสารสนเทศหนึ่งมีความลับไม่ควรถูกเผยแพร่ให้ผู้ไม่มีหน้าที่เกี่ยวข้องรับทราบ แต่ไม่ถูกกำหนดมาตรการควบคุมการเข้าถึงอย่างเหมาะสม อาจถูกเข้าถึงโดยผู้ใช้งานทั่วไป และนำข้อมูลนั้นไปเผยแพร่อันเป็นการทำลายความลับของทรัพยากรนั้น ๆ ทั้งนี้การกระทำดังกล่าวอาจเกิดขึ้นโดยเจตนาหรืออาจเกิดขึ้นจากอุบัติเหตุ การโจมตีอีกลักษณะหนึ่งที่ได้รับความนิยมคือการโจมตีต่อโครงสร้างพื้นฐานที่สำคัญของเป้าหมาย เช่น การทำให้ระบบปฏิเสธการให้บริการและการโจมตีด้วยเทคนิคเชิงสังคมอื่น ๆ เช่น การแอบอ้างเป็นพนักงานคอลเซนเตอร์เพื่อล่อลวงเป้าหมายให้กระทำการอย่างใดอย่างหนึ่งโดยเปิดเผยข้อมูลพิสูจน์ตัวจริงหรือการหลอกลวงให้ทำรายการบัญชีผ่านเอทีเอ็ม เป็นต้น

2.2.3.4 ผู้ไม่ประสงค์ดี (attacker) คือบุคคลหรือกี่ระบวนการที่เกิดขึ้นจากมนุษย์เพื่อกระทำการโจมตีต่อทรัพยากรสารสนเทศเป้าหมาย จากินยามดังกล่าวจะเห็นได้ว่ามีความหมายใกล้เคียงกับภัยคุกคามแต่จำกัดสาเหตุไว้ที่มนุษย์เท่านั้น ซึ่งผู้ไม่ประสงค์ดีอาจมีแรงจูงใจในการโจมตีต่อระบบที่แตกต่างกันออกไปเช่น ความประมาท ค่าตอบแทน และความสะใจ เป็นต้น ในปัจจุบันนิยมใช้คำว่า แฮกเกอร์ (hacker) สามารถจำแนกประเภทจากแรงจูงใจในการโจมตีต่อระบบได้หลายลักษณะ เช่น แฮกเกอร์สมัครเล่น แฮกเกอร์ หมวกขาว แฮกเกอร์หมวกดำ เป็นต้น

1. แฮกเกอร์มือสมัครเล่น (script kiddy) หมายถึง บุคคลทั่วไปที่โจมตีต่อช่องโหว่ของระบบด้วยเครื่องมือหรือซอฟต์แวร์ที่ผู้ไม่ประสงค์ดีคนอื่นเผยแพร่ไว้โดยปราศจากความเข้าใจถึงกระบวนการทำงานของซอฟต์แวร์นั้น ๆ รวมไปถึงบุคคลทั่ว ๆ ไปที่ล่วงรู้ช่องโหว่ของการรักษาความมั่นคงปลอดภัยที่เข้าถึงหรือแก้ไขทรัพยากรที่ไม่มีสิทธิ์โดยไม่ได้ตั้งใจ เช่น การลบไฟล์เอกสารที่ใช้งานร่วมกันผ่านเครือข่ายได้เนื่องจากผู้ดูแลระบบกำหนดสิทธิ์ไว้ผิด เป็นต้น

2. แฮกเกอร์หมวกขาว (white hat) หมายถึง ผู้เชี่ยวชาญระบบคอมพิวเตอร์ที่ใช้ความสามารถดังกล่าวในการค้นหาช่องโหว่ และการโจมตีต่อระบบคอมพิวเตอร์ในเชิงป้องกันและรักษาความมั่นคงปลอดภัยให้กับระบบแล้วรายงานช่องโหว่หรือการโจมตีดังกล่าวต่อเจ้าของหรือผู้มีหน้าที่รับผิดชอบเพื่อให้ผู้ที่เกี่ยวข้องดำเนินการปรับปรุงความมั่นคงปลอดภัยและแก้ไขข้อบกพร่องนั้น ๆ ก่อนที่ช่องโหว่หรือข้อบกพร่องดังกล่าวจะถูกตรวจพบหรือถูกประกาศให้ทราบในที่สาธารณะ เช่น เว็บบอร์ดหรืออินเตอร์เน็ต เป็นต้น

3. แฮกเกอร์หมวกดำ (blackhat) หมายถึง ผู้เชี่ยวชาญระบบคอมพิวเตอร์ที่ใช้ความสามารถดังกล่าวในการค้นหาและโจมตีต่อระบบคอมพิวเตอร์ เพื่อการทำลายความมั่นคงปลอดภัยโดย

มีผลประโยชน์ส่วนตัวเป็นแรงจูงใจ เช่น ค่าตอบแทนจากองค์กรอาชญากรรม การล้างแค้น หรือความคิดเห็นทางการเมือง เป็นต้น

2.2.3.5 เอกซ์พลอยต์ (exploit) คือแม้ว่าเอกซ์พลอยต์จะมีความหมายตามพจนานุกรมว่า “การใช้ประโยชน์หรือการทำประโยชน์” แต่เอกซ์พลอยต์ในที่นี้จะหมายถึงการโจมตีต่อช่องโหว่ที่มีในระบบสารสนเทศ เพื่อทำลายความมั่นคงปลอดภัย หรือเข้าใช้ประโยชน์จากช่องโหว่ที่มีอยู่ เช่น ช่องโหว่ของระบบจัดการเนื้อหาผ่านเว็บที่ถูกค้นพบและรายงาน อาจมีผู้ไม่ประสงค์ดีพัฒนาโปรแกรมที่สามารถโจมตีต่อช่องโหว่ดังกล่าวสำเร็จ แล้วแจกจ่ายให้กับผู้ที่สนใจนำโปรแกรมนี้ไปโจมตีต่อช่องโหว่นั้น นอกจากนี้ยังหมายถึงเทคนิควิธีที่ใช้ในการโจมตีด้วยเทคนิควิศวกรรมเชิงสังคม เช่น การพยายามตีสนิทกับเหยื่อซึ่งทำหน้าที่สำคัญในระบบสารสนเทศเพื่อให้ได้มาซึ่งข้อมูลที่เป็นประโยชน์ต่อการโจมตีหรือการล่อลวงเพื่อใช้ประโยชน์จากเหยื่อในการเข้าถึงทรัพยากรสารสนเทศ เป็นต้น

2.2.3.6 เป้าหมาย (target) คือบุคคล องค์กร ทรัพยากรสารสนเทศที่มีช่องโหว่และได้รับผลกระทบโดยตรงจากการการโจมตีที่อาจเกิดขึ้น

2.2.3.7 วิธีการโจมตี (attack vector) คือกระบวนการวิธีการเครื่องมือและเทคนิคที่ใช้โจมตีต่อช่องโหว่ที่มีในเป้าหมายของการโจมตี

บทที่ 3
วิธีดำเนินการวิจัย

ในการพัฒนาสื่อวิดีโอสตรีมมิ่งแบบปฏิสัมพันธ์ เรื่อง ความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และการสื่อสารข้อมูล คณะวิทยาการสื่อสาร มหาวิทยาลัยสงขลานครินทร์ ผู้วิจัยได้ดำเนินการดังนี้

3.1 ประชากรและกลุ่มตัวอย่าง

3.2 เครื่องมือที่ใช้ในการวิจัย

3.3 การเก็บรวบรวมข้อมูล

3.4 การวิเคราะห์ข้อมูล

3.1 ประชากรและกลุ่มตัวอย่าง

ประชากร

ประชากรที่ในการศึกษาวิจัยครั้งนี้ ได้แก่ นักศึกษาระดับปริญญาตรี สาขาวิชาเทคโนโลยีสารสนเทศและการสื่อสารเพื่อการจัดการ คณะวิทยาการสื่อสาร มหาวิทยาลัยสงขลานครินทร์ วิทยาเขตปัตตานี ภาคเรียนที่ 2 ปีการศึกษา 2563 จำนวน 103 คน

กลุ่มตัวอย่าง

กลุ่มตัวอย่างที่ใช้ในการศึกษาวิจัยครั้งนี้ ได้แก่ นักศึกษาระดับปริญญาตรี สาขาวิชาเทคโนโลยีสารสนเทศและการสื่อสารเพื่อการจัดการ คณะวิทยาการสื่อสาร มหาวิทยาลัยสงขลานครินทร์ วิทยาเขตปัตตานี ได้มาจากการเลือกแบบเฉพาะเจาะจง (Purposive Sampling) จำนวน 63 คน

3.2 เครื่องมือที่ใช้ในการวิจัย

ในการพัฒนาสื่อวิดีโอสตรีมมิ่งแบบปฏิสัมพันธ์ เรื่อง ความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และการสื่อสารข้อมูล คณะวิทยาการสื่อสาร มหาวิทยาลัยสงขลานครินทร์ ผู้วิจัยได้สร้างเครื่องมือที่ใช้ในการวิจัยดังนี้

3.2.1 สื่อวิดีโอสตรีมมิ่งแบบปฏิสัมพันธ์ เรื่อง ความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และการสื่อสารข้อมูล คณะวิทยาการสื่อสาร มหาวิทยาลัยสงขลานครินทร์ โดยแบ่งเนื้อหาออกเป็น ความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และการสื่อสารข้อมูล ได้แก่ ความรู้เบื้องต้นความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และการสื่อสารข้อมูล หลักการพื้นฐานในการรักษาความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และการสื่อสารข้อมูล หลักการอื่นในการรักษาความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และการสื่อสารข้อมูล การเข้ารหัสและการถอดรหัส และการรักษาความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และการสื่อสารข้อมูลด้วยไฟร์วอลล์

3.2.2 แบบประเมินคุณภาพสื่อวิดีโอสตรีมมิ่งแบบปฏิสัมพันธ์ เรื่อง ความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และการสื่อสารข้อมูล คณะวิทยาการสื่อสาร มหาวิทยาลัยสงขลานครินทร์ จำนวน 10 ข้อ โดยใช้เกณฑ์ของลิเคิร์ท แบบ 5 ระดับ

ระดับคะแนน 5 หมายถึง คุณภาพระดับดีมาก

ระดับคะแนน 4 หมายถึง คุณภาพระดับดี

ระดับคะแนน 3 หมายถึง คุณภาพระดับปานกลาง

ระดับคะแนน 2 หมายถึง คุณภาพระดับน้อย

ระดับคะแนน 1 หมายถึง คุณภาพระดับน้อยที่สุด

3.2.3 แบบประเมินความพึงพอใจของผู้เรียนที่มีต่อวิดีโอสตรีมมิ่ง เรื่อง ความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และการสื่อสารข้อมูล คณะวิทยาการสื่อสาร มหาวิทยาลัยสงขลานครินทร์ จำนวน 15 ข้อ

ระดับคะแนน 5 หมายถึง ความพึงพอใจระดับมากที่สุด

ระดับคะแนน 4 หมายถึง ความพึงพอใจระดับมาก

ระดับคะแนน 3 หมายถึง ความพึงพอใจระดับปานกลาง

ระดับคะแนน 2 หมายถึง ความพึงพอใจระดับน้อย

ระดับคะแนน 1 หมายถึง ความพึงพอใจระดับมากน้อยที่สุด

ในการพัฒนาสื่อวิดีโอสตรีมมิ่งแบบปฏิสัมพันธ์ เรื่องความมั่นคงปอดภัยของระบบคอมพิวเตอร์และการสื่อสารข้อมูล คณะวิทยาการสื่อสาร มหาวิทยาลัยสงขลานครินทร์ ผู้วิจัยได้ดำเนินการวิจัยและพัฒนา ดังนี้

1. ขั้นเตรียมการ

ศึกษาแนวคิด วิเคราะห์ สังเคราะห์เอกสารและงานวิจัยที่เกี่ยวข้องกับระบบวิดีโอสตรีมมิ่งแบบปฏิสัมพันธ์ ความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และการสื่อสารข้อมูล

2. ขั้นสร้างเครื่องมือและทดสอบเครื่องมือ

2.1 ดำเนินการพัฒนาและทดสอบวิดีโอปฏิสัมพันธ์ เรื่อง ความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และการสื่อสารข้อมูล โดยใช้กระบวนการออกแบบและพัฒนาตามหลักของ ADDIE Model มี 5 ขั้นตอนดังนี้

2.1.1 การวิเคราะห์ (Analyst)

2.2.2 การออกแบบ (Design)

2.2.3 การสร้างและพัฒนา (Development)

2.2.4 การนำไปทดลองใช้ (Implement)

2.2.5 การประเมินผล (Evaluation)

2.2 ดำเนินการสร้างแบบประเมินเพื่อหาคุณภาพ เป็นแบบมาตราส่วนประมาณค่าและแบบปลายเปิดในส่วนท้ายของแบบประเมิน เพื่อสอบถามความคิดเห็นและข้อเสนอแนะต่างๆ โดยกำหนดค่าคะแนนเป็น 5 ระดับ ตามแนวคิดของลิเกิร์ต จากนั้นนำแบบประเมินที่สร้างขึ้นไปให้ผู้เชี่ยวชาญ จำนวน 5 คน ทำการประเมินคุณภาพ

2.3 ดำเนินการสร้างแบบประเมินความพึงพอใจผู้เรียน เป็นแบบมาตราส่วนประมาณค่าและแบบปลายเปิดในส่วนท้ายของแบบประเมิน เพื่อสอบถามความคิดเห็นและข้อเสนอแนะต่างๆ โดยกำหนดค่าคะแนนเป็น 5 ระดับ ตามแนวคิดของลิเกิร์ต

3. ขั้นดำเนินการทดลองและเก็บรวบรวมข้อมูล

นำสื่อวิดีโอสตรีมมิ่งแบบปฏิสัมพันธ์ เรื่อง ความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และการสื่อสารข้อมูล มาทดสอบกับกลุ่มตัวอย่างเพื่อหาประสิทธิภาพ โดยศึกษาผ่านบทเรียนวิดีโอปฏิสัมพันธ์ที่ได้พัฒนาขึ้นมา เปรียบเทียบความแตกต่างระหว่างผลการเรียน ก่อนเรียนและหลังเรียน โดยใช้สถิติ t-test จากนั้นให้กลุ่มตัวอย่างทำแบบประเมินความพึงพอใจ โดยใช้สถิติ ค่าคะแนนเฉลี่ย ($\bar{x}$) และส่วนเบี่ยงเบนมาตรฐาน (S.D.)

3.3 การเก็บรวบรวมข้อมูลและวิเคราะห์ข้อมูล

ผู้วิจัยได้ดำเนินการเก็บรวบรวมข้อมูลดังนี้

3.3.1 ขั้นการประเมินคุณภาพและประสิทธิภาพจากผู้เชี่ยวชาญ

ผู้วิจัยได้นำเสนอวิดีโอสตรีมมิ่งแบบปฏิสัมพันธ์ให้ผู้เชี่ยวชาญดำเนินการประเมินคุณภาพและประสิทธิ โดยผู้เชี่ยวชาญแสดงความคิดเห็นผ่านแบบประเมินคุณภาพและประสิทธิภาพของผู้เชี่ยวชาญ จากนั้นนำแบบประเมินมาวิเคราะห์ข้อมูล

3.4.2 การประเมินความพึงพอใจของผู้เรียน

หลังจากกลุ่มตัวอย่างได้เรียนรู้แล้ว ผู้วิจัยได้ให้กลุ่มตัวอย่างทำแบบสอบถามความพึงพอใจ จากนั้นนำแบบสอบถามมาวิเคราะห์ข้อมูล

3.4.3 การหาผลสัมฤทธิ์ทางการศึกษา

การหาผลสัมฤทธิ์ทางการศึกษาผู้วิจัยได้ให้ให้กลุ่มตัวอย่างทำแบบทดสอบก่อนเรียนระหว่างเรียนและหลังเรียน จากนั้นนำคะแนนแบบทดสอบมาตรวจนับและเปรียบเทียบผลการเรียนรู้

3.4 การวิเคราะห์ข้อมูล

1. การหาคุณภาพของบทเรียนวิดีโอสตรีมมิ่งแบบปฏิสัมพันธ์ เรื่อง ความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และการสื่อสารข้อมูล คณะวิทยาการสื่อสาร มหาวิทยาลัยสงขลานครินทร์ โดยใช้สูตร E1/E2

2. วิเคราะห์ข้อมูลเพื่อเปรียบเทียบความแตกต่างระหว่างผลการเรียน ก่อนเรียนและหลังเรียนด้วยบทเรียนวิดีโอสตรีมมิ่งแบบปฏิสัมพันธ์ เรื่อง ความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และการสื่อสารข้อมูล คณะวิทยาการสื่อสาร มหาวิทยาลัยสงขลานครินทร์ โดยใช้สถิติ t-test

3. ความพึงพอใจ ใช้เกณฑ์ ค่าคะแนนเฉลี่ย ($\bar{x}$) ส่วนเบี่ยงเบนมาตรฐาน (S.D.) และเกณฑ์การแปลความหมาย

3.5 สถิติที่ใช้ในการวิเคราะห์ข้อมูล

การศึกษาวิจัยในครั้งนี้ผู้วิจัยได้ใช้ค่าสถิติสำหรับการแปรผลข้อมูลดังนี้

3.5.1 ค่าร้อยละ ค่าเฉลี่ยและค่าความเบี่ยงเบนมาตรฐาน

3.5.1.1 ค่าร้อยละ (Percentage) ใช้สูตรดังนี้

$$P = \frac{f}{N} \times 100$$

เมื่อ P = ร้อยละ

f = ความถี่ต้องแปลงเป็นร้อยละ

N = จำนวนความถี่ทั้งหมด

3.5.1.2 ค่าเฉลี่ยเลขคณิต (Mean: $\bar{X}$) ใช้สูตรดังนี้

$$\bar{X} = \frac{\sum X}{N}$$

เมื่อ $\bar{X}$ = ค่าเฉลี่ยเลขคณิต

$\sum X$ = ผลรวมทั้งหมดของข้อมูล

N = จำนวนข้อมูล

3.5.1.3 ค่าความเบี่ยงเบนมาตรฐาน (S.D.:Standard Deviation) ใช้สูตรดังนี้

$$SD = \sqrt{\frac{\sum_{i=1}^{n}\left(x_i - \bar{x}\right)^2}{n-1}}$$

เมื่อ SD = ค่าส่วนเบี่ยงเบนมาตรฐาน

x = ข้อมูลแต่ละตัว

$\bar{X}$ = ค่าเฉลี่ยเลขคณิต

n = จำนวนข้อมูล

3.5.2 ค่าความยากง่าย (p) และค่าอำนาจจำแนก (r)

3.5.2.1 ค่าความยากง่าย (p) ใช้สูตรดังนี้

$$P = \frac{R}{N}$$

เมื่อ P = ค่าความยากง่าย

R = จำนวนคนที่ทำข้อนั้นถูก

N = จำนวนคนที่ทำข้อสอบนั้นทั้งหมด

3.5.2.2 ค่าอำนาจจำแนก (r) ใช้สูตรดังนี้

$$D = \frac{R_U - R_L}{\frac{N}{2}}$$

เมื่อ D = ค่าอำนาจจำแนก

R_U = จำนวนนักเรียนที่ตอบถูกในกลุ่มเก่ง

R_L = จำนวนนักเรียนที่ตอบถูกในกลุ่มอ่อน

N = จำนวนคนในกลุ่มเก่งและกลุ่มอ่อน

3.5.3 ค่าความเที่ยงตรงเชิงเนื้อหา (IOC : Item Objective Congruence) ใช้สูตรดังนี้

$$IOC = \frac{\sum R}{N}$$

เมื่อ IOC = ดัชนีความสอดคล้องระหว่างข้อสอบกับจุดประสงค์

R = ผลรวมของคะแนนความคิดเห็นของผู้เชี่ยวชาญทั้งหมด

N = จำนวนผู้เชี่ยวชาญทั้งหมด

3.5.4 ค่าความเชื่อมั่นของแบบทดสอบ โดยใช้วิธีของคูเดอร์ ริชาร์ดสัน (KR-20) (Kuder Richardson Method) (พวงทิพย์ ทวีรัตน์, 2540) ซึ่งมีสูตรดังนี้

$$r_{tt} = \frac{n}{n-1}\left[1 - \frac{\sum pq}{s_t^2}\right]$$

เมื่อ r_{tt} = ค่าความเชื่อมั่นที่คำนวณจากสูตร

n = จำนวนข้อของเครื่องมือวัด

p = สัดส่วนของผู้ตอบข้อสอบถูกแต่ละข้อ

q = สัดส่วนของผู้ตอบข้อสอบผิดแต่ละข้อ (1-p)

s_t^2 = ความแปรปรวนของคะแนนรวมทั้งหมด

บทที่ 4
ผลการวิจัย

การพัฒนาวิดีโอสตรีมมิ่งแบบปฏิสัมพันธ์ เรื่อง ความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และการสื่อสารข้อมูล คณะวิทยาการสื่อสารมหาวิทยาลัยสงขลานครินทร์ มีผลการศึกษาวิจัยดังนี้

4.1 ผลการพัฒนา การหาคุณภาพและประสิทธิภาพวิดีโอปฏิสัมพันธ์ เรื่อง ความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และการสื่อสารข้อมูล

4.2 ผลการเปรียบเทียบผลสัมฤทธิ์ทางการเรียนก่อนเรียนกับหลังเรียนของนักศึกษาที่เรียนด้วยวิดีโอปฏิสัมพันธ์ เรื่อง ความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และการสื่อสารข้อมูล

4.3 ผลการศึกษาความพึงพอใจของนักศึกษาที่มีต่อวิดีโอปฏิสัมพันธ์ เรื่อง ความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และการสื่อสารข้อมูล

4.1 ผลการพัฒนา การหาคุณภาพและประสิทธิภาพวิดีโอปฏิสัมพันธ์ เรื่อง ความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และการสื่อสารข้อมูล

ผู้วิจัยได้พัฒนาวิดีโอสตรีมมิ่งแบบปฏิสัมพันธ์ เรื่อง ความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และการสื่อสารข้อมูล คณะวิทยาการสื่อสารมหาวิทยาลัยสงขลานครินทร์ ดำเนินการพัฒนาวิดีโอปฏิสัมพันธ์ประกอบด้วยเนื้อหาภายในบทเรียน 5 หน่วยการเรียน ดังนี้

หน่วยที่ 1. ความรู้เบื้องต้นเกี่ยวกับความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และการสื่อสารข้อมูล

หน่วยที่ 2. หลักการพื้นฐานการรักษาความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และการสื่อสารข้อมูล

หน่วยที่ 3. หลักการอื่นในการรักษาความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และการสื่อสารข้อมูล

หน่วยที่ 4. การเข้ารหัสและถอดรหัส

หน่วยที่ 5. การรักษาความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และการสื่อสารข้อมูลด้วยไฟร์วอลล์

วิดีโอสตรีมมิ่งแบบปฏิสัมพันธ์ เรื่อง ความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และการสื่อสารข้อมูล พัฒนาขึ้นโดยใช้กระบวนการออกแบบและพัฒนาตามหลักของ ADDIE Model สร้างรูปแบบปฏิสัมพันธ์โดยใช้แบบทดสอบ โดยมีคุณภาพดังนี้

ตาราง 1. ผลการประเมินคุณภาพของวิดีโอสตรีมมิ่งแบบปฏิสัมพันธ์ เรื่อง ความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และการสื่อสารข้อมูล โดยผู้เชี่ยวชาญ จำนวน 5 ท่าน

รายการประเมิน	$\overline{X}$	**S.D.**	**ระดับของคุณภาพ**
ด้านภาพ	**4.52**	**0.55**	**ดีมาก**
1. ขนาดของภาพเคลื่อนไหวมีความน่าสนใจ	4.60	0.55	ดีมาก
2. ความเหมาะสมของภาพเคลื่อนไหว	4.40	0.55	ดี
3. ความชัดเจนในการสื่อความหมายของภาพเคลื่อนไหว	4.60	0.55	ดีมาก
4. คุณภาพของภาพเคลื่อนไหว	4.20	0.45	ดี
5. ความเหมาะสมของภาพประกอบเนื้อหา	4.60	0.55	ดีมาก
ด้านเสียง	**0.46**	**0.67**	**ดีมาก**
6. ความชัดเจนของเสียงบรรยาย	4.80	0.45	ดีมาก
7. ความเหมาะสมของเสียงดนตรี	4.40	0.89	ดี
ด้านเทคนิควิธีการ	**4.60**	**0.55**	**ดีมาก**
8. ความเหมาะสมในการลำดับภาพและเสียง	4.60	0.55	ดีมาก
9. สร้างความรู้และประสบการณ์ได้โดยตรง	4.60	0.55	ดีมาก
10. ความเหมาะสมของรูปแบบการนำเสนอ	4.80	0.45	ดีมาก
ด้านเนื้อหา	**4.67**	**0.50**	**ดีมาก**
11. เนื้อหามีความสอดคล้องกับจุดประสงค์	4.80	0.45	ดีมาก
12. แบ่งเนื้อหามีความเหมาะสม	4.60	0.55	ดีมาก
13. ความถูกต้องของเนื้อหา	4.80	0.45	ดีมาก
14. ความเหมาะสมในการจัดลำดับเนื้อหาการนำเสนอ	4.60	0.55	ดีมาก
15. บทเรียนมีแรงจูงใจ น่าสนใจในการเรียน	4.40	0.55	ดี
16. บทเรียนนำไปใช้งานได้จริง	4.80	0.45	ดีมาก
รวมเฉลี่ย	**4.60**	**0.53**	**ดีมาก**

จากตาราง 1. ผลการประเมินคุณภาพของบทเรียนวิดีโอสตรีมมิ่งแบบปฏิสัมพันธ์ เรื่อง ความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และการสื่อสารข้อมูล โดยผู้เชี่ยวชาญทั้ง 5 ท่าน พบว่า บทเรียนมีคุณภาพโดยรวมอยู่ในระดับดีมาก มีรายละเอียดดังนี้ ด้านภาพ ด้านเสียง ด้านเทคนิควิธีการ และด้านเนื้อหา มีคุณภาพระดับดีมาก

ข้อเสนอแนะจากผู้เชี่ยวชาญ

1. ปรับปรุงส่วนนำให้มีความตื่นเต้นและน่าสนใจมากขึ้น
2. ตัวอักษรมีขนาดเล็ก อ่านลำบาก

3. เสียงประกอบบางจังหวะดังเกินไป
4. ควรเพิ่มขนาดตัวอักษรให้ใหญ่ จัดข้อความให้ดูสวยงาม และควรมีการตัดคำ
5. ไม่มี

ผู้วิจัยได้ปรับปรุงคุณภาพให้ดีขึ้นตามข้อเสนอแนะของผู้เชี่ยวชาญ ดังนี้

1. ปรับปรุงส่วนนำให้มีความน่าสนใจและเร้าความสนใจมากขึ้น โดยใช้ภาพกราฟิก และใช้วิธีการแสดงภาพแบบ STOP Motion ประกอบเสียงเพลงบรรเลง
2. ปรับปรุงขนาดตัวอักษรใหญ่ขึ้นและเน้นใช้สีของข้อความที่มีความสำคัญ
3. ปรับปรุงเสียงเพลงประกอบให้เบาลง
4. ปรับปรุงขนาดตัวอักษรใหญ่ขึ้น เน้นใช้สีของข้อความที่มีความสำคัญ และจัดข้อความใหม่

ตาราง 2 ผลประสิทธิภาพของบทเรียนวิดีโอสตรีมมิ่งแบบปฏิสัมพันธ์

จำนวนนักศึกษา (คน)	**คะแนนระหว่างเรียน**			**คะแนนหลังเรียน**			**ประสิทธิภาพ E_1/E_2**
	คะแนนเต็ม	**ค่าเฉลี่ย**	**E_1**	**คะแนนเต็ม**	**ค่าเฉลี่ย**	**E_2**	
60	10	8.133	81.33	10	8.367	83.67	81.33/83.67

จากตาราง 2. พบว่า บทเรียนวิดีโอสตรีมมิ่งแบบปฏิสัมพันธ์ เรื่อง ความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และการสื่อสารข้อมูล มีประสิทธิภาพโดยรวมอยู่ที่ 81.33/83.67 ซึ่งมีประสิทธิภาพตามเกณฑ์ 80/80

4.2 ผลการเปรียบเทียบผลสัมฤทธิ์ทางการเรียนก่อนเรียนกับหลังเรียนของนักศึกษาที่เรียนด้วยวิดีโอสตรีมมิ่งแบบปฏิสัมพันธ์ เรื่อง ความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และการสื่อสารข้อมูล

ตาราง 3 เปรียบเทียบผลสัมฤทธิ์ทางการเรียนก่อนเรียนกับหลังเรียนของนักศึกษาที่เรียนด้วยวิดีโอสตรีมมิ่งแบบปฏิสัมพันธ์ ก่อนเรียนและหลังเรียน

วิดีโอสตรีมมิ่งแบบปฏิสัมพันธ์	**N**	$\overline{X}$	**S.D.**	**t**	**df**	**P**
ก่อนเรียน	60	3.17	1.32	25.30	59	0.00**
หลังเรียน	60	8.37	1.22			

** มีนัยสำคัญทางสถิติที่ระดับ .05

จากตาราง 3 ผลการเปรียบเทียบผลสัมฤทธิ์ทางการเรียนพบว่า นักศึกษาที่เรียนด้วยบทเรียนวิดีโอสตรีมมิ่งแบบปฏิสัมพันธ์ เรื่อง ความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และการสื่อสารข้อมูล หลังเรียนมีระดับผลสัมฤทธิ์ทางการเรียนสูงกว่าก่อนเรียนอย่างมีนัยสำคัญทางสถิติที่ .05

4.3 ผลการศึกษาความพึงพอใจของนักศึกษาที่มีต่อวิดีโอสตรีมมิ่งแบบปฏิสัมพันธ์ เรื่อง ความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และการสื่อสารข้อมูล

ตาราง 4 ผลการวิเคราะห์ความพึงพอใจของนักศึกษาที่เรียนด้วยวิดีโอสตรีมมิ่งแบบปฏิสัมพันธ์ เรื่อง ความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และการสื่อสารข้อมูล

ลำดับ	รายการประเมินความพึงพอใจ	$\bar{X}$	S.D.	ระดับความพึงพอใจ
1	เนื้อหาที่นำเสนอเข้าใจง่าย	4.50	0.60	ดีมาก
2	ความคมชัดของสื่อ	4.72	0.52	ดีมาก
3	ความเหมาะสมของภาพสื่อความหมาย	4.75	0.47	ดีมาก
4	ความเหมาะสมของตัวอักษรและสีตัวอักษร	4.77	0.43	ดีมาก
5	ความสัมพันธ์ระหว่างภาพและเสียง	4.63	0.52	ดีมาก
6	ความชัดเจนของเสียงดนตรี	4.47	0.57	ดี
7	ความชัดเจนของเสียงบรรยาย	4.35	0.55	ดี
8	ความเหมาะสมในการจัดลำดับการนำเสนอ	4.35	0.58	ดี
9	ความน่าสนใจในการนำเสนอ	4.52	0.57	ดีมาก
10	สามารถถ่ายทอดและสื่อสารให้เกิดความเข้าใจได้	4.52	0.54	ดีมาก
11	สามารถสร้างความรู้และประสบการณ์ได้โดยตรง	4.32	0.68	ดี
12	นักศึกษาสามารถทบทวนความรู้ในบทเรียนจากสื่อได้ด้วยตนเอง	4.50	0.60	ดีมาก
13	หลังจากใช้สื่อแล้วนักศึกษามีความรู้ความเข้าใจในเรื่องความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และการสื่อสารข้อมูล	4.55	0.50	ดีมาก
14	สื่อวิดีโอปฏิสัมพันธ์มีความเหมาะสมที่นำมาใช้ในการเรียนการสอน	4.53	0.54	ดีมาก
15	ระยะเวลาของสื่อวิดีโอปฏิสัมพันธ์มีความเหมาะสม	4.38	0.61	ดี
เฉลี่ย		**4.52**	**0.55**	**ดีมาก**

จากตาราง 5 ผลการวิเคราะห์ความพึงพอใจของนักศึกษาที่เรียนด้วยวิดีโอสตรีมมิ่งแบบปฏิสัมพันธ์ที่พัฒนาขึ้นมา พบว่า นักศึกษามีความพึงพอใจเฉลี่ยทุกรายการประเมินอยู่ในระดับดีมาก ยกเว้น ความชัดเจนของเสียงดนตรี ความชัดเจนของเสียงบรรยาย ความเหมาะสมในการจัดลำดับในการนำเสนอ การสร้างความรู้และประสบการณ์ได้โดยตรง และระยะเวลาของสื่อวิดีโอปฏิสัมพันธ์มีความเหมาะสม นักศึกษามีความพึงพอใจในระดับมาก มีรายละเอียดดังนี้

นักศึกษามีความพึงพอใจรายการความเหมาะสมของตัวอักษรและสีตัวอักษร มากที่สุดเป็นอันดับแรก ส่วนความเหมาะสมของภาพสื่อความหมาย มีความพึงพอใจในระดับดีมากเป็นอันดับสอง และความคมชัดของสื่อ มีความพึงพอใจในระดับดีมากเป็นอันดับสาม

สำหรับความสัมพันธ์ระหว่างภาพและเสียง สื่อวิดีโอปฏิสัมพันธ์มีความเหมาะสมที่นำมาใช้ในการเรียนการสอน ความน่าสนใจในการนำเสนอ เนื้อหาที่นำเสนอเข้าใจง่าย และนักศึกษาสามารถทบทวนความรู้ในบทเรียนจากสื่อได้ด้วยตนเอง นักศึกษามีความพึงพอใจดีมาก ส่วนความชัดเจนของเสียงดนตรี ระยะเวลาของสื่อวิดีโอปฏิสัมพันธ์มีความเหมาะสม ความชัดเจนของเสียงบรรยายและความเหมาะสมในการจัดลำดับการนำเสนอ นักศึกษามีความพึงพอใจดี โดยความการสามารถสร้างความรู้และประสบการณ์ได้โดยตรง นักศึกษามีความพึงพอใจในมากเป็นอันดับสุดท้าย

บทที่ 5
สรุป อภิปรายผลและข้อเสนอแนะ

ผลการวิจัย

1. ได้วิดีโอสตรีมมิ่งแบบปฏิสัมพันธ์ เรื่อง ความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และการสื่อสารข้อมูล สำหรับนักศึกษาที่เรียนในรายวิชา 871-310 การปฏิสัมพันธ์ระหว่างมนุษย์และคอมพิวเตอร์ (Human Computer Interaction) และ 871-411 ความมั่นคงของระบบคอมพิวเตอร์และการสื่อสารข้อมูล (Computer System and Data Communication Security) ประกอบด้วยเนื้อหา จำนวน 5 หน่วยการเรียน ดังนี้

หน่วยที่ 1. ความรู้เบื้องต้นเกี่ยวกับความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และการสื่อสารข้อมูล

หน่วยที่ 2. หลักการพื้นฐานการรักษาความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และการสื่อสารข้อมูล

หน่วยที่ 3. หลักการอื่นในการรักษาความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และการสื่อสารข้อมูล

หน่วยที่ 4. การเข้ารหัสและถอดรหัส

หน่วยที่ 5. การรักษาความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และการสื่อสารข้อมูลด้วยไฟร์วอลล์

2. คุณภาพวิดีโอสตรีมมิ่งแบบปฏิสัมพันธ์ เรื่อง ความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และการสื่อสารข้อมูล มีคุณภาพโดยรวมอยู่ในระดับดีมาก

3. วิดีโอสตรีมมิ่งแบบปฏิสัมพันธ์ เรื่อง ความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และการสื่อสารข้อมูล มีประสิทธิภาพ 81.33/83.67

4. การเปรียบเทียบผลสัมฤทธิ์ทางการเรียนของนักศึกษาที่เรียนด้วยวิดีโอสตรีมมิ่งแบบปฏิสัมพันธ์ เรื่อง ความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และการสื่อสารข้อมูล หลังเรียนมีระดับผลสัมฤทธิ์ทางการเรียนสูงกว่าก่อนเรียน อย่างมีนัยสำคัญทางสถิติที่ระดับ .05

5. นักศึกษาที่เรียนด้วยวิดีโอสตรีมมิ่งแบบปฏิสัมพันธ์ เรื่อง ความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และการสื่อสารข้อมูล มีความพึงพอใจมากที่สุด

อภิปรายผลการวิจัย

จากผลการวิจัยวิดีโอสตรีมมิ่งแบบปฏิสัมพันธ์ เรื่อง ความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และการสื่อสารข้อมูล สามารถนำมาอภิปรายผลได้ดังนี้

1. การพัฒนาวิดีโอสตรีมมิ่งแบบปฏิสัมพันธ์ เรื่อง ความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และการสื่อสารข้อมูล มีคุณภาพโดยรวมอยู่ในระดับดีมาก และและมีประสิทธิภาพ 81.33/83.67 ซึ่งเป็นไปตามเกณฑ์ที่กำหนด คือ 80/80 เนื่องมาจากการศึกษาวิจัยครั้งนี้มีการดำเนินการออกแบบและพัฒนาวีดิโอแบบปฏิสัมพันธ์อย่างเป็นระบบ ตั้งแต่การวิเคราะห์เนื้อหา การเขียนผล การเรียนรู้ที่คาดหวัง การเรียบเรียงเนื้อหา ดำเนินการผลิตวิดีโอ ดำเนินการผลิตวิดีโอแบบปฏิสัมพันธ์ มีผู้เชี่ยวชาญตรวจสอบแต่ละขั้นตอน เพื่อปรับปรุงแก้ไขให้มี

คุณภาพก่อนนำไปทดลองใช้กับกลุ่มตัวอย่าง เพื่อตรวจสอบประสิทธิภาพตามกระบวนการวิจัยและพัฒนา (Research and Development) จึงทำให้วิดีโอแบบปฏิสัมพันธ์นี้มีประสิทธิภาพตามเกณฑ์ที่กำหนด การสร้างวิดีโอสตรีมมิ่งแบบปฏิสัมพันธ์ในครั้งนี้ใช้หลักการผลิตรายการโทรทัศน์ของณรงค์ สมพงษ์ (2530 : 312-350) และสังคม ภูมิพันธ์ (2535 : 12-22) แล้วนำวิดีโอที่ได้นำมาสร้างการปฏิสัมพันธ์โดยใช้โปรแกรม Microsoft Form สร้างแบบทดสอบ ซึ่งสอดคล้องกับงานวิจัยของชลิต ลิ้มพระคุณ (2556) นรินธน์ นนทมาลย์ (2554) พรสุข ตันตระรุ่งโรจน์ (2557) และยุพยงค์ กลั่นประเสริฐ (2551)

2. การพัฒนาวิดีโอสตรีมมิ่งแบบปฏิสัมพันธ์ เรื่อง ความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และการสื่อสารข้อมูล พบว่า ผู้เรียนมีผลสัมฤทธิ์ทางการเรียนหลังเรียนสูงกว่าก่อนเรียนซึ่งเป็นไปตามสมมุติฐาน ทั้งนี้อาจเป็นได้จากการเรียนด้วยวิดีโอสตรีมมิ่งแบบปฏิสัมพันธ์ โดยใช้เสียงการบรรยายประกอบภาพอินโฟกราฟิกเป็นไปอย่างมีลำดับขั้นตอน ใช้ระยะเวลาเหมาะสม เพื่อกระตุ้นความสนใจและความคิดของผู้เรียนได้อย่างเป็นรูปธรรม

3. จากผลการศึกษาความพึงพอใจของผู้เรียนที่มีต่อวิดีโอสตรีมมิ่งแบบปฏิสัมพันธ์ เรื่อง ความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และการสื่อสารข้อมูล พบว่า ผู้เรียนมีความพึงพอใจโดยรวมในระดับมากที่สุด เนื่องจากวิดีโอสตรีมมิ่งแบบปฏิสัมพันธ์ที่พัฒนาขึ้นมีเนื้อมีความน่าสนใจ เข้าใจง่ายและชัดเจน

ข้อเสนอแนะ

ข้อเสนอแนะจากนักศึกษา

1. ข้อความเร็วไป บางครั้งอ่านข้อความไม่ทัน กรณีเนื้อหายาว ต้องย้อนหรือหยุดวีดีโอก่อน เพื่ออ่าน
2. แบบทดสอบกับสื่อยังไม่สอดคล้องกันมากนัก เนื้อหาในสื่อบางเรื่องอาจจะยังไม่ค่อยชัดเจน
3. อักษรตัวเล็กเกินไป เนื้อหาในแต่ละหน้าค่อนข้างเยอะเวลานั้นไม่อาจจะอ่านทัน ทำให้พลาดเนื้อหาไปเยอะพอสมควร

ข้อเสนอแนะจากผู้วิจัย

1. ควรนำสื่อวิดีโอสตรีมมิ่งแบบปฏิสัมพันธ์สามารถนำมาใช้ในการเรียนการสอนของมหาวิทยาลัยสงขลานครินทร์ได้ทุกวิชา
2. สื่อวิดีโอสตรีมมิ่งแบบปฏิสัมพันธ์รองรับการเรียนรู้ทุกช่วงวัย

บรรณานุกรม

กฤช พลไพรสรรพ์. (2554). การวิเคราะห์และศึกษาประสิทธิภาพไฟล์วีดีโอ บนเทคโนโลยี 3 จี และ ไวไฟฮอต สปอร์ต กรณีศึกษาวีดีโอสตรีมมิ่ง ประเภทวีดีโออนดีมาน. (ปัญหาพิเศษวิทยาศาสตร์มหาบัณฑิต). ภาควิชาเทคโนโลยีสารสนเทศ คณะเทคโนโลยีสารสนเทศ มหาวิทยาลัยพระจอมเกล้าพระนครเหนือ.

กิดานันท์ มลิทอง. (2548). เทคโนโลยีและการสื่อสารเพื่อการศึกษา. กรุงเทพมหานคร: สำนักพิมพ์แห่งจุฬาลงกรณ์มหาวิทยาลัย.

ชลิต ลิ้มพระคุณ. (2556). การพัฒนาบทเรียนวีดิทัศน์ เรื่อง การซ่อมแซมเสื้อผ้าเบื้องต้นสำหรับนักเรียนชั้นประถมศึกษาปีที่ 5. Veridian E-Journal, 182.

ณรงค์ สมพงษ์. (2530) เทคโนโลยีทางการศึกษา. กรุงเทพฯ : จุฬาลงกรณ์มหาวิทยาลัย, 2530.

นรินธน์ นนทมาลย์. (2554). ผลของการแทรกเทคนิคการตั้งค าถาม 5W1H ในวิดีโอบรรยายออนดีมานด์บนเว็บ 2.0 ที่มีต่อผลสัมฤทธิ์ทางการเรียนและความสามารถในการแก้ปัญหาของนิสิตปริญญาตรี. กรุงเทพมหานคร: จุฬาลงกรณ์มหาวิทยาลัย.

นรินธน์ นนทมาลย์. (2561). วิดีโอปฏิสัมพันธ์ในการเรียนแบบเปิดในศตวรรษที่ 21. ครุศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, 211-227.

พรสุข ตันตระรุ่งโรจน์. (2557). การใช้สตรีมมิ่งวิดีโอ (Streaming Video) ในการเรียนการสอน รวมบทความเรื่อง เทคโนโลยีและสื่อสารการศึกษา : นวัตกรรมการเรียนรู้แบบผสมผสาน (pp201-215). กรุงเทพมหานคร: สำนักพิมพ์แห่งจุฬาลงกรณ์มหาวิทยาลัย.

พวงรัตน์ ทวีรัตน์. 2540. วิธีการวิจัยทางพฤติกรรมศาสตร์และสังคมศาสตร์. พิมพ์ครั้งที่ 7. กรุงเทพฯ : สำนักทดสอบทางการศึกษาและจิตวิทยา มหาวิทยาลัยศรีนครินทร์วิโรฒ ประสานมิตร.

ยุพยงค์ กลั่นประเสริฐ. (2551). การพัฒนาบทเรียนวีดิทัศน์แบบปฏิสัมพันธ์เรื่อง การขยายพันธุ์พืชรายวิชาการงานอาชีพและเทคโนโลยีชั้นมัธยมศึกษาปีที่ 2. การศึกษาค้นคว้าอิสระปริญญามหาบัณฑิต สาขาวิชาเทคโนโลยีการศึกษา. บัณฑิตวิทยาลัย มหาวิทยาลัยมหาสารคาม.

วรพจน์ นวลสกุล. (2540). ผลของการเลือกช่วงการทำแบบฝึกหัดในบทเรียนคอมพิวเตอร์ช่วยสอนกับระดับผลสัมฤทธิ์ทางการเรียน. (วิทยานิพนธ์ปริญญาดุษบัณฑิต), คณะครุศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย.

วิภา อุตมฉันท์. (2538). กระบวนการสร้างสรรค์และเทคนิคการผลิตสื่อโทรทัศน์และสื่อคอมพิวเตอร์. กรุงเทพมหานคร.

ศิรินทิพย์ นันทวาศ. (2555). การพัฒนากิจกรรมการเรียนการสอนโดยใช้วีดิทัศน์เชิงโต้ตอบเพื่อส่งเสริมทักษะการอ่านและการเขียน สำหรับนักเรียนชั้นประถมศึกษาปีที่ 3. (วิทยานิพนธ์ปริญญามหาบัณฑิต). วิทยานิพนธ์ปริญญามหาบัณฑิต สาขาวิชาการสอนภาษาไทย มหาวิทยาลัยเชียงใหม่.

สังคม ภูมิพันธุ์. (2535). การผลิตรายการโทรทัศน์. พิมพ์ครั้งที่ 2. มหาสารคาม : ภาควิชาเทคโนโลยีทางการศึกษา มหาวิทยาลัยศรีนครินทรวิโรฒ มหาสารคาม.

A. D., & Zanetis, J Greenberg. (2012). The impact of broadcast and streaming video in education. Duxbury, MA: Wainhouse Research.

A. D., & Zanetis, J. Greenberg. (2012). The impact of broadcast and streaming video in education. Duxbury, MA: Wainhouse Research.

B., & Fadel, C Trilling. (2009). 21st century skills: Learning for life in our times. Hoboken, NJ: John Wiley & Sons.

D Denning. (1992). Video in theory and practice: Issues for classroom use and teacher video evaluation. Victoria: InNATURE productions.

J. C Taylor. (2001). Fifth generation distance education. Instructional Science and Technology, 4(1), 1-14.

J. F., & Prinsloo, P Heydenrych. (2010). Revisiting the five generations of distance education . South African Journal for Open and Distance Learning Practice, 32(1), 5-26.

Jeremy Howell. (no.4 (June 1960)). The Use of Television in Agriculture Extension. Education Televisional, 6-7.

Joubel. (2017). เข้าถึงได้จาก https://h5p.org/interactive-video.

M., & Weynand, D Weise. (2012). How Video Works: from analog to high definition. Amsterdam: Focal Press.

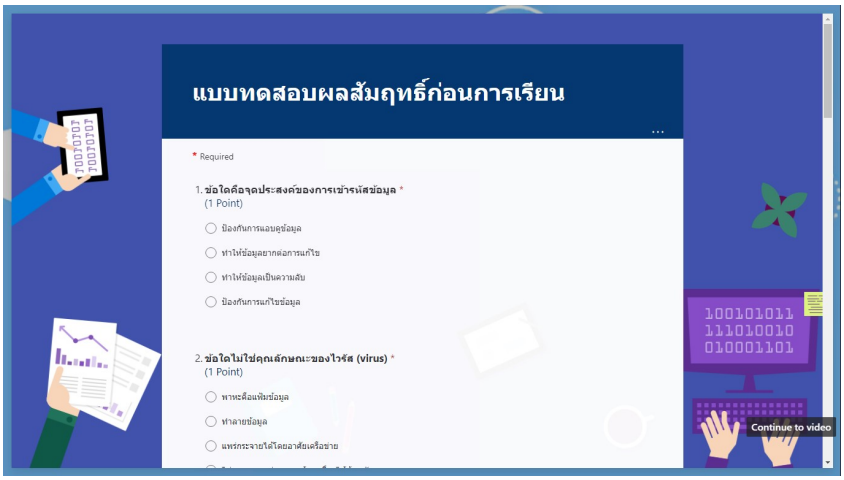
S. E., Lowther, D. L., & Russell, J. D Smaldno. (2012). Instruction Technology and Media for Learning tenth edition : Enhancing Learning with video. Boston: Pearson.

T.,&Dron,J Anderson. (2011). Three generations of distance education pedagogy. International Review of Research on Distance and Open Learning,12(3), 80-97.

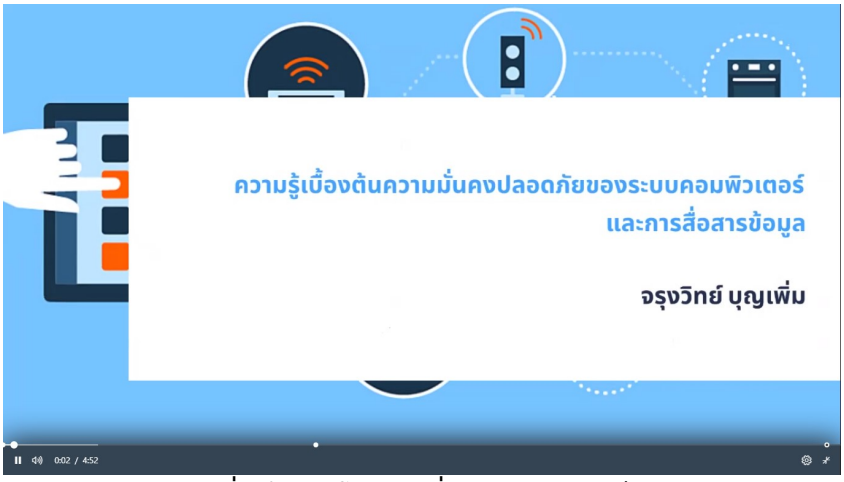
ภาคผนวก

ก.วิดีโอสตรีมมิ่งแบบปฏิสัมพันธ์

เรื่อง ความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และการสื่อสารข้อมูล

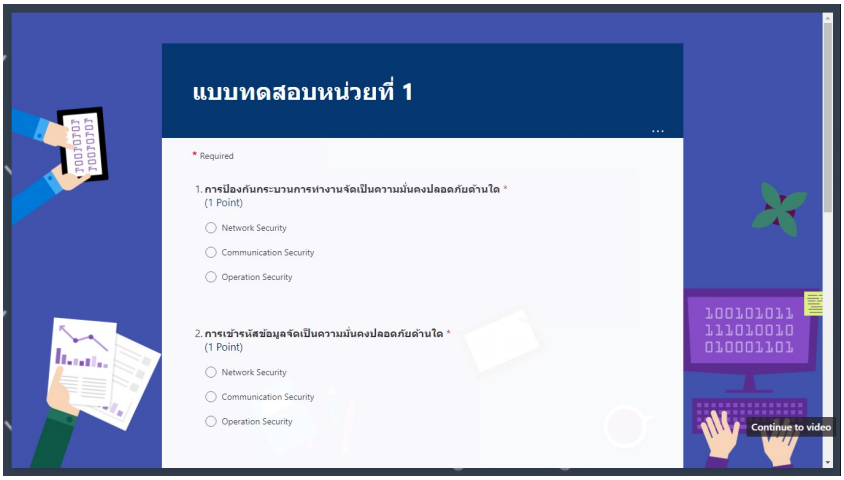


แบบทดสอบก่อนเรียน



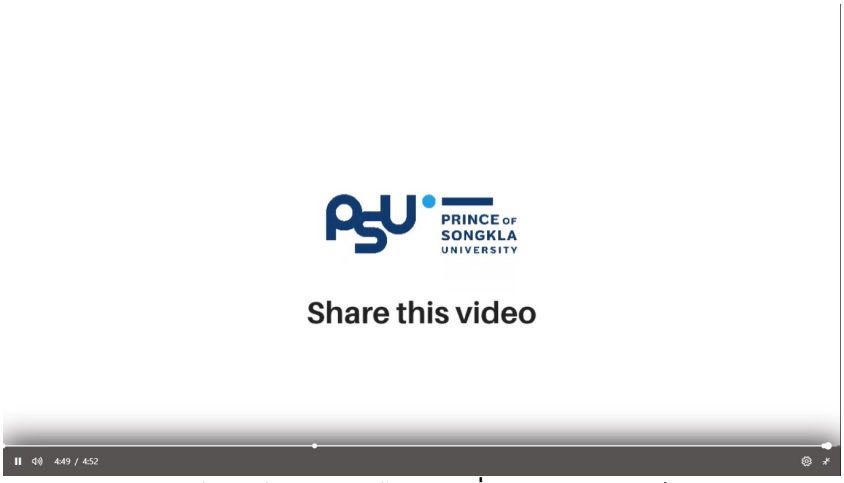
เริ่มเข้าสู่วิดีโอสตรีมมิ่งแบบปฏิสัมพันธ์

เนื้อหาวิดีโอสตรีมมิ่งแบบปฏิสัมพันธ์



แบบทดสอบระหว่างเรียน

แบบทดสอบหลังเรียน



หน้าสุดท้ายของวิดีโอสตรีมมิ่งแบบปฏิสัมพันธ์

ภาคผนวก

ข.แบบทดสอบก่อนเรียน ระหว่างเรียน และหลังเรียน

แบบทดสอบก่อนการเรียน

เรื่อง ความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และการสื่อสารข้อมูล

คะแนนเต็ม 10 คะแนน

<u>คำอธิบาย</u>

ให้นักศึกษาเลือกคำตอบที่ถูกต้องโดยการทำเครื่องหมาย ✖ บนหัวข้อตัวเลือก

1. ข้อใดคือจุดประสงค์ของการเข้ารหัสข้อมูล
   - ก. ป้องกันการแก้ไขข้อมูล
   - ข. ป้องกันการแอบดูข้อมูล
   - ค. ทำให้ข้อมูลเป็นความลับ
   - ง. ทำให้ข้อมูลยากต่อการแก้ไข
2. ข้อใดไม่ใช่คุณลักษณะของไวรัส (virus)
   - ก. ทำลายข้อมูล
   - ข. แพร่กระจายได้โดยอาศัยเครือข่าย
   - ค. พาหะคือแฟ้มข้อมูล
   - ง. ไม่สามารถแพร่กระจายข้ามเครื่องได้ด้วยตัวเอง
3. ข้อใดคือคุณลักษณะของเวิร์ม (worm)
   - ก. ทำความเสียหายได้น้อยกว่าไวรัส
   - ข. ไม่สามารถแพร่กระจายทางเมล์ได้
   - ค. ไม่สามารถแพร่กระจายข้ามเครื่องได้ด้วยตัวเอง
   - ง. สามารถแพร่กระจายผ่านระบบเครือข่ายได้
4. ข้อใดคือคุณลักษณะของโทรจัน (trojan)
   - ก. ไม่ใช่โปรแกรมคอมพิวเตอร์
   - ข. ไม่มีพาหะในการแพร่กระจาย
   - ค. ล้วงความลับข้อมูล
   - ง. ถูกทุกข้อ
5. IDS (Intrusion Detection System) คืออะไร
   - ก. ระบบแจ้งเตือนการบุกรุก
   - ข. ระบบป้องกันการบุกรุก
   - ค. ระบบทำลายการบุกรุก
   - ง. ระบบวิเคราะห์การบุกรุก

6. DoS ย่อมาจากคำว่าอะไร

ก. Deny of Server

ข. Deny of Service

ค. Denial of Server

ง. Denial of Service

7. ข้อใดไม่ใช่คุณสมบัติของ message digest

ก. มีขนาดคงที่

ข. สามารถทำย้อนกลับไปหาข้อมูลตั้งต้นได้

ค. ได้มาจากการผ่าน hash function

ง. เปรียบเสมือนลายนิ้วมือของข้อมูล

8. ชื่อ url ที่ขึ้นต้นด้วย https ใช้มาตรฐานใด

ก. SSL

ข. SET

ค. SSH

ง. OSI

9. การเข้ารหัสแบบ Caesar Cipher มีการขยับตัวอักษรไปกี่ตำแหน่ง

ก. 3 ตำแหน่ง

ข. 4 ตำแหน่ง

ค. 5 ตำแหน่ง

ง. 6 ตำแหน่ง

10. การเข้ารหัสแบบ DES จะมีวงรอบการทำงานที่ทำซ้ำๆ กันจำนวนกี่รอบ

ก. 16 รอบ

ข. 32 รอบ

ค. 64 รอบ

ง. 128 รอบ

แบบทดสอบระหว่างเรียน

เรื่อง ความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และการสื่อสารข้อมูล

คะแนนเต็ม 5 คะแนน

<u>คำอธิบาย</u>

ให้นักศึกษาเลือกคำตอบที่ถูกต้องโดยการทำเครื่องหมาย ✖ บนหัวข้อตัวเลือก

1. การแบ่งเครือข่ายออกเป็นเครือข่ายย่อยจัดเป็นความมั่นคงปลอดภัยด้านใด

ก. Network Security

ข. Communication Security

ค. Operation Security

2. การป้องกันกระบวนการทำงานจัดเป็นความมั่นคงปลอดภัยด้านใด

ก. Network Security

ข. Operation Security

ค. Communication Security

3. การกำหนดสิทธิ์ของผู้รับผิดชอบจัดเป็นความมั่นคงปลอดภัยด้านใด

ก. Personal Security

ข. Physical Security

ค. Operation Security

4. การเข้ารหัสข้อมูลจัดเป็นความมั่นคงปลอดภัยด้านใด

ก. Network Security

ข. Operation Security

ค. Communication Security

5. การตั้งรหัสผ่านเข้าไวไฟจัดเป็นความมั่นคงปลอดภัยด้านใด

ก. Operation Security

ข. Physical Security

ค. Personal Security

แบบทดสอบหลังการเรียน

เรื่อง ความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และการสื่อสารข้อมูล

คะแนนเต็ม 10 คะแนน

<u>คำอธิบาย</u>

ให้นักศึกษาเลือกคำตอบที่ถูกต้องโดยการทำเครื่องหมาย ✖ บนหัวข้อตัวเลือก

1. ข้อใดคือจุดประสงค์ของการเข้ารหัสข้อมูล
   - ก. ป้องกันการแก้ไขข้อมูล
   - ข. ป้องกันการแอบดูข้อมูล
   - ค. ทำให้ข้อมูลเป็นความลับ
   - ง. ทำให้ข้อมูลยากต่อการแก้ไข
2. ข้อใดไม่ใช่คุณลักษณะของไวรัส (virus)
   - ก. ทำลายข้อมูล
   - ข. แพร่กระจายได้โดยอาศัยเครือข่าย
   - ค. พาหะคือแฟ้มข้อมูล
   - ง. ไม่สามารถแพร่กระจายข้ามเครื่องได้ด้เวยตัวเอง
3. ข้อใดคือคุณลักษณะของเวิร์ม (worm)
   - ก. ทำความเสียหายได้น้อยกว่าไวรัส
   - ข. ไม่สามารถแพร่กระจายทางเมล์ได้
   - ค. ไม่สามารถแพร่กระจายข้ามเครื่องได้ด้วยตัวเอง
   - ง. สามารถแพร่กระจายผ่านระบบเครือข่ายได้
4. ข้อใดคือคุณลักษณะของโทรจัน (trojan)
   - ก. ไม่ใช่โปรแกรมคอมพิวเตอร์
   - ข. ไม่มีพาหะในการแพร่กระจาย
   - ค. ล้วงความลับข้อมูล
   - ง. ถูกทุกข้อ
5. IDS (Intrusion Detection System) คืออะไร
   - ก. ระบบแจ้งเตือนการบุกรุก
   - ข. ระบบป้องกันการบุกรุก
   - ค. ระบบทำลายการบุกรุก
   - ง. ระบบวิเคราะห์การบุกรุก

6. DoS ย่อมาจากคำว่าอะไร

ก. Deny of Server

ข. Deny of Service

ค. Denial of Server

ง. Denial of Service

7. ข้อใดไม่ใช่คุณสมบัติของ message digest

ก. มีขนาดคงที่

ข. สามารถทำย้อนกลับไปหาข้อมูลตั้งต้นได้

ค. ได้มาจากการผ่าน hash function

ง. เปรียบเสมือนลายนิ้วมือของข้อมูล

8. ชื่อ url ที่ขึ้นต้นด้วย https ใช้มาตรฐานใด

ก. SSL

ข. SET

ค. SSH

ง. OSI

9. การเข้ารหัสแบบ Caesar Cipher มีการขยับตัวอักษรไปกี่ตำแหน่ง

ก. 3 ตำแหน่ง

ข. 4 ตำแหน่ง

ค. 5 ตำแหน่ง

ง. 6 ตำแหน่ง

10. การเข้ารหัสแบบ DES จะมีวงรอบการทำงานที่ทำซ้ำๆ กันจำนวนกี่รอบ

ก. 16 รอบ

ข. 32 รอบ

ค. 64 รอบ

ง. 128 รอบ

ภาคผนวก

ค.บทโทรทัศน์ วิดีโอสตรีมมิ่งแบบปฏิสัมพันธ์

เรื่อง ความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และการสื่อสารข้อมูล

บทโทรทัศน์

เรื่อง : ความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และการสื่อสารข้อมูล

ตอน : ความรู้เบื้องต้นเกี่ยวกับความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และการสื่อสารข้อมูล

เจ้าของเนื้อหา : อาจารย์จรุงวิทย์ บุญเพิ่ม **ผู้เขียนสคริปต์ :** นายอำนาจ สุคนเขตร์

ลำดับ	ภาพ	เสียง	เวลา
1	Info.	ปัจจุบันความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และการสื่อสารข้อมูลถือเป็นส่วนสำคัญของการนำระบบสารสนเทศเข้ามาใช้ในองค์กร เนื่องจากระบบสารสนเทศใช้คอมพิวเตอร์เป็นหลักในการเก็บรักษาข้อมูล และใช้ระบบเครือข่ายเป็นสื่อกลางในการติดต่อสื่อสารข้อมูล จึงเป็นเรื่องง่ายต่อการคุกคามจากผู้ไม่ประสงค์ดี ภัยคุกคามต่อคอมพิวเตอร์และการสื่อสารข้อมูลมีหมายความครอบคลุมทั้งการคุกคามทางฮาร์ดแวร์ ซอฟต์แวร์ และข้อมูล โดยสาเหตุของภัยคุกคามจากทางกายภาพ เช่น อัคคีภัย ปัญหาวงจรไฟฟ้า ระบบสื่อสารข้อมูล ความผิดพลาดของฮาร์ดแวร์ ความผิดพลาดของซอฟต์แวร์ หรือภัยคุกคามที่เกิดจากคนหรือผู้ใช้ระบบ เช่น การบุกรุกจากผู้ที่ไม่ได้รับอนุญาตหรือผู้ใช้ที่ไม่ตระหนักถึงความมั่นคงปลอดภัย ทำให้ระบบเกิดความเสียหาย ภัยคุกคามเหล่านี้เป็นสาเหตุให้ข้อมูลในระบบเสียหาย สูญหาย ถูกขโมยหรือแก้ไขบิดเบือน	
2	Info.	การรักษาความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และการสื่อสารข้อมูล หมายถึง การทำให้มั่นใจได้ว่าทรัพยากรสารสนเทศที่มีอยู่มีความถูกต้องสมบูรณ์และพร้อมใช้งานสำหรับผู้ใช้งานที่ได้รับสิทธิ์ในการเข้าถึงทรัพยากรนั้นๆ เช่น การรักษาความมั่นคงปลอดภัยของเครื่องคอมพิวเตอร์ส่วนบุคคลซึ่งจัดเก็บข้อมูลที่มีข้อมูลที่ไม่ต้องการให้ผู้อื่นล่วงรู้ ตลอดจนต้องการรักษาความครบถ้วนสมบูรณ์ของไฟล์ต่าง ๆ ที่ถูกจัดเก็บไว้ในคอมพิวเตอร์ไม่ให้ถูกทำลายโดยมัลแวร์และป้องกันการแพร่ระบาดของหนอนอินเทอร์เน็ต ซึ่งอาจทำให้เครื่องคอมพิวเตอร์ไม่สามารถใช้งานได้ อาจพิจารณาตั้งรหัสผ่านหรือพาสเวิร์ด เพื่อควบคุมการเข้าถึงเข้าถึงเครื่องคอมพิวเตอร์ จัดการเข้ารหัสลับฮาร์ดดิสก์ ติดตั้งซอฟต์แวร์ตรวจจับไวรัสคอมพิวเตอร์ ตลอดจนเปิดการใช้งานไฟร์วอลส่วนบุคคล เป็นต้น	
3	Info.	โดยทั่วไปความมั่นคงปลอดภัยของทรัพยากรสารสนเทศจำแนกได้ดังต่อไปนี้ 1. ความมั่นคงปลอดภัยเชิงกายภาพ หรือ physical security ใช้ในการป้องกันอุปกรณ์สิ่งของ หรือ บริเวณให้ปราศจากการเข้าถึงโดยไม่ได้รับอนุญาตและการใช้งานที่ไม่ถูกต้อง เช่น การตั้งรหัสผ่านเพื่อ เข้าใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล การสร้างห้องสำหรับจัดเก็บระบบ	

		คอมพิวเตอร์และอุปกรณ์การสื่อสารข้อมูล การจัดให้มีระบบไฟฟ้าสำรอง การจัดให้มีระบบดับเพลิง หรือการตั้งรหัสผ่านเข้าใช้งานไวไฟ เป็นต้น	
4	Info.	2. ความมั่นคงปลอดส่วนบุคคล หรือ Personal Security เพื่อรักษาบุคลากรหรือกลุ่มของผู้ใช้งานที่ได้รับสิทธิ์ให้เข้าถึงและดำเนินงานได้อย่างมั่นคงปลอดภัย เช่น การกำหนดสิทธิ์ให้กับเจ้าหน้าที่ตามความรับผิดชอบ โดยการกำหนดให้เจ้าหน้าที่ทั่วไปไม่สามารถอ่านข้อมูลที่ถูกสร้างขึ้นโดยหัวหน้างานของตนเองสามารถแก้ไขและตรวจสอบผู้ทำการแก้ไขทรัพยากรนั้นๆ ได้ การบังคับให้ผู้ใช้งานเปลี่ยนรหัสผ่านเมื่อเข้าสู่ระบบครั้งแรกและเปลี่ยนรหัสผ่านทุกสามเดือน เป็นต้น	
5	Info.	3. ความมั่นคงปลอดภัยของการดำเนินงาน หรือ operation security เพื่อปกป้องหรือป้องกันกระบวนการทำงาน ตลอดจนกิจกรรมอื่น ๆ ที่เกี่ยวข้อง	
6	Info	4. ความมั่นคงปลอดภัยของการสื่อสาร หรือ communication security เพื่อป้องกันสื่อนำสัญญาณข้อมูลต่าง ๆ ที่รับส่งผ่านช่องทางการสื่อสาร โดยมุ่งเน้นการรักษาความมั่นคงปลอดภัยของอุปกรณ์ต่าง ๆที่เชื่อมต่อกันเป็นระบบสื่อสาร รวมถึงการแพร่สัญญาณให้มีความมั่นคงปลอดภัย เช่น การกำหนดมาตรการเฝ้าตรวจการดักรับข้อมูล การเข้ารหัสข้อมูลที่มีการรับส่งกันในเครือข่ายหรือระหว่างเครือข่าย การใช้บริการวีพีเอ็นในการเชื่อมต่อระบบคอมพิวเตอร์ระหว่างสาขาซึ่งทำให้มั่นใจได้ว่าการรับส่งข้อมูลระหว่างจุดจะถูกเข้ารหัสทำให้ผู้ไม่ประสงค์ดีที่ดักรับข้อมูลได้ไม่สามารถวิเคราะห์หรือแปลความหมายข้อมูลที่ดักรับได้ เป็นต้น	
7	Info.	5. ความมั่นคงปลอดภัยของเครือข่าย หรือ network security เพื่อป้องกันการเข้าถึงอุปกรณ์ เครือข่ายต่าง ๆ และอุปกรณ์ที่นำมาเชื่อมต่อเข้ากับเครือข่าย เช่น การแบ่งเครือข่ายออกเป็นเครือข่ายย่อย ๆ เพื่อจำแนกกลุ่มผู้ใช้งานและระบบบริการต่าง ๆ รวมถึงการจัดให้มีการเฝ้าตรวจความมั่นคงปลอดภัย และการจัดให้มีการพิสูจน์ตัวจริงของผู้ใช้งานก่อนจึงจะสามารถใช้งานเครือข่ายได้จะเห็นได้ว่ามีความแตกต่างจากความมั่นคงปลอดภัยของการสื่อสารโดยมีขอบเขตที่แคบกว่าและพิจารณาทุกการเชื่อมต่อในบริเวณที่เกี่ยวข้อง เช่น ระบบเครือข่ายภายในบ้าน ระบบเครือข่ายภายในบริษัท เป็นต้น	
8	Info		
9	Info	ดังนั้น การนำระบบสารสนเทศเข้ามาใช้งานต้องคำนึงถึงเรื่องความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และการสื่อสารข้อมูลควบคู่ไปด้วยอย่างหลีกเลี่ยงไม่ได้ อีกทั้งควรนำหลักการจำแนกความมั่นคงปลอดภัยของทรัพยากรสารสนเทศดังกล่าว มาคำนึงถึงมาตรการรักษาความมั่นคงปลอดของระบบคอมพิวเตอร์และการสื่อสารข้อมูลที่จะได้อธิบายในเนื้อถัดไป	

บทโทรทัศน์

เรื่อง : ความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และการสื่อสารข้อมูล

ตอน : หลักการพื้นฐานในการรักษาความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และการสื่อสารข้อมูล

เจ้าของเนื้อหา : อาจารย์จรุงวิทย์ บุญเพิ่ม **ผู้เขียนสคริปต์ :** นายอำนาจ สุคนเขตร์

ลำดับ	ภาพ	เสียง	เวลา
1	Info.	สำหรับหลักการพื้นฐานในการรักษาความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และการสื่อสารข้อมูล มีดังนี้ หลักการพื้นฐาน การรักษาความมั่นคงปลอดภัยจะสำเร็จได้ก็ต่อเมื่อองค์กรหรือบุคคลนั้น ๆ ได้มีการจัดการกำหนดนโยบายที่เกี่ยวข้อง การควบคุมการดำเนินการให้เป็นไปตามนโยบาย การเสริมสร้างความรู้ความเข้าใจที่เกี่ยวข้อง การฝึกอบรม การสร้างความตระหนักรู้และการประยุกต์ใช้เทคโนโลยีที่เกี่ยวข้องอย่างเหมาะสม ซึ่งประกอบด้วย	
2	Info.	1. การรักษาความลับ หรือ confidentiality หมายถึง กระบวนการ มาตรการและการจัดการที่เกี่ยวข้องกับการรักษาความลับของสารสนเทศที่ถูกประมวลผล ส่งต่อและจัดเก็บให้สามารถเข้าถึงและเข้าใจความหมายได้เฉพาะผู้ที่มีสิทธิ์เข้าถึงทรัพยากรนั้น ๆ ตัวอย่างข้อมูลที่ควรมีการจัดเก็บและมีการกำหนดมาตรการควบคุมการเข้าถึงเพื่อรักษาความลับของข้อมูลที่สำคัญ	
3	Info.	2. การรักษาความครบถ้วนสมบูรณ์ หรือ integrity หมายถึง กระบวนการมาตรการและการจัดการที่เกี่ยวข้องกับการตรวจสอบความครบถ้วนสมบูรณ์ของสารสนเทศที่ถูกประมวลผล ส่งต่อและจัดเก็บให้มีความถูกต้องสมบูรณ์และสามารถตรวจสอบความครบถ้วนสมบูรณ์นั้นได้	
		3. การรักษาความพร้อมใช้ หรือ availability หมายถึง กระบวนการมาตรการและการจัดการที่เกี่ยวข้องกับการรักษาความพร้อมใช้ของสารสนเทศที่ถูกประมวลผล ส่งต่อและจัดเก็บให้มีความพร้อมใช้อยู่เสมอ ทำให้ผู้ใช้ที่มีสิทธิ์เข้าถึงและใช้งานทรัพยากรสารสนเทศนั้น ๆ สามารถเข้าใช้งานได้เช่นเมื่อกล่าวถึงความพร้อมใช้ของระบบบริการธนาคารอิเล็กทรอนิกส์อาจหมายถึงลูกค้าสามารถเข้าถึงและใช้งานบริการนั้นได้เสมอตลอด 24 ชั่วโมง และอาจหมายรวมถึงเจ้าหน้าที่ๆ เกี่ยวข้องสามารถเข้าถึงและบริหารจัดการซอฟต์แวร์นั้นได้ เป็นต้น	
4	Info.	จากที่ได้อธิบายมาทั้งหมดนิยมเรียกกันสั้นๆ ว่าหลัก CIA ซึ่งปัจจุบันหลัก CIA ยังถูกนำมาใช้งานอยู่ และถัดไปเราจะได้เรียนรู้หลักการอื่นในการรักษาความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และการสื่อสารข้อมูล	

บทโทรทัศน์

เรื่อง : ความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และการสื่อสารข้อมูล

ตอน : หลักการอื่นในการรักษาความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และการสื่อสารข้อมูล

เจ้าของเนื้อหา : อาจารย์จรุงวิทย์ บุญเพิ่ม **ผู้เขียนสคริปต์ :** นายอำนาจ สุคนเขตร์

ลำดับ	ภาพ	เสียง	เวลา
1	Info.	นอกจากหลักการพื้นฐานในการรักษาความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และการสื่อสารข้อมูลแล้ว เราจะใช้หลักการอื่นในการรักษาความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และการสื่อสารข้อมูลด้วย ซึ่งหลักการนี้เป็นกระบวนการเชิงบริหารที่นำเอานโยบาย การดำเนินงานและการประยุกต์ใช้เทคโนโลยีที่เกี่ยวข้องเพื่อป้องกันและจำกัดผลเสียหายต่อการรักษาความลับ ความครบถ้วนสมบูรณ์และความพร้อมใช้ของทรัพยากรสารสนเทศนั้น ๆ ได้แก่	
2	Info.	1. ช่องโหว่ หรือ vulnerability คือ ความบกพร่อง หรือจุดอ่อนที่มีอยู่ในทรัพยากรสารสนเทศโดยเป็นผลมาจากการออกแบบ การพัฒนาซอฟต์แวร์การจัดการกระบวนการทำงาน หรือการบำรุงรักษาระบบนั้น ๆ เช่น ช่องโหว่ของระบบปฏิบัติการช่องโหว่ของซอฟต์แวร์เว็บบราวเซอร์ การอนุญาตให้ผู้ไม่มีบัตรเข้าถึงห้องสำคัญๆ ที่เกี่ยวข้องกับกระบวนการทำงานโดยไม่มีการตรวจสอบหรือการไม่ควบคุมให้มีการตรวจสอบเอกสารลับก่อนการทิ้งขยะ เป็นต้น เมื่อพิจารณาตามกลุ่มของทรัพยากรจะสามารถจำแนกประเภทของช่องโหว่ได้ 3 ลักษณะ ดังต่อไปนี้	

3	Info.	(1) ช่องโหว่ที่เกี่ยวข้องกับฮาร์ดแวร์ หมายถึง ข้อบกพร่องที่เกี่ยวข้องกับความมั่นคงปลอดภัยของฮาร์ดแวร์ เช่น ช่องโหว่ของการเข้ารหัสของระบบขายปลีกครบวงจร (Point of Sale; POS) ซึ่งส่งผลให้ผู้โจมตีสามารถขโมยข้อมูลบัตรเครดิตของผู้ใช้บริการ หรือช่องโหว่ของระบบสมองกลที่ใช้ควบคุมรถยนต์ ที่เมื่อถูกโจมตีผ่านเครือข่ายแล้วทำให้ผู้โจมตีสามารถควบคุมระบบต่างๆ ภายในรถยนต์คันนั้น ๆ ได้ เป็นต้น (2) ช่องโหว่ที่เกี่ยวข้องกับซอฟต์แวร์ หมายถึง ข้อบกพร่องที่เกี่ยวข้องกับซอฟต์แวร์ต่าง ๆ ที่เมื่อเกิดการโจมตีต่อซอฟต์แวร์นั้น ๆ แล้วจะส่งผลกระทบต่อความมั่นคงปลอดภัยของซอฟต์แวร์ และซอฟต์แวร์ระบบอื่น ๆ ที่เกี่ยวข้อง เช่น ช่องโหว่ของระบบปฏิบัติการที่เกี่ยวข้องกับการแชร์ไฟล์ผ่านระบบเครือข่ายคอมพิวเตอร์ที่หากผู้ไม่ประสงค์ดีโจมตีตอบริการแชร์ไฟล์สำเร็จอาจทำการลบโฟลเดอร์หรือไฟล์ต่าง ๆ โดยไม่ได้รับอนุญาต เป็นต้น (3) ช่องโหว่ที่เกี่ยวข้องกับการบริหารจัดการข้อมูล หมายถึง ข้อบกพร่องที่เกี่ยวข้องกับการจัดการข้อมูลต่าง ๆ ทั้งที่เป็นข้อมูลที่ไม่ได้จัดเก็บในรูปแบบดิจิทัลและข้อมูลในรูปแบบดิจิทัล เช่น หากองค์กรหรือบุคคลจัดเก็บข้อมูลซึ่งใช้ในการพิสูจน์ตัวจริงอย่างไม่เหมาะสม เมื่อข้อมูลนั้นรั่วไหลออกไปอาจส่งผลให้เกิดการโจมตีต่อองค์กรนั้น ๆ ได้หรือเปิดโอกาสให้มีการโจมตีต่อทรัพยากรอื่น ๆ เป็นต้น	
4	Info.	2. ภัยคุกคาม หรือ threat คือบุคคลหรือผู้ใดก็ตามที่สามารถใช้ประโยชน์จากช่องโหว่ที่มีเข้าถึงและทำลายความมั่นคงปลอดภัยของทรัพยากรสารสนเทศได้ ภัยคุกคามต่อทรัพยากรสารสนเทศจำแนกได้ 4 ลักษณะ คือ (1) การดักรับ หรือ interception หมายถึง เหตุการณ์ที่ผู้ไม่ประสงค์ดีเข้าถึงหรือดักรับข้อมูลโดยปราศจากสิทธิ์โดยถูกต้อง เช่น การดักรับที่รับส่งกันระหว่างผู้รับและผู้ส่งในระบบเครือข่ายคอมพิวเตอร์ (sniffing) การแอบอ่านข้อมูลจากหน้าจอของผู้อื่น การแอบฟังผู้อื่นพูดคุยกันเพื่อให้ได้ข้อมูลที่ตนเองไม่มีสิทธิ์เข้าถึง (2) การขัดจังหวะ หรือ interruption หมายถึง เหตุการณ์ที่ผู้ไม่ประสงค์ดีกระทำแล้วส่งผลให้ผู้ใช้งานที่มีสิทธิ์ไม่สามารถเข้าถึงหรือใช้งานทรัพยากรนั้น ๆ ได้ เช่น การตัดสายสัญญาณเครือข่ายการลบไฟล์ข้อมูล การทำลายคอมพิวเตอร์ หรือการนำเข้าข้อความที่ระบบประมวลผลแล้วทำให้ระบบปฏิเสธการให้บริการ เป็นต้น (3) การดัดแปลงแก้ไข หรือ modification หมายถึง การเข้าถึงและแก้ไขทรัพยากรสารสนเทศโดยไม่มีสิทธิ์เช่น การเปลี่ยนแปลงการปรับตั้งค่าต่าง ๆ ของระบบปฏิบัติการการอนุญาตให้มีการเข้าถึงจากระยะไกลโดยไม่มีการพิสูจน์ตัวจริง ซึ่งอาจส่งผลกระทบต่อความมั่นคงปลอดภัย การดักรับโดยการเปลี่ยนเส้นทางและการเปลี่ยนแปลงข้อมูลที่ถูกรับส่งผ่านเครือข่าย เป็นต้นโดยการดัดแปลงแก้ไขดังกล่าวอาจ	

		กระทำได้ในกรณีอื่น ๆ เช่น เพื่อนของนักศึกษาอาจแก้ไขไฟล์รายงานของนักศึกษาที่ถูกบันทึกไว้ในสื่อจัดเก็บข้อมูล เช่น แฟลชไดร์ฟโดยที่นักศึกษาไม่ทราบ เมื่อนักศึกษาส่งรายงานไปยังอาจารย์จึงพบว่าข้อมูลนั้นไม่ใช้ข้อมูลที่ถูกต้อง เป็นต้น (4) การปลอมแปลง หรือ fabrication หมายถึง การสร้างข้อมูลหรือสิ่งแปลกปลอมเข้าสู่ระบบสารสนเทศ เช่น การเพิ่มข้อมูลลงในระบบจัดการฐานข้อมูล การตั้งเครือข่ายไร้สายที่มีชื่อสถานีเหมือนกับเครือข่ายเป้าหมาย เพื่อดักรับข้อมูลต่าง ๆ และการปลอมแปลงหมายเลขไอพีเพื่อหลบเลี่ยงกลไกพิสูจน์ ตัวจริงเพื่อเข้าใช้งานเครือข่าย การปลอมแปลงตนเองเป็นบุคคลอื่นเพื่อหลอกถามข้อมูล เป็นต้น วัตถุประสงค์หลักของการปลอมแปลงจึงเกี่ยวข้องกับการล่อลวงให้เหยื่อเข้าใจผิดว่าข้อมูลหรือสารสนเทศนั้นเป็นข้อมูลหรือตัวตนจริง ๆ ของผู้นั้น หากเหยื่อตายใจและให้ข้อมูลหรือเปิดเผยข้อมูลสำคัญจะทำให้เกิดการละเมิดความมั่นคงปลอดภัยต่อเหยื่อนั้น ๆ เช่น การส่งจดหมายโดยอ้างว่าผู้ส่งเป็นหัวหน้างานและให้ส่งความลับขององค์กรไปยังอีเมล หรือให้จัดพิมพ์เอกสารแล้วส่งไปยังผู้โจมตี เป็นต้น	
5	Info.	3. การโจมตี หรือ attack คือการกระทำหรือผลที่เกิดขึ้นเมื่อเกิดภัยคุกคามต่อช่องโหว่ต่าง ๆ ที่มีอยู่ในทรัพยากรสารสนเทศ ทั้งนี้การโจมตีอาจไม่ได้มีต้นกำเนิดจากผู้ไม่ประสงค์ดีแต่เพียงอย่างเดียวก็เป็นได้เช่น ทรัพยากรสารสนเทศหนึ่งมีความลับไม่ควรถูกเผยแพร่ให้ผู้ไม่มีหน้าที่เกี่ยวข้องรับทราบ แต่ไม่ถูกกำหนดมาตรการควบคุมการเข้าถึงอย่างเหมาะสม อาจถูกเข้าถึงโดยผู้ใช้งานทั่วไป และนำข้อมูลนั้นไปเผยแพร่อันเป็นการทำลายความลับของทรัพยากรนั้น ๆ ทั้งนี้การกระทำดังกล่าวอาจเกิดขึ้นโดยเจตนาหรืออาจเกิดขึ้นจากอุบัติเหตุ การโจมตีอีกลักษณะหนึ่งที่ได้รับความนิยมคือการโจมตีต่อโครงสร้างพื้นฐานที่สำคัญของเป้าหมาย เช่น การทำให้ระบบปฏิเสธการให้บริการและการโจมตีด้วยเทคนิคเชิงสังคมอื่น ๆ เช่น การแอบอ้างเป็นพนักงานคอลเซนเตอร์เพื่อล่อลวงเป้าหมายให้กระทำการอย่างใดอย่างหนึ่งโดยเปิดเผยข้อมูลพิสูจน์ตัวจริงหรือการหลอกลวงให้ทำรายการบัญชีผ่านเอทีเอ็ม เป็นต้น	
6	Info.	4. ผู้ไม่ประสงค์ดี หรือ attacker คือ บุคคลหรือกระบวนการที่เกิดขึ้นจากมนุษย์เพื่อกระทำการโจมตีต่อทรัพยากรสารสนเทศเป้าหมาย จากนิยามดังกล่าวจะเห็นได้ว่ามีความหมายใกล้เคียงกับภัยคุกคามแต่จำกัดสาเหตุไว้ที่มนุษย์เท่านั้น ซึ่งผู้ไม่ประสงค์ดีอาจมีแรงจูงใจในการโจมตีต่อระบบที่แตกต่างกันออกไปเช่น ความประมาท ค่าตอบแทน และความสะใจ เป็นต้น ในปัจจุบันนิยมใช้คำว่า แฮกเกอร์ (hacker) สามารถจำแนกประเภทจากแรงจูงใจในการโจมตีต่อระบบได้หลายลักษณะ เช่น แฮกเกอร์สมัครเล่น แฮกเกอร์ หมวกขาว แฮกเกอร์หมวกดำ เป็นต้น คราวนี้เรามาเจาะลึกกันว่าลักษณะของแฮกเกอร์มีอะไรบ้าง (1) แฮกเกอร์มือสมัครเล่น หรือ script kiddy หมายถึง บุคคลทั่วไปที่โจมตีต่อ	

		ช่องโหว่ของระบบด้วยเครื่องมือหรือซอฟต์แวร์ที่ผู้ไม่ประสงค์ดีคนอื่นเผยแพร่ไว้โดยปราศจากความเข้าใจถึงกระบวนการทำงานของซอฟต์แวร์นั้น ๆ รวมไปถึงบุคคลทั่ว ๆ ไปที่ล่วงรู้ช่องโหว่ของการรักษาความมั่นคงปลอดภัยที่เข้าถึงหรือแก้ไขทรัพยากรที่ไม่มีสิทธิ์โดยไม่ได้ตั้งใจ เช่น การลบไฟล์เอกสารที่ใช้งานร่วมกันผ่านเครือข่ายได้เนื่องจากผู้ดูแลระบบกำหนดสิทธิ์ไว้ผิด เป็นต้น (2) แฮกเกอร์หมวกขาว หรือ white hat หมายถึง ผู้เชี่ยวชาญระบบคอมพิวเตอร์ที่ใช้ความสามารถดังกล่าวในการค้นหาช่องโหว่ และการโจมตีต่อระบบคอมพิวเตอร์ในเชิงป้องกันและรักษาความมั่นคงปลอดภัยให้กับระบบแล้วรายงานช่องโหว่หรือการโจมตีดังกล่าวต่อเจ้าของหรือผู้มีหน้าที่รับผิดชอบเพื่อให้ผู้ที่เกี่ยวข้องดำเนินการปรับปรุงความมั่นคงปลอดภัยและแก้ไขข้อบกพร่องนั้น ๆ ก่อนที่ช่องโหว่หรือข้อบกพร่องดังกล่าวจะถูกตรวจพบหรือถูกประกาศให้ทราบในที่สาธารณะ เช่น เว็บบอร์ดหรืออินเตอร์เน็ต เป็นต้น (3) แฮกเกอร์หมวกดำ หรือ black hat หมายถึง ผู้เชี่ยวชาญระบบคอมพิวเตอร์ที่ใช้ความสามารถดังกล่าวในการค้นหาและโจมตีต่อระบบคอมพิวเตอร์เพื่อการทำลายความมั่นคงปลอดภัยโดยมีผลประโยชน์ส่วนตัวเป็นแรงจูงใจ เช่น ค่าตอบแทนจากองค์กรอาชญากรรม การล้างแค้น หรือความคิดเห็นทางการเมือง เป็นต้น	
7	Info.	5. เอกซ์พลอยต์ หรือ exploit หมายถึง การโจมตีต่อช่องโหว่ที่มีในระบบสารสนเทศ เพื่อทำลายความมั่นคงปลอดภัย หรือเข้าใช้ประโยชน์จากช่องโหว่ที่มีอยู่ เช่น ช่องโหว่ของระบบจัดการเนื้อหาผ่านเว็บที่ถูกค้นพบและรายงาน อาจมีผู้ไม่ประสงค์ดีพัฒนาโปรแกรมที่สามารถโจมตีต่อช่องโหว่ดังกล่าวสำเร็จ แล้วแจกจ่ายให้กับผู้ที่สนใจนำโปรแกรมนี้ไปโจมตีต่อช่องโหว่นั้น นอกจากนี้ยังหมายถึงเทคนิควิธีที่ใช้ในการโจมตีด้วยเทคนิควิศวกรรมเชิงสังคม เช่น การพยายามตีสนิทกับเหยื่อซึ่งทำหน้าที่สำคัญในระบบสารสนเทศเพื่อให้ได้มาซึ่งข้อมูลที่เป็นประโยชน์ต่อการโจมตีหรือการล่อลวงเพื่อใช้ประโยชน์จากเหยื่อในการเข้าถึงทรัพยากรสารสนเทศ เป็นต้น	
8	Info.	6. เป้าหมาย (target) คือ บุคคล องค์กร ทรัพยากรสารสนเทศที่มีช่องโหว่และได้รับผลกระทบโดยตรงจากการการโจมตีที่อาจเกิดขึ้น	
9	Info.	7. วิธีการโจมตี (attack vector) คือ กระบวนการวิธีการเครื่องมือและเทคนิคที่ใช้โจมตีต่อช่องโหว่ที่มีในเป้าหมายของการโจมตี	

บทโทรทัศน์

เรื่อง : ความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และการสื่อสารข้อมูล

ตอน : การเข้ารหัสและการถอดรหัส

เจ้าของเนื้อหา : อาจารย์จรุงวิทย์ บุญเพิ่ม **ผู้เขียนสคริปต์ :** นายอำนาจ สุคนเขตร์

ลำดับ	ภาพ	เสียง	เวลา
1	Info.	จากเนื้อหาที่ผ่านมานักศึกษาได้ศึกษาถึงการจำแนกการรักษาความมั่นคงปลอดภัยรวมถึงหลักในการรักษาความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และการสื่อสารข้อมูลสำหรับในเนื้อหานี้เราจะได้ศึกษาเรื่อง การเข้ารหัส หรือ Encryption และการถอดรหัส หรือ Decryption ซึ่งเป็นการรักษาความมั่นคงปลอดภัยอีกวิธีการหนึ่งที่ได้รับความนิยมตั้งแต่ในอดีตมาจนถึงปัจจุบัน การเข้ารหัสและถอดรหัสนั้น มีวัตถุประสงค์เพื่อรักษาความลับของข้อมูล ข้อมูลนั้นจะถูกเปิดอ่านโดยบุคคลที่ได้รับอนุญาตเท่านั้น	
2	Info.	“การเข้ารหัส” หมายถึง การแปลงข้อความหรือข้อมูลอิเล็กทรอนิกส์รูปหนึ่งที่อ่านได้ (plaintext) ให้อยู่ในอีกรูปแบบหนึ่ง ที่เปลี่ยนแปลงไปจากเดิมซึ่งอ่านไม่ได้เรียกว่า cipher text ส่วน “การถอดรหัส” หมายถึง การแปลงข้อความหรือข้อมูลอิเล็กทรอนิกส์จากรูปแบบที่เปลี่ยนแปลงไปจากเดิม หรือ cipher textให้กลับไปอยู่ในรูปของข้อความหรือข้อมูลอิเล็กทรอนิกส์รูปแบบเดิม ก่อนการเปลี่ยนแปลง หรือ plain text สำหรับกระบวนการข้างต้นในการแปลงข้อมูลอิเล็กทรอนิกส์ที่อ่านได้เป็นข้อมูลอิเล็กทรอนิกส์ที่อ่านไม่ได้นี้เรียกว่า “การเข้ารหัส หรือ Encryption และการแปลงข้อมูลอิเล็กทรอนิกส์กลับให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ที่อ่านได้เรียกว่า “การถอดรหัส หรือ Decryption	
3	Info.	การเข้ารหัสแบ่งออกเป็น 2 ประเภทใหญ่ๆ คือ การเข้ารหัสแบบสมมาตร หรือ Symmetric Cryptography และ การเข้ารหัสแบบอสมมาตร หรือ Asymmetric Cryptography การเข้ารหัสแบบสมมาตรนี้เป็นการเข้ารหัสอย่างง่าย เช่น กำหนดเพียงให้เลื่อนพยัญชนะออกไปอีก 1 ตำแหน่ง กล่าวคือคำว่า “กฎหมาย” หากเลื่อนตำแหน่งพยัญชนะไป 1 ตัวพยัญชนะ ก็จะปรากฏเป็นดังนี้ “ขฏพาย” แทนคำว่า “กฎหมาย” จะเป็นการนำข้อมูลอิเล็กทรอนิกส์แบบธรรมดาเข้ารหัสโดยการแปลงข้อมูลนั้นให้อยู่ในรูป ที่ไม่สามารถอ่านได้ด้วยการใช้กุญแจดอกเดียวกันหรือสูตรเดียวกันผ่านกระบวนการทางคณิตศาสตร์ทั้งในการเข้ารหัสและถอดรหัสเพื่อแปลงข้อมูลอิเล็กทรอนิกส์ที่อ่านไม่ได้ให้เป็นข้อมูลอิเล็กทรอนิกส์ที่อ่านได้ ดังนั้นเมื่อใช้กุญแจในการเข้ารหัสแล้วก็ต้องส่งมอบกุญแจนั้นให้กับผู้รับอีกฝ่าย ซึ่งต้องใช้กุญแจดอกเดียวกันในการถอดรหัส และต้องมีการเก็บรายละเอียดเกี่ยวกับกุญแจไว้เป็นความลับเพื่อความปลอดภัยของข้อมูลอิเล็กทรอนิกส์ กรณีที่ไม่ประสงค์ให้	3

		บุคคลที่สามหรือบุคคลอื่นได้ล่วงรู้อันอาจนำกุญแจไปใช้ในทางมิชอบโดยการเปิดเผยข้อมูลให้สาธารณะชนได้รับรู้ อย่างไรก็ตามระบบการเข้ารหัสแบบสมมาตรมีข้อดี คือ กลงให้มีการเข้ารหัสแบบง่ายๆ เช่น การเลื่อนพยัญชนะ หรือกรณีที่มีการใช้เทคโนโลยีซับซ้อนขึ้น การเข้ารหัสแบบนี้จะช่วยให้สามารถเข้ารหัสและถอดรหัสได้รวดเร็ว แต่ก็มีข้อเสียเพราะข้อตกลงให้มีการเข้ารหัสแบบง่ายๆ อาจทำให้บุคคลอื่นล่วงรู้ได้ง่ายและในกรณีที่มีการใช้ระบบกุญแจก็จะประสบปัญหาในด้านการบริหารจัดการกุญแจ เพราะในการใช้กุญแจเพื่อเข้ารหัส และถอดรหัสนั้นจะต้องใช้กุญแจอันเดียวกัน ผู้สร้างกุญแจจึงต้องแจ้งให้บุคคลอื่นทราบเพื่อใช้ในการถอดรหัส ซึ่งการจะทำสำเนาให้บุคคลหลายคนเพื่อใช้ร่วมกันอาจจะก่อให้เกิดปัญหาในการระบุตัวบุคคล การแสดงความผูกพันหรือความรับผิดที่เกิดขึ้นจากการทำธุรกรรมในครั้งนั้น ดังนั้นโดยทั่วไปในการใช้กุญแจในระบบสมมาตรจึงมักมีการสร้างกุญแจขึ้นแบบสำหรับคนสองคนใช้ร่วมกัน ดังนั้นหากมีหลายคน ถ้าไม่ต้องการให้กุญแจซ้ำกันก็ต้องให้กุญแจหลายดอก เป็นจำนวนมากเพื่อความคล่องตัว และสะดวกในการใช้งานสำหรับกรณีที่ต้องติดต่อสื่อสารกับคนเป็นจำนวนมาก เช่น คนสี่คนติดต่อกันจะต้องใช้กุญแจคนละ 3 แบบ รวมทั้งสิ้นมีคู่กรณีได้ 6 คู่ รวมกุญแจทั้งสิ้น 6 แบบ ถ้าคน 100 คนจะต้องใช้กุญแจจำนวนมากซึ่งก็จะเกิดปัญหามากมายติดตามมาเช่นกันในการบริหจัดการกุญแจซึ่งมีเป็นจำนวนมาก	

บทโทรทัศน์

เรื่อง : ความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และการสื่อสารข้อมูล

ตอน : การรักษาความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และการสื่อสารข้อมูลด้วยไฟร์วอลล์

เจ้าของเนื้อหา : อาจารย์จรุงวิทย์ บุญเพิ่ม **ผู้เขียนสคริปต์ :** นายอำนาจ สุคนเขตร์

ลำดับ	ภาพ	เสียง	เวลา
1	Info.	ปัจจุบันอินเตอร์เน็ตมีบทบาทสำคัญต่อการดำเนินกิจกรรมต่างๆ เป็นอย่างมาก ไม่ว่าจะเป็นด้านการติดต่อสื่อสาร ธุรกิจ การศึกษา หรือว่าเพื่อความบันเทิง องค์กรต่างๆ ทั้งภาครัฐและเอกชน ต่างก็นำเอาเน็ตเวิร์กของตนเชื่อมต่อเข้ากับอินเตอร์เน็ต เพื่อที่จะได้รับประโยชน์เหล่านี้ แต่เราต้องไม่ลืมว่าการนำเอาเน็ตเวิร์กไปเชื่อมต่อกับอินเตอร์เน็ตนั้น ทำให้ใครก็ได้บนอินเตอร์เน็ตสามารถเข้ามายังเน็ตเวิร์กนั้นๆ ได้ ปัญหาที่ตามมาก็คือความปลอดภัยของระบบเน็ตเวิร์ก เช่น ทำให้เกิดความเสี่ยงต่อการถูกเจาะระบบ และ ขโมยข้อมูล เป็นต้น จากปัญหาดังกล่าวทำให้เราต้องมีวิธีการในการรักษาความปลอดภัย สิ่งที่สามารถช่วยลดความเสี่ยงนี้ได้ก็คือ ไฟร์วอลล์ โดยไฟร์วอลล์นั้นทำหน้าที่ป้องกันอันตรายต่างๆ จากภายนอกที่จะเข้ามายังเน็ตเวิร์กของเรา	
2	Info.	ในความหมายทางด้านการก่อสร้างแล้ว ไฟร์วอลล์ จะหมายถึง กำแพงที่เอาไว้ป้องกันไฟไม่ให้ลุกลามไปยังส่วนอื่นๆ ส่วนทางด้านคอมพิวเตอร์นั้นก็จะมีความหมายคล้ายๆ กันก็คือ เป็นระบบที่เอาไว้ป้องกันอันตรายจากอินเตอร์เน็ตหรือเน็ตเวิร์กภายนอกนั่นเอง ไฟร์วอลล์ เป็นคอมโพเน็นต์หรือกลุ่มของคอมโพเน็นต์ที่ทำหน้าที่ในการควบคุมการเข้าถึงระหว่างเน็ตเวิร์กภายนอกหรือเน็ตเวิร์กที่เราคิดว่าไม่ปลอดภัย กับเน็ตเวิร์กภายในหรือเน็ตเวิร์กที่เราต้องการจะป้องกัน โดยที่คอมโพเน็นต์นั้นอาจจะเป็นเราเตอร์ คอมพิวเตอร์ หรือเน็ตเวิร์ก ประกอบกันก็ได้ ขึ้นอยู่กับวิธีการหรือ Firewall Architecture ที่ใช้การควบคุมการเข้าถึงของไฟร์วอลล์นั้น สามารถทำได้ในหลายระดับและหลายรูปแบบขึ้นอยู่ชนิดหรือเทคโนโลยีของไฟร์วอลล์ที่นำมาใช้ เช่น เราสามารถกำหนดได้ว่าจะให้มีการเข้ามาใช้เซอร์วิสอะไรได้บ้าง จากที่ไหน เป็นต้น	
3	Info.	ไฟร์วอลล์ช่วยเพิ่มความปลอดภัยให้กับระบบได้โดยบังคับใช้นโยบายด้านความปลอดภัย โดยการกำหนดกฎให้กับไฟร์วอลล์ว่าจะอนุญาตหรือไม่ให้ใช้เซอร์วิสชนิดใดทำให้การพิจารณาดูแลและการตัดสินใจด้านความปลอดภัยของระบบเป็นไปได้ง่ายขึ้น เนื่องจากการติดต่อทุกชนิดกับเน็ตเวิร์กภายนอกจะต้องผ่านไฟร์วอลล์ การดูแลที่จุดนี้เป็นการดูแลความปลอดภัยในระดับของเน็ตเวิร์ก (Network-based Security) บันทึกข้อมูล กิจกรรมต่างๆ ที่ผ่านเข้าออกเน็ตเวิร์กได้อย่างมี	

		ประสิทธิภาพ ป้องกันเน็ตเวิร์กบางส่วนจากการเข้าถึงของเน็ตเวิร์กภายนอก เช่นถ้าหากเรามีบางส่วนที่ต้องการให้ภายนอกเข้ามาใช้เซอร์วิส (เช่นถ้ามีเว็บเซิร์ฟเวอร์) แต่ส่วนที่เหลือไม่ต้องการให้ภายนอกเข้ามากรณีเช่นนี้เราสามารถใช้ไฟร์วอลล์ช่วยได้ ไฟร์วอลล์บางชนิดสามารถป้องกันไวรัสได้ โดยทำการตรวจไฟล์ที่โอนย้ายผ่านทางโปรโตคอล HTTP, FTP และ SMTP	
4	Info.	ถึงแม้ว่าไฟร์วอลล์จะสามารถช่วยเพิ่มความปลอดภัยให้กับเน็ตเวิร์กได้มากโดยการตรวจดูข้อมูลที่ผ่านเข้าออก แต่อย่าลืมว่าสิ่งเหล่านี้ไม่สามารถป้องกันได้จากการใช้ไฟร์วอลล์ อันตรายที่เกิดจากเน็ตเวิร์กภายใน ไม่สามารถป้องกันได้เนื่องจากอยู่ภายในเน็ตเวิร์กเอง ไม่ได้ผ่านไฟร์วอลล์เข้ามา อันตรายจากภายนอกที่ไม่ได้ผ่านเข้ามาทางไฟร์วอลล์ เช่นการ Dial-up เข้ามายังเน็ตเวิร์กภายในโดยตรงโดยไม่ได้ผ่านไฟร์วอลล์ อันตรายจากวิธีใหม่ๆ ที่เกิดขึ้น ทุกวันนี้มีการพบช่องโหว่ใหม่ๆ เกิดขึ้นทุกวัน เราไม่สามารถไว้ใจไฟร์วอลล์โดยการติดตั้งเพียงครั้งเดียวแล้วก็หวังให้มันปลอดภัยตลอดไป เราต้องมีการดูแลรักษาอย่างต่อเนื่องสม่ำเสมอ ไวรัส ถึงแม้จะมีไฟร์วอลล์บางชนิดที่สามารถป้องกันไวรัสได้ แต่ก็ยังไม่มีไฟร์วอลล์ชนิดใดที่สามารถตรวจสอบไวรัสได้ในทุกๆ โปรโตคอล	
5	Info.	ชนิดของไฟร์วอลล์แบ่งตามเทคโนโลยีที่ใช้ในการตรวจสอบและควบคุม แบ่งได้เป็น Packet Filtering Proxy Service และ Stateful Inspection Packet Filter คือเราเตอร์ที่ทำการหาเส้นทางและส่งต่อ (route) อย่างมีเงื่อนไข โดยจะพิจารณาจากข้อมูลส่วนที่อยู่ในเฮดเดอร์ (header) ของแพ็กเก็ตที่ผ่านเข้ามา เทียบกับกฎ (rules) ที่กำหนดไว้และตัดสินว่าควรจะทิ้ง (drop) แพ็กเก็ตนั้นไปหรือว่าจะยอม (accept) ให้แพ็กเก็ตนั้นผ่านไปได้ ในการพิจารณาเฮดเดอร์ Packet Filter จะตรวจสอบในระดับของอินเตอร์เน็ตเลเยอร์ (Internet Layer) และทรานสปอร์ตเลเยอร์ (Transport Layer) ในอินเตอร์เน็ตโมเดล ซึ่งในอินเตอร์เน็ตเลเยอร์จะมีแอตทริบิวต์ที่สำคัญต่อ Packet Filtering ดังนี้ ☐ ไอพีต้นทาง ☐ ไอพีปลายทาง ☐ ชนิดของโปรโตคอล (TCP UDP และ ICMP) และในระดับของทรานสปอร์ตเลเยอร์ มีแอตทริบิวต์ที่สำคัญคือ ☐ พอร์ตต้นทาง ☐ พอร์ตปลายทาง	

		☐ แฟล็ก (Flag ซึ่งจะมีเฉพาะในเฮดเดอร์ของแพ็กเก็ต TCP) ☐ ชนิดของ ICMP message (ในแพ็กเก็ต ICMP) ซึ่งพอร์ตของทรานสปอร์ตเลเยอร์ คือทั้ง TCP และ UDP นั้นจะเป็นสิ่งที่บอกถึงแอพพลิเคชันที่แพ็กเก็ตนั้นต้องการติดต่อด้วยเช่น พอร์ต 80 หมายถึง HTTP, พอร์ต 21 หมายถึง FTP เป็นต้น ดังนั้นเมื่อ Packet Filter พิจารณาเฮดเดอร์ จึงทำให้สามารถควบคุมแพ็กเก็ตที่มาจากที่ต่างๆ และมีลักษณะต่างๆ (ดูได้จากแฟล็กของแพ็กเก็ต หรือ ชนิดของ ICMP ในแพ็กเก็ต ICMP) ได้ เช่น ห้ามแพ็กเก็ตทุกชนิดจาก crack.cracker.net เข้ามายังเน็ตเวิร์ก 203.154.207.0/24 , ห้ามแพ็กเก็ตที่มีไอพีต้นทางอยู่ในเน็ตเวิร์ก 203.154.207.0/24 ผ่านเราเตอร์เข้ามา (ในกรณีนี้เพื่อเป็นการป้องกัน ip spoofing) เป็นต้น Packet Filtering สามารถอิมพลีเมนต์ได้จาก 2 แพล็ตฟอร์ม คือ ☐ เราเตอร์ที่มีความสามารถในการทำ Packet Filtering (ซึ่งมีในเราเตอร์ส่วนใหญ่อยู่แล้ว) ☐ คอมพิวเตอร์ที่ทำหน้าที่เป็นเราเตอร์	
6	Info.	ซึ่งจะมีข้อได้เปรียบเสียเปรียบกันดังนี้ **เราเตอร์** **ข้อดี** ประสิทธิภาพสูงมีจำนวนอินเตอร์เฟสมาก **ข้อเสีย** เพิ่มเติมฟังก์ชันการทำงานได้ยาก, อาจต้องการหน่วยความจำมาก **คอมพิวเตอร์ที่ทำหน้าที่เป็นเราเตอร์** **ข้อดี** เพิ่มฟังก์ชันการทำงานได้ไม่จำกัด **ข้อเสีย** ประสิทธิภาพปานกลาง,จำนวนอินเตอร์เฟสน้อย,อาจมีความเสี่ยงจากระบบปฏิบัติการที่ใช้	
7	Info.	ข้อดี-ข้อเสียของ Packet Filtering **ข้อดี** 1. ไม่ขึ้นกับแอพพลิเคชัน 2.. มีความเร็วสูง 3. รองรับการขยายตัวได้ดี **ข้อเสีย**	

		บางโปรโตคอลไม่เหมาะสมกับการใช้ Packet Filtering เช่น FTP, ICQ	
8	Info.	**Proxy** Proxy หรือ Application Gateway เป็นแอพพลิเคชันโปรแกรมที่ทำงานอยู่บนไฟร์วอลล์ที่ตั้งอยู่ระหว่างเน็ตเวิร์ก 2 เน็ตเวิร์ก ทำหน้าที่เพิ่มความปลอดภัยของระบบเน็ตเวิร์กโดยการควบคุมการเชื่อมต่อระหว่างเน็ตเวิร์กภายในและภายนอก Proxy จะช่วยเพิ่มความปลอดภัยได้มากเนื่องจากมีการตรวจสอบข้อมูลถึงในระดับของแอพพลิเคชันเลเยอร์ (Application Layer) เมื่อไคลเอนต์ต้องการใช้เซอร์วิสภายนอก ไคลเอนต์จะทำการติดต่อไปยัง Proxy ก่อน ไคลเอนต์จะเจรจา (negotiate) กับ Proxy เพื่อให้ Proxy ติดต่อไปยังเครื่องปลายทางให้ เมื่อ Proxy ติดต่อไปยังเครื่องปลายทางให้แล้วจะมีการเชื่อมต่อ (connection) 2 การเชื่อมต่อ คือ ไคลเอนต์กับ Proxy และ Proxy กับเครื่องปลายทาง โดยที่ Proxy จะทำหน้าที่รับข้อมูลและส่งต่อข้อมูลให้ใน 2 ทิศทาง ทั้งนี้ Proxy จะทำหน้าที่ในการตัดสินใจว่าจะให้มีการเชื่อมต่อกันหรือไม่ จะส่งต่อแพ็กเก็ตให้หรือไม่ **ข้อดี-ข้อเสียของ Proxy** **ข้อดี** 1. มีความปลอดภัยสูง 2.รู้จักข้อมูลในระดับแอพพลิเคชัน **ข้อเสีย** 1. ประสิทธิภาพต่ำ 2. แต่ละบริการมักต้องการโปรเซสของตนเอง 3. สามารถขยายตัวได้ยาก	
9	Info.	**Stateful Inspection Technology** โดยปกติแล้ว Packet Filtering แบบธรรมดา (ที่เป็น Stateless แบบที่มีอยู่ในเราเตอร์ทั่วไป) จะควบคุมการเข้าออกของแพ็กเก็ตโดยพิจารณาข้อมูลจากเฮดเดอร์ของแต่ละแพ็กเก็ต นำมาเทียบกับกฎที่มีอยู่ ซึ่งกฎที่มีอยู่ก็จะเป็นกฎที่สร้างจากข้อมูลส่วนที่อยู่ในเฮดเดอร์เท่านั้น ดังนั้น Packet Filtering แบบธรรมดาจึงไม่สามารถทราบได้ว่า แพ็กเก็ตนี้อยู่ส่วนใดของการเชื่อมต่อ เป็นแพ็กเก็ตที่เข้ามาติดต่อใหม่หรือเปล่า หรือว่าเป็นแพ็กเก็ตที่เป็นส่วนของการเชื่อมต่อที่เกิดขึ้นแล้ว เป็นต้น	

		Stateful Inspection เป็นเทคโนโลยีที่เพิ่มเข้าไปใน Packet Filtering โดยในการพิจารณาว่าจะยอมให้แพ็กเก็ตผ่านไปนั้น แทนที่จะดูข้อมูลจากเฮดเดอร์เพียงอย่างเดียว Stateful Inspection จะนำเอาส่วนข้อมูลของแพ็กเก็ต (message content) และข้อมูลที่ได้จากแพ็กเก็ตก่อนหน้านี้ที่ได้ทำการบันทึกเอาไว้ นำมาพิจารณาด้วย จึงทำให้สามารถระบุได้ว่าแพ็กเก็ตใดเป็นแพ็กเก็ตที่ติดต่อเข้ามาใหม่หรือว่าเป็นส่วนหนึ่งของการเชื่อมต่อที่มีอยู่แล้ว ตัวอย่างผลิตภัณฑ์ทางการค้าที่ใช้ Stateful Inspection Technology ได้แก่ Check Point Firewall-1 , Cisco Secure Pix Firewall, SunScreen Secure Net และส่วนที่เป็น open source แจกฟรี ได้แก่ NetFilter ใน Linux (iptables ในลีนุกซ์เคอร์เนล 2.3 เป็นต้นไป)	