รายงานการวิจัย

เรื่อง

การพัฒนาแนวทางการสืบสวนอาชญากรรมทางไซเบอร์ต่อบริการธนาคารอิเล็กทรอนิกส์ และวิเคราะห์เทคนิคเทคโนโลยีสารสนเทศเพื่อสร้างต้นแบบที่เสริมสร้างความมั่นคง

Development of Guidelines for Cyber-crime Investigation towards Electronic Banking Services and Analysis of Information Technology Techniques to Build a Security-enhanced Prototype

เอกชัย พ่วงพรพิทักษ์ และคณะ

กรมสอบสวนคดีพิเศษ กระทรวงยุติธรรม

พฤษภาคม 2565

รายงานการวิจัย

เรื่อง

การพัฒนาแนวทางการสืบสวนอาชญากรรมทางไซเบอร์ ต่อบริการธนาคารอิเล็กทรอนิกส์ และวิเคราะห์เทคนิคเทคโนโลยีสารสนเทศ เพื่อสร้างต้นแบบที่เสริมสร้างความมั่นคง

Development of Guidelines for Cyber-crime Investigation towards Electronic Banking Services and Analysis of Information Technology Techniques to Build a Security-enhanced Prototype

เอกชัย พ่วงพรพิทักษ์ และคณะ

กรมสอบสวนคดีพิเศษ กระทรวงยุติธรรม

พฤษภาคม 2565

งานวิจัยนี้ได้รับการสนับสนุนจากกรมสอบสวนคดีพิเศษ โดยทุนอุดหนุนจากงบประมาณกองทุนส่งเสริมวิทยาศาสตร์ วิจัยและนวัตกรรม (ววน.) ปีงบประมาณ 2564

กิตติกรรมประกาศ

งานวิจัยนี้ได้รับการสนับสนุนจากสำนักงานคณะกรรมการส่งเสริมวิทยาศาสตร์ วิจัยและนวัตกรรม (สกสว) โดยเป็นความร่วมมือระหว่างกรมสอบสวนคดีพิเศษ กระทรวงยุติธรรม กับกลุ่มวิจัย Information Security & Advanced Network (ISAN) คณะวิทยาการสารสนเทศ มหาวิทยาลัยมหาสารคาม ขอขอบคุณ นายไตรยฤทธิ์ เตมหิวงศ์ อธิบดีกรมสอบสวนคดีพิเศษ พันตำรวจโท วิชัย สุวรรณประเสริฐ (อดีตผู้อำนวยการกองคดีเทคโนโลยีและสารสนเทศ) นางสาวรัศมี สีตลวรางค์ ผู้อำนวยการกองคดีเทคโนโลยีและสารสนเทศ และขอบคุณ คณะวิทยาการสารสนเทศ มหาวิทยาลัยมหาสารคาม ที่ให้การสนับสนุนการดำเนินการวิจัยนี้ ขอขอบคุณ พันตำรวจเอก ญาณพล ยั่งยืน กรรมการผู้ทรงคุณวุฒิ คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (และอดีตรองอธิบดีกรมสอบสวนคดีพิเศษ) เป็นอย่างยิ่ง ที่ให้คำปรึกษาในการจัดทำการวิจัย ผู้วิจัยยังขอขอบคุณ ผศ.ดร.ดรุณี พ่วงพรพิทักษ์ (ผู้ช่วยวิจัย) นายภารเดช คะเชนรัมย์ (ผู้ช่วยวิจัย) นายคธาวุฒิ จันบัวลา (ผู้ช่วยวิจัย) นางสาวอุมาพร จันโสภา (ผู้ช่วยวิจัย) นายณัฐวุฒิ ศรีวิบูลย์ (ผู้ช่วยวิจัย) และทีมงานจาก ISAN ที่ได้มีส่วนร่วมมือในการวิจัย สุดท้ายขอขอบพระคุณพ่อและแม่ของนักวิจัยทั้งสองอย่างสูงสุด ที่ให้กำเนิดและอบรมเลี้ยงดู เราทั้งสองคนมาเป็นอย่างดี จนได้มีโอกาสทำงานวิจัยนี้ร่วมกันให้กับสังคม.

คณะผู้วิจัย

พฤษภาคม 2565

บทคัดย่อ

อาชญากรรมที่เกี่ยวข้องกับระบบธนาคารอิเล็กทรอนิกส์นั้นเป็นปัญหาที่มีความสำคัญต่อเศรษฐกิจและสังคมของประเทศอย่างมาก อีกทั้งยังเป็นปัญหาที่มีความซับซ้อนด้านกฎหมาย การสืบสวน และเทคนิควิธีที่อาชญากรใช้อีกด้วย ดังนั้น จึงมีความจำเป็นต้องบูรณาการความสามารถของทั้งฝ่ายสืบสวนสอบสวนทางกฎหมาย และความสามารถทางเทคนิคความมั่นคงเทคโนโลยีสารสนเทศเพื่อใช้ในการแก้ไขปัญหา งานวิจัยนี้ เป็นการร่วมมือของฝ่ายกฎหมายที่ทำด้านการสืบสวนสอบสวนคดีเทคโนโลยีสารสนเทศ และฝ่ายเทคนิคความมั่นคงเทคโนโลยีสารสนเทศ จากศาสตร์วิทยาการคอมพิวเตอร์ที่เกี่ยวข้อง เพื่อทำการวิเคราะห์ปัญหาทั้งทางข้อกฎหมายและแนวทางในการสืบสวนสอบสวน และปัญหาทางเทคนิคความมั่นคงไซเบอร์ของการจู่โจมเอชทีทีพีเอส ซึ่งเป็นเทคนิคสำคัญในการป้องกัน ผลลัพธ์จากงานวิจัยนี้ ได้ให้แนวคิดทางกฎหมายในการสืบสวนสอบสวน ที่มีประสิทธิภาพ ทั้งได้ผลวิเคราะห์ปัญหาทางเทคนิคเพื่อเพิ่มความสามารถในการสืบสวนสอบสวน รวมถึงออกแบบและพัฒนาต้นแบบระบบและแนวทางในการสำหรับป้องกัน เพื่อเสริมความมั่นคงให้กับระบบ

คำสำคัญ ระบบธนาคารอิเล็กทรอนิกส์, คดีเทคโนโลยีสารสนเทศ, โครงสร้างกุญแจสาธารณะ, เอชทีทีพีเอส

Abstract

Crimes related to electronic banking systems are significant problems, impacting the national economy and society. In addition, the problems are complicated in terms of laws, crime investigation, and cyber-security techniques deployed by the criminal. So, it is necessary to integrate the abilities of both crime investigators and IT security technicians to solve the problems. This research is the cooperation between IT crime investigators and IT security technicians from the computer science field. The purposes are to analyze the problems in terms of law and crime-investigation techniques as well as cybersecurity techniques, particularly the attacks on HTTPS, which is an important technique to protect e-banking systems. The outcomes of this research are an efficient crime investigation approach, an analysis of the cybersecurity techniques that would enhance the crime investigation, and the design & development of a system prototype as well as the protection method to enhance the security of the e-banking systems.

Keywords Electronic Banking Systems, IT Crimes, Public Key Infrastructure (PKI), HTTPS

สารบัญ

หน้า

สารบัญตาราง

หน้า

สารบัญภาพ

หน้า

บทที่ 1
บทนำ

1.1 ความเป็นมาและความสำคัญ

ในการก้าวเข้าสู่ยุค Thailand 4.0 หน่วยงานทั้งรัฐและเอกชน ได้ให้บริการต่าง ๆ แก่ประชาชนและลูกค้า ผ่านเครือข่ายอินเทอร์เน็ต ทั้งใช้ในเรื่องของการพาณิชย์อิเล็กทรอนิกส์ (e-commerce), ธนาคารอิเล็กทรอนิกส์ (e-banking), ระบบการเงิน ระบบยื่นฟอร์มจ่ายภาษีออนไลน์ และระบบอื่น ๆ รวมถึงใช้ในการบริการข้อมูลข่าวสาร ที่สามารถเข้าถึงได้อย่างกว้างขวาง โดยเฉพาะอย่างยิ่งจากข้อมูลล่าสุด เมื่อ 18 กุมภาพันธ์ พ.ศ. 2561 จาก internetworldstats.com พบว่าประเทศไทยมีจำนวนผู้ใช้อินเทอร์เน็ตสูงเป็นอันดับที่ 16 ของโลก จำนวนมากกว่า 57 ล้านคน คิดเป็น 82.4% ของประชากรทั้งประเทศ แต่บริการสารพัดอย่างผ่านระบบเว็บไซต์เหล่านี้ ได้ตกเป็นเป้าหมายสำคัญของการก่ออาชญากรรมทางด้านเทคโนโลยีสารสนเทศ ดังจะเห็นได้จากรายงานข่าว การจู่โจมระบบ e-banking, ระบบการเงิน ระบบ e-commerce และระบบต่าง ๆ ผ่านเว็บไซต์ของหน่วยงานในประเทศไทยทั้งภาครัฐและเอกชน ในรอบหลายปีที่ผ่านมา

อาชญากรได้อาศัยประโยชน์และคุณสมบัติของเทคโนโลยีเหล่านี้ มาใช้ก่ออาชญากรรมมากขึ้น โดยเฉพาะอย่างยิ่งกับบริการธนาคารอิเล็กทรอนิกส์ (e-banking) ทำให้รูปแบบการก่ออาชญากรรมมีความสลับซับซ้อน ซ่อนเร้น ทำให้ในการดำเนินการทางกฎหมาย มีความยากต่อการสืบสวนสอบสวน ประกอบกับพยานหลักฐานที่เกิดจากผลของการก่ออาชญากรรมหาได้ยาก ทั้งยังถูกแก้ไข เปลี่ยนแปลง และสูญหายหรือถูกทำลายได้ง่าย นอกจากนี้ผลของการก่ออาชญากรรมทำให้เกิดผลเสียหายอย่างมาก และแพร่กระจายในวงกว้าง จึงมีความจำเป็นต้องพัฒนาแนวทางการติดตามตรวจสอบ เพื่อช่วยในขบวนการสืบสวนสอบสวนของเจ้าหน้าที่รัฐให้เหมาะสม

ในทางด้านเทคนิคความมั่นคงเทคโนโลยีสารสนเทศ กลไกหลักสำหรับการรักษาความมั่นคงของระบบเว็บไซต์ คือการกำหนดให้เว็บไซต์ทำงานบนโพรโทคอล Hyper-Text Transfer Protocol (HTTP) Over Transport Layer Security (TLS) ที่เรียกว่า HTTPS [1] และประยุกต์รหัสผ่านใช้ครั้งเดียว (One Time Password) ในการพิสูจน์ตัวจริงชั้นที่สอง แต่ปรากฏว่า ก็ยังมีข่าวให้เห็นว่ามิจฉาชีพสามารถหาจุดอ่อนและก่ออาชญากรรมต่อระบบได้ กล่าวคือ การใช้ HTTPS และ OTP ตามมาตรฐานที่ใช้อยู่ในประเทศไทย ยังมีจุดอ่อนทางเทคนิคที่ควรวิจัยเพื่อวิเคราะห์จุดอ่อนและเสนอแนวทางแก้ไข

จากการศึกษางานวิจัยที่เกี่ยวข้อง พบว่าในส่วนของการโจมตี HTTPS นั้นมีเทคนิคหลายวิธีที่ถูกนำใช้ เช่น SSL Strip [2], DROWN [3], POODLE [4], Homograph phishing [5] และอื่น ๆ โดย SSL Strip เป็นเทคนิคการถอด TLS ออกจากกลไกการป้องกัน ถูกเสนอโดย Marlinspike [2] ในปี

ค.ศ. 2009 DROWN (Decrypting RSA with Obsolete and Weakened eNcryption) และ POODLE (Padding Oracle On Downgraded Legacy Encryption) ถูกเสนอในปี ค.ศ. 2014 และ 2016 เพื่อใช้ลดระดับการเข้ารหัสไปสู่อัลกอริทึมที่ล้าสมัยหรือสามารถที่จะโจมตีได้ Homograph Phishing ถูกเสนอในปี ค.ศ. 2017 อาศัยการจดชื่อโดเมนด้วย Unicode ให้ได้ชื่อเหมือนหรือคล้ายกับระบบที่เหยื่อใช้งานและใช้การ Phishing ในการโจมตี นอกจากนี้ ยังมีเทคนิคอื่น ๆ อีกมากมายที่ถูกใช้โจมตี HTTPS ไปทั่วโลก ในช่วง 3-4 ปีที่ผ่านมา จนมีการกล่าวกันว่าระบบความมั่นคงโดยอาศัย HTTPS แทบจะล่มสลาย [6] โดยหลายเทคนิคก็เคยถูกใช้ในการโจมตีระบบ e-banking และระบบต่าง ๆ ของหน่วยงานรัฐและเอกชน ในประเทศไทยมาแล้ว ในส่วนของ OTP โดยทั่วไปจะใช้เป็นปราการด่านสองในการพิสูจน์ความเป็นตัวจริง OTP ที่นิยมใช้มากที่สุดในประเทศไทยคือ SMS OTP แต่ว่า SMS OTP โดนวิจารณ์โดยหลายงานวิจัย [7, 8] ว่าสามารถถูกปลอมแปลงได้ง่าย และอาจถูกจู่โจมด้วย Trojan Horse จนกระทั่งในช่วงหลายปีที่ผ่านมา จุดอ่อนนี้ ได้เกิดเป็นคดีการโจมตีระบบ e-banking ในประเทศไทยหลายแห่ง โดยสามารถจู่โจม SMS OTP ที่เป็นด่านป้องกันด่านที่สองนี้ได้ นอกจากนี้ ด้วยความไม่มั่นคงของ SMS OTP เมื่อเดือนมิถุนายน ค.ศ. 2017 เอกสาร NIST SP 800-63B [9] เกี่ยวกับข้อปฏิบัติด้านการพิสูจน์ตัวจริง ออกโดย National Institute of Standards and Technology (NIST) ของประเทศสหรัฐอเมริกา จึงไม่แนะนำให้ใช้ SMS OTP สำหรับการพิสูจน์ตัวจริงอีกต่อไป ในข้อเสนองานวิจัยนี้ จะได้วิเคราะห์ปัญหา และออกแบบแนวทางแก้ไข โดยมีการต่อยอดบูรณาการ ระบบ OTP เข้ากับแนวทางแก้ไขฝั่ง HTTPS เพื่อแก้ปัญหาได้ดียิ่งขึ้น

จะเห็นได้ว่าการจัดการกับอาชญากรรมที่เกี่ยวข้องกับระบบธนาคารอิเล็กทรอนิกส์นั้น มีปัญหาทั้งความซับซ้อนด้านกฎหมาย การสืบสวน และยังมีความซับซ้อนของเทคนิควิธีที่อาชญากรใช้อีกด้วย ดังนั้นจึงมีความจำเป็นต้องบูรณาการความสามารถของทั้งฝ่ายสืบสวนสอบสวนทางกฎหมายและความสามารถทางเทคนิคความมั่นคงเทคโนโลยีสารสนเทศ เพื่อใช้ในการแก้ไขปัญหา

ข้อเสนองานวิจัยนี้ เป็นการร่วมมือของฝ่ายกฎหมายที่ทำด้านการสืบสวนสอบสวนคดีเทคโนโลยีสารสนเทศ และฝ่ายเทคนิคความมั่นคงเทคโนโลยีสารสนเทศ จากศาสตร์วิทยาการคอมพิวเตอร์ที่เกี่ยวข้อง เพื่อทำการวิเคราะห์ปัญหาทั้งทางข้อกฎหมายและแนวทางในการสืบสวนสอบสวน และปัญหาทางเทคนิคของการจู่โจม HTTPS และ OTP ซึ่งเป็นปราการสำคัญในการป้องกันซึ่งการโจมตีและก่ออาชญากรรมทางคอมพิวเตอร์ดังกล่าว เป็นปัญหาที่มีความสำคัญต่อเศรษฐกิจสังคม และการบริหารประเทศ อย่างมาก โดยข้อเสนองานวิจัยนี้ จะได้ให้แนวคิดทางกฎหมายในการสืบสวนสอบสวนที่มีประสิทธิภาพและเป็นรูปธรรม ทั้งยังได้ผลวิเคราะห์ปัญหาทางเทคนิคเพื่อเพิ่มความสามารถในการสืบสวนสอบสวน รวมถึงออกแบบและพัฒนาต้นแบบซอฟต์แวร์ และแนวทางสำหรับป้องกันเพื่อเสริมความมั่นคงให้กับระบบ ผลลัพธ์ที่ได้จากโครงการนี้ คือได้แนวคิดใหม่ทางวิจัยที่วิเคราะห์ข้อจำกัดและข้อที่อาจเป็นไปด้านทั้งทางกฎหมายและทางเทคนิค ในการรับมือกับปัญหาที่

เกิดขึ้น และยังได้ต้นแบบซอฟต์แวร์ ที่สามารถนำไปประยุกต์ใช้กับระบบเว็บไซต์ของหน่วยงานทั้งภาครัฐและเอกชน ให้มีความมั่นคง สามารถป้องกันการโจมตีได้ดียิ่งขึ้น ซึ่งในที่สุดจะช่วยป้องกันการเกิดอาชญากรรมทางคอมพิวเตอร์ที่เป็นภัยคุกคามทางเทคโนโลยีสารสนเทศที่เป็นอุปสรรคสำคัญ ต่อการบริการประชาชนผ่านเครือข่ายอินเทอร์เน็ต และอาจสร้างความเสียหาย ทั้งกับระบบการให้บริการประชาชน ระบบธนาคาร และระบบอื่น ๆ ที่มีความสำคัญต่อเศรษฐกิจ สังคม และการบริหารประเทศ

1.2 วัตถุประสงค์ของการวิจัย

1) วิเคราะห์ปัญหาอาชญากรรม กรณีการกระทำความผิดอาญาในรูปแบบต่าง ๆ ต่อระบบธนาคารอิเล็กทรอนิกส์ที่เกิดขึ้น ทั้งทางเทคนิคความมั่นคงเทคโนโลยีสารสนเทศ และเทคนิคทางกฎหมายที่เกี่ยวกับการสืบสวนสอบสวน

2) วิเคราะห์กฎหมาย ระเบียบ ที่เกี่ยวข้องกับการบริการธนาคารอิเล็กทรอนิกส์ และคดีเทคโนโลยีสารสนเทศ ในประเทศไทยที่มีอยู่ในปัจจุบัน

3) วิเคราะห์เทคนิควิธีทางด้านความมั่นคงเทคโนโลยีสารสนเทศ ที่เกี่ยวข้องกับการโจมตี HTTPS และ PKI

4) บูรณการผลที่ได้ในข้อที่ 1 ถึง 3 เพื่อออกแบบ แนวทางในการติดตาม ตรวจสอบ การกระทำผิดอาญาต่อระบบธนาคารอิเล็กทรอนิกส์

5) ออกแบบและพัฒนาต้นแบบระบบและเทคนิควิธี เพื่อการป้องกันปัญหาอาชญากรรมต่อระบบธนาคารอิเล็กทรอนิกส์

1.3 ขอบเขตการวิจัย

1) รวบรวม วิเคราะห์ กฎหมาย ระเบียบ ที่เกี่ยวข้องกับบริการธนาคารอิเล็กทรอนิกส์ในประเทศไทยที่มีอยู่ในปัจจุบัน และสามารถนำผลวิจัยเป็นแนวทางในการพัฒนากฎหมายในอนาคตได้

2) ศึกษา วิเคราะห์กรณีการกระทำความผิดอาญาในรูปแบบต่าง ๆ ที่เกี่ยวข้องกับบริการธนาคารอิเล็กทรอนิกส์ในประเทศไทย โดยบูรณาการทั้งด้านกฎหมายและด้านเทคนิคทาง IT Security

3) วิเคราะห์หาแนวทางในการติดตาม ตรวจสอบและการสืบสวน อาชญากรรมที่เกี่ยวข้องกับบริการธนาคารอิเล็กทรอนิกส์ในประเทศไทย ซึ่งส่งผลกระทบโดยตรงต่อด้านระบบเศรษฐกิจ ระบบสังคมที่เกี่ยวข้องกับ ความสงบเรียบร้อย และศีลธรรมอันดีของประชาชน รวมถึงความมั่นคงของประเทศ

4) การวิเคราะห์ปัญหาของระบบเว็บไซต์ โดยมองปัญหา HTTPS (ทั้งตัวเทคนิควิธีของมันเองและจุดอ่อนในส่วนของ PKI ที่เป็นพื้นฐาน) โดยเน้นที่การจู่โจมด้วยเทคนิค SSL Strip และเสนอแนวทางในการแก้ไข โดยมุ่งพัฒนา Software API สำหรับให้ผู้พัฒนา Web Site เรียกใช้งานเพื่อเสริมความมั่นคงของ HTTPS ที่อาจมีจุดอ่อน และ ยังพัฒนา Mobile Application ที่เสริมประสิทธิภาพของระบบ OTP ให้มีความมั่นคงมากขึ้น และสามารถบูรณาการเข้ากับ HTTPS ให้เสริมความมั่นคงมากยิ่งขึ้น ผลการวิจัยจะได้ต้นแบบ ที่สามารถนำไปพัฒนาต่อยอด เพื่อใช้กับระบบเว็บไซต์ของหน่วยงานภาครัฐและเอกชน เพื่อป้องกันความเสียหายที่จะเกิดจากการโจมตี ซึ่งช่วยทำให้ ระบบการให้บริการเว็บไซต์ของหน่วยงานภาครัฐของประเทศไทยมีความมั่นคงมากขึ้น และประชาชนผู้ใช้งานปลอดภัยจากการถูกแอบอ้างชื่อ เข้าใช้งานระบบ

1.4 คำจำกัดความที่ใช้ในงานวิจัย

1) Hyper Text Transfer Protocol (HTTP) คือ โพรโทคอลในระดับชั้นแอปพลิเคชันของชุด โพรโทคอล Transmission Control Protocol/Internet Protocol (TCP/IP) ซึ่งกำหนดรูปแบบการร้องขอข้อมูลของไคลเอนท์ ในรูปแบบ HTTP Request ผ่านทางโปรแกรมเว็บเบราว์เซอร์ไปยังเซิร์ฟเวอร์ และกำหนดรูปแบบการถ่ายโอนไฟล์จากทางด้านเซิร์ฟเวอร์ไปยังไคลเอนท์ ซึ่งเมื่อเซิร์ฟเวอร์ได้รับการร้องขอ ก็จะทำการค้นหาไฟล์ที่ถูกระบุใน Uniform Resource Locator (URL) ซึ่งเป็นที่อยู่ของไฟล์หรือเว็บไซต์บนอินเทอร์เน็ต ถ้าพบก็จะทำการตอบกลับ HTTP Response พร้อมกับส่งไฟล์ดังกล่าวไปให้กับเว็บเบราว์เซอร์เพื่อแสดงผลที่ฝั่งของไคลเอนท์

2) การโจมตีแบบแทรกกลางการสื่อสาร (Man In The Middle Attack: MITM) เป็นรูปแบบการโจมตีที่ผู้โจมตีเข้าแทรกกลางการสื่อสารระหว่างคอมพิวเตอร์สองเครื่อง โดยทำการดักจับข้อมูลที่รับและส่ง ในระหว่างการสื่อสาร ซึ่งข้อมูลที่เป็นเป้าหมายการดักจับได้แก่ ชื่อผู้ใช้ (Username), รหัสผ่าน (Password) ที่ใช้ในการตรวจสอบสิทธิ์เข้าใช้งานระบบ ข้อมูลบัตรเครดิต เป็นต้น

3) HTTP Strict Transport Security (HSTS) คือ กลไกที่บังคับใช้ HTTPS โดยกำหนดให้เว็บเบราว์เซอร์ที่กำลังทำงานอยู่บนเว็บไซต์ต้องสื่อสารผ่าน HTTPS เท่านั้น โดยฝั่งเซิร์ฟเวอร์ (Server) จะไม่สื่อสารผ่าน HTTP รูปแบบการขอ Request ระหว่าง Client กับ Web Server จะเป็นลักษณะสื่อสารผ่าน HTTPS เท่านั้น

4) เกณฑ์วิธีป้องกันชั้นซ็อกเก็ต (Secure Socket Layer Protocol: SSL) เป็นโพรโทคอลที่ถูกพัฒนาโดย Netscape Communications เพื่อใช้ในโพรโทคอล HTTP โดยโพรโทคอล SSL

จะทำงานระหว่าง Application Protocol และ TCP เพื่อใช้เข้ารหัสของข้อมูลและการพิสูจน์ตัวตนในการสื่อสารระหว่างเซิร์ฟเวอร์และไคลเอนท์ ซึ่งทำให้การสื่อสารผ่านเว็บมีความ

ปลอดภัยขึ้น เป็นเทคโนโลยีที่ถูกพัฒนาขึ้น เพื่อสนับสนุนการค้าอิเล็กทรอนิกส์ (E-Commerce) ผ่านหน้าเว็บ

5) การโจมตีโดยการเปลือยเอสเอสแอล (SSL Stripping Attack) คือ การโจมตีที่อาศัยวิธีโจมตีแบบแทรกกลางการสื่อสาร ร่วมกับวิธีการโจมตีเว็บไซต์ที่ทำงานบน HTTPS ซึ่งเมื่อเหยื่อถูกโจมตี โปรแกรมเว็บเบราว์เซอร์จะใช้โพรโทคอล HTTP ทำให้ไม่มีความปลอดภัยในการสื่อสาร

บทที่ 2
แนวคิด ทฤษฎี เอกสารและงานวิจัยที่เกี่ยวข้อง

2.1 Electronic Banking

Electronic Banking หรือ e-banking เป็นระบบธนาคารผ่านทางอินเทอร์เน็ต เป็นการทำธุรกรรมต่าง ๆ กับธนาคารผ่านเครือข่ายอินเทอร์เน็ต เช่น ตรวจสอบยอดเงิน โอนเงิน ดูรายการเดินบัญชี อายัดบัตร หรือชำระค่าสินค้า และบริการต่าง ๆ โดยผู้ใช้งานไม่จำเป็นต้องเดินทางไปยังธนาคาร สามารถกระทำผ่านทางเว็บเบราว์เซอร์ ได้ทุกที่ ทุกเวลา ปัจจุบัน e-banking มีรูปแบบการให้บริการอยู่ 2 รูปแบบ คือ Internet Banking และ Mobile Banking

Internet Banking หรือ iBanking เป็นรูปแบบการให้บริการ e-banking ผ่านเว็บไซต์ (Website) ซึ่งสามารถเข้าถึงได้จากเว็บเบราว์เซอร์ (Web Browser) สำหรับ Mobile Banking หรือ mBanking เป็นรูปแบบการให้บริการผ่านแอปพลิเคชันของอุปกรณ์เคลื่อนที่ เช่น สมาร์ทโฟน หรือแท็บเล็ต เป็นต้น ซึ่งจุดประสงค์ก็เพื่อให้บริการด้านธุรกรรมธนาคาร แก่ลูกค้า เช่นเดียวกับ Internet Banking ดังภาพที่ 2.1

ภาพที่ 2.1 ตัวอย่าง Mobile Banking ในสมาร์ทโฟน

หากดูจากสถิติ [10] ของธนาคารแห่งประเทศไทย เกี่ยวกับธุรกรรมการชำระเงินผ่านบริการ Mobile Banking และ Internet Banking ในเดือน มิถุนายน พ.ศ. 2560 นำมาเทียบกับ มิถุนายน พ.ศ. 2561 เป็นดังตารางที่ 2.1

ตารางที่ 2.1 ธุรกรรมการชำระเงินผ่านบริการ Internet Banking และ Mobile Banking

		มิถุนายน 2561	มิถุนายน 2560
1	**ธุรกรรมการชำระเงินผ่าน Internet Banking**		
	1) จำนวนบัญชีลูกค้าที่ใช้บริการ	**23,125,388**	18,523,590
	2) ปริมาณรายการ (พันรายการ)	22,525	**23,157**
	3) มูลค่ารายการ (พันล้านบาท)	**2,187**	1,989
2	**ธุรกรรมการชำระเงินผ่าน Mobile Banking**		
	1) จำนวนบัญชีลูกค้าที่ใช้บริการ	**37,973,421**	26,322,671
	2) ปริมาณรายการ (พันรายการ)	**203,232**	91,174
	3) มูลค่ารายการ (พันล้านบาท)	**1,269**	695

ที่มา : ธนาคารแห่งประเทศไทย [10]

จากตารางที่ 2.1 จะเห็นได้ว่า การใช้งาน Internet Banking ในเดือนมิถุนายน พ.ศ. 2560 มีจำนวนบัญชีลูกค้าที่ใช้งาน เป็นจำนวน 18,523,590 ราย มีปริมาณรายการจำนวน 23,157,000 รายการ และมีมูลค่า 1,989,000 ล้านบาท ในส่วนของ Mobile Banking มีจำนวนบัญชีลูกค้าที่ใช้งาน เป็นจำนวน 26,322,671 ราย มีปริมาณรายการจำนวน 91,174,000 รายการ และมีมูลค่า 695,000 ล้านบาท ส่วนในเดือนมิถุนายน ปี พ.ศ. 2561 พบว่า การใช้งาน Internet Banking มีจำนวนบัญชีลูกค้าที่ใช้งาน เป็นจำนวน 23,125,388 ราย มีปริมาณรายการจำนวน 22,525,000 รายการ ลดลงเล็กน้อยจากปีก่อนหน้า และมีมูลค่า 2,187,000 ล้านบาท ในส่วนของ Mobile Banking มีจำนวนบัญชีลูกค้าที่ใช้งาน เป็นจำนวน 37,973,421 ราย มีปริมาณรายการจำนวน 203,232,000 รายการ และมีมูลค่า 1,269,000 ล้านบาท จะเห็นได้ว่า จำนวนลูกค้า ปริมาณรายการ และมูลค่ารายการสูงขึ้นเป็นอย่างมาก แสดงให้เห็นถึงความนิยมในการใช้งานระบบ e-banking ของประเทศไทยในช่วงเวลาที่ผ่านมา และมีแนวโน้มที่จะมากขึ้นเรื่อย ๆ ในปัจจุบัน การรักษาความมั่นคงของ Internet Banking เนื่องจาก ระบบนี้ต้องทำงานผ่านเครือข่ายอินเทอร์เน็ต ซึ่งเป็นเครือข่ายสาธารณะขนาดใหญ่ ทำให้จำเป็นต้องมีการปกป้องข้อมูล ที่สื่อสารกันระหว่างผู้ใช้งาน กับธนาคาร (Client Browser กับ Web Server) ทั้งยังจำเป็นที่จะต้องมีการพิสูจน์ความเป็นตัวจริงทั้งสองฝ่าย จึงจำเป็นที่จะต้องมีระบบหรือกลไก ในการรักษาความมั่นคงและการพิสูจน์ความเป็นตัวจริงดังกล่าว ซึ่งปัจจุบันมีการใช้งาน Public Key Infrastructure (PKI) หรือ เทคโนโลยีโครงสร้างพื้นฐานกุญแจ

สาธารณะ แต่จากการศึกษาพบว่า PKI ยังมีข้อบกพร่องซึ่งอาจทำให้การใช้งาน Internet Banking นั้นไม่มีความมั่นคงและปลอดภัยดังรายละเอียดที่จะกล่าวถึงในหัวข้อถัดไป

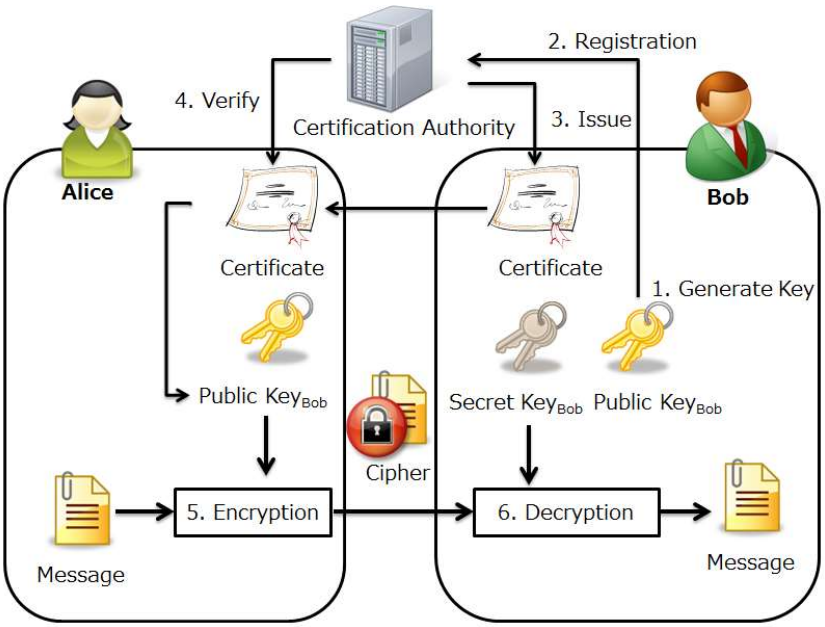
2.2 คดีระบบบริการธนาคารอิเล็กทรอนิกส์

อาชญากรรมทางไซเบอร์หรือการกระทำความผิดอาญาที่เกิดขึ้นต่อระบบบริการธนาคารอิเล็กทรอนิกส์ที่มีผลกระทบต่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศด้านการเงิน ซึ่งเป็นส่วนหนึ่งของคดีในอำนาจของกรมสอบสวนคดีพิเศษ ตามบัญชีท้ายประกาศคณะกรรมการคดีพิเศษ (ฉบับที่ 7) พ.ศ. 2562 เรื่อง การกำหนดรายละเอียดของลักษณะของการกระทำความผิด ตามมาตรา 21 วรรคหนึ่ง (1) แห่งพระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 ข้อ 11 ซึ่งที่ผ่านมาได้มีคดีพิเศษเกี่ยวข้องกับกรณีนี้แล้วหลายคดี [54-56] โดยมักพบปัญหาในการดำเนินการสืบสวนสอบสวน รวบรวมพยานหลักฐานในคดี ที่พบว่าเป็นการกระทำความผิดที่มีโทษตามกฎหมายอาญาฐานใช้บัตรอิเล็กทรอนิกส์ของผู้อื่นโดยมิชอบ ในประการที่น่าจะก่อให้เกิดความเสียหายแก่ผู้อื่นหรือประชาชนและเป็นการกระทำเกี่ยวกับบัตรอิเล็กทรอนิกส์ที่ผู้ออกได้ออกให้แก่ผู้ใช้สิทธิใช้ เพื่อประโยชน์ในการชำระค่าสินค้า ค่าบริการ หรือหนี้อื่นแทนการชำระด้วยเงินสด หรือใช้เบิกถอนเงินสดตามประมวลกฎหมายอาญา และเป็นการกระทำความผิดฐานเข้าถึงโดยมิชอบซึ่งระบบคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน การกระทำความผิดฐานเข้าถึงโดยมิชอบ ซึ่งข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน และการกระทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง หรือเพิ่มเติมไม่ว่าทั้งหมดหรือบางส่วนซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ ตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 และที่แก้ไขเพิ่มเติม โดยลักษณะการกระทำความผิดอาญา หรืออาชญากรรมทางไซเบอร์ต่อบริการธนาคารอิเล็กทรอนิกส์ จะพบปัญหาทางเทคนิค ตั้งแต่การระบุวัน เวลา และสถานที่ในการกระทำความผิด มักเกิดขึ้นโดยผู้เสียหายไม่รู้ว่าโดนกระทำหรือเข้าสู่ระบบธนาคารอิเล็กทรอนิกส์ วัน เวลา ใด เมื่อตรวจพบการกระทำความผิดก็มักจะเกิดขึ้นนอกราชอาณาจักร ซึ่งอำนาจหน้าที่ในการสอบสวนก็เป็นอำนาจโดยตรงของอัยการสูงสุด ก็จะพบปัญหาเรื่องอำนาจการสอบสวนของพนักงานสอบสวนผู้รับผิดชอบ ตามประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 20 รวมถึงปัญหาในการรวบรวมพยานหลักฐานทางเทคโนโลยีสารสนเทศ เนื่องจากเป็นพยานหลักฐานที่แตกต่างจากพยานหลักฐานทั่วไป เช่น พยานเอกสาร พยานวัตถุอื่น ๆ ที่เคยอยู่ในรูปแบบทางกายภาพที่สามารถจับต้องและสัมผัสได้ ก็กลับกลายมาเป็นพยานหลักฐานรูปแบบอิเล็กทรอนิกส์ ซึ่งเกิดขึ้นในระบบคอมพิวเตอร์และระบบเครือข่าย โดยไม่สามารถที่จะจับต้องได้ทางกายภาพ แต่สามารถตรวจพิสูจน์ได้โดยอาศัยเครื่องมือทางเทคโนโลยีสารสนเทศ เข้าช่วยเหลือในการสืบสวนสอบสวนและรวบรวมพยานหลักฐาน จากปัญหาดังกล่าวมาแล้ว ทำให้การดำเนินคดีกับผู้กระทำ

ความผิดทางอาญาเกี่ยวข้องกับบริการธนาคารอิเล็กทรอนิกส์ เป็นเรื่องยากลำบาก ทั้งทางกฎหมายและเทคนิควิธีทางวิทยาการคอมพิวเตอร์ จึงควรแสวงหาแนวทางป้องกันอาชญากรรมทางไซเบอร์ลักษณะนี้เพื่อไม่ให้ประชาชนได้รับความเดือดร้อนต่อไป

2.3 HTTPS, TLS และ PKI

Transport Layer Security (TLS) [11] ถูกออกแบบมาเพื่อให้การสื่อสารมีความมั่นคง โดยมีหน่วยงานกลางคือ Certificate Authority (CA) มีหน้าที่สำหรับออกใบประกาศ (Certificate) เพื่อรับรอง Public Key ของเซิร์ฟเวอร์เมื่อระบบเว็บไซต์นำ TLS มาใช้สำหรับสื่อสารข้อมูลจะใช้โพรโทคอล HTTP Over TLS หรือที่เรียกว่า HTTPS [1] โดยกระบวนการทั้งหมดอาศัย Public Key Infrastructure (PKI) [12] แสดงดังภาพที่ 2.2 (ที่มา: [12])



ภาพที่ 2.2 Public Key Infrastructure (PKI)

กระบวนการ PKI อาศัยการประยุกต์ใช้ใบรับรองบนเว็บไซต์จะสื่อสารบน TLS โดยการนำ TLS มาประยุกต์ใช้กับ HTTP ซึ่งเป็นพื้นฐานการสื่อสารข้อมูลบนเว็บไซต์ เพื่อเพิ่มความมั่นคงในการสื่อสาร เรียกว่า HTTPS ซึ่งมีรายละเอียดของขั้นตอนการทำงานดังต่อไปนี้

1) Bob เป็นเจ้าของเซิร์ฟเวอร์ที่ให้บริการเว็บไซต์ เพื่อให้เว็บไซต์ของ Bob ใช้งาน HTTPS จึงสร้าง Key Pair ขึ้นมาซึ่งประกอบด้วย Public Key และ Private Key

2) Bob นำ Public Key ให้กับ CA เพื่อให้ CA ใช้ Private Key ลงลายมือชื่อดิจิทัลรับรอง Public Key ของ Bob ผลลัพธ์ที่ได้คือ Bob จะได้ Certificate เพื่อนำไปติดตั้งบนเว็บเซิร์ฟเวอร์

3) เมื่อ Alice ต้องการสื่อสารไปที่เว็บไซต์ของ Bob การทำงานของ Alice จะส่งคำร้องขอไปที่เว็บไซต์ของ Bob แล้วกระบวนการของเว็บเซิร์ฟเวอร์จะส่ง Certificate มาที่เครื่องของ Alice

4) เครื่องของ Alice จะมีการตรวจสอบว่า Certificate ที่ถูกส่งมาเป็นของเว็บไซต์ของ Bob จริงหรือไม่ โดยการพิสูจน์ลายมือชื่อดิจิทัล (Verify Digital Signature) ของ CA ที่มีการลงนามรับรองไว้ในขั้นตอนที่ 2

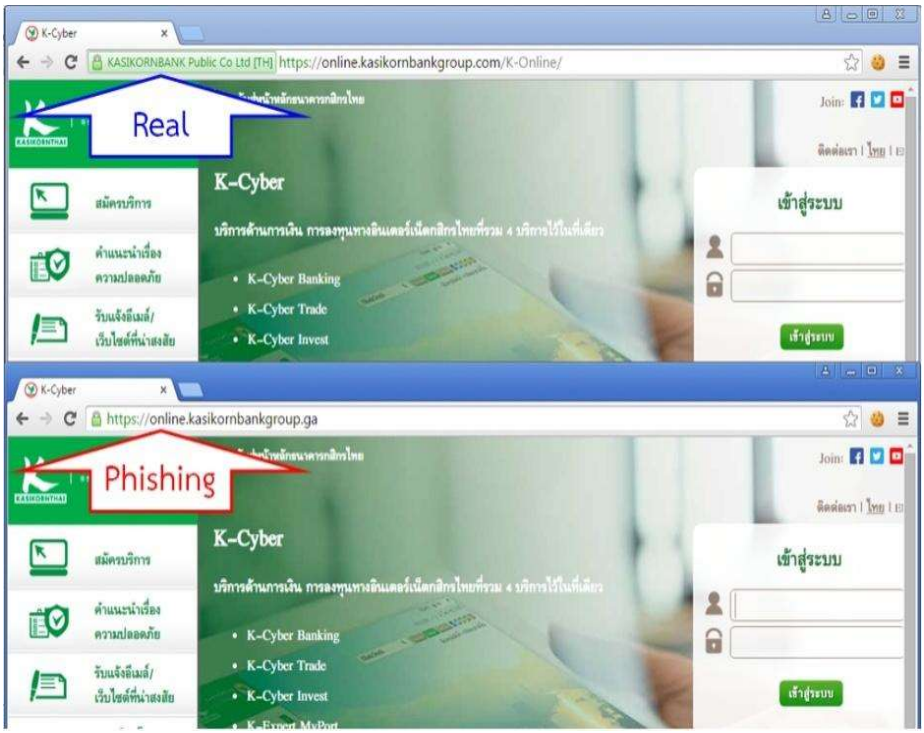
5) เมื่อกระบวนการ Verify Certificate เว็บไซต์ของ Bob ถูกต้อง Alice จะมั่นใจได้ว่า Server ที่คุยอยู่เป็น Server จริง ตัวเองไม่ได้โดนโจมตีด้วยเทคนิค Web Site Hijacking และจะใช้ Public Key ของ Bob ที่อยู่ในใบประกาศ (Certificate) ของ Bob เพื่อเข้ารหัส Session Key ที่สร้างขึ้น แล้วส่ง Session Key ที่โดนเข้ารหัส ไปที่เว็บไซต์ของ Bob

6) จากนั้น Bob จากใช้ Private Key ถอดรหัส Session Key ที่ได้รับ เพื่อใช้เข้ารหัสข้อมูลที่จะมีการส่งระหว่าง เครื่องของ Alice กับเว็บไซต์ของ Bob ทำให้ข้อมูลเป็นความลับ ไม่อาจถูกดักรับ (Sniff) ได้

2.4 ปัญหาการจู่โจม HTTPS และ TLS

มีเทคนิคมากมายที่ใช้ในการโจมตี HTTPS และ TLS ที่ถูกเสนอช่วงหลายปีที่ผ่านมา เช่น SSL Strip [2] โดยจากหลักการทำงานของ HTTPS ที่มีการกำหนดให้ระบบเว็บไซต์ทำงานบนโพรโทคอล HTTPS โดย Web Server เป็นผู้ redirect จาก HTTP ไปเป็น HTTPS ดังนั้น SSL Strip จึงอาศัยจุดอ่อนที่ Web Browser โดยทั่วไปจะไม่ได้ส่งคำร้องเป็น HTTPS แต่ต้น ทำการเปลือยเอา TLS ออก จากนั้น redirect กลับไปเป็น HTTP

วิธีโจมตีแบบ Phishing Attack แบบลงทะเบียน HTTPS คือการหลอกลวงทางเครือข่ายอินเทอร์เน็ตตัวอย่างเช่น ผู้โจมตีสร้าง E-Mail ปลอมของธนาคารเพื่อหลอกลวงเหยื่อโดยเนื้อหาภายใน E-Mail Phishing Attack เป็นเนื้อหาเหมือน E-Mail จริงที่ถูกส่งมาจากธนาคาร หลอกให้เหยื่อเปลี่ยนแปลงรหัสผ่านที่เข้าใช้งานระบบ โดยสร้างเว็บไซต์ปลอมที่มีเนื้อหาเหมือนกับเว็บไซต์จริงเพื่อหลอกเหยื่อ เมื่อเหยื่อเข้าใช้งานเว็บไซต์ซึ่งอาจจะเป็นในส่วนของการผ่านชื่อผู้ใช้และรหัสผ่านเพื่อเข้าใช้งานระบบผู้โจมตีก็สามารถใช้วิธีนี้ดักจับข้อมูลสำคัญของเหยื่อได้ ดังตัวอย่างการโจมตีแบบ Phishing Attack ของเว็บไซต์ธนาคารแห่งหนึ่ง (ดังภาพที่ 2.3) ค้นพบเมื่อวันที่ 11 กันยายน ค.ศ. 2015 จะเห็นได้ว่าเนื้อหาภายในเว็บไซต์เหมือนกันระหว่างเว็บไซต์จริงและเว็บไซต์ Phishing Attack อีกทั้งการสื่อสารของเว็บไซต์สื่อสารบนโพรโทคอล HTTPS ที่มีความมั่นคงซึ่งสิ่งที่แตกต่างคือ Domain name ที่ของปลอมเป็น .ga



ภาพที่ 2.3 Phishing Attack + HTTPS

ซึ่งเทคนิคนี้ภายหลังมีการต่อยอดโดยการเลือกจดโดเมนด้วย Unicode อักขระภาษาอื่นที่ไม่ใช่ภาษาอังกฤษแต่มีอักษรเดียวกันหรือเหมือนกับโดเมนภาษาอังกฤษที่ต้องการจู่โจม ซึ่งถูกเรียกว่า IDN (International Domain Name) Phishing หรือ Homograph Phishing

POODLE (Padding Oracle On Downgraded Legacy Encryption) หมายเลขช่องโหว่ CVE-2014-3566 ถูกค้นพบการโจมตีครั้งแรกในเดือนกันยายน ปี ค.ศ. 2014 เทคนิคการโจมตี POODLE Attack อาศัยความผิดพลาดของการเข้ารหัสข้อมูลบนโพรโทคอล SSL v3 ร่วมกับการโจมตีแบบแทรกกลางการสื่อสาร เพื่อดักจับข้อมูลที่ถูกเข้ารหัสด้วยโพรโทคอล SSL v3 ซึ่งการเข้ารหัสข้อมูลบนโพรโทคอล SSL จะมีการเข้ารหัสข้อมูลในลักษณะเป็น block ถ้าข้อมูลไม่เต็ม block จะมีการทำการเติมค่าลงไปให้เต็มเรียกว่า padding ดังนั้นในกรณีที่ผู้โจมตีสามารถเติมค่าในการ padding ทำให้สามารถโจมตีเพื่อถอดรหัสข้อมูลได้ ต่อมาได้เกิด DROWN Attack ซึ่งเทคนิคในทำนองเดียวกันที่อาศัยการ downgrade เทคนิคการเข้ารหัสของ HTTPS ไปยังอัลกอริทึมที่ล้าสมัยแล้ว

2.5 ปัญหาความมั่นคงของ PKI จาก Certificate Authority

Durumeric และคณะ [13] ได้ทำการสแกน (scan) เว็บไซต์ที่ทำงานบน HTTPS จำนวน 109 ล้านโฮสต์ เมื่อ ค.ศ. 2013 เพื่อวิเคราะห์ปัญหากระบวนการทำงานของ PKI โดยได้ผลสรุปว่ามี 80% ของ Certificate Authority (CA) ที่ออกใบรับรองที่ไม่เป็นหน่วยงานที่น่าเชื่อถือ โดย CA ลักษณะนี้เช่น ห้องสมุด พิพิธภัณฑ์ โบสถ์ เป็นต้น และใบรับรองที่ใช้งานโดยส่วนใหญ่ถูกออกโดย Intermediate Certificate ซึ่งเป็นหน่วยงานส่วนกลาง ที่ถูกมอบอำนาจโดย Root Certificate ในการออกใบรับรอง ทำให้การใช้งาน HTTPS ขาดความน่าเชื่อถือ เนื่องจากใบรับรองที่ถูกใช้งานสามารถออกได้ง่ายไม่มีค่าใช้จ่าย และกว่า 70% ของ CA ใช้งาน Key สำหรับเข้ารหัสข้อมูลที่ไม่มั่นคง เพราะใช้ Key Size ขนาดต่ำกว่ามาตรฐานขั้นต่ำ เช่น ขนาด Key Size ของ RSA Algorithm สำหรับลายมือชื่อดิจิทัลล่าสุด ต้องมีขนาดอย่างน้อย 2048 บิตขึ้นไป

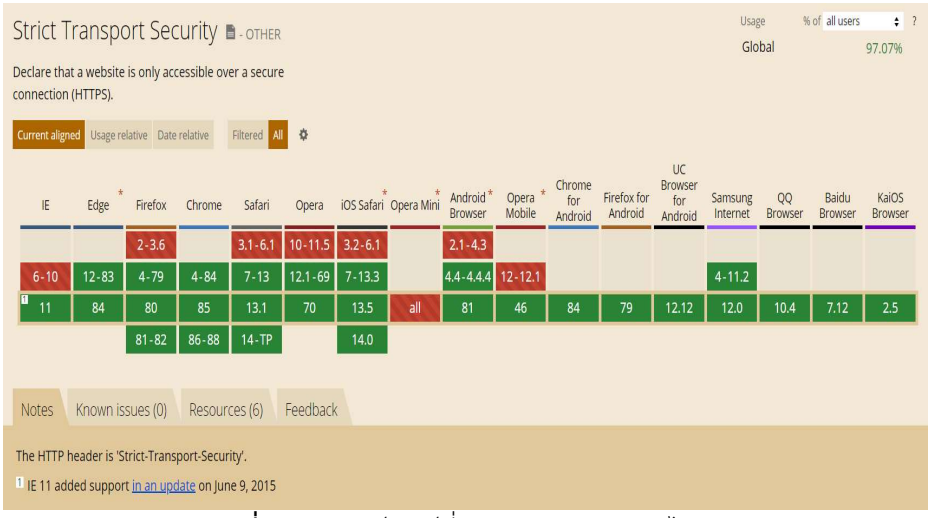
นอกจากนี้ ความน่าเชื่อถือของ CA ยังเป็นปัญหาใหญ่ เช่น DigiNotar ซึ่งเป็น Root CA ของประเทศเนเธอร์แลนด์ ที่ได้รับการยอมรับในเว็บเบราว์เซอร์ทั่วไป ถูกโจมตี โดยโดนคัดลอกกุญแจส่วนตัวไป แล้วนำไปใช้ออกใบรับรองปลอมจำนวน 531 ใบ ซึ่งจากกรณีดังกล่าวพบการโจมตีที่สำคัญหลังวันที่ 4 สิงหาคม ค.ศ. 2011 ในประเทศอิหร่านเป็นจำนวนมาก โดยผู้โจมตีสร้างรับรองปลอมเพื่อโจมตีเว็บไซต์ที่อยู่ภายใต้โดเมน เช่น *.facebook.com, update.windows.com, *.cia.gov และ *.google.com จนในที่สุด CA รายนี้ ก็ไม่ได้รับความเชื่อถืออีก เหตุการณ์ทำนองเดียวกัน เกิดกับ Comodo อีกราย ในเดือนมีนาคม ในปีเดียวกัน ซึ่งจากจุดอ่อนของบาง CA นี้ทำให้เห็นประเด็นปัญหาว่า แม้เว็บไซต์จะใช้ HTTPS ที่ออกใบประกาศมาจาก CA ที่เข้มแข็ง หากมีแค่ CA ใด CA หนึ่งในโลกเกิดมีจุดอ่อน แล้วโดน Hack ก็จะสามารถล้มเหลวไปด้วย เรียกเหตุการณ์แบบนี้ว่า “Any Points of Failure” ซึ่งถือเป็นจุดอ่อนที่สำคัญ

นอกจากนี้ ยังพบเหตุการณ์ที่บาง CA มีเจตนาออกใบรับรองปลอม โดยตั้งใจ เช่น ดังที่พบกับ Symantec ในเดือนตุลาคม ค.ศ. 2012, StartSSL ในเดือนกันยายน ค.ศ. 2015, IndiaCCA ในเดือน กรกฎาคม ค.ศ. 2014 เป็นต้น กรณีแบบนี้เรียกว่า “trust turn evil” คือ CA ที่เราเชื่อถือในระบบ PKI กับมีเจตนาโกงเสียเอง ทำให้ระบบ HTTPS โดนเจาะได้

ในปี ค.ศ. 2015 มีกรณีปัญหาที่เรียกว่า Lenovo Superfish ในเดือนกุมภาพันธ์ และ Dell Ghost CA ในเดือนพฤศจิกายน โดยทั้งสองบริษัทดังกล่าวเป็นบริษัทผลิตเครื่อง Desktop และ Notebook พร้อม preload MS Windows เป็นระบบปฏิบัติการให้ลูกค้า พบว่าทำการแอบฝัง Root Certificate ของตนเองเข้าไปในระบบปฏิบัติการและ Web Browser โดยมิชอบ ทำให้มีสิทธิ์เสมือน root CA ทั้งที่ทั้งสองบริษัทไม่ได้เป็น CA แต่อย่างใด การจู่โจมแบบนี้ ก็สามารถที่จะทำให้ PKI และ HTTPS ล้มเหลวได้เช่นกัน

2.6 กลไก HTTP Strict Transport Security

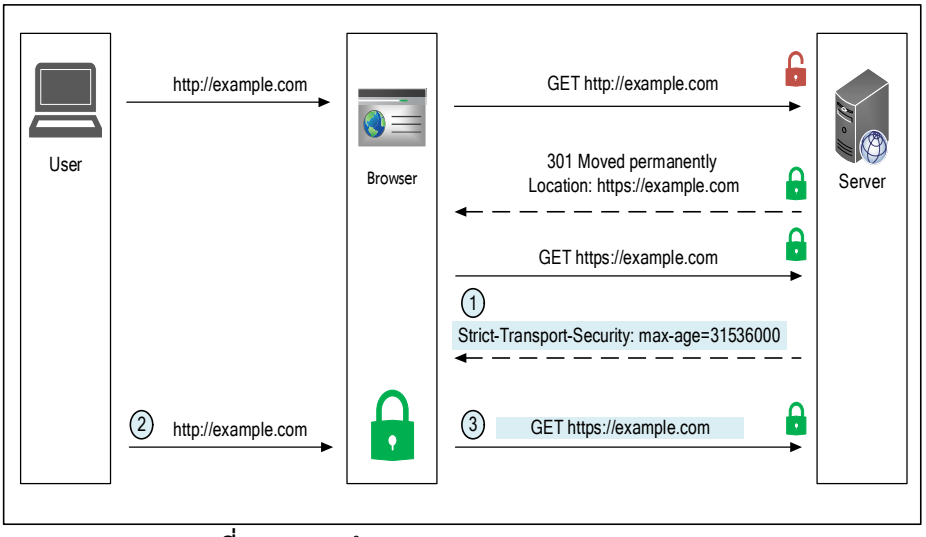
HTTP Strict Transport Security (HSTS) [14] เป็นกลไกมาตรฐานการสื่อสารของ Internet Engineering Task Force (IETF) ตามเอกสาร RFC 6797 ในปี ค.ศ. 2012 ที่ถูกสร้างขึ้นเพื่อรักษาความมั่นคงเว็บไซต์ที่ทำงานผ่านเว็บเบราว์เซอร์ (Web Browser) โดยมีจุดประสงค์หลักคือป้องกันการถูกโจมตีด้วยวิธีแทรกกลางการสื่อสาร (Man In The Middle) [2] รูปแบบการทำงานโดยเซิร์ฟเวอร์ (Web Server) จะมีการตอบกลับ (Response) ในส่วนของ HTTP Header เมื่อเว็บเบราว์เซอร์ตรวจสอบพบ HTTP Header ชื่อ Strict-Transport-Security: max-age=31536000; include SubDomains เว็บเซิร์ฟเวอร์จะบังคับให้สื่อสารผ่านช่องทางการเข้ารหัส HTTPS เท่านั้น และเว็บเบราว์เซอร์จะปฏิเสธการเชื่อมต่อ HTTP ทั้งหมด ทำให้ HSTS มีประสิทธิภาพในการป้องกันการถูกโจมตีด้วยด้วยวิธีแทรกกลางการสื่อสาร เช่น SSL Stripping Attack ซึ่งเป็นเทคนิคที่นิยมในการโจมตี และปัจจุบันกลไก HSTS รองรับการทำงาน Browser หลักทุกตัว [15] ดังภาพที่ 2.4



ภาพที่ 2.4 เบราว์เซอร์ที่รองรับการทำงานกลไก HSTS

2.7 การทำงานในเว็บเซิร์ฟเวอร์ HTTP Strict Transport Security

โดยทั่วไปเมื่อไคลเอนท์ (Client) ป้อน URL ในเว็บเบราว์เซอร์ (Web Browser) ตัวอย่าง เช่น www.example.com ในกรณีเช่นนี้เว็บเบราว์เซอร์จะอนุมานว่าไคลเอนท์ต้องการที่จะสื่อสาร ผ่านโพรโทคอล HTTP ในขั้นตอนนี้เอง HSTS จะทำงานโดยบังคับให้เว็บเซิร์ฟเวอร์ทำการเปลี่ยน เส้นทาง (301 Redirect) ชี้ไปยังโพรโทคอล HTTPS ลักษณะการทำงาน ดังภาพที่ 2.5



ภาพที่ 2.5 การทำงาน HTTP Strict Transport Security

ที่มา: [16]

การใช้งานในเว็บเซิร์ฟเวอร์ HTTP Strict Transport Security (HSTS) เพื่อให้เว็บเบราว์เซอร์ (Web Browser) ทำงานโดยบอกให้เว็บเบราว์เซอร์ที่กำลังสื่อสารผ่านเว็บไซต์ต้องเชื่อมต่อผ่าน HTTPS เท่านั้น สามารถทำได้โดยเพิ่มชุดคำสั่ง HTTP Header ในเว็บเซิร์ฟเวอร์ ตัวอย่างที่เป็นมาตรฐาน Strict-Transport-Security: max-age=31536000;includeSubDomains ซึ่งมีลักษณะการทำงานแต่ละพารามิเตอร์ดังนี้

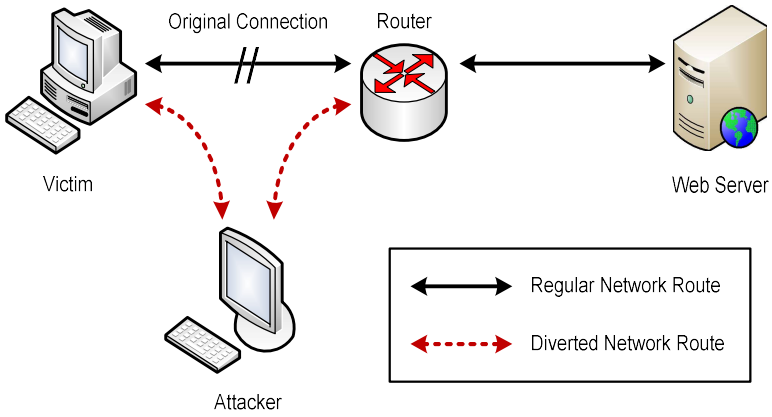
1) Strict-Transport-Security คือ ส่วนหัว (Header) ที่สำคัญสำหรับบอกเว็บเบราว์เซอร์ เพื่อให้เข้าใจว่าเว็บไซต์ต้องการเรียกใช้ HSTS

2) max-age คือ อายุของการบังคับใช้ HSTS เช่น ตั้งค่า max-age=31536000 มีหน่วยเป็น วินาที แสดงว่าเซิร์ฟเวอร์ (Server) จะไม่สื่อสารผ่าน HTTP บนเว็บเบราว์เซอร์ (Web Browser) เลย เป็นเวลา 1 ปี

3) includeSubDomains กรณีสื่อสารผ่าน Sub Domains ของเว็บไซต์ก็ต้องสื่อสารผ่าน HSTS เช่นเดียวกัน

2.8 การโจมตีแบบแทรกกลางการสื่อสาร

การโจมตีแบบแทรกกลางการสื่อสาร (Man in The Middle Attack) [17, 18] หมายถึง การที่มีผู้ไม่ประสงค์ดีเข้ามาทำการแทรกกลางในการสนทนาระหว่างคอมพิวเตอร์สองเครื่อง โดยทำหน้าที่เป็นตัวกลางในการรับส่งข้อมูลของคู่สนทนา โดยที่คู่สนทนาไม่สามารถทราบได้ว่ามีผู้ไม่ประสงค์ดีทำหน้าที่เป็นผู้รับและส่งข้อมูลต่อให้กับเครื่องคอมพิวเตอร์ที่เป็นคู่สนทนาของตนอยู่ดังภาพที่ 2.6 ทำให้ผู้ไม่ประสงค์ดีสามารถใช้รูปแบบการโจมตีในลักษณะนี้ กระทำการดักจับ (Sniffing) หรือเปลี่ยนแปลงข้อมูลที่ทั้ง 2 ฝ่ายสื่อสารกันอยู่ได้ ซึ่งการโจมตีในรูปแบบนี้ถูกนำมาประยุกต์ใช้กับการสื่อสารต่าง ๆ ในระบบคอมพิวเตอร์ ตัวอย่างเช่น การโจมตีแบบ MITM ในระบบเครือข่ายไร้สาย Wi-Fi ทำให้ผู้ไม่ประสงค์ดีสามารถแทรกแซงการเชื่อมต่อระหว่างเครื่องคอมพิวเตอร์และอุปกรณ์ Wi-Fi Access Point เพื่ออ่าน ปลอมแปลง หรือแก้ไขข้อมูลที่รับส่งระหว่างคอมพิวเตอร์ทั้ง 2 เครื่องนั้นได้ซึ่งการเข้ารหัสลับข้อมูลในการสื่อสารเพียงอย่างเดียวไม่สามารถป้องกันการโจมตีในรูปแบบนี้ได้เสมอไป ถ้าหากผู้รับและส่งสารไม่ได้มีกลไกใด ๆ ที่นำมาใช้ในการยืนยันความถูกต้องของเครื่องคอมพิวเตอร์ที่เป็นคู่สนทนา การโจมตีด้วยวิธี MITM ดังกล่าวก็จะสามารถใช้โจมตีการสื่อสารของระบบได้โดยง่าย เนื่องจากรูปแบบและมาตรฐานในการสื่อสารข้อมูลต่าง ๆ บนระบบเครือข่ายอินเทอร์เน็ตไม่ได้ถูกออกแบบมาให้มีการรักษาความมั่นคงปลอดภัยของข้อมูล เช่น การสื่อสารข้อมูลผ่านทาง Hyper Text Transfer Protocol (HTTP) เพื่อเรียกดูข้อมูลหรือใช้บริการเว็บไซต์ต่าง ๆ ซึ่งส่วนใหญ่มักจะไม่มีการเข้ารหัสในการป้องกันข้อมูล จึงทำให้ผู้ไม่ประสงค์ดีสามารถใช้โปรแกรมสำหรับดักจับข้อมูลในเครือข่าย เช่น Driftnet [19], Dsniff [20], Bettercap [21], Ettercap [22], Wireshark [23] และ TCPDump [24] โจมตีเพื่อทำการดักจับแพ็กเก็ตหรือเฟรมข้อมูลที่ถูกส่งผ่านทางระบบเครือข่ายได้



ภาพที่ 2.6 การโจมตีแบบแทรกกลางการสื่อสาร

ที่มา: [25]

ในงานวิจัยนี้ได้นำเครื่องมือซึ่งได้รับความนิยมที่มีการอัพเดตต่อเนื่อง คือ โปรแกรม Kali Linux, Bettercap และ Ettercap มาใช้เป็นเครื่องมือในการทดสอบการโจมตีแบบแทรกกลางการสื่อสาร ซึ่งการใช้เครื่องมือดังกล่าวข้างต้นมีรูปแบบการใช้งานดังต่อไปนี้

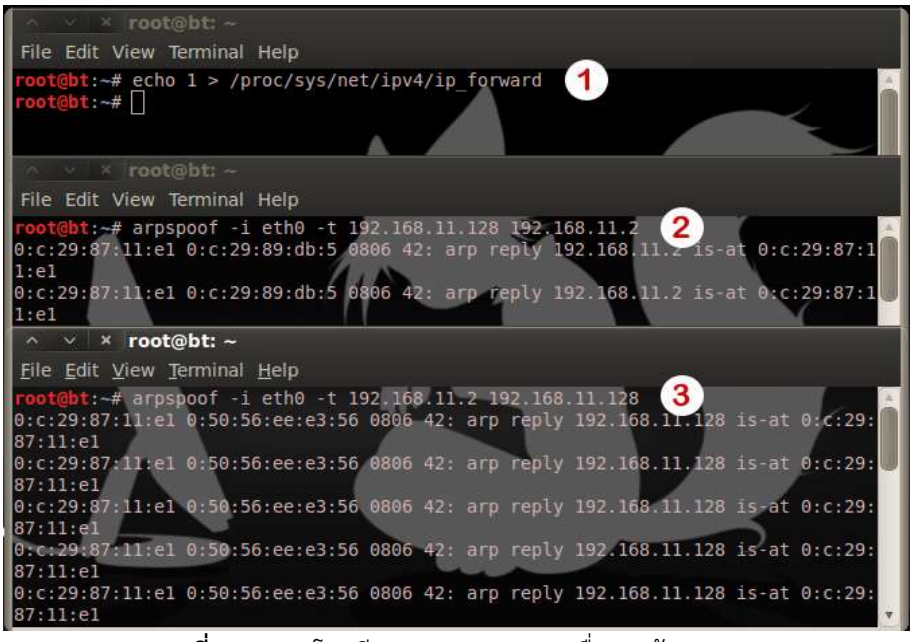
2.9 การโจมตีแบบแทรกกลางการสื่อสารด้วย Kali linux

การโจมตีแบบแทรกกลางการสื่อสารด้วย Kali linux ที่ใช้ในโครงการวิจัยนี้นั้น อาศัยเทคนิค ARP Spoof คำสั่งในการใช้งานจะเป็นในลักษณะแบบคอมมานไลน์ (Command line) เป็นหลัก มีขั้นตอนในการโจมตีดังต่อไปนี้

1) ใช้คำสั่ง echo 1>/proc/sys/net/ipv4/ip_forward เพื่อกำหนดให้ระบบทำการส่งต่อข้อมูลของเหยื่อที่ผ่านเข้ามายังเครื่องผู้โจมตีส่งต่อไปที่เว็บเซิร์ฟเวอร์

2) ใช้คำสั่ง arpspoof -t [ไอพีของเครื่องเหยื่อ] [ไอพีเกตเวย์ของเครื่องเหยื่อ] เพื่อทำการหลอกเกตเวย์ว่าเครื่องผู้โจมตีนั้นเป็นเครื่องเหยื่อ

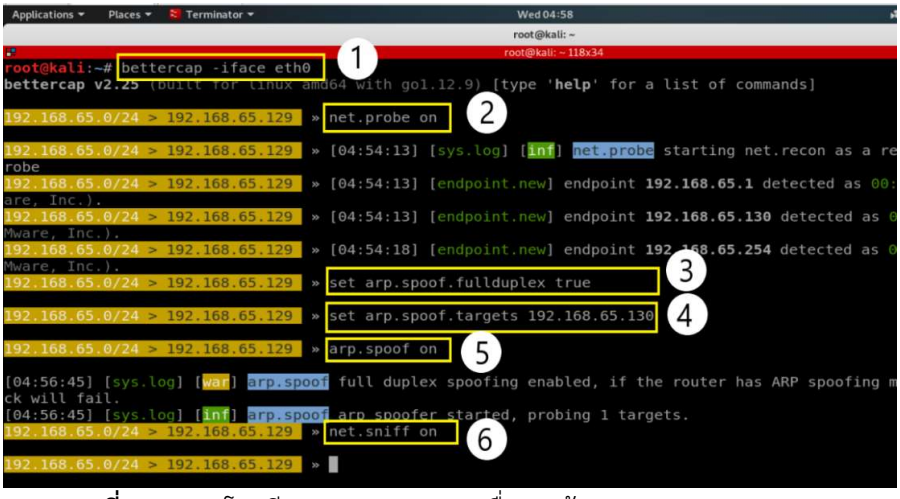
3) ใช้คำสั่ง arpspoof -t [ไอพีเกตเวย์ของเครื่องเหยื่อ] [ไอพีของเครื่องเหยื่อ] เพื่อหลอกเครื่องเหยื่อว่าเครื่องผู้โจมตีเป็นเกตเวย์ ดังภาพที่ 2.7



ภาพที่ 2.7 การโจมตีแบบแทรกกลางการสื่อสารด้วย Backtrack

2.10 การโจมตีแบบแทรกกลางการสื่อสารด้วย Bettercap

การโจมตีแบบแทรกกลางการสื่อสารด้วย Bettercap โดยใช้เทคนิค ARP Spoof นั้น คำสั่งในการใช้งานจะเป็นในลักษณะแบบคอมมานไลน์ (Command line) เป็นหลัก มีขั้นตอนในการโจมตีดังภาพที่ 2.8



ภาพที่ 2.8 การโจมตีแบบแทรกกลางการสื่อสารด้วย Bettercap: ARP Spoofing

1) ใช้คำสั่ง bettercap –iface eth0 เพื่อทำการเลือกอุปกรณ์อินเทอร์เฟส

```
# bettercap -iface eth0
```

2) ใช้คำสั่ง net.probe on เพื่อทำการค้นหาโฮสต์เครือข่ายเดียวกันโดยพื้นฐานจะส่งเป็นแพ็คเก็ต UDP แบบสุ่มไปยังทุก IP ที่เป็นไปได้ในซับเน็ต สามารถเรียกดูผลลัพธ์โดยใช้คำสั่ง net.show จะแสดงผลแบบเรียลไทม์

```
# net.probe on
```

3) ใช้คำสั่ง **set arp.spoof.fullduplex true** เพื่อทำการหลอกเกตเวย์ว่าเครื่องผู้โจมตีนั้นเป็นเครื่องเหยื่อ และหลอกเครื่องเหยื่อว่าเครื่องผู้โจมตีเป็นเกตเวย์

```
# set arp.spoof.fullduplex true
```

4) ใช้คำสั่ง **set arp.spoof.targets 192.168.65.130** เพื่อทำการกำหนด IP เป้าหมายที่จะโจมตี

```
# set arp.spoof.targets 192.168.65.130
```

5) ใช้คำสั่ง arp.spoof on เพื่อทำการ start ARP spoof เริ่มกระบวนการปลอมแปลง

```
# arp.spoof on
```

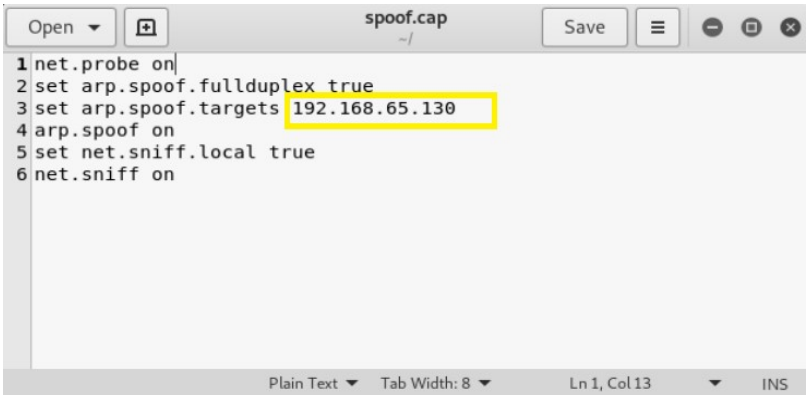
6) ใช้คำสั่ง net.sniff on เพื่อทำการดักจับข้อมูลในเครือข่ายอินเทอร์เน็ต

```
# net.sniff on
```

2.11 การโจมตีเพื่อ bypass HTTPS โดย Bettercap

การโจมตีแบบแทรกกลางการสื่อสารด้วย Bettercap แล้วทำการ bypassing HTTPS จะอยู่ในรูปแบบของการลดระดับโพรโทคอล HTTPS ให้เป็น HTTP คำสั่งในการใช้งานจะเป็นในลักษณะแบบคอมมานไลน์ (Command line) เป็นหลัก มีขั้นตอนในการโจมตีดังต่อไปนี้

1) ให้ทำการสร้าง script โดยการเขียนคำสั่งเพื่อทำการแทรกกลางการสื่อสารโดยตรง สามารถใช้ Text Editor ใน Kali linux ได้ ดังภาพที่ 2.9



ภาพที่ 2.9 สร้าง script เพื่อทำการแทรกกลางการสื่อสาร

2) ให้ใช้คำสั่ง **bettercap -iface eth0 -caplet /root/spoof.cap** เพื่อทำการ Run Script ที่ได้ทำการบันทึกไว้ก่อนหน้านี้

```
# bettercap -iface eth0 -caplet /root/spoof.cap
```

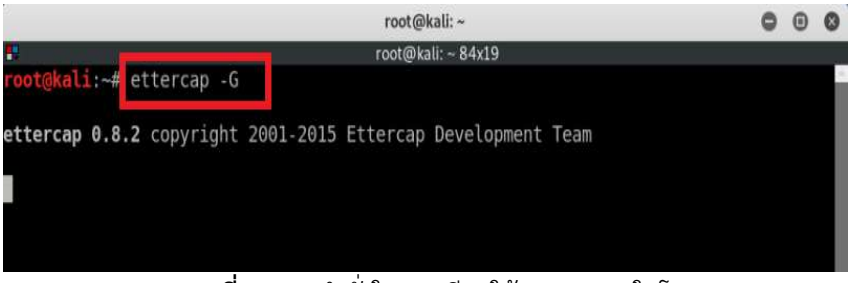
3) ให้ใช้คำสั่ง caplets.show เพื่อเช็คความพร้อมในการทำงาน หลังจากนั้นให้ใช้คำสั่ง hstshijack/hstshijack เพื่อทำการแทรกกลางการสื่อสารและทำการ Bypass HTTPS ดังภาพที่ 2.10

ภาพที่ 2.10 คำสั่งในการ Bypass HTTPS

2.12 การโจมตีแบบแทรกกลางการสื่อสารด้วย Ettercap

การโจมตีแบบแทรกกลางการสื่อสารด้วย Ettercap จะเป็นการใช้งานคำสั่งจะอยู่บนรูปแบบของ GUI ซึ่งมีขั้นตอนในการโจมตีดังต่อไปนี้

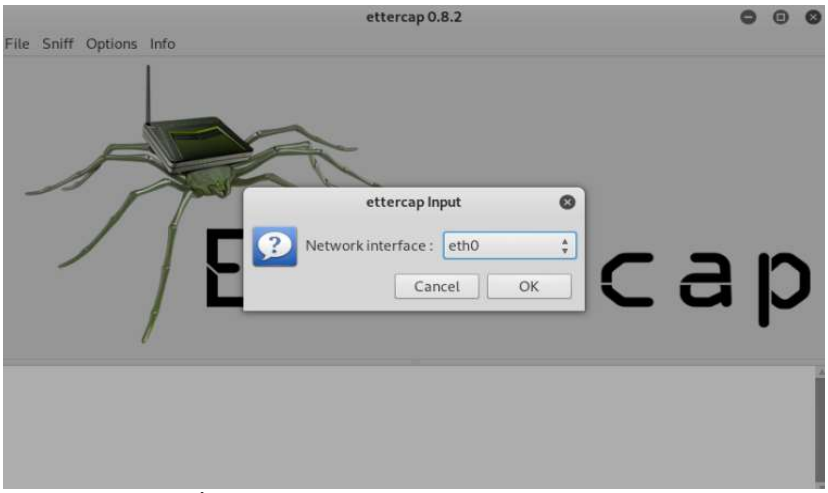
1) ใช้คำสั่ง ettercap –G เพื่อเรียกใช้งานโปรแกรม Ettercap ในโหมดของ GUI ดังภาพที่ 2.11



ภาพที่ 2.11 คำสั่งในการเรียกใช้ Ettercap ในโหมด GUI

2) คลิกเมนู Sniff ตามด้วยคลิก Unified Sniffing หรือกดปุ่ม Shift+U เพื่อกำหนดการ์ดเน็ตเวิร์กให้กับโปรแกรม ซึ่งปกติจะถูกกำหนดให้เป็น “eth0” ดังภาพที่ 2.12 และ 2.13

ภาพที่ 2.12 การกำหนดโหมดของการดักจับข้อมูล



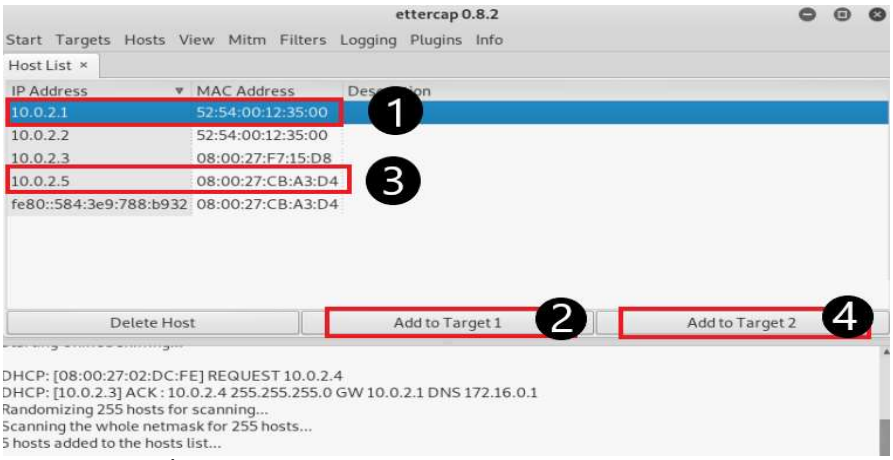
ภาพที่ 2.13 การกำหนดการ์ดเน็ตเวิร์กให้กับโปรแกรม Ettercap

3) คลิกเมนู Hosts ตามด้วยคลิกที่ Scan for Hosts หรือกดปุ่ม Ctrl+S เพื่อค้นหาเครื่องเหยื่อ จากนั้นคลิกเลือก Hosts List เพื่อแสดงไอพีของเกตเวย์และเครื่องเหยื่อ ดังภาพที่ 2.14 และ 2.15

ภาพที่ 2.14 ค้นหาเป้าหมายที่จะทำการโจมตี

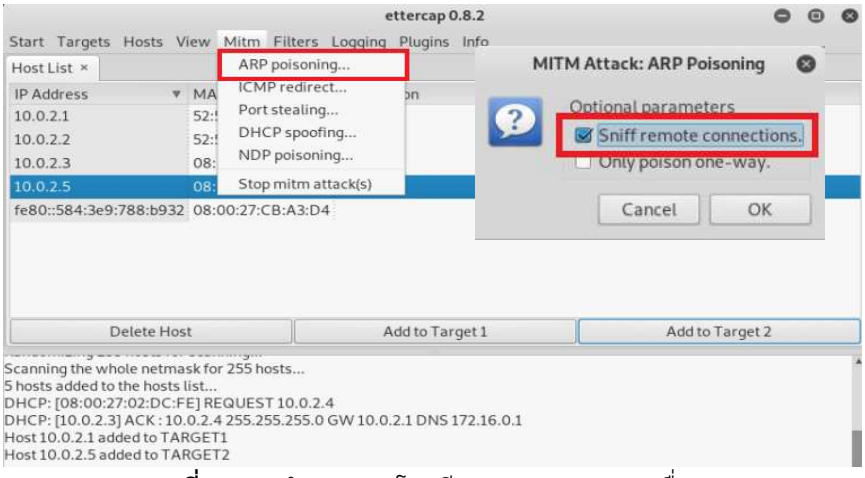
ภาพที่ 2.15 กำหนดให้ Ettercap แสดงผลลัพธ์ของการค้นหา

4) เลือกไอพีของเกตเวย์ แล้วคลิกปุ่ม Add to Target1 จากนั้นเลือกไอพีของเครื่องเหยื่อ แล้วคลิกปุ่ม Add to Target2 ดังภาพที่ 2.16



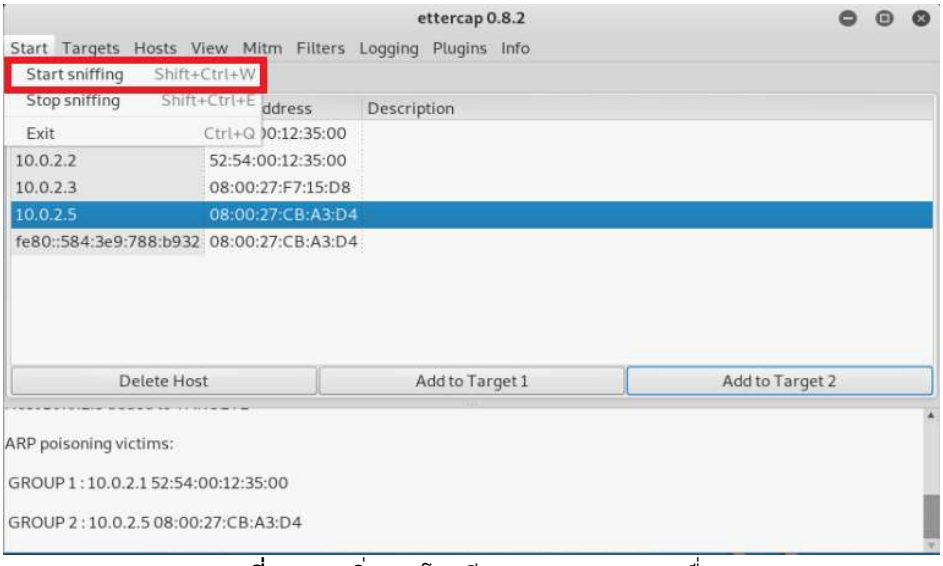
ภาพที่ 2.16 กำหนดไอพีของเกตเวย์และไอพีของเป้าหมายในการโจมตี

5) เริ่มการโจมตีแทรกกลางการสื่อสารระหว่างเครื่องเหยื่อกับเกตเวย์ โดยคลิกที่เมนู Mitm ตามด้วย ARP poisoning แล้วคลิกเลือก Sniff remote connections ดังภาพที่ 2.17



ภาพที่ 2.17 กำหนดการโจมตีแบบแทรกกลางการสื่อสาร

6) คลิกเลือกเมนู Start ตามด้วยคลิก Start sniffing เพื่อโจมตีเครื่องเหยื่อ ดังภาพที่ 2.18

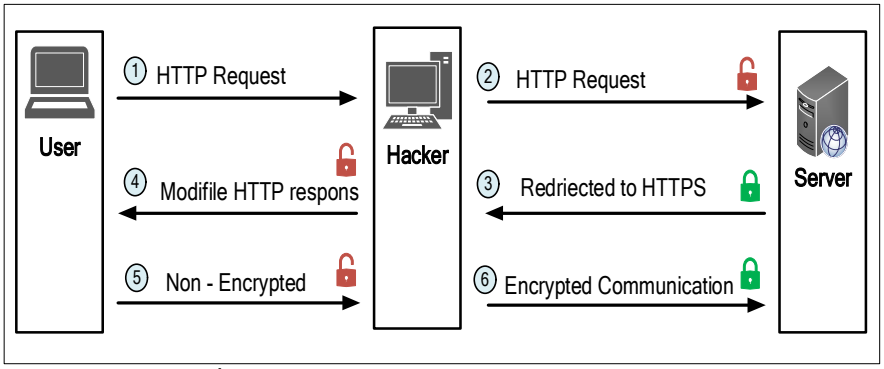


ภาพที่ 2.18 เริ่มการโจมตีแบบแทรกกลางการสื่อสาร

2.13 การโจมตี SSL Stripping Attack

ในปี ค.ศ. 2009 Marlinspike [2] ได้เสนอวิธีการโจมตี SSL ด้วยวิธี SSL Stripping Attack ในงาน Blackhat Conference 2009 โดยใช้ SSL Strip ซึ่งเป็นเครื่องมือที่ถูกติดตั้งใน Backtrack Linux ซึ่งเป็น Linux-base Penetration Testing ที่ถูกกลุ่มผู้เชี่ยวชาญทางด้านความมั่นคงไซเบอร์ทั่วโลก นำไปใช้งานในงานทางด้านการทดสอบเจาะและประเมินความมั่นคงของระบบ ซึ่งรวมถึงการถูกนำไปใช้โดยผู้ที่ไม่ประสงค์ดีเช่นเดียวกัน

การเปลือยเอสเอสแอล หรือ SSL Stripping Attack มีรูปแบบการโจมตีโดยอาศัยวิธีโจมตีแบบแทรกกลางการสื่อสารร่วมกับวิธีการโจมตีแบบ SSL Stripping Attack ควบคู่กัน โดยการโจมตีเว็บไซต์ที่มีการกำหนดช่องทางการสื่อสารผ่านโพรโทคอล HTTPS เมื่อเครื่องเหยื่อถูกแฮกเกอร์โจมตีเว็บเบราว์เซอร์จะถูกบังคับเปลี่ยนการทำงานที่โพรโทคอล HTTP ทำให้ข้อมูลไม่ได้รับการเข้ารหัสการสื่อสาร โดยข้อมูลต่าง ๆ ที่เครื่องเหยื่อส่งไปที่เว็บเซิร์ฟเวอร์จะถูกส่งผ่านไปยังเครื่องแฮกเกอร์ก่อน ซึ่งแฮกเกอร์สามารถดักจับข้อมูลของเหยื่อได้อย่างง่ายดาย เนื่องจากข้อมูลที่สื่อสารผ่าน HTTP อยู่ในรูปของ Clear Text ที่สามารถอ่านเข้าใจได้ หลังจากนั้นการทำงานต่อไปของ SSL Stripping Attack จะทำหน้าที่นำข้อมูลของเหยื่อมาเข้ารหัสด้วย HTTPS แล้วส่งต่อไปที่เว็บเซิร์ฟเวอร์ ด้วยเหตุนี้ผลของการโจมตีที่เว็บเบราว์เซอร์ของเครื่องเหยื่อจึงไม่สามารถตรวจสอบหรือแสดงข้อความแจ้งเตือนความผิดพลาดได้ เนื่องจากเครื่องของเหยื่อสามารถสื่อสารกับเว็บเซิร์ฟเวอร์ได้ตามปกติ เพียงแต่เป็นการสื่อสารที่ถูกบังคับให้อยู่บนโพรโทคอล HTTP แทนที่จะเป็นโพรโทคอล HTTPS ที่มีการทำงานอย่างปลอดภัย ดังภาพที่ 2.19



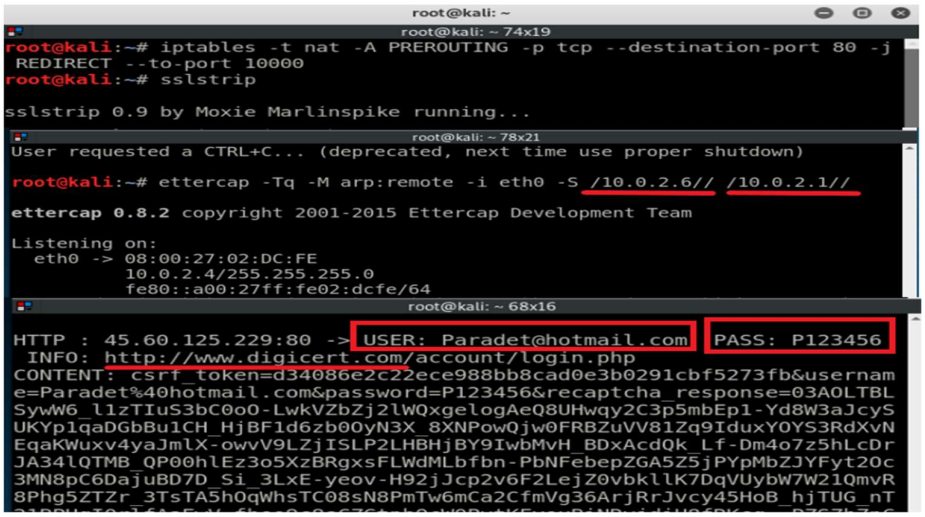
ภาพที่ 2.19 รูปแบบการโจมตี SSL Stripping Attack

ในงานวิจัยนี้ใช้การโจมตีระบบเว็บไซต์ที่ใช้งาน SSL/TLS ด้วยเครื่องมือ SSL Strip ที่ถูกติดตั้งอยู่บนระบบปฏิบัติการ Kali Linux เวอร์ชัน 2019.3 ดังภาพที่ 2.20 ซึ่งมีขั้นตอนดังต่อไปนี้

1) ใช้คำสั่ง iptables –t nat –A PREROUTING -p tcp --dport 80 -j REDIRECT --to-port 10000 เพื่อการกำหนดให้ข้อมูลที่เข้ามายังเครื่องผู้โจมตีทาง Port หมายเลข 80 ให้ส่งต่อไปที่ port หมายเลข 10000

2) ใช้คำสั่ง sslstrip เพื่อโจมตีเว็บไซต์ที่ใช้งาน SSL/TLS เมื่อเครื่องของเหยื่อเข้าใช้งานเว็บไซต์ แล้วตามปกติบนเว็บเบราว์เซอร์จะแสดงโพรโทคอล HTTPS แต่เมื่อถูกโจมตีด้วยวิธี SSL Stripping Attack นี้แล้ว ผลของการโจมตีจะส่งผลให้บนเว็บเบราว์เซอร์ถูกกำหนดให้ใช้งานโพรโทคอล HTTP แทน

3) ใช้คำสั่ง Ettercap -Tq -M arp:remote -I eth0 -S /10.0.2.6// /10.0.2.1// เพื่อแสดงข้อมูลของเครื่องเหยื่อที่สามารถดักจับได้ เช่น ชื่อบัญชีผู้ใช้และรหัสผ่านที่ใช้ในการตรวจสอบสิทธิ์ในการเข้าใช้งานระบบ ดังภาพที่ 2.20



ภาพที่ 2.20 การโจมตี SSL/TLS ด้วยวิธี SSL Stripping Attack

2.14 Hashcat

Hashcat [26] เป็นโปรแกรม Open Source Software ถูกสร้างขึ้นเพื่อใช้ในการถอดรหัสทั้งรหัสผ่านและค่าแฮช (Password & Hash Cracking) โดยสามารถใช้ถอดค่า Hash Algorithm ได้หลากหลาย เช่น MD5, SHA1, SHA256, HMAC, WPA, JWT รวมถึง BitCoin, Ethereum และยังทำงานทั้งโดยใช้ CPU และ GPU โดยสามารถเลือกประเภทการโจมตีในการถอดรหัส Password Cracking ที่ได้รับความนิยมได้ เช่น Dictionary Attack เป็นการสุ่มเดา Password จากไฟล์ที่มีการ

รวบรวมคำศัพท์ต่าง ๆ ที่พบอยู่ใน Dictionary ซึ่งจัดว่าเป็นวิธีการที่ถูกนำมาใช้ในการถอดรหัสผ่านมากที่สุด หรือ Brute Force Attack เป็นการเดา password ทุกความเป็นไปได้ของตัวอักษรในแต่ละหลัก เช่น รหัส ATM มีจำนวน 4 หลัก แต่ละหลักสามารถตั้งค่าตัวเลข 0-9 ดังนั้น โปรแกรมจะทำการไล่ตัวเลขจาก 0000 ไปจนถึง 9999 หมื่นวิธีจนได้ password ที่ถูกต้อง เป็นต้น

2.15 งานวิจัยที่เกี่ยวข้อง

Hodges และคณะ [14] ได้เสนอ HTTP Strict Transport Security (HSTS) ได้กำหนดให้เป็นกลไกมาตรฐานการสื่อสาร IETF ตามเอกสาร RFC 6797 เพื่อแก้ปัญหาการถูกโจมตี HTTPS เช่น การโจมตีด้วยวิธี SSL Stripping Attack การทำงานของ HSTS ในเว็บเบราว์เซอร์ (Web Browser) ล่าสุดมีการรองรับการทำงานสำหรับเว็บเบราว์เซอร์หลักทุกตัว เช่น Google Chrome, Mozilla Firefox, Safari, Opera, IE เป็นต้น รูปแบบการทำงานโดยเซิร์ฟเวอร์ (Server) จะมีการตอบกลับ (Response) ในส่วนของ HTTP Header เมื่อเว็บเบราว์เซอร์ตรวจสอบพบ HTTP Header ชื่อ Strict-Transport-Security: max-age=31536000; include SubDomains ซึ่งเป็นส่วนหัวที่สำคัญสำหรับบอกเว็บเบราว์เซอร์เพื่อให้เข้าใจว่าเว็บไซต์ต้องการเรียกใช้ HSTS และยังมีส่วนที่เป็นค่าเวลาในการกำหนดการเชื่อมต่อ HSTS เพื่อบังคับใช้โพรโทคอล HTTPS โดยเว็บเบราว์เซอร์จะทำการบังคับใช้โพรโทคอล HTTPS ตามระยะเวลาที่กำหนดไว้ใน HTTP Header นอกจากนี้ยังมีการเรียกใช้งาน HSTS Preload ลักษณะการทำงานคือจะมีการติดตั้ง HSTS ไว้ที่เว็บเบราว์เซอร์ทำให้เว็บไซต์ที่อยู่ในรายการ HSTS Preload มีประสิทธิภาพในการป้องกันการถูกโจมตี เช่น Google, Paypal, Twitter, Facebook, Lastpass เป็นต้น การทำงาน HSTS enforced on specific names คือการดูแลแบบพิเศษรวมถึงชื่อโดเมนของเว็บไซต์ทั้งหมดตัวอย่างของ Facebook ดังภาพที่ 2.21

```
{
  "name": "facebook.com", "policy": "custom",
  "mode": "force-https", "pins": "facebook", "include_subdomains_for_pinning": true
},
{ "name": "www.facebook.com", "policy": "custom", "mode": "force-https", "include_subdomains": true, "pins": "facebook" },
{ "name": "m.facebook.com", "policy": "custom", "mode": "force-https", "include_subdomains": true, "pins": "facebook" },
{ "name": "tablet.facebook.com", "policy": "custom", "mode": "force-https", "include_subdomains": true, "pins": "facebook" },
{ "name": "secure.facebook.com", "policy": "custom", "mode": "force-https", "include_subdomains": true, "pins": "facebook" },
{ "name": "pixel.facebook.com", "policy": "custom", "mode": "force-https", "include_subdomains": true, "pins": "facebook" },
{ "name": "apps.facebook.com", "policy": "custom", "mode": "force-https", "include_subdomains": true, "pins": "facebook" },
{ "name": "upload.facebook.com", "policy": "custom", "mode": "force-https", "include_subdomains": true, "pins": "facebook" },
{ "name": "developers.facebook.com", "policy": "custom", "mode": "force-https", "include_subdomains": true, "pins": "facebook" },
{ "name": "touch.facebook.com", "policy": "custom", "mode": "force-https", "include_subdomains": true, "pins": "facebook" },
{ "name": "mbasic.facebook.com", "policy": "custom", "mode": "force-https", "include_subdomains": true, "pins": "facebook" },
{ "name": "code.facebook.com", "policy": "custom", "mode": "force-https", "include_subdomains": true, "pins": "facebook" },
{ "name": "t.facebook.com", "policy": "custom", "mode": "force-https", "include_subdomains": true, "pins": "facebook" },
{ "name": "mtouch.facebook.com", "policy": "custom", "mode": "force-https", "include_subdomains": true, "pins": "facebook" },
{ "name": "business.facebook.com", "policy": "custom", "mode": "force-https", "include_subdomains": true, "pins": "facebook" },
{ "name": "research.facebook.com", "policy": "custom", "mode": "force-https", "include_subdomains": true, "pins": "facebook" },
{
  "name": "messenger.com", "policy": "custom",
  "mode": "force-https", "pins": "facebook", "include_subdomains_for_pinning": true
},
{ "name": "www.messenger.com", "policy": "custom", "mode": "force-https", "include_subdomains": true, "pins": "facebook" },
```


ภาพที่ 2.21 HSTS enforced on specific names

ปัจจุบันทาง Google ในโครงการ chromium ที่เป็นองค์กรดูแล HSTS Preload ได้เปิดให้เว็บไซต์ทั่วไปลงทะเบียนใช้งาน HSTS Preload ที่ต้องการความมั่นคงในการสื่อสารอินเทอร์เน็ต การบังคับใช้โพรโทรคอล HTTPS สำหรับการสื่อสารผ่านเว็บเบราว์เซอร์จากการเช็ครายชื่อที่มีการลงทะเบียนใช้งานทั้งหมด เมื่อวันที่ 4 พ.ย 2562 จากไฟล์ transport_security_state_static.json จากทั่วโลกที่มีการลงทะเบียนใช้งาน HSTS Preload พบว่ามีเว็บไซต์ทั้งหมดประมาณ 88,803 รายชื่อโดเมน และพบหน่วยงานไทยที่มีการลงทะเบียน HSTS Preload ดังตารางที่ 2.2

ตารางที่ 2.2 ชื่อเว็บไซต์ที่ถูก HSTS Preload .or.th และ .ac.th (เมื่อ 4 พ.ย. 2562)

No	สกุลเว็บไซต์ .or.th และ .ac.th
1	www.etda.or.th
2	san.ac.th

ตารางที่ 2.3 ชื่อเว็บไซต์ที่ถูก HSTS Preload .co.th (เมื่อ 4 พ.ย. 2562)

No	สกุลเว็บไซต์ .co.th
1	insightera.co.th
2	ginja.co.th
3	infura.co.th
4	cipher.co.th
5	dotbrick.co.th
6	odoo.co.th
7	officeprint.co.th
8	officeprint.co.th
9	extreme.co.th
10	nexthop.co.th
11	dotsiam.co.th
12	saleduck.co.th
13	vsoy.co.th
14	begintravel.co.th
15	thaihong.co.th
16	jaisiam.co.th

จากข้อมูลที่ตรวจสอบเมื่อ 4 พฤศจิกายน พ.ศ. 2562 (แสดงในตารางที่ 2.2 และ 2.3) พบว่าเว็บไซต์ในประเทศไทยที่ต้องการความมั่นคง ยังทำการ Preload HSTS อยู่ในจำนวนที่น้อยมาก โดยเฉพาะอย่างยิ่ง มีเว็บไซต์ของธนาคารออนไลน์ในประเทศไทยเพียง 1 เว็บเท่านั้นที่ทำการ Preload HSTS

Fairweather และคณะ [28] ได้นำเสนอ CAT + S ที่ถูกพัฒนาระบบด้วยภาษา JavaScript โดยทำการพัฒนาระบบขึ้นเป็น Browser Extension ที่ทำงานอยู่บน Google Chrome เพื่อป้องกันการโจมตีแบบแทรกกลางการสื่อสารและการโจมตีด้วย SSL Stripping Attack โดยมีการพัฒนาให้ระบบสามารถตรวจสอบความไม่มั่นคงของเว็บไซต์อัตโนมัติ โดยใช้ JavaScript ในการเข้าถึงองค์ประกอบของเว็บไซต์ผ่าน HTML สร้างอินสแตนซ์ LinkMonitor เพื่อจัดเก็บรูปแบบ HTML ทั้งหมดที่ใช้ฟังก์ชัน getElementsBy TagName กระบวนการนี้จะทำซ้ำทุก ๆ 100 วินาที เป็นการตรวจสอบแบบ Dynamic เพื่อหาการเปลี่ยนแปลงของโพรโทคอลที่ผิดปกติของเว็บไซต์ ในการตรวจสอบว่าเว็บไซต์ที่กำลังใช้งานอยู่นั้นทำงานอยู่บนโพรโทคอล HTTPS หรือไม่ และหากพบว่ามีการสื่อสารผ่านโพรโทคอล HTTP ระบบ CAT + S จะเปลี่ยนการสื่อสารเป็น HTTPS อัตโนมัติโดยที่ผู้ใช้ไม่ต้องดำเนินการใด ๆ ทั้งสิ้น และยังสามารถรักษาความปลอดภัยแบบฟอร์มที่มีการสื่อสารผ่าน HTTP ในเว็บไซต์ให้คงเดิมให้อีกด้วย ในการนำมาใช้จริงระบบ CAT + S พบว่ายังเป็นข้อเสนอที่ใช้ป้องกันการถูกโจมตีด้วย SSL Stripping Attack เท่านั้น และจากการวิเคราะห์ระบบ CAT + S ยังพบว่ามีข้อจำกัดเรื่องของเวลาในการโหลดข้อมูลมาเช็คเพื่อตรวจสอบความผิดปกติของโพรโทคอล HTTPS ในระบบเว็บไซต์ หากถูกโจมตีด้วย SSL Stripping Attack จะทำให้ระบบมีการตรวจสอบวนลูป ในการคืนค่าระหว่างโพรโทคอล HTTP ไปยังโพรโทคอล HTTPS ซึ่งจะส่งผลให้ระบบเว็บไซต์ทำงานต่อไม่ได้จึงเกิดเหตุการณ์ที่เรียกว่า DoS (Denial-of-Service)

Selvi [29] ได้เสนอวิธีการโจมตี HSTS ใน Blackhat Conference โดยมีการวิเคราะห์ข้อดีและข้อเสียของ HSTS แล้วเสนอวิธีการโจมตีโดยอาศัยการโจมตีที่ Network Time Protocol (NTP) ของเครื่องเหยื่อเพื่อเปลี่ยนแปลงเวลาบนเครื่องเหยื่อให้เพิ่มมากขึ้น ทำให้การทำงานของ HSTS มองว่าค่าใน Parameter ที่ชื่อ max-age หมดอายุ ดังนั้นเมื่อ Web Browser เปรียบเทียบเวลาที่ระบุใน max-age กับเวลาปัจจุบันบนเครื่องเหยื่อแล้วได้ผลว่าเวลาใน max-age หมดอายุการประมวลผลของ Web Browser ก็จะไม่ทำตามเงื่อนไขของ HSTS แล้วผู้โจมตีสามารถใช้วิธีโจมตีแบบ SSL Strip ได้สำเร็จ โดยในงานวิจัยได้พัฒนาเครื่องมือชื่อ Delorean แล้วทดสอบโจมตีทั้งในระบบปฏิบัติการ Ubuntu Linux, Fedora Linux, Mac OS X Lion, Mac OS X Mavericks และ Microsoft Windows และกับ Web Browser ได้แก่ Safari, Firefox และ Google Chrome

Fung และคณะ [30] ได้เสนอ SSLock โดยเป็นข้อเสนอวิธีการบังคับใช้โพรโทคอล SSL กับเว็บไซต์ โดยการพิจารณาการแบ่ง Domain Name สำหรับการใช้งาน SSL โดยในการใช้งานนั้น

ผู้พัฒนาเว็บไซต์ต้องกำหนดรูปแบบการทำงานของระบบเว็บไซต์ตามกระบวนการที่ SSLock เสนอ เพื่อตอบกลับ HTTP Header ที่ชื่อ SSLock-Candidates ซึ่งทำหน้าที่จัดเก็บค่าของ Domain Name เช่น gmail.com พร้อมด้วย JavaScript ที่ใช้อ่านค่า HTTP Header จากนั้นในการทำงานของเว็บเบราว์เซอร์ของไคลเอนต์จะทำการเปลี่ยนแปลงชื่อ Domain Name เสียใหม่ และทำการส่งคำขอไปที่เว็บเซิร์ฟเวอร์ด้วย Domain Name ที่มีความมั่นคงปลอดภัยไปบนโพรโทคอล HTTPS เช่น https://secure.gmail.com แต่วิธีการป้องกันการโจมตีของ SSLock นี้ยังมีข้อเสียในด้านของการพัฒนาระบบให้เป็นมาตรฐาน ซึ่ง SSLock สามารถทำได้เพียงการตรวจสอบการโจมตีเท่านั้น แต่ไม่สามารถป้องกันการโจมตีด้วยวิธี SSL Stripping Attack ได้

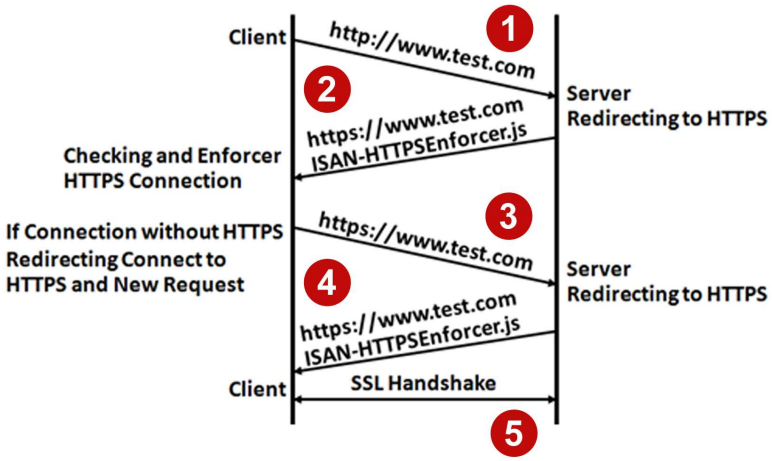
Fung และคณะ [31] ได้เสนอ HTTPSLock โดยเป็นข้อเสนอวิธีการบังคับใช้งาน HTTPS สำหรับเว็บไซต์ที่มีการใช้งาน Certificate ใบรับรองที่ถูกต้อง โดยอาศัย JavaScript ในการตรวจสอบ Certificate หากเว็บไซต์ที่กำลังใช้งานถูกตรวจสอบแล้วพบว่ามีสถานะเป็น ใบรับรองที่ไม่ถูกต้อง ซึ่งอาจเกิดจากการถูกโจมตี SSL/TLS ด้วยวิธี SSL Sniff การทำงานของ HTTPSLock จะไม่อนุญาตให้มีการใช้งานเว็บไซต์ดังกล่าว และสำหรับเว็บไซต์ที่มีการใช้งาน ใบรับรองที่ไม่ถูกต้อง แต่เมื่อเข้าใช้งานเว็บไซต์โดยที่การแสดงผลของโพรโทคอลใน URL ที่ช่อง Address Bar บนเว็บเบราว์เซอร์เป็น HTTP ซึ่งแทนที่จะเป็น HTTPS การทำงานของ HTTPSLock ก็จะแสดงผลของการตรวจสอบว่า ผู้ใช้กำลังใช้งานเว็บไซต์ที่ไม่ถูกต้องและมีความเสี่ยง ซึ่งยังพบว่าวิธีการทำงานของระบบ HTTPSLock ยังมีข้อเสียอยู่ เพราะสามารถตรวจสอบการโจมตี HTTPS ได้เท่านั้น ซึ่งแจ้งเตือนการโจมตีด้วย SSL Stripping Attack โดยเฉพาะรวมถึงปัญหาการใช้งาน เนื่องมาจากระบบรองรับการใช้งาน 70% ของเว็บเบราว์เซอร์ทั้งหมด ดังนั้นเมื่อถูกโจมตี จะส่งผลกระทบให้ผู้ใช้ไม่สามารถเข้าใช้งานเว็บไซต์ได้ตามปกติ

Puangpronpitag และ Sriwiboon [32] ได้เสนอ ISAN-HTTPS Enforcer ซึ่งถูกพัฒนาขึ้นโดยใช้ JavaScript เพื่อเป็นระบบต้นแบบ ที่สามารถทำงานได้กับทุกโปรแกรมเว็บเบราว์เซอร์ที่รองรับการใช้งาน JavaScript โดยไม่ต้องทำการปรับเปลี่ยนหรือติดตั้ง Plug-in เพิ่ม ขั้นตอนการทำงานประกอบด้วย

1) เมื่อคำขอของผู้ใช้ถูกส่งไปยังเว็บไซต์ โดยทั่วไปจะไม่ได้ระบุ “https” ใน URL ในแถบของ Address Bar ตัวอย่างเช่น test.com หรือ www.test.com

2) ทางด้านฝั่งเว็บเซิร์ฟเวอร์ หากมีการร้องขอหน้าเว็บที่เป็นความลับ หรือต้องการความมั่นคงปลอดภัย เว็บเซิร์ฟเวอร์ก็จะเปลี่ยนเส้นทางการเชื่อมต่อจาก HTTP เป็นการเชื่อมต่อกับ HTTPS แทน หลังจากที่เว็บเซิร์ฟเวอร์ตอบสนองต่อข้อความที่ถูกร้องขอมา เช่น ข้อมูลของหน้าเว็บ และ JavaScript ให้กับผู้ใช้ การสื่อสารระหว่างไคลเอนต์และเว็บเซิร์ฟเวอร์นั้นจะใช้เชื่อมต่อ HTTPS

3) ในกรณีหน้าเว็บถูกโหลดเสร็จสิ้นแล้ว และมีการสื่อสารอยู่บน HTTP ปกติ ISAN-HTTPS Enforcer ที่ทำงานทางด้านไคลเอนต์จะทำการตรวจสอบ URL ถ้ามีข้อมูลอยู่ในรายชื่อของการบังคับใช้ โพรโทคอล HTTPS แล้ว ISAN-HTTPS Enforcer จะทำการเปลี่ยนเส้นทางการเชื่อมต่อไปเป็น HTTPS ซึ่งอัลกอริทึม แสดงดังภาพที่ 2.22



ภาพที่ 2.22 แผนภาพการทำงานของ ISAN-HTTPS Enforcer

ที่มา: [33]

สมนึก พ่วงพรพิทักษ์ และอภิรักษ์ ทูลธรรม [34] ได้ทำการประเมินวิธีแก้ไขปัญหาการโจมตีด้วยการเปลือยเอสเอสแอล โดยคัดเลือกระบบป้องกันที่มีการเสนอขึ้นเพื่อทำการทดสอบ พบว่า ISAN-HTTPS Enforcer, HSTS และ SSLock มีความสามารถในการบังคับให้เว็บเบราว์เซอร์กลับมาใช้โพรโทคอล HTTPS อีกครั้ง เมื่อถูกโจมตีด้วยวิธี SSL Stripping Attack ในขณะที่ HProxy, HTTPSLock และ EV-SSL มีความสามารถในการตรวจจับการโจมตีแล้วแจ้งเตือนให้กับผู้ใช้ทราบ แต่ไม่ได้ป้องกันการโจมตีได้ และในด้านของการใช้งานนั้น SSLock, HTTPSLock และ HSTS สามารถรองรับได้เฉพาะบางเว็บเบราว์เซอร์เท่านั้น ซึ่งในผลการทดลองได้แสดงให้เห็นว่า ISAN-HTTPS Enforcer สามารถใช้งานได้กับ Platform ที่หลากหลายของโปรแกรมเว็บเบราว์เซอร์และระบบปฏิบัติการ ในแง่ของการเป็นมิตรต่อผู้ใช้ ISAN-HTTPS Enforcer มีมากกว่า HSTS แม้แต่การพิมพ์ที่ “https://” ในช่องของ Address Bar ก็ยังให้ผลของ KLM ที่ดีกว่า แต่อย่างไรก็ตามวิธีที่นำเสนอนี้มี Overhead ในแง่ของการตอบสนองต่อเวลา (Response Time) อยู่บ้างเล็กน้อย ซึ่งสาเหตุมาจากเวลาที่ถูกใช้ไปในการประมวลผลของ JavaScript แต่ข้อเสียที่สำคัญที่สุดของงานวิจัยนี้ก็คือ หาก SSL Stripping Attack สามารถปลดการใช้งานโพรโทคอล HTTPS ออกได้ การปลด

JavaScript ที่ใช้ในการป้องกันนี้ก็สามารถทำได้เช่นเดียวกัน โดยการแก้ไขโปรแกรม SSLStrip ซึ่งเป็น Python Script ให้ทำการลบ

<script type="text/JavaScript" src="ISAN-HTTPSEnforcer.js"></script> ออก เมื่อ Tag ที่เรียกใช้งาน JavaScript ที่ใช้ป้องกันถูกปลดออกไปก็จะไม่มีระบบป้องกันที่มาทำหน้าที่ในการบังคับให้มีการใช้โพรโทคอล HTTPS อีก การจู่โจมก็จะสามารถกระทำได้

ณัฐวุฒิ ศรีวิบูลย์ และสมนึก พ่วงพรพิทักษ์ [35] ได้เสนอการแก้ไขปัญหาการโจมตีเว็บไซต์ที่ทำงานบน HTTPS ด้วยวิธีการโจมตีแบบ SSL Stripping Attack โดยใช้การสังเกต EV-SSL และโพรโทคอล HTTPS โดยทำการจัดเก็บรายชื่อเว็บไซต์ที่มีการกำหนดให้เรียกใช้โพรโทคอล HTTPS ไว้ใน เครื่องมือ Bookmark ของเว็บเบราว์เซอร์ เพื่อแก้ไขปัญหาของวิธีการป้องกันการโจมตี SSL ของงานวิจัยที่ถูกนำเสนอก่อนหน้านี้ ที่ไม่สามารถป้องกันการโจมตี SSL ด้วยวิธี SSL Stripping Attack ได้ อย่างมีประสิทธิภาพ รวมถึงปัญหาความไม่สะดวกในการเรียกใช้งานของผู้ใช้ ปัญหาเรื่องความสามารถ ในการปรับใช้กับระบบเว็บไซต์เดิมที่มีอยู่ปัจจุบัน และปัญหาที่ระบบไม่รองรับการทำงานกับทุก โปรแกรมเว็บเบราว์เซอร์ ซึ่งจากผลการทดสอบของงานวิจัยแสดงให้เห็นว่า วิธีที่นำเสนอสามารถทำงาน ได้อย่างมีประสิทธิภาพ ผู้ใช้ได้รับความสะดวกในการใช้งานมากกว่าวิธีแก้ไขปัญหาแบบเดิม โดยทำการ วัดจากเวลาทั้งหมดในการทำกิจกรรมบนเว็บเบราว์เซอร์ ด้วยวิธี Keystroke-level Model (KLM) โดยวิธีการที่นำเสนอนี้สามารถรองรับการทำงานได้บนทุกเว็บเบราว์เซอร์ และไม่ต้องเปลี่ยนแปลงวิธีการทำงานของเว็บเซิร์ฟเวอร์แต่อย่างใด ซึ่งผลการทดสอบระบบป้องกันการโจมตี HTTPS ได้

แต่พบว่าการใช้งานวิธีดังกล่าวนี้ยังมีข้อเสียคือ ความยุ่งยากของผู้ใช้ ซึ่งจะต้องทำการบันทึก URL ที่ขึ้นต้นด้วย “https://” ของเว็บไซต์ที่ต้องการเรียกใช้ลงใน Bookmark ของโปรแกรมเว็บเบราว์เซอร์เสมอทุกครั้งเมื่อมีการใช้งานเว็บไซต์ใหม่ ที่ยังไม่ได้ถูกบันทึกลงใน Bookmark List และในกรณีที่ใช้โปรแกรมเว็บเบราว์เซอร์หลายโปรแกรม ผู้ใช้ก็จะต้องทำการเพิ่มข้อมูลของ URL ลงใน Bookmark ของทุกโปรแกรมด้วย ทำให้สูญเสียเวลาไปโดยไม่จำเป็น

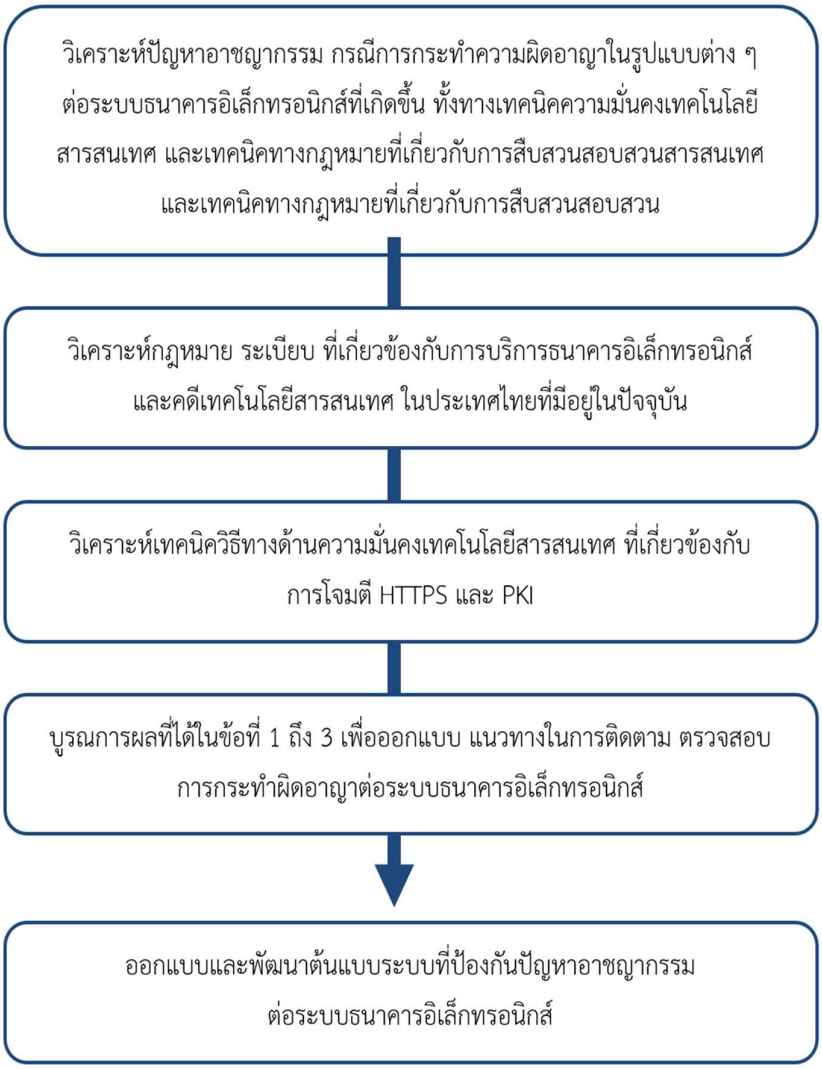
จากงานวิจัยที่เกี่ยวข้องจะเห็นว่าวิธีการต่อสู้ทางเทคนิคเพื่อโจมตีและปกป้องระบบ HTTPS ซึ่งเกี่ยวพันกับระบบ e-banking นั้นมีการดำเนินการและเปลี่ยนแปลงต่อเนื่องตลอดมา งานวิจัยนี้จะได้ศึกษาสถานการณ์ล่าสุดของปัญหาความมั่นคงและภัยคุกคามของระบบ e-banking ในประเทศไทย และเสนอวิธีการในการป้องกัน

นอกจากนี้ ปัญหาด้านการสืบสวนสอบสวนคดีด้าน e-banking ในประเทศไทยยังแทบจะไม่มีการศึกษาวิจัย อย่างจริงจัง ทั้งที่การดำเนินการในฝั่งกฎหมายและการสอบสวนเองนั้นก็เป็นปัญหาอยู่มาก ในงานวิจัยนี้จะได้ศึกษาข้อกฎหมายและกรณีคดีที่เคยเกิดขึ้น กับกรณีทางเทคนิคที่พบ เพื่อเสนอแนวทางในการสืบสวนคดีด้านนี้อีกด้วย

บทที่ 3
วิธีดำเนินการวิจัย

ในบทนี้จะกล่าวถึงกระบวนการวิเคราะห์ปัญหาอาชญากรรม กรณีการกระทำความผิดอาญาในรูปแบบต่าง ๆ ต่อระบบธนาคารอิเล็กทรอนิกส์ที่เกิดขึ้น และวิเคราะห์ปัญหาการทำงานที่ผิดปกติของระบบ HSTS การกลับมาถูกโจมตีได้ใหม่ด้วยการเปลือยเอสเอสแอล (SSL Stripping Attack) กระบวนการทดสอบโจมตีและเสนอกลไกป้องกันการถูกดักจับข้อมูลเป็นกลไกชั้นที่ 2 ป้องกันกรณี HTTPS ถูกทำลาย ตลอดจนเครื่องมือและสภาพแวดล้อมที่ใช้ในการทดลอง

3.1 กรอบแนวคิดในการศึกษา



3.2 วิเคราะห์ปัญหาอาชญากรรม

งานวิจัยนี้จะได้ศึกษาคดีที่เคยเกิดขึ้น เช่น [54-56] เพื่อทำการวิเคราะห์อาชญากรรมทั้งในเชิงกฎหมายและเทคนิควิธีที่ใช้ โดยเฉพาะอย่างยิ่งเทคนิคที่ได้กล่าวไปแล้วเบื้องต้นในบทที่ 2 จากรายงานของ Accenture and the Ponemon Institute [57] พบว่าความเสียหายของการโจมตีทางไซเบอร์ (Cyber-attack) ต่อธนาคารต่าง ๆ ทั่วโลก มีมูลค่าถึง 18.3 ล้านเหรียญสหรัฐ ต่อปี ต่อธนาคาร เมื่อปี ค.ศ. 2019 และ จากรายงานของ Clearswift [58] พบว่า 70% ของสถาบันการเงินและธนาคารทั่วโลก เคยถูกโจมตีทางไซเบอร์ในช่วงปี ค.ศ. 2019 และมีแนวโน้มจะเพิ่มขึ้นไปเรื่อย ๆ

3.3 วิเคราะห์กฎหมาย ระเบียบ ที่เกี่ยวข้องกับการบริการธนาคารอิเล็กทรอนิกส์

งานวิจัยนี้จะได้ศึกษา วิเคราะห์กฎหมายที่เกี่ยวข้อง ระเบียบวิธี อุปสรรคต่างที่พบในคดีที่เคยเกิดขึ้น เช่น [54-56] เพื่อทำการวิเคราะห์เพื่อหาแนวทางในการกำหนดวิธีการสืบสวนคดีที่เหมาะสมต่อไป ดังรายงานที่จะได้กล่าวต่อในบทที่ 4

3.4 วิเคราะห์เทคนิควิธีทางด้านความมั่นคงเทคโนโลยีสารสนเทศ ที่เกี่ยวข้อง

การรักษาความมั่นคงของเว็บไซต์มีประเด็นที่ต้องให้ความสำคัญ คือ ข้อมูลที่มีการสื่อสารระหว่างผู้ใช้งานกับผู้ให้บริการ (Client Browser กับ Web Server) จำเป็นต้องมีการเข้ารหัสในการสื่อสาร ซึ่งเทคโนโลยีที่มีการใช้กัน ได้แก่ HTTPS (Hypertext Transfer Protocol Secure) [1] ร่วมกับ TLS (Transport Layer Security) [11] เพื่อปกป้องข้อมูลระหว่างการสื่อสาร โดยอาศัยเทคนิคโครงสร้างพื้นฐานกุญแจสาธารณะที่เรียกว่า Public Key Infrastructure (PKI) [36] โครงสร้างดังกล่าวจะมีกระบวนการออกใบรับรอง (Certificate) ของเซิร์ฟเวอร์สำหรับการพิสูจน์ตัวจริง (Authentication) ซึ่งใบรับรองดังกล่าวจะถูกรับรองโดยหน่วยงานที่เรียกว่า Certificate Authority (CA) เพื่อรับประกันว่าเว็บเซิร์ฟเวอร์ของผู้ให้บริการนั้นเป็นตัวจริง ไม่ได้ถูกปลอมแปลง ซึ่งมีกระบวนการเข้ารหัสแบบสมมาตร (Symmetric) และอสมมาตร (Asymmetric) ทำให้การสื่อสารผ่านโพรโทคอล HTTPS อยู่ในรูปแบบ Cipher Text มีความมั่นคงระหว่างการสื่อสารเพื่อป้องกันปัญหาการถูกดักจับข้อมูล

แต่อย่างไรก็ตาม HTTPS ที่ใช้รักษาความมั่นคงในเว็บไซต์ก็ยังถูกโจมตีได้ด้วยวิธีการต่าง ๆ ซึ่งมีเทคนิคที่สำคัญในการโจมตีได้แก่การเปลือยเอสเอสแอล (SSL Stripping Attack) ถูกเสนอโดย Moxie Marlinspike และคณะ [2] ในปี ค.ศ 2009 ทำให้ระบบธนาคารออนไลน์ (Internet Banking) และระบบการค้าอิเล็กทรอนิกส์ (E-Commerce) หรือในหลายเว็บไซต์ถูกโจมตีและตกเป็นคดีที่สำคัญในทั่วโลกรวมถึงประเทศไทย ผลลัพธ์จากการถูกโจมตีด้วยเทคนิค SSL Stripping Attack ส่งผล

กระทบต่อการทำงานของโพรโทคอล HTTPS ซึ่งจะถูกเปลี่ยนการทำงานเป็น HTTP ทำให้ระบบเว็บไซต์ธนาคารออนไลน์ถูกแฮกเกอร์โจมตีได้ SSL Stripping Attack จึงถือเป็นภัยคุกคามร้ายแรงที่สร้างปัญหาให้กับระบบเว็บไซต์มายาวนาน มีหลายงานวิจัยที่พยายามเข้ามาวิเคราะห์แก้ไขปัญหาดังกล่าว เช่น SSLock [30], HProxy [37], HTTPSLock [31], ISAN-HTTPS Enforcer [33], Click2Enforce [38], HTTP Strict Transport Security (HSTS) [14] กระทั่งปัจจุบันมาตรฐานที่ถูกเลือกมาแก้ไขปัญหาดังกล่าวก็คือกลไก HSTS และยังเป็นหนึ่งในมาตรฐานของ Internet Engineering Task Force (IETF)ตามเอกสาร RFC 6797 ที่ถูกเสนอให้ใช้ป้องกันการถูกโจมตีด้วยวิธี SSL Stripping Attack และยังรองรับการทำงานในทุกเว็บเบราว์เซอร์ โดยหน้าที่ผู้ดูแลเว็บเซิร์ฟเวอร์ต้องทำการ Configuration ให้กลไก HSTS ทำงาน ซึ่งเว็บไซต์ทั่วโลกรวมถึงในประเทศไทยหลายแห่งมีการดำเนินการปรับใช้กลไกดังกล่าวเป็นที่เรียบร้อยแล้ว โดยการทำงานของกลไก HSTS จะบังคับให้เว็บเบราว์เซอร์ที่กำลังทำงานอยู่บนเว็บไซต์ต้องสื่อสารผ่าน HTTPS เท่านั้น แม้ผู้ใช้จะไม่ระบุว่าต้องการใช้ HTTPS ก็ตามจึงทำให้เว็บไซต์ที่ต้องการความมั่นคงสูงอย่าง เช่น ธนาคารออนไลน์ เว็บไซต์การค้าอิเล็กทรอนิกส์ สามารถป้องกันการถูกโจมตีได้ ยกเว้นแต่ว่ามีบางเว็บไซต์ที่ไม่มีการดำเนินการปรับใช้กลไก HSTS เท่านั้น

จากที่กล่าวมาข้างต้นจะพบว่าปัญหาการโจมตีแบบ SSL Stripping Attack เหมือนจะสิ้นสุดลงแล้ว กระทั่งเมื่อเดือน ตุลาคม พ.ศ. 2562 ISAN Lab [39] ได้ทำการวิเคราะห์ปัญหา Web Security ในประเทศไทย สำรวจเว็บไซต์ที่ให้บริการธนาคารออนไลน์ รวมถึงระบบเซอร์วิสที่สำคัญต่าง ๆ ของประเทศไทย ค้นพบว่าระบบเว็บไซต์ธนาคารออนไลน์ที่เคยได้รับการป้องกัน ล้วนแล้วแต่ถูกโจมตีได้อีกครั้งเกือบทั้งสิ้น ในการทดสอบครั้งนี้ใช้การจู่โจมทั้งสคริปต์การโจมตีแบบใหม่ของแฮกเกอร์และสูตรการโจมตีแบบเก่าของ Moxie Marlinspike พบว่าถึงแม้มีการ Configuration ปรับใช้กลไกของ HSTS ตามสูตรที่รู้กัน HSTS กลับไม่ประสบผลสำเร็จในการป้องกัน ทำให้การโจมตีด้วย SSL Stripping Attack ที่ไม่สามารถโจมตีได้มานานหลายปีกลับมาเป็นภัยคุกคามต่อความมั่นคงของระบบเว็บไซต์ใหม่อีกครั้ง

ดังนั้นโครงการวิจัยนี้ จึงเสนอที่จะทำการวิเคราะห์ปัญหาด้านเทคนิคของกลไก HSTS ซึ่งเป็นกลไกที่สำคัญของการทำงานร่วมกับโพรโทคอล HTTPS ในการรักษาความมั่นคงของเว็บไซต์ และเพื่อเข้าใจสาเหตุที่เทคนิค SSL Stripping Attack กลับมาโจมตีได้ใหม่อีกครั้ง และเพื่อเสนอวิธีแก้ไขปัญหาต่อไป

3.4.1 เว็บไซต์ที่ใช้ในการทดลอง SSL Stripping Attack

จากการที่ SSL Stripping Attack เป็นเทคนิคที่ถูกใช้งานอย่างแพร่หลายในการโจมตีระบบ Online Banking, ระบบ E-Commerce และ Web Applications อื่น ๆ ปัจจุบันการแก้ปัญหาที่ดีที่สุดและเป็นที่ยอมรับก็คือกลไก HSTS ซึ่งเว็บไซต์ส่วนใหญ่ที่ต้องการความมั่นคงสูง ได้หันมาปรับใช้กันอย่างแพร่หลาย แต่กลับยังพบว่าระบบธนาคารออนไลน์ก็ยังมีผู้ไม่ประสงค์ดีโจมตีดักจับข้อมูลบัญชีผู้ใช้ และรหัสผ่าน ให้เห็นอยู่ในปัจจุบัน ดังนั้นงานวิจัยนี้จึงได้นำเสนอการประเมินปัญหาของ SSL Stripping Attack บนระบบเว็บไซต์ของ Online Banking และระบบ E-Commerce ทำการทดลองบน Test-bed พร้อมทั้งเว็บเบราว์เซอร์ที่หลากหลายประกอบด้วย Google Chrome, Edge, Mozilla Firefox, Internet Explorer และ Safari ซึ่งผลที่ได้นี้จะสามารถนำมาวิเคราะห์ช่องโหว่ที่เกิดขึ้นและนำมาเป็นแนวทางในการแก้ไขปัญหาของ SSL Stripping Attack ได้ โดยมีรายละเอียดดังต่อไปนี้

1) กลุ่มตัวอย่างเว็บไซต์ที่ใช้งาน SSL/TLS ของระบบเว็บไซต์ ซึ่งประกอบด้วยระบบที่ให้บริการธนาคารออนไลน์ในไทย จำนวน 11 เว็บไซต์ โดยเลือกจากผู้ให้บริการในปัจจุบันซึ่งเป็นที่นิยมและจากฐานข้อมูล Internet Banking ของธนาคารแห่งประเทศไทย [40] ระบบที่ให้บริการ E-commerce จำนวน 5 เว็บไซต์ โดยการเลือกระบบของต่างประเทศ และในประเทศไทยที่ได้รับความนิยม

2) เพื่อให้เข้าใจปัญหาการทำงานของกลไก HSTS อย่างแท้จริง ในการทดลองนี้จึงได้ทำการตรวจสอบและวิเคราะห์ HTTP Response Header ของเว็บไซต์กลุ่มดังกล่าว ว่ามีการตั้งค่าปรับใช้กลไก HSTS หรือไม่อย่างไร

3) ทดลองโจมตีเว็บไซต์ โดยใช้วิธี SSL Stripping Attack ในการโจมตี ซึ่งประเมินปัญหาโดยการใช้ระบบปฏิบัติการ Kali linux ในการโจมตีแบบแทรกกลางการสื่อสารและใช้ Wireshark ในการโจมตีเพื่อดักจับรหัสผ่านของเครื่องเป้าหมายและทำการทดสอบบนเว็บเบราว์เซอร์จำนวน 5 โปรแกรมประกอบด้วยโปรแกรม Google Chrome, Edge, Mozilla Firefox, Internet Explorer และ Safari

4) สรุปผลการทดลองโจมตี SSL Stripping Attack

ตารางที่ 3.1 รายชื่อเว็บไซต์ระบบให้บริการธนาคารออนไลน์ในไทย

ลำดับ	เว็บไซต์*	URL
1	A	https://**********.com
2	B	https://**********.com
3	C	https://**********.com
4	D	https://**********.com
5	E	https://**********.com
6	F	https://**********.com
7	G	https://**********.com
8	H	https://**********.com
9	I	https://**********.com
10	J	https://**********.com
11	K	https://**********.com

** เพื่อสงวนชื่อเว็บไซต์ธนาคารออนไลน์ในไทย จึงใช้อักษรย่อแทน*

ตารางที่ 3.2 รายชื่อเว็บไซต์ระบบผู้ให้บริการ E-commerce

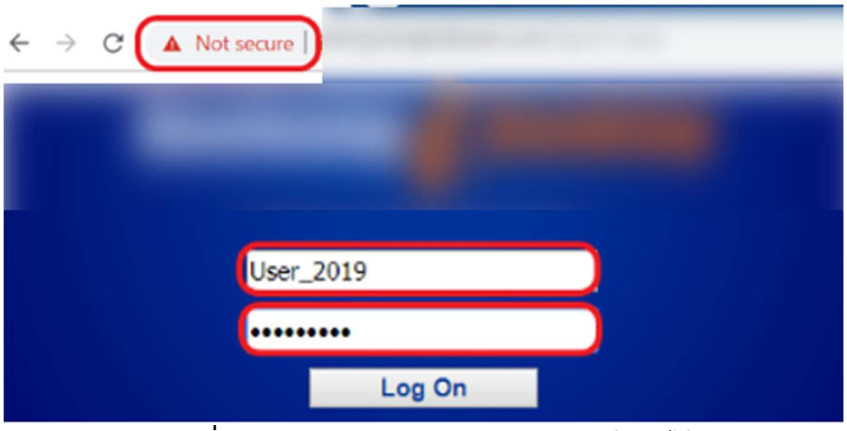
ลำดับ	เว็บไซต์*	URL
1	L	https://**********.com
2	M	https://**********.com
3	N	https://**********.com
4	O	https://**********.com
5	P	https://**********.com

** เพื่อสงวนชื่อเว็บไซต์ E-commerce จึงใช้อักษรย่อแทน*

3.4.2 เกณฑ์การประเมินจากเทคนิคการโจมตี SSL Stripping Attack

เกณฑ์การประเมินที่ถูกใช้เพื่อพิจารณาผลลัพธ์ที่เกิดจากการโจมตีด้วยเทคนิค SSL Stripping Attack มีเกณฑ์การประเมินดังนี้

1) SSL Stripping Attack สามารถโจมตีได้ หมายถึง เว็บไซต์ที่นำมาทดสอบถูกทำลายระบบป้องกัน SSL/TLS ออกได้ และเปลี่ยนไปใช้โพรโทคอล HTTP ในการสื่อสารแทน ดังภาพที่ 3.1

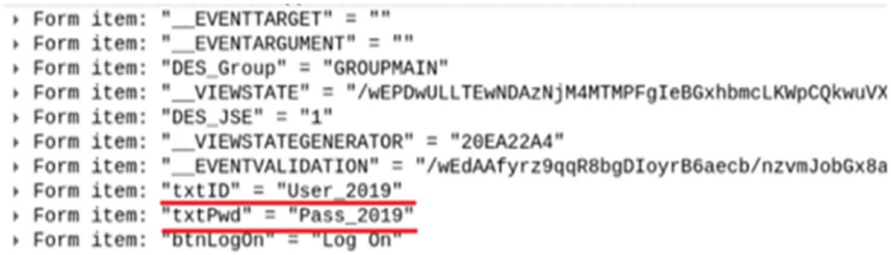


ภาพที่ 3.1 SSL Stripping Attack สามารถโจมตีได้

2) SSL Stripping Attack ไม่สามารถโจมตีได้ หมายถึง เว็บไซต์ที่นำมาทดสอบไม่ถูกทำลายระบบป้องกัน SSL/TLS ออก และยังคงใช้โพรโทคอล HTTPS ในการสื่อสาร ดังภาพที่ 3.2

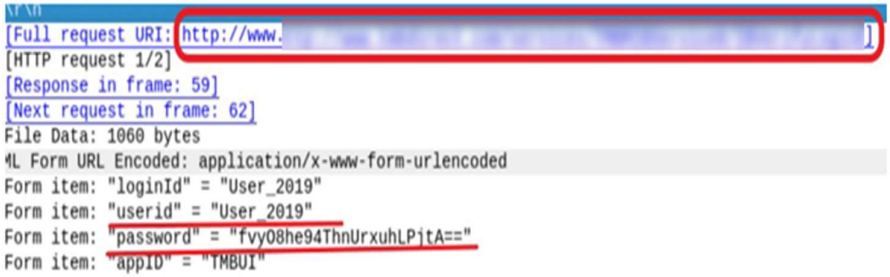
ภาพที่ 3.2 SSL Stripping Attack ไม่สามารถโจมตีได้

3) Data Sniffing Attack สามารถโจมตีได้ หมายถึง หลังจากถูกโจมตีด้วย SSL Stripping Attack แล้ว สามารถดักจับข้อมูลของชื่อผู้ใช้และรหัสผ่านได้ ดังภาพที่ 3.3



ภาพที่ 3.3 Data Sniffing Attack สามารถโจมตีได้

4) Data Sniffing Attack ไม่สามารถโจมตีได้ หมายถึง หลังทำการโจมตีแล้วไม่สามารถดักจับข้อมูลของชื่อผู้ใช้หรือดักจับรหัสผ่านแบบ Clear Text ได้ ดังภาพที่ 3.4



ภาพที่ 3.4 Data Sniffing Attack ไม่สามารถโจมตีได้

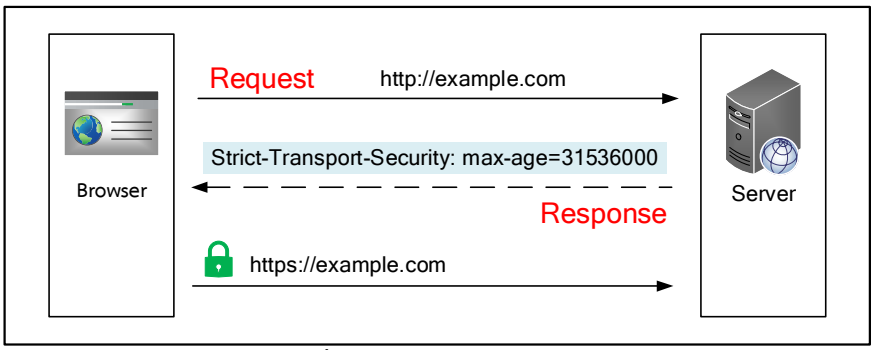
3.4.3 การวิเคราะห์ปัญหาการกลับมาจู่โจมได้ใหม่ของ SSL Stripping Attack

ในวงการวิจัยเป็นที่ทราบกันดีว่า HSTS ได้เข้ามาแก้ปัญหาการถูกโจมตีด้วย SSL Striping Attack และระบบ HSTS ยังเป็นหนึ่งในมาตรฐานของ Internet Engineering Task Force (IETF) ตามเอกสาร RFC 6797 ทำให้ทุกเบราว์เซอร์ทุกตัวรองรับการทำงานระบบ HSTS โดยมีกลไกการทำงาน 2 รูปแบบด้วยกันคือ 1) HSTS Directive 2) HSTS Preload ซึ่งระบบ HSTS จะทำหน้าที่เป็นกลไกส่วนเสริมของโพรโทคอล HTTPS ที่เปิดให้เว็บเซิร์ฟเวอร์ "บังคับ" ให้เว็บเบราว์เซอร์เชื่อมต่อผ่าน HTTPS เท่านั้น แม้ผู้ใช้จะไม่ระบุว่าต้องการใช้ HTTPS ก็ตาม ทำให้ผู้ใช้งานเว็บไซต์ระหว่าง Web Browser กับ Web Server ไม่มีการเชื่อมต่อแบบ HTTP ที่มีปัญหาเรื่องการถูกดักจับข้อมูลแบบ Clear Text สำหรับเว็บไซต์ที่ต้องการความมั่นคงสูงอย่างเช่น ระบบธนาคารออนไลน์ (Internet Banking) ระบบการค้าอิเล็กทรอนิกส์ (E-commerce) จึงมีการปรับใช้ระบบป้องกัน HSTS

อย่างแพร่หลาย เพื่อรักษาความมั่นคง Web Application ในงานวิจัยนี้จึงเกิดคำถามว่าวิธีการแก้ไขปัญหา HTTPS จากการถูกโจมตีด้วย SSL Striping Attack ที่มีการปรับใช้กลไก HSTS เพียงอย่างเดียวนั้น มีประสิทธิภาพในการป้องกันการโจมตีจริงหรือไม่ ซึ่งจากการทดลอง ISAN Lab ค้นพบว่าระบบเว็บไซต์ธนาคารออนไลน์ที่เคยได้รับการป้องกันจาก HSTS ล้วนแล้วแต่ถูกโจมตีได้อีกครั้งเกือบทั้งสิ้นด้วยเทคนิค SSL Striping Attack และแฮกเกอร์ที่มีความเชี่ยวชาญก็สามารถปรับปรุงโค้ดเพื่อต่อยอดความสามารถในการโจมตีได้ ดังนั้นในงานวิจัยนี้จึงมีแนวคิดทดสอบกลไก HSTS เพื่อวิเคราะห์การทำงานที่ผิดปกติของกลไก HSTS ซึ่งเป็นส่วนเสริมที่สำคัญในการบังคับการสื่อสารผ่านโพรโทคอล HTTPS ระหว่าง Web Browser กับ Web Server โดยมีรายละเอียดการวิเคราะห์ ดังต่อไปนี้

3.4.4 แนวคิดการทดลอง HSTS Directive

การทำงานของ HSTS Directive มีลักษณะการทำงานโดยเว็บเซิร์ฟเวอร์จะมีการตอบกลับ (Response) ในส่วนของ HTTP Header ชื่อ Strict-Transport-Security: max-age=31536000; include SubDomains เมื่อเว็บเบราว์เซอร์ตรวจสอบพบ HTTP Header ดังกล่าวเว็บเซิร์ฟเวอร์ก็จะบังคับให้เว็บเบราว์เซอร์เชื่อมต่อผ่านโพรโทคอล HTTPS ทำให้การสื่อสารมีความมั่นคงปลอดภัย จากที่กล่าวมาข้างต้นจะพบว่าชุดคำสั่ง Header HSTS ถูกเพิ่มและตั้งค่าเก็บไว้ที่เว็บเซิร์ฟเวอร์การทำงานที่เบราว์เซอร์จะถูกประมวลผลทุกครั้งที่ไคลเอนต์เพื่อตรวจสอบการบังคับใช้โพรโทคอล HTTPS ดังนั้นการเรียกใช้งานกลไก HSTS Directive จึงเป็นช่องโหว่ที่ใช้ในการโจมตีได้ด้วยเทคนิค SSL Stripping Attack ซึ่งลักษณะการทำงานของ HSTS Directive ดังภาพที่ 3.5



ภาพที่ 3.5 การทำงาน HSTS Directive

3.4.5 แนวคิดการทดลอง HSTS Preload

HSTS Preload เข้ามาแก้ปัญหาการสื่อสารผ่านโพรโทคอล HTTP ที่ไม่มั่นคงปลอดภัย โดยการทำงานของ HSTS Preload จะบังคับให้เชื่อมต่อผ่านโพรโทคอล HTTPS ตั้งแต่เริ่มต้นการสื่อสารทำให้เว็บเบราว์เซอร์กับเว็บเซิร์ฟเวอร์มีความมั่นคงปลอดภัยจากการถูกโจมตีดักจับข้อมูล ซึ่งการเปิดใช้งาน HSTS Preload นั้น ให้เพิ่มชุดคำสั่ง

Strict-Transport-Security: max-age=31536000;includeSubDomains; preload

โดยสามารถอธิบายโค้ด ได้ดังนี้

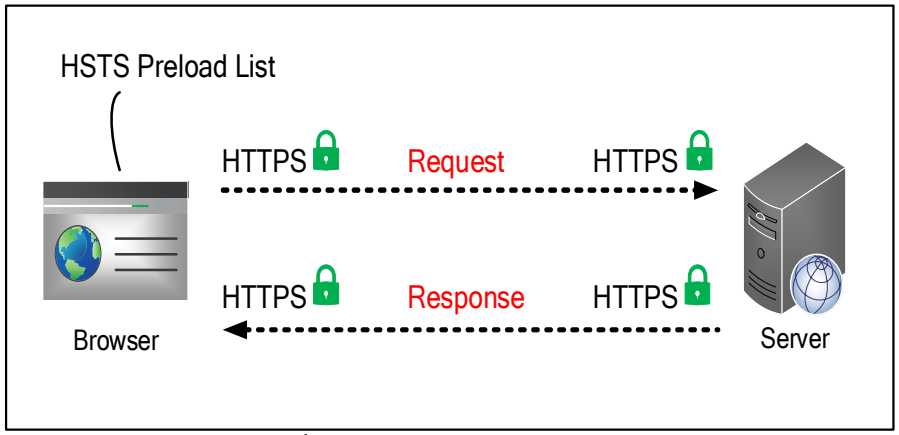
1) *max-age* ระยะเวลาของการบังคับใช้โพรโทคอล HSTS ที่กำหนดให้สื่อสารผ่านโพรโทคอล HTTPS นานเท่าใด โดยมีหน่วยเป็นวินาที

2) *includeSubDomains* กรณีสื่อสารผ่าน subdomains ของเว็บไซต์ก็ต้องสื่อสารผ่าน HSTS เช่นเดียวกัน

3) *preload* คือ domain ที่ถูกติดตั้งอยู่ในรายการ HSTS preload บน Web Browser กำหนดให้เชื่อมต่อ HTTPS จากเว็บเบราว์เซอร์ไปที่เซิร์ฟเวอร์ตั้งแต่เริ่มต้นการสื่อสาร

ให้นำชุดคำสั่งดังกล่าว ไปตั้งค่า HTTP Header จากนั้นนำ Domain Name ไปลงทะเบียนเป็น domain ใน HSTS Preload List ที่ https:// hstspreload.org ในโครงการของ Chromium ซึ่งข้อมูล Domain Name ดังกล่าวจะถูกอัพโหลดไปยังทุกเบราว์เซอร์ที่รองรับการทำงานของกลไก HSTS เมื่อมีการติดตั้งหรือ update version ของ Web Browser

จากที่กล่าวมาข้างต้น จะพบว่าสุดท้ายแล้วการบังคับเชื่อมต่อโพรโทคอล HTTPS จะอยู่ที่ Domain Name ที่กำลังเรียกใช้ Admin ของ Domain ได้ทำการลงทะเบียนและถูก list ไว้ในฐานข้อมูล ที่เรียกว่า HSTS Preload List หรือไม่ การทำงานสรุปได้ ดังภาพที่ 3.6



ภาพที่ 3.6 การทำงาน HSTS Preload

3.4.6 เทคโนโลยีรหัสผ่านใช้ครั้งเดียวชนิดต่าง ๆ และปัญหาการโดนโจมตี

OTP นั้นมีหลายชนิด ที่ปรากฏใช้ ได้แก่ Paper OTP, E-mail OTP, SMS OTP, Token OTP และ Mobile OTP เป็นต้น Paper OTP คือ ชุดของ codes ที่ถูกสร้างขึ้นโดยการสุ่ม เช่น อาจเป็นตัวเลข 6 หลัก 10 ชุด แล้วถูกพิมพ์ออกมาบนกระดาษ หรือจดออกมาเก็บไว้ โดยจะถูกใช้เป็นปัจจัยยืนยันตัวตนชั้นที่สอง ต่อจากรหัสผ่าน ซึ่งเป็นที่รู้กันดีว่า Paper OTP เป็น OTP ชนิดที่มั่นคงน้อยที่สุด เพราะหาก codes ดังกล่าวที่พิมพ์หรือจดออกมาเกิดรั่วไหลก็ไม่ปลอดภัย

E-mail OTP นั้น ก็เป็นที่รู้กันว่า มีปัญหาทางด้านความมั่นคงมากเช่นกัน เพราะช่องทางการส่ง E-mail คือช่องทางเดียวกัน กับการส่งรหัสผ่าน ทำให้ เมื่อแฮกเกอร์สามารถดักจับรหัสผ่านได้ ก็ย่อมสามารถดักจับ E-mail OTP ได้ด้วย ดังจะเห็นได้จากการทดลองของ ประพจน์ ธรรมศิลารักษ์ และสมนึก พ่วงพรพิทักษ์ [7] นอกจากนี้ จะเห็นว่าระบบ online banking ของประเทศไทย ได้ยกเลิกการใช้งาน E-mail OTP ไปตั้งแต่ พ.ศ. 2552 เนื่องจากมีความเสี่ยงสูง

สำหรับ SMS OTP ปัจจุบันเป็นที่นิยมมากที่สุดในระบบ online banking ของประเทศไทย แต่ก็มีปัญหาที่ SMS นั้นสามารถปลอมแปลง (Spoof) ได้โดยง่าย ดังถูกเปิดเผยในหลายงานวิจัย เช่น งานวิจัยของประพจน์ ธรรมศิลารักษ์ และสมนึก พ่วงพรพิทักษ์ [7] และ งานวิจัยของ Mulliner และคณะ [8] อีกทั้ง ยังมี Trojan Horse หลายตัว เช่น Zeus-in-the-Mobile (ZitMo) [41] , WUC's Conference.apk [42], และ Svpeng [43] ที่ถูกสร้างขึ้นมา เพื่อเป็น Malware ใช้จู่โจม SMS OTP โดยเฉพาะ จนตกเป็นข่าว และเห็นชัดว่า การจู่โจมระบบ online-banking ในประเทศไทย โดยการโจมตี SMS OTP สามารถทำได้ เช่น ข่าวตั้งแต่เดือนกุมภาพันธ์ พ.ศ. 2556 [44] ว่า SMS OTP โดนโจมตีด้วยวิธีการปลอมแปลง SMS (SMS spoofing) ไปหลอกลวง ให้เหยื่อคลิกลิงค์ที่ส่งมาให้เพื่อติดตั้ง Malware โดยแอบอ้างว่าเป็น SMS ที่ส่งมาจากธนาคาร เมื่อเหยื่อหลงเชื่อและติดตั้ง Malware ดังกล่าวแล้ว เหยื่อคนนั้นก็จะไม่ได้รับ SMS OTP แต่ SMS OTP จะถูกส่งต่อไปยังเครื่องแฮกเกอร์ และทำให้เหยื่อโดนปล้น online banking ในที่สุด

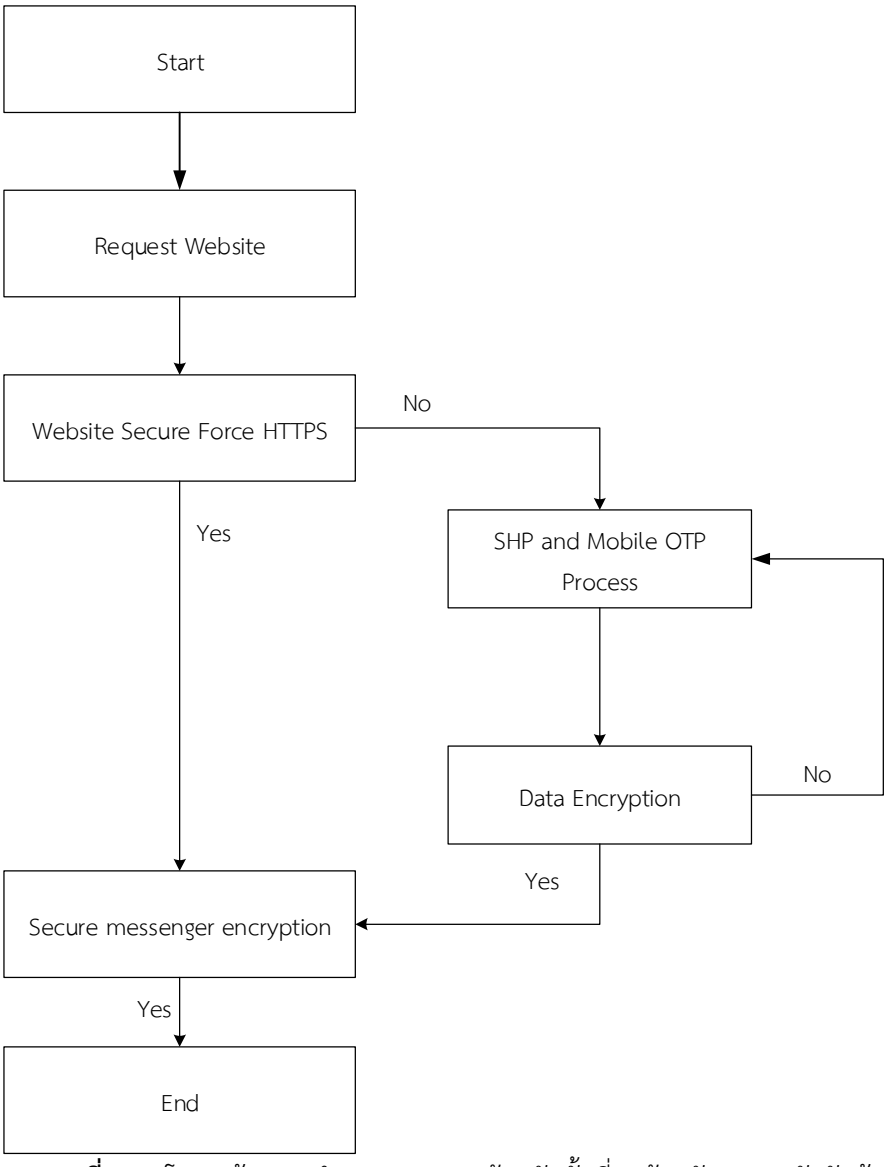
สำหรับ Token OTP เป็นรูปแบบที่มีความมั่นคงที่สุดในขณะนี้ แต่มีปัญหาคือ (1) การลงทุนที่สูงมากจากการสั่งซื้ออุปกรณ์ token มาใช้ ทำให้ธนาคารหรือบริษัทหลายแห่งยังไม่เปลี่ยนมาใช้รูปแบบนี้ ดังจะเห็นได้จากธนาคารในประเทศไทย ยังไม่ให้บริการกับลูกค้าส่วนบุคคล ด้วย Token OTP มีเพียงธนาคารต่างชาติบางแห่ง เท่านั้นที่บริการ Token OTP แก่ลูกค้าส่วนบุคคล เช่น ธนาคาร HSBC (2) นอกจากนี้ Token OTP ยังมีปัญหาการถือครอง คือผู้ใช้ที่ต้องถือพวงกุญแจ โทรศัพท์มือถือ กระเป๋าสตางค์ และสิ่งต่าง ๆ มากอยู่แล้ว จะต้องเพิ่มการถือ Token OTP อีก ทำให้บ่อยครั้งมีปัญหาคือลืมนำเอา Token OTP ติดตัวไปด้วย จนทำให้ไม่อาจใช้งานระบบได้

โครงงานวิจัยนี้ เห็นว่า Mobile OTP น่าจะเป็นทางออกที่ดี เพราะ Mobile OTP คือ Mobile Application ที่ run อยู่บน Smartphone โดยทำหน้าที่คล้ายกับ Token OTP แต่เป็น

ลักษณะ Software หรือ Soft Token โดยมีข้อดีที่ (1) ลดเรื่องค่าใช้จ่ายในการซื้อ token hardware โดยติดตั้ง Mobile Application แทน (2) โทรศัพท์มือถือ (Mobile Phone) เป็นสิ่งถือครองที่ผู้ใช้ไม่รู้สึกว่าเป็นภาระ และเป็นที่ยินดี เห็นเป็นสิ่งสำคัญ ที่ต้องพกติดตัวไปแล้ว จนถึงขนาดว่าบางคนหากลืมโทรศัพท์มือถือ ก็ต้องยอมย้อนกลับ ไปเอามาก่อน ถึงไปทำงานได้ ดังนั้น Mobile OTP จึงมีปัญหาเรื่องความรู้สึกว่าเป็นภาระการถือครอง หรือลืมทิ้งไว้ไม่พกติดตัวน้อยกว่า token OTP มาก แต่ Mobile OTP มีปัญหาที่เรื่องของความมั่นคง คือ Hacker อาจ ติดตั้ง OTP Mobile Application แล้ว ขโมย Initial Seed จากเครื่องเหยื่อ เพื่อใช้งานเป็น OTP ของเหยื่อก็อาจทำได้ อีกทั้งอัลกอริทึมของ OTP ยังมีจุดอ่อน ดังแสดงในงานวิจัย [45] ดังนั้น ข้อเสนองานวิจัยนี้ จะได้เสนอพัฒนาต่อยอดเทคนิคจาก งานวิจัย [45] เพื่อเพิ่มความมั่นคงและเสนอบูรณาการข้อมูลบางอย่างเข้ากับระบบ HTTPS

3.5 ออกแบบและพัฒนาต้นแบบเพื่อป้องกันปัญหาอาชญากรรมต่อระบบธนาคารอิเล็กทรอนิกส์

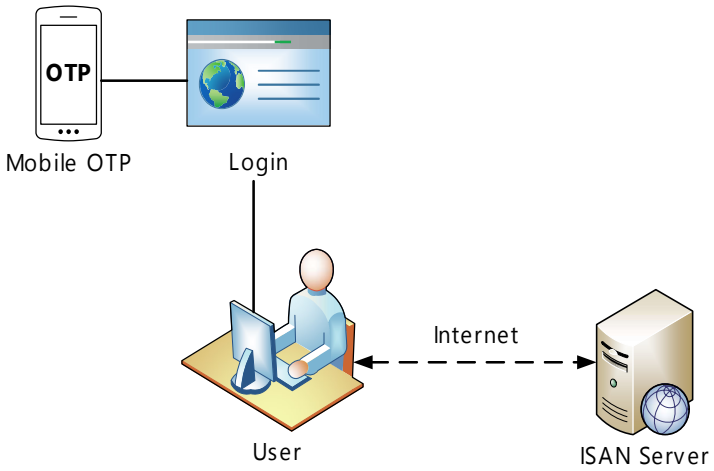
การออกแบบและพัฒนาต้นแบบด้านซอฟต์แวร์ เพื่อแก้ปัญหาการถูกดักจับข้อมูลจากเทคนิคการโจมตีด้วย SSL Stripping Attack มีแนวคิดในการออกแบบ ISAN Banking ดังแสดงโครงสร้างการทำงานในภาพที่ 3.7 โดยเริ่มจากการเรียกใช้งานเว็บไซต์ที่ตำแหน่ง (Start Point) ในสภาพแวดล้อมที่ใช้ในการทดสอบ จากนั้นเมื่อเว็บไซต์ถูกโจมตีด้วย SSL Stripping Attack จะมีกระบวนการทำงานคือ เมื่อถูกโจมตีจากเทคนิคดังกล่าวเว็บไซต์มีการบังคับใช้ HTTPS ตลอดกระบวนการใช้งานใช่หรือไม่ หากมีการใช้งาน HTTPS ถือว่าข้อมูลมีการเข้ารหัสการสื่อสารก็จะสิ้นสุดการทำงาน แต่หากไม่มั่นคง ก็จะส่งข้อมูลเริ่มกระบวนการป้องกันชั้นที่ 2 โดยนำข้อมูลเข้ารหัส Salted Hash Password (SHP) ร่วมกับ Mobile OTP จากนั้นเมื่อตรวจสอบข้อมูลมีการเข้ารหัสก็เป็นจุดสิ้นสุดการทำงาน (End) ใช่หรือไม่ ถ้าพบว่าไม่ใช่จุดสิ้นสุดการทำงานระบบจะวนกลับไปเริ่มกระบวนการทำงานตั้งแต่การแฮชค่า SHP ใหม่อีกครั้ง



ภาพที่ 3.7 โครงสร้างการทำงานของระบบป้องกันชั้นที่ 2 ป้องกันการถูกดักจับข้อมูล

จากเทคนิคการโจมตีด้วยวิธี SSL Stripping Attack มีลักษณะบังคับเปลี่ยนแปลงการทำงานของโพรโทคอลในการสื่อสารจาก HTTPS เป็น HTTP ซึ่งทำให้ไม่ปลอดภัยระหว่างการส่งข้อมูลของระบบเว็บไซต์ที่กำลังสื่อสารกับเว็บเซิร์ฟเวอร์ จึงมีแนวคิดออกแบบและพัฒนาระบบป้องกันชั้นที่ 2 ซ้อนทับ HTTPS อีกชั้น โดยมีเหตุผลที่ว่าเมื่อเหยื่อถูกจู่โจมจากเทคนิค SSL Stripping Attack โพรโทคอลเดิมที่เป็น HTTPS จะถูกบังคับให้สื่อสารผ่าน HTTP ที่ไม่ปลอดภัย จึงเกิดช่องโหว่ที่ผู้โจมตีสามารถดักจับข้อมูลของเหยื่อได้ เนื่องจากข้อมูลอยู่ในรูป Clear Text แต่หากมีการปรับใช้ระบบป้องกันในชั้นที่ 2 คือ Salted Hash Password สร้างเกราะป้องกันซ้อนทับ HTTPS พร้อมกับเสริม

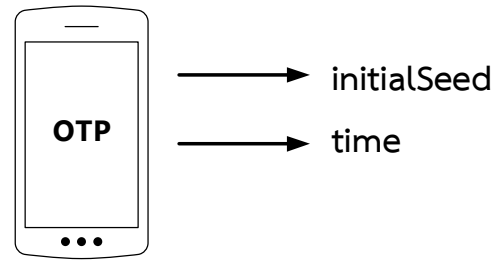
ความมั่นคงด้วย Mobile OTP เป็นตัวสร้างรหัสที่ใช้เพียงครั้งเดียวในการเข้าสู่ระบบ ถึงแม้ผู้จู่โจมสามารถทะลุผ่านชั้นมาตรฐานไปได้ แต่ก็ยังมีด่านป้องกันชั้นที่ 2 คอยป้องกันข้อมูลอีกชั้น ทั้งนี้ ได้เลือกใช้ TOTP (Time-Based One Time Password) ที่เป็นมาตรฐาน RFC 6238 มาเป็นฐานในการพัฒนาระบบ OTP เพราะปัจจุบันเครื่องสมาร์ทโฟนส่วนใหญ่ไม่มีปัญหาเวลาที่ไม่ตรงกับเวลามาตรฐานสากล ซึ่งการทำงานของสมาร์ทโฟนจะถูกตั้งค่าตามเวลาของ Network ISP ในการ Sync เวลาสากล จึงทำให้ไม่มีข้อผิดพลาดเรื่องเวลาในสมาร์ทโฟนที่ใช้ในปัจจุบัน ซึ่งมีภาพรวมและส่วนประกอบมาตรการสร้างความมั่นคงให้กับระบบเว็บไซต์ ดังภาพที่ 3.8



ภาพที่ 3.8 ภาพรวมและส่วนประกอบมาตรการสร้างความมั่นคงให้กับระบบเว็บไซต์

การสร้างมาตรการความมั่นคงชั้นที่ 2 ให้กับระบบเว็บไซต์ จะอาศัยระบบ Mobile OTP บนสมาร์ทโฟน เป็นตัวช่วยเพื่อสร้าง OTP ที่ใช้สำหรับการเข้าสู่ระบบของเว็บไซต์ โดย OTP ที่ถูกสร้างขึ้น จะเปลี่ยนไปตามช่วงเวลา NTP (Network Time Protocol) ที่เปลี่ยนไปและทางฝั่งของ Server ก็จะมีการสร้างค่า OTP ที่ตรงกันขึ้นเพื่อยืนยันความถูกต้องในการเข้าสู่ระบบ

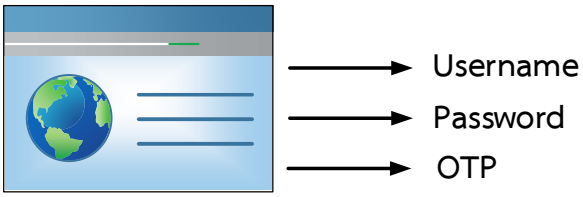
3.5.1 กระบวนการสร้าง OTP ของ Mobile OTP



ภาพที่ 3.9 กระบวนการสร้าง OTP ของ Mobile OTP

จากภาพที่ 3.9 การสร้าง OTP ในฝั่งของ Mobile OTP จะมีกระบวนการรับค่าจาก initialSeed และ Time โดยที่ initialSeed จะเป็นค่า Secret Key ที่ไม่ซ้ำกัน (อาจเป็นข้อมูลความลับจากกระบวนการยืนยันตัวตน ก่อนเข้าใช้งานระบบเว็บไซต์) จากนั้นนำข้อมูลไป Hash ด้วย SHA 256 และในส่วน Time เป็นค่าที่ได้จาก Network Time Protocol ที่ดึงข้อมูลมาจากสมาร์ทโฟน ซึ่งจะนำค่าที่ได้ทั้ง 2 มาเข้ากระบวนการสร้าง OTP เพื่อนำมาใช้ร่วมกับการเข้าสู่ระบบเว็บไซต์ ซึ่ง OTP จะแสดงค่าใหม่ในทุก ๆ 30 หรือ 60 วินาที

3.5.2 กระบวนการเข้าสู่ระบบ



ภาพที่ 3.10 กระบวนการเข้าสู่ระบบ

จากภาพที่ 3.10 การเข้าสู่ระบบเว็บไซต์จะใช้ทั้ง 3 ค่า คือ Username, Password และ OTP โดยขั้นตอนแรกให้ยืนยัน Username เมื่อกรอกและยืนยัน ระบบจะนำข้อมูลต้นฉบับมาทำการ Hash ด้วย SHA 256 ซ้ำ 2 รอบ กระบวนการนี้จะเกิดขึ้นที่ฝั่งของ Client ทำการส่งค่า Hash ไปตรวจสอบที่ฝั่ง Server ในรูปแบบ Client Side Script บนภาษา JavaScript เพื่อป้องกันการดักจับข้อมูลระหว่างการสื่อสาร หน้าถัดไปให้กรอก Password และ OTP ในส่วน Password จะนำไป Hash ด้วย SHA 256 ซ้ำ 2 รอบและนำมาต่อด้วยค่า Salt (ซึ่งใช้ค่า OTP) แล้ว Hash ซ้ำอีก 1 รอบ เสร็จกระบวนการนี้ จะได้ค่า OTP พร้อมนำไปใช้งานยืนยันความถูกต้องเพื่อเข้าสู่ระบบเว็บไซต์

3.5.3 เครื่องมือที่ใช้ในการพัฒนา

เครื่องมือที่ถูกนำมาใช้ในการพัฒนาระบบแก้ปัญหาป้องกันการถูกดักจับข้อมูลที่ถูกโจมตีด้วยวิธี SSL Stripping Attack

1) PHP เป็นภาษาประเภท Script Language ที่ทำงานแบบ Server-Side Script กระบวนการทำงานจะทำงานแบบโปรแกรมแปลคำสั่ง interpreter คือแปลภาษาทุกครั้งที่มีคนเรียกสคริปต์ ข้อดีคือ ไม่ต้องนำไปประมวลผลใหม่ (Compiler) เมื่อจะนำโปรแกรมไปใช้งาน ภาษา PHP จัดอยู่ในประเภท การเขียนโปรแกรมบนเว็บ (Web-based Programming) เพราะจะเก็บโค้ดคำสั่งหรือสคริปต์ทั้งหมดที่เขียนขึ้นมาไว้บนเครื่องเซิร์ฟเวอร์ที่เดียว (Web Server) และให้ผู้ใช้งาน (Client) เรียกใช้งานโปรแกรมผ่านเว็บเบราว์เซอร์ต่าง ๆ เช่น Internet Explorer, Mozilla Firefox, Google Chrome, Opera, และ Safari เป็นต้น เพื่อนำข้อมูลมาแสดงผลที่หน้าจอของผู้ใช้แต่ละคนนั่นเอง

2) JQuery คือ JavaScript Library ยอดนิยมที่โปรแกรมเมอร์นำมาใช้พัฒนาเว็บไซต์ สามารถรองรับการทำงานทุกเบราว์เซอร์ โดย Library นี้มีวัตถุประสงค์ที่จะเอามาแก้ปัญหาการใช้งาน JavaScript ที่มีความยุ่งยากในการใช้งานให้สามารถใช้งานได้ง่ายขึ้น เช่น การรวบคำสั่งหลาย ๆ บรรทัดของ JavaScript ที่ซับซ้อนมาเป็นการใช้งานผ่าน JQuery เพียงแค่ 1 บรรทัด หรือ การเรียกใช้งานคำสั่งประเภท AJAX, DOM ให้ใช้งานได้ง่ายขึ้น เป็นต้น บริษัทใหญ่ ๆ หลายบริษัททั่วโลกนำ JQuery ไปใช้งานในเว็บของเขา เช่น Google, Microsoft, IBM ทำให้ JQuery ถูกใช้งานได้อย่างกว้างขวาง

3) CryptoJS เป็นไลบรารีการเข้ารหัสของ JavaScript ที่มีไว้เพื่อเรียกใช้อัลกอริทึมต่าง ๆ ประกอบด้วยไซเฟอร์ต่อไปนี้: AES-128, AES-192, AES-256, DES, Triple DES, Rabbit, RC4, RC4Drop และแฮช: MD5, RIPEMD-160, SHA-1, SHA-256, SHA-512, SHA -3 (ทั้ง 224, 256, 384 และ 512 บิต)

4) Bootstrap คือ Frontend Framework ที่รวม HTML, CSS และ JS เข้าด้วยกันสำหรับพัฒนา Web ที่รองรับทุก Smart Devices ที่เรียกว่า Responsive Web

3.5.4 เครื่องมือที่ใช้ในการทดลอง

การทดลองในงานวิจัยนี้มีการเลือกใช้เครื่องมือต่าง ๆ ซึ่งประกอบไปด้วยโปรแกรมที่ใช้เพื่อวัตถุประสงค์ในการแทรกกลางการสื่อสาร โปรแกรมที่ใช้ในการดักจับข้อมูล โปรแกรมที่ใช้ในการโจมตี SSL ด้วยวิธี SSL Stripping Attack และโปรแกรมเว็บเบราว์เซอร์ เครื่องมือที่ใช้ในการทดสอบได้แก่

1) เครื่องมือที่ใช้ในการโจมตี

เครื่องมือที่ใช้ในการโจมตีเหล่านี้จะถูกนำมาใช้งานร่วมกันเพื่อทำการแทรกกลางการสื่อสารระบบเว็บไซต์ที่ทำงานบน HTTPS จากนั้นก็จะทำการโจมตีด้วยวิธี SSL Stripping Attack แล้วดักจับข้อมูลที่สำคัญของผู้ใช้ออกมา เครื่องเหยื่อใช้ CPU Intel i5 RAM 8GB โดยมี MS Windows 10 เป็นระบบปฏิบัติการ เครื่องของผู้โจมตีใช้ CPU Intel i5 RAM 8GB โดยใช้ Kali Linux 2020.1 เป็นระบบปฏิบัติการประกอบไปด้วยการใช้งานคำสั่ง SSL Strip, Ettercap, Bettercap และ Wireshark ซึ่งถูกติดตั้งอยู่บนระบบปฏิบัติการ Kali Linux

2) เว็บเบราว์เซอร์

ในการทดสอบโจมตีเว็บไซต์ที่ทำงานบน HTTPS นั้น เพื่อให้เห็นถึงความแตกต่างในการแสดงผลบนแต่ละโปรแกรมเว็บเบราว์เซอร์ รวมถึงประสิทธิภาพในการป้องกันการโจมตี SSL/TLS ในงานวิจัยนี้จึงได้เลือกใช้เว็บเบราว์เซอร์จำนวน 5 โปรแกรม โดยการเลือกโปรแกรมที่นำมาทำการทดสอบนี้ ใช้การอ้างอิงข้อมูลจากส่วนแบ่งทางการตลาดของเว็บเบราว์เซอร์ซึ่งเป็นที่นิยมจำนวน 5 อันดับ มีรายละเอียด ดังภาพที่ 3.11 และตารางที่ 3.3 โดยประกอบไปด้วย

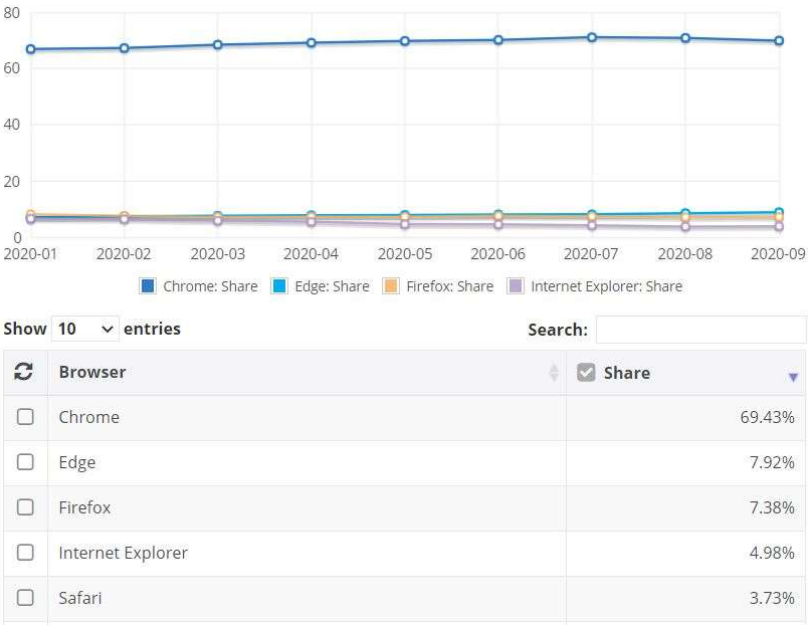
(1) Google Chrome [46] ในงานวิจัยนี้เลือกใช้ Google Chrome เวอร์ชัน 79 (เวอร์ชันล่าสุดขณะทดลอง) ซึ่งมีการใช้งานอย่างแพร่หลายเป็นอันดับหนึ่ง สามารถติดตั้งได้ทั้งบนระบบปฏิบัติการ Windows, Mac OSX, และ Linux

(2) Microsoft Edge [47] เป็นเว็บเบราว์เซอร์ที่รองรับการทำงานบนระบบปฏิบัติการ Windows, Mac OSX, และ Linux โดยในงานวิจัยนี้เลือกใช้ Microsoft Edge เวอร์ชัน 85 (เวอร์ชันล่าสุดขณะทดลอง) ในการทดสอบ

(3) Mozilla Firefox [48] ในงานวิจัยนี้ใช้ Mozilla Firefox เวอร์ชัน 72 (เวอร์ชันล่าสุดขณะทดลอง) ซึ่งการใช้งานสามารถนำมาติดตั้งได้ทั้งบนระบบปฏิบัติการ Windows, Mac OSX, และ Linux

(4) Internet Explorer [49] รองรับการทำงานบนระบบปฏิบัติการ Windows ซึ่งในงานวิจัยนี้ได้เลือกใช้ Internet Explorer เวอร์ชัน 11 (เวอร์ชันล่าสุดขณะทดลอง) มาใช้ในการทดสอบ

(5) Safari รองรับการทำงานบนระบบปฏิบัติการ Windows, Mac OSX และ IOS โดยในงานวิจัยนี้เลือกใช้ Apple Safari [50] เวอร์ชัน 13 (เวอร์ชันล่าสุดขณะทดลอง) มาทำการทดสอบ



ภาพที่ 3.11 กราฟแสดงส่วนแบ่งทางการตลาดของเว็บเบราว์เซอร์ สำรวจเมื่อ ค.ศ. 2020

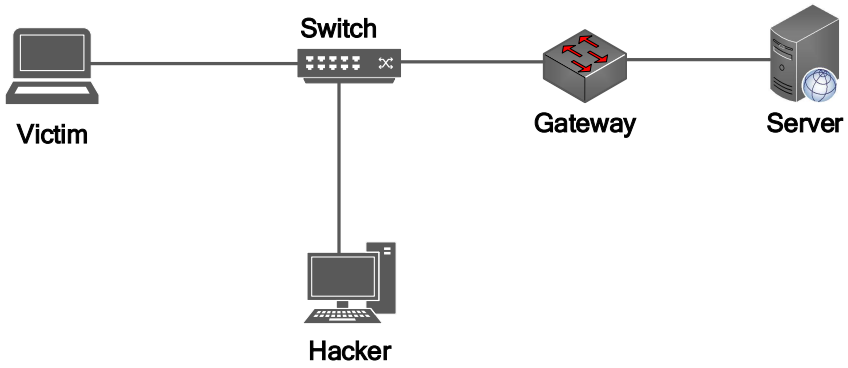
ที่มา: [51]

ตารางที่ 3.3 แสดงส่วนแบ่งทางการตลาดของเว็บเบราว์เซอร์ใน ปี ค.ศ. 2020

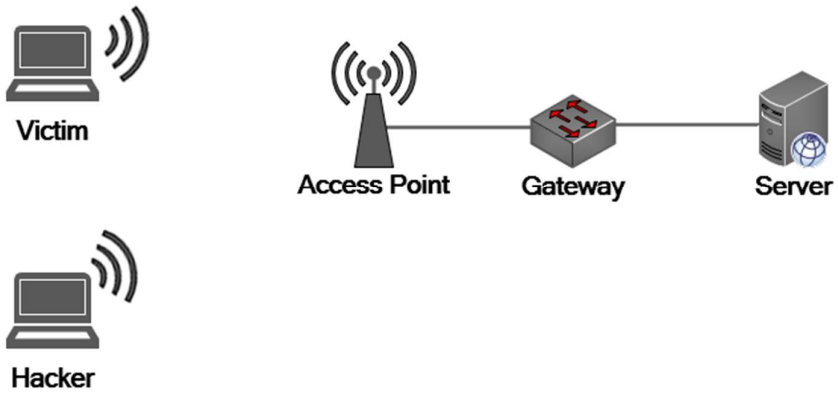
Month	Chrome	Edge	Firefox	Internet Explorer	Safari
September 2020	69.94%	8.84%	7.19%	3.88%	3.57%
August 2020	70.89%	8.52%	7.11%	3.79%	3.53%
July 2020	71.11%	8.09%	7.36%	4.23%	3.36%
June 2020	70.19%	8.07%	7.58%	4.53%	3.56%
May 2020	69.81%	7.86%	7.23%	4.61%	3.90%
April 2020	69.18%	7.76%	7.25%	5.45%	3.94%

3.5.5 สภาพแวดล้อมที่ใช้ในการทดลอง

สภาพแวดล้อมที่ถูกกำหนดเป็น Test-bed เพื่อใช้ในการทดสอบโจมตี แบ่งออกเป็น 2 รูปแบบ ประกอบด้วย Wired Network ใช้สำหรับทดสอบการโจมตีบนแพลตฟอร์มประเภท PC Desktop ดังภาพที่ 3.12 และ Wireless Network ใช้สำหรับทดสอบการโจมตีแบบเชื่อมต่อไร้สาย ดังภาพที่ 3.13



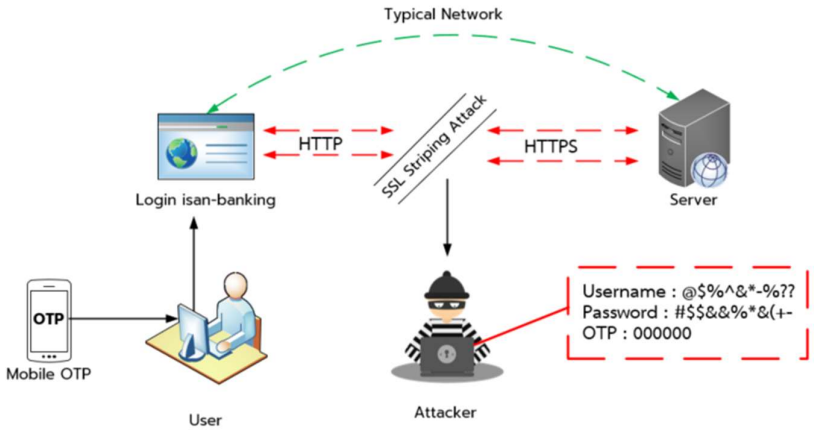
ภาพที่ 3.12 ระบบ Wired Network ที่ใช้ทดสอบการโจมตี



ภาพที่ 3.13 ระบบ Wireless Network ที่ใช้ทดสอบการโจมตี

3.5.6 วิธีการทดลองความมั่นคงของต้นซอฟต์แวร์ ISAN Banking

ในการทดสอบความมั่นคงของระบบ isan-Banking ทำการทดลองบนเครือข่าย (Test-bed) ซึ่งใกล้เคียงกับระบบ i-Banking ของธนาคารโดยทั่วไป ดังภาพที่ 3.14



ภาพที่ 3.14 จำลองเครือข่ายที่ใช้ทดสอบ isan-banking

จากรูป ผู้ใช้งาน (User) เข้าใช้งานหน้าเข้าสู่ระบบของ isan-banking ผ่าน Web Browser โดยทางผู้ใช้งานจะกรอกข้อมูลเพื่อพิสูจน์ความเป็นตัวจริง ได้แก่ Username, Password และ OTP เพื่อส่งไปยังเครื่องเซิร์ฟเวอร์ (Server) ในระหว่างที่มีการสื่อการข้อมูลผู้โจมตี (Attacker) จะใช้เทคนิค SSL Stripping Attack และดักจับ (Sniffing) ข้อมูลระหว่างเครื่องผู้ใช้งานและเครื่องเซิร์ฟเวอร์ ด้วยการใช้เทคนิคการโจมตีแบบแทรกกลางการสื่อสาร (MITM Attack)

3.6 ข้อจรรยาบรรณในการวิจัย

การทดลองโจมตีเว็บไซต์ด้วยเทคนิค SSL Stripping Attack และเทคนิคอื่น ๆ ในงานวิจัยนี้นั้น ไม่ได้มีวัตถุประสงค์ในการเจาะเข้าไปในระบบผู้ให้บริการของเว็บไซต์ที่ใช้ในการทดสอบหรือก่อให้เกิดผลกระทบต่อการทำงานของระบบผู้ให้บริการแต่อย่างใด หากแต่เป็นการทดสอบโจมตี เพื่อทดสอบการดักจับข้อมูลในระหว่างการสื่อสาร บนเครือข่ายสำหรับการทดลอง (Test-bed) ที่จัดตั้งขึ้นมาเฉพาะ เพื่อการทดลองเท่านั้น โดยการทดลอง ไม่ได้ใช้ชื่อผู้ใช้หรือรหัสผ่านจริง แต่เป็นค่าสมมติที่ทดสอบการดักจับเท่านั้น โดยการทดลองดังกล่าวไม่เป็นการเข้าถึงหรือพยายามเข้าถึงโดยมิชอบซึ่งระบบคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะ

บทที่ 4
ผลการวิจัย

ในบทนี้จะกล่าวถึงผลการวิเคราะห์ปัญหาอาชญากรรม กรณีการกระทำความผิดอาญาในรูปแบบต่าง ๆ ต่อระบบธนาคารอิเล็กทรอนิกส์ ผลการวิเคราะห์กฎหมาย ระเบียบ ที่เกี่ยวข้องกับการบริการธนาคารอิเล็กทรอนิกส์ และคดีเทคโนโลยีสารสนเทศ ในประเทศไทยที่มีอยู่ในปัจจุบัน และผลการวิเคราะห์เทคนิควิธีทางด้านความมั่นคงเทคโนโลยีสารสนเทศในการทดลอง SSL Stripping Attack จากกลุ่มเว็บไซต์ตัวอย่างที่นำมาทดสอบ และผลการวิเคราะห์ปัญหากลไก HSTS อย่างละเอียดเพื่อให้เข้าใจสาเหตุของการกลับมาโจมตีได้ใหม่ของการเปลือยเอสเอสแอลต่อความมั่นคงของเว็บไซต์ และส่วนสุดท้ายเพื่อออกแบบและพัฒนาต้นแบบในการป้องกันปัญหาอาชญากรรมต่อระบบธนาคารอิเล็กทรอนิกส์ โดยมีรายละเอียดดังนี้

4.1 วิเคราะห์ลักษณะการกระทำความผิด

4.1.1 แนวคิดทางอาชญากรรมไซเบอร์กับเงินในบัญชีที่หายไป

“อาชญากรรมไซเบอร์” ยังไม่มีนิยามที่เป็นที่ยอมรับสากล หากแต่อาจแยกลักษณะร่วมกันได้ เช่น เหตุเกิดในพื้นที่ไซเบอร์หรือเครือข่ายอินเทอร์เน็ต ลักษณะการกระทำ ผลของการกระทำ ผู้กระทำ เป้าหมาย วัตถุประสงค์ อุปกรณ์เครื่องมือหรือวิธีการ เป็นต้น และอาจจะกล่าวได้ว่าอาชญากรรมไซเบอร์เป็นส่วนหนึ่งของอาชญากรรมคอมพิวเตอร์ โดยมีองค์ประกอบสำคัญคือเครือข่ายอินเทอร์เน็ตนั่นเอง

จากเหตุการณ์ที่มีผู้ได้รับความเสียหายจำนวนมากเนื่องจากเงินในบัญชี หรือบัตรเครดิต/เดบิตหายไป ได้สร้างความตื่นตระหนกให้กับประชาชนอย่างยิ่ง บางท่านอาจต้องเปิดดูเงินในบัญชีออนไลน์ซ้ำแล้วซ้ำเล่าเพื่อตรวจสอบให้แน่ใจว่าเงินในบัญชีไม่หายไปใช่หรือไม่

ข้อสันนิษฐานหนึ่งที่เป็นสาเหตุดังกล่าวคือ “เกิดจากมิจฉาชีพสุ่มยิงบอท” ซึ่งกรณีดังกล่าวอาจจัดได้ว่าเป็นอาชญากรรมไซเบอร์ ในกลุ่มความผิดต่อความมั่นคงปลอดภัยของระบบหรือข้อมูลคอมพิวเตอร์

ตามอนุสัญญาอาชญากรรมไซเบอร์และกฎหมายของประเทศไทยยังไม่ได้มีการกำหนดความผิดสำหรับ Botnet ไว้โดยเฉพาะ แต่ฐานความผิดที่มีอยู่อาจนำมาปรับใช้ได้ตามลักษณะพฤติกรรมและข้อเท็จจริงเป็นกรณี ๆ ไป และอาจเกี่ยวข้องกับความผิดหลายฐานได้ เช่น

ตาม พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 มาตรา 14 (2) ผู้ใดนำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายต่อการรักษาความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคง

ในทางเศรษฐกิจของประเทศ หรือโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะของประเทศ หรือก่อให้เกิดความตื่นตระหนกแก่ประชาชน ต้องระวางโทษจำคุกไม่เกิน 5 ปี หรือปรับไม่เกิน 100,000 บาท หรือทั้งจำทั้งปรับ

เรื่องนี้ไม่ใช่เพียงเรื่องอาชญากรรมทางด้านความมั่งคงปลอดภัยทางคอมพิวเตอร์โดยตรงเท่านั้น แต่เป็นเรื่องของอาชญากรรมที่มีเป้าหมายและก่อให้เกิดผลกระทบในด้านอื่น ๆ ด้วย เช่น ความปลอดภัยสาธารณะ ความมั่นคงในทางเศรษฐกิจของประเทศ และก่อให้เกิดความตื่นตระหนกแก่ประชาชนเป็นอย่างมาก โดยเฉพาะในเรื่องสิทธิในทรัพย์สินของประชาชน ความน่าเชื่อถือของระบบการเงินการธนาคาร อย่างไรก็ตาม กรณีนี้จะเป็นความผิดหรือไม่จะต้องพิจารณาองค์ประกอบความผิดของกฎหมายที่มีในปัจจุบันเป็นหลัก

กิตติยา พรหมจันทร์ [61] ได้กล่าวถึง ตามแนวคิดทางอาชญาวิทยาที่พยายามอธิบายถึงสาเหตุแห่งการเกิดอาชญากรรม เช่น แนวคิดของ Jonathan Clough ได้อธิบายถึงการพัฒนาของเทคโนโลยีดิจิทัลว่ามีส่วนในการส่งเสริมสนับสนุนให้เกิดอาชญากรรมคอมพิวเตอร์หรืออาชญากรรมไซเบอร์ได้ เนื่องจาก

- ความรุนแรงของผลกระทบ (Scale) ด้วยการที่ผู้ใช้งานติดต่อกับบุคลลอื่นได้เป็นวงกว้างได้ง่ายด้วยต้นทุนต่ำแต่ส่งกระทบในวงกว้างที่ในทางกายภาพไม่สามารถทำได้ เช่น กรณี Botnet ที่อาจส่งผลกระทบต่อผู้ใช้หลายสิบล้านคนต่อวันได้

- การเข้าถึงได้ (Accessibility) ของอุปกรณ์คอมพิวเตอร์แบบพกพาชนิดต่าง ๆ เช่น สมาร์ทโฟน สามารถทำได้เข้าถึงได้โดยง่าย ส่งผลให้เกิดตลาดออนไลน์ที่เป็นแหล่งรวมอาชญากรรมและเหยื่อได้ อย่างกรณีโอน/หักเงินผ่านระบบธนาคารออนไลน์ เราสามารถทำได้ง่ายและรวดเร็วอย่างยิ่ง

- ความนิรนามหรือไร้ตัวตน (Anonymity) ที่ทำให้สามารถปกปิดตัวตนด้วยเทคนิคต่าง ๆ รวมทั้งอาจใช้ข้อมูลระบุตัวตนของผู้อื่นเพื่อปกปิดการกระทำของตนได้ เช่น การใช้สื่อสังคมออนไลน์ปลอมแล้วนำรูปของผู้อื่นมาใส่เพื่อหลอกขายของออนไลน์ เป็นต้น

- การพกพาและการโอนข้อมูล (Portability and Transferability) เทคโนโลยีดิจิทัลทำให้สามารถเก็บข้อมูลและโอนข้อมูลจำนวนมากได้โดยต้นทุนต่ำ รวมทั้งเชื่อมโยงกันโดยไม่จำกัดเขตแดน ในขณะที่กฎหมายของแต่ละประเทศมีข้อจำกัดในแง่ของเขตแดนในการบังคับใช้

- ความท้าทายและอุปสรรคของผู้บังคับใช้กฎหมาย (Absence of capable guardians) ซึ่งต้องใช้เทคนิคเฉพาะในการสืบสวนสอบสวน ทั้งในแง่การเก็บข้อมูล การนำข้อมูลมาใช้เป็นพยานหลักฐานในการพิจารณาคดี [60]

นอกจากนี้ ยังมีนักอาชญาวิทยาชาวอินเดีย Karuppannan Jaishankar ได้ตั้งทฤษฎีใหม่ที่เรียกว่า ทฤษฎีการเปลี่ยนพื้นที่ (Space Transition Theory of Cyber Crimes) โดยมีสมมติฐานที่

อาจสรุปได้ว่า พฤติกรรมของมนุษย์ในโลกกายภาพกับในโลกไซเบอร์มีความแตกต่างกัน และโดยธรรมชาติมนุษย์มักมีความเปลี่ยนแปลงเมื่อเคลื่อนย้ายหรือเปลี่ยนแปลงพื้นที่

พฤติกรรมที่แสดงออกมาอาจจะสอดคล้องหรือไม่สอดคล้องกันในสองพื้นที่นั้น [62] เราอาจจะสังเกตง่าย ๆ เช่น เพื่อนในโลกออนไลน์อาจไม่เคยรู้จักหรือเคยเจอกันในชีวิตจริงก็ได้ และเมื่ออยู่ในพื้นที่ออนไลน์ พฤติกรรมที่แสดงออกอาจแตกต่างกับตัวตนในความเป็นจริงก็ได้ ดังนั้น แนวโน้มในการจูงใจให้เกิดอาชญากรรมไซเบอร์จึงอาจจะเกิดจากปัจจัยทางเทคโนโลยีดิจิทัลที่เอื้ออำนวยรวมทั้งโดยธรรมชาติมนุษย์เองที่มีต่อเทคโนโลยีดิจิทัลด้วย จึงต้องเรียนรู้เพิ่มเติมหรืออย่างน้อยต้องระมัดระวังมากยิ่งขึ้น เพราะถึงแม้เทคโนโลยีจะช่วยให้เราสะดวกสบายยิ่งขึ้น แต่ก็อาจจะมีผู้ที่ใช้ช่องว่างนี้เพื่อแสวงหาผลประโยชน์ที่มิชอบได้ ส่วนทางด้านอาชญาวิทยาและกฎหมายอาญา ก็อาจจะต้องปรับเปลี่ยนแนวทางในการพิจารณาจากฐานความผิดที่เคยมีมาแต่เดิม และกำหนดฐานความผิดใหม่ที่สอดคล้องกับเทคโนโลยีมากขึ้น เพราะบางฐานความผิดที่อาจไม่มีทางเกิดขึ้นได้ในทางโลกกายภาพ แต่ในทางโลกไซเบอร์อาจเกิดขึ้นได้โดยที่เราคาดคิดไม่ถึง และต้องเร่งพัฒนาผู้เชี่ยวชาญทางด้านนี้ให้มากยิ่งขึ้น

ทั้งนี้ เพื่อเป็นประโยชน์ในการป้องกันและปราบปรามอาชญากรรมใหม่ ทางคอมพิวเตอร์และไซเบอร์ เรียนรู้ในการบริหารจัดการระบบเทคโนโลยีสารสนเทศของตนเอง และเพื่อให้สามารถนำไปใช้ในการพิจารณาความรับผิดทางกฎหมายได้.

ปัจจุบันทั่วโลก ได้จำแนกประเภทอาชญากรรมทางคอมพิวเตอร์ได้ 9 ประเภท (ตามข้อมูลคณะอนุกรรมการเฉพาะกิจร่างกฎหมายอาชญากรรมทางคอมพิวเตอร์)

1. การขโมยข้อมูลทางอินเทอร์เน็ต รวมถึงการขโมยประโยชน์ในการลักลอบใช้บริการ
2. การปกปิดความผิดของตัวเอง โดยใช้ระบบการสื่อสาร
3. การละเมิดลิขสิทธิ์ ปลอมแปลงรูปแบบเลียนแบบระบบซอฟแวร์โดยมิชอบ
4. การเผยแพร่ภาพ เสียง ลามก อนาจารและข้อมูลไม่เหมาะสม
5. การฟอกเงิน
6. การก่อกวนระบบคอมพิวเตอร์ เช่น ทำลายระบบสาธารณูปโภค
7. การหลอกลวงให้ร่วมค้าขาย หรือลงทุนปลอม (การทำธุรกิจไม่ชอบด้วยกฎหมาย)
8. การลักลอบใช้ข้อมูลเพื่อแสวงหาผลประโยชน์ในทางมิชอบ
9. การใช้คอมพิวเตอร์ในการโอนบัญชีผู้อื่นเป็นของตัวเอง

4.1.2 พฤติการณ์หลอกลวงในรอบปี พ.ศ.2563 ถึง 2564 และวิเคราะห์แนวทางการป้องกัน

กระทำความผิดที่เกี่ยวข้องกับอาชญากรรมทางคอมพิวเตอร์ ในช่วงปี พ.ศ.2561 ที่ผ่านมา กรมสอบสวนคดีพิเศษ ขอแจ้งเตือนถึงรูปแบบการกระทำความผิด และวิธีการป้องกันเพื่อให้ประชาชนรู้เท่าทันอาชญากรรมรูปแบบต่าง ๆ ดังนี้

1) การหลอกลวง หรือฉ้อโกงในการพาณิชย์อิเล็กทรอนิกส์ (E-Commerce) เช่น การซื้อขายสินค้า/บริการ การชำระเงิน การโฆษณาโดยผ่านสื่ออิเล็กทรอนิกส์ประเภทต่าง ๆ ที่ไม่มีอยู่จริง (Fraudulent)

ประชาชนควรใช้ความระมัดระวัง ตรวจสอบการมีอยู่จริงของผู้ขายสินค้าหรือบริการ และหากเกิดความสงสัยหรือไม่แน่ใจประชาชนต้องทำการตรวจสอบกลับไปยังหน่วยงานของรัฐที่มีหน้าที่โดยตรงในการกำกับดูแลการจำหน่ายสินค้าหรือให้บริการประเภท นั้น ๆ ก่อนตัดสินใจ เช่น สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ สำนักงานคณะกรรมการอาหารและยา ธนาคารแห่งประเทศไทย สำนักงานคณะกรรมการคุ้มครองผู้บริโภค เป็นต้น

2) การหลอกลวงให้เข้าเว็บไซต์ปลอมที่ทำเลียนแบบเว็บไซต์จริง ซึ่งเป็นวิธีการหลอกลวงที่แพร่หลายมากในด้านการเงิน โดยจะหลอกให้ผู้เสียหายกรอกข้อมูลสำคัญส่วนบุคคล จากนั้นคนร้ายจะนำข้อมูลดังกล่าวไปทำธุรกรรมทางการเงินแทนผู้เสียหาย เป็นการหลอกลวงเพื่อให้ได้ข้อมูลส่วนบุคคล โดยเฉพาะข้อมูลส่วนบุคคลที่เกี่ยวกับการทำธุรกรรมทางธนาคาร (Phishing) ประชาชนต้องใช้ความระมัดระวัง โดยต้องไม่เผลอเลอหรือรีบเร่งดำเนินการให้ หรือคีย์ข้อมูลสำคัญโดยเฉพาะข้อมูลเกี่ยวกับการดำเนินการธุรกรรมที่เกี่ยวข้องทางด้านการเงิน การธนาคารใด ๆ ผ่านช่องทางใด ๆ ที่เกิดความไม่มั่นใจ และทำการตรวจสอบความถูกต้องของระบบการทำธุรกรรมเกี่ยวกับการเงิน การธนาคารทุกครั้ง อย่าหลงเชื่อการขอข้อมูลธุรกรรม ไม่ว่าขอมาในช่องทางใด ๆ

3) การหลอกลวงว่าเป็นบุคคลอื่นโดยการปลอม (Fake Mail) และการเข้าถึงข้อมูลอีเมลโดยไม่ชอบให้ได้ไปซึ่งทรัพย์สิน กรณีนี้จะมีการจัดทำอีเมลปลอม ที่มีชื่อ (Account) ที่เหมือนอีเมลจริง หรือการลักลอบเข้าถึงหรือทำการยึดอีเมลของบุคคลอื่นโดยมิชอบและทำการหลอกลวงบุคคลที่ติดต่อทางอีเมล ว่ามีความจำเป็นต้องการใช้เงิน เกิดเหตุการณ์เดือดร้อน และขอยืมเงินบุคคลที่อยู่ในอีเมลทำให้ผู้ได้รับการร้องขอช่วยเหลือทางการเงินเกิดความเสียหายจำนวนมาก ประชาชนควรดำเนินการตรวจสอบกลับไปยังตัวบุคคลเจ้าของอีเมล ที่ได้รับการติดต่อมาก่อนทุกครั้ง

4) การกระทำความผิดโดยการเผยแพร่ หรือส่งต่อภาพลามก อนาจาร หรือเผยแพร่หรือส่งต่อข้อความอันเป็นเท็จที่จะทำให้บุคคลอื่นถูกดูหมิ่น เกลียดชัง อันเป็นความผิดตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ และกฎหมายอาญา ประชาชนควรใช้วิจารณญาณ และความรอบคอบ ก่อนทำการเผยแพร่หรือส่งต่อ โดยเฉพาะการใช้ช่องทางผ่าน Social Network ต่าง ๆ

5) การหลอกลวงผู้หญิงหรือเพศอื่นด้วยการพูดคุยผ่านโปรแกรมการแชท การส่งข้อความเป็นการจีบ ทำให้เหยื่อเชื่อว่าตกหลุมรัก ยอมเชื่อใจไว้ใจตายใจ จนในที่สุดก็จะโดนขอยืมเงิน หลอกให้ส่งยาเสพติด หรือทำสิ่งผิดกฎหมาย (Romance Scam) ประชาชนควรใช้วิจารณญาณ และความรอบคอบ

6) การรับจ้างเปิดบัญชีเงินฝาก ประชาชนควรทราบว่าการรับจ้างเปิดบัญชีเงินฝาก เข้าข่ายการกระทำความผิดในฐานะตัวการ ผู้ใช้ หรือผู้สนับสนุนการกระทำความผิดอาญา

4.1.3 กรณีศึกษากับคดีพิเศษที่ได้รับมอบหมาย

อาชญากรรมทางไซเบอร์หรือการกระทำความผิดอาญาที่เกิดขึ้นต่อระบบบริการธนาคารอิเล็กทรอนิกส์ที่มีผลกระทบต่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศด้านการเงิน ซึ่งเป็นส่วนหนึ่งของคดีในอำนาจของกรมสอบสวนคดีพิเศษ ตามบัญชีท้ายประกาศคณะกรรมการคดีพิเศษ (ฉบับที่ 7) พ.ศ. 2562 เรื่อง การกำหนดรายละเอียดของลักษณะของการกระทำความผิด ตามมาตรา 21 วรรคหนึ่ง (1) แห่งพระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 ข้อ 11 ที่กำหนดให้การกระทำที่มีรายละเอียดของลักษณะของการกระทำความผิดที่กล่าวมาแล้วเป็นคดีพิเศษ โดยต้องมีลักษณะอย่างหนึ่งอย่างใดดังต่อไปนี้ (ก) คดีความผิดทางอาญาที่มีความซับซ้อน จำเป็นต้องใช้วิธีการสืบสวนสอบสวนและรวบรวมพยานหลักฐานเป็นพิเศษ (ข) คดีความผิดทางอาญาที่มีหรืออาจมีผลกระทบอย่างรุนแรงต่อความสงบ เรียบร้อยและศีลธรรมอันดีของประชาชน ความมั่นคงของประเทศ ความสัมพันธ์ระหว่างประเทศหรือ ระบบเศรษฐกิจหรือการคลังของประเทศ (ค) คดีความผิดทางอาญาที่มีลักษณะเป็นการกระทำความผิดข้ามชาติที่ สำคัญหรือเป็นการกระทำขององค์กรอาชญากรรม (ง) คดีความผิดทางอาญาที่มีผู้ทรงอิทธิพลที่สำคัญเป็นตัวการ ผู้ใช้หรือ ผู้สนับสนุน

ซึ่งที่ผ่านมาได้มีคดีพิเศษเกี่ยวข้องกับกรณีนี้แล้วหลายคดี [54-56] ภายหลังที่ได้ทำการประชุมกับหัวหน้าโครงการวิจัยฯ และผู้ร่วมวิจัย” ทำให้ทราบถึงข้อเท็จจริงเฉพาะสามารถเปิดเผยได้ และได้ทำการสรุปกรณีศึกษาคดีพิเศษที่เกี่ยวข้องกับกรณีนี้แล้วหลายคดี เช่น คดีพิเศษที่ 74/2559, 142/2561, 117/2561, 118/2561 และ 119/2561 โดยมักพบประเด็นปัญหาข้อกฎหมายในการดำเนินการสืบสวนสอบสวน รวบรวมพยานหลักฐานในคดี ที่พบว่าเป็นการกระทำความผิดที่มีโทษตามกฎหมายอาญาฐานใช้บัตรอิเล็กทรอนิกส์ของผู้อื่นโดยมิชอบ ในประการที่น่าจะก่อให้เกิดความเสียหายแก่ผู้อื่นหรือประชาชนและเป็นการกระทำเกี่ยวกับบัตรอิเล็กทรอนิกส์ที่ผู้ออกได้ออกให้แก่ผู้ใช้สิทธิใช้เพื่อประโยชน์ในการชำระค่าสินค้า ค่าบริการ หรือหนี้อื่นแทนการชำระด้วยเงินสด หรือใช้เบิกถอนเงินสด ตามประมวลกฎหมายอาญา และเป็นการกระทำความผิดฐานเข้าถึงโดยมิชอบซึ่งระบบคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน การกระทำความผิดฐานเข้าถึงโดยมิชอบซึ่งข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน และการกระทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง หรือเพิ่มเติมไม่

ว่าทั้งหมดหรือบางส่วนซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ ตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 และที่แก้ไขเพิ่มเติม โดยลักษณะการกระทำความผิดอาญา หรืออาชญากรรมทางไซเบอร์ต่อบริการธนาคารอิเล็กทรอนิกส์ อีกทั้ง ได้พบปัญหาทางเทคนิค ตั้งแต่การระบุวัน เวลา และสถานที่ในการกระทำความผิด มักเกิดขึ้นโดยผู้เสียหายไม่รู้ว่าโดนกระทำหรือเข้าสู่ระบบธนาคารอิเล็กทรอนิกส์ วัน เวลา ใด เมื่อตรวจพบการกระทำความผิดก็มักจะเกิดขึ้นนอกราชอาณาจักร ซึ่งอำนาจหน้าที่ในการสอบสวนก็เป็นอำนาจโดยตรงของอัยการสูงสุด ก็จะพบปัญหาเรื่องอำนาจการสอบสวนของพนักงานสอบสวนผู้รับผิดชอบ ตามประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 20 รวมถึงปัญหาในการรวบรวมพยานหลักฐานทางเทคโนโลยีสารสนเทศ เนื่องจากเป็นพยานหลักฐานที่แตกต่างจากพยานหลักฐานทั่วไป เช่น พยานเอกสาร พยานวัตถุอื่น ๆ ที่เคยอยู่ในรูปแบบทางกายภาพที่สามารถจับต้องและสัมผัสได้ ก็กลับกลายมาเป็นพยานหลักฐานรูปแบบอิเล็กทรอนิกส์ ซึ่งเกิดขึ้นในระบบคอมพิวเตอร์และระบบเครือข่าย โดยไม่สามารถที่จะจับต้องได้ทางกายภาพ แต่สามารถตรวจพิสูจน์ได้โดยอาศัยเครื่องมือทางเทคโนโลยีสารสนเทศ เข้าช่วยเหลือในการสืบสวนสอบสวนและรวบรวมพยานหลักฐาน จากปัญหาดังกล่าวมาแล้ว ทางการสอบสวนทำให้การดำเนินการทางการสอบสวนคดีพิเศษบางคดีจากการรวบรวมพยานหลักฐานไม่ปรากฏว่าผู้ใดเป็นผู้กระทำความผิดและความผิดนั้นมีอัตราโทษอย่างสูงเกินกว่าสามปี และคณะพนักงานสอบสวนคดีพิเศษ คณะพนักงานสอบสวนคดีพิเศษจึงเคยมีมติเห็นควรงดการสอบสวนและส่งสำนวนการสอบสวนคดีพิเศษไปยังพนักงานอัยการตามประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 140 (1) ซึ่งพนักงานอัยการคดีพิเศษได้มีความเห็นงดการสอบสวนเช่นเดียวกับคณะพนักงานสอบสวน ทำให้เห็นว่าการดำเนินคดีกับผู้กระทำความผิดทางอาญาเกี่ยวข้องกับบริการธนาคารอิเล็กทรอนิกส์เป็นเรื่องยากลำบาก ทั้งทางกฎหมายและเทคนิควิธีทางวิทยาการคอมพิวเตอร์ จึงควรแสวงหาแนวทางป้องกันอาชญากรรมทางไซเบอร์ลักษณะนี้เพื่อไม่ให้ประชาชนได้รับความเดือดร้อนต่อไป

4.1.4 วิเคราะห์จุดอ่อน ปัญหาในการสืบสวนสอบสวน

การรับฟังพยานหลักฐาน

ประมวลกฎหมายวิธีพิจารณาความแพ่ง และประมวลกฎหมายวิธีพิจารณาความอาญาได้แบ่งแยกพยานหลักฐานออกตามวิธีการนำสืบเป็น 4 ประเภท พยานบุคคล พยานเอกสาร พยานวัตถุ และพยานผู้เชี่ยวชาญ มีหลักเกณฑ์ในการรับฟังพยานหลักฐานทั้ง 4 ชนิดแตกต่างกัน พิจารณาได้ดังนี้

พยานบุคคล หมายถึง บุคคลที่มาให้การด้วยปากต่อหน้าศาลตามนิยามนี้ พยานบุคคลก็คือตัวคนที่รู้เห็นเหตุการณ์อันเป็นข้อเท็จจริงในคดี และได้มาเบิกความต่อหน้าศาลในฐานะพยาน ซึ่งเป็นความหมายที่เข้าใจกันโดยทั่วไป แต่มีนักกฎหมายบางท่านนิยามว่าพยานบุคคล หมายถึง ถ้อยคำของบุคคลที่มาให้การต่อหน้าศาล และศาลได้จดบันทึกข้อความไว้ในสำนวนความ 3 นิยามหลังนี้มุ่งหมายถึง “ถ้อยคำที่ศาลจดลงไว้ในสำนวนความ” เป็นหลักมิได้มุ่งถึงตัวคน เมื่อพิจารณาแล้วเห็นว่าความเห็นของนักกฎหมายดังกล่าวถูกต้องทั้งสองฝ่าย กล่าวคือ ถ้ามองตามความเข้าใจของคนธรรมดาพยานบุคคลก็ควรจะหมายถึงตัว“คน” ที่รู้เห็นเหตุการณ์ แต่ถ้ามองตามความเข้าใจของผู้พิพากษาที่กำลังจะตัดสินคดีว่าจะจำแนกพยานที่อยู่ต่อหน้าเป็นพยานบุคคล พยานเอกสาร หรือพยานวัตถุ พยานบุคคลก็ต้องหมายถึงถ้อยคำของบุคคลซึ่งศาลจดลงไว้ในสำนวนความ ไม่ใช่ตัวคน เพราะขณะนั้นตัวคนซึ่งมาเบิกความมิได้อยู่ต่อหน้าศาลแล้ว

พยานเอกสาร หมายถึง ข้อความใด ๆ ในเอกสารที่มีการอ้างอิงเป็นพยาน โดยอาศัยการสื่อความหมายของข้อความนั้นพิสูจน์ความจริง แต่การอ้างเอกสารเป็นพยานมิใช่หมายความว่าจะเป็นพยานเอกสารเสมอไป การอ้างข้อความตอนหนึ่งในเอกสารเพื่อพิสูจน์ว่าข้อเท็จจริงเกิดขึ้นตามข้อความนั้น ดังนี้ เป็นพยานเอกสาร แต่ถ้าอ้างลงลายมือชื่อในเอกสารเพื่อพิสูจน์ว่าเป็นลายมือที่จำเลยทำปลอมขึ้นในความผิดปลอมเอกสารหรืออ้างหนังสือทั้งเล่มเพื่อแสดงว่าเป็นการทำซ้ำงานอันมีลิขสิทธิ์ของโจทก์ ดังนี้เป็นการอ้างในฐานะวัตถุพยาน

พยานวัตถุคือ สิ่งของใด ๆ ที่คู่ความอ้างอิงให้ศาลตรวจดูเพื่อประโยชน์แก่คดีของตน เมื่อพิจารณาเปรียบเทียบกับพยานเอกสารแล้วจะเห็นได้ว่า เอกสารฉบับหนึ่งอาจเป็นพยานเอกสารหรือพยานวัตถุก็ได้สุดแต่วัตถุประสงค์ของการอ้าง ถ้าเป็นการอ้างเพื่อให้ศาลดูข้อความในเอกสารก็เป็นพยานเอกสาร แต่ถ้าเป็นการอ้างเพื่อให้ศาลดูรูปลักษณะของเอกสารก็เป็นพยานวัตถุ

พยานวัตถุมีความสำคัญมากในคดีอาญา เพราะเป็นพยานที่ดีที่สุดในการพิสูจน์ว่าข้อเท็จจริงบางประเด็นได้เกิดขึ้น เช่น ยาเสพติด หรือไม้ของกลางในคดี ปลอกกระสุนปืน บาดแผลที่ถูกทำร้าย สถานที่เกิดเหตุ ส่วนในคดีแพ่งส่วนมากอาจเป็นการไปตรวจดูที่ดินพิพาทเพื่อดูหลักเขตที่ฟ้องร้องกัน

การรับฟังพยานวัตถุไม่มีข้อจำกัดโดยกฎหมาย ดังนั้น พยานวัตถุที่มีการอ้างอิงในบัญชีพยานโดยถูกต้องตามระเบียบแล้วก็สามารถนำเข้าสืบได้เสมอ และไม่มีข้อบังคับว่าข้อเท็จจริงใดจะต้องพิสูจน์

ด้วยพยานวัตถุ หรือห้ามพิสูจน์ด้วยพยานวัตถุ จึงอยู่ในดุลพินิจของคู่ความที่จะพิจารณาว่า ควรนำสืบข้อเท็จจริงด้วยพยานวัตถุหรือไม่

พยานผู้เชี่ยวชาญเป็นพยานบุคคลประเภทหนึ่ง แต่มาเบิกความในลักษณะแสดงความเห็นมิใช่เป็นความจากการประสบพบเห็นข้อเท็จจริงและนำมาเล่าให้ศาลฟัง เช่น แพทย์ซึ่งตรวจบาดแผลของผู้เสียหายมาเป็นพยาน ผู้เชี่ยวชาญเพื่อให้ความเห็นว่าบาดแผลเกิดจากอะไร ดังนั้น พยานผู้เชี่ยวชาญจึงไม่มีปัญหาว่าจะได้พบเห็นข้อเท็จจริงมาด้วยตนเองหรือไม่ดังเช่นพยานบุคคล

การรับฟังพยานหลักฐานในการกระทำผิดที่เกี่ยวข้องกับเทคโนโลยีและสารสนเทศต้องอาศัยพยานหลักฐานแวดล้อมหรือพยานหลักฐานประกอบ ตามประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 277/1 วรรคสอง หมายถึง พยานหลักฐานอื่นที่รับฟังได้และมีแหล่งที่มาเป็นอิสระต่างหากจากพยานหลักฐานที่ต้องการพยานหลักฐานประกอบนั้น ทั้งจะต้องมีคุณค่าเชิงพิสูจน์ที่สามารถสนับสนุนให้พยานหลักฐานอื่นที่ไปประกอบมีความเชื่อถือมากขึ้นด้วย

ดังนั้น การนำความรู้ด้านวิทยาศาสตร์มาประยุกต์ใช้กับกระบวนการยุติธรรมหรือทางกฎหมายเพื่อพิสูจน์ข้อเท็จจริง จากพยานหลักฐานที่ปรากฏอยู่ในคดีความต่าง ๆ ทำให้ผู้พิพากษา สามารถรับฟังและใช้ดุลพินิจตัดสินคดีไม่ว่าจะเป็นคดีแพ่งหรือคดีอาญาได้นั้นต้องอาศัยองค์ประกอบของการเก็บวัตถุพยาน การรวบรวมพยานหลักฐาน การสืบสวน สอบสวน และการตรวจพิสูจน์ทางวิทยาศาสตร์หรือทางการแพทย์ และจะต้องเป็นไปตามหลักสากลที่สามารถตรวจสอบความถูกต้อง ตามหลักวิชาการได้ ซึ่งกระบวนการดังกล่าวทำให้คู่ความหรือผู้ที่เกี่ยวข้องกับกระบวนการดังกล่าว ได้รับความเป็นธรรม องค์ประกอบดังกล่าวต้องมีการฝึกฝนเจ้าหน้าที่ให้เกิดทักษะและความชำนาญ บางครั้งต้องอาศัยเทคโนโลยี หรือวิทยาการสมัยใหม่ ซึ่งมีการพัฒนาและมีการค้นพบ รวมทั้งมีการวิจัยทางด้านวิทยาศาสตร์อย่างต่อเนื่อง การนำเอาวิทยาศาสตร์สาขาต่าง ๆ ไปใช้ในการพิสูจน์พยานหลักฐานในศาลจึงเรียกกันว่า “นิติวิทยาศาสตร์” พยานหลักฐานทางนิติวิทยาศาสตร์ อาจหมายถึงพยานหลักฐานที่สามารถพิสูจน์ข้อเท็จจริงในเชิงหลักวิชาทางวิทยาศาสตร์ และสามารถอธิบายให้เข้าใจได้ โดยอาศัยผู้เชี่ยวชาญด้านสาขาต่าง ๆ ที่มีความรู้ด้านนั้น ๆ ทำให้เข้าใจเหตุผลต่าง ๆ โดยอาศัยพยานที่มีอยู่สามารถใช้ประโยชน์จากการพิสูจน์ข้อเท็จจริงที่พิสูจน์ได้ในการคลี่คลายคดีต่าง ๆ และผู้ทำหน้าที่ตรวจพิสูจน์สามารถให้การในฐานะพยานผู้เชี่ยวชาญต่อศาลได้ บทบาทและสถานะของพยานผู้เชี่ยวชาญจึงมีสถานะเป็นผู้ช่วยเจ้าพนักงานตำรวจจนถึงผู้พิพากษาทั้งในคดีแพ่งและคดีอาญา พยานผู้เชี่ยวชาญจึงแตกต่างจากพยานบุคคลซึ่งพยานผู้เชี่ยวชาญหลังจากที่พิสูจน์ข้อเท็จจริงจากพยานหลักฐานแล้วมาให้การต่อศาลโดยอาศัยความรู้ความเชี่ยวชาญ เพื่อศาลจะได้วินิจฉัยให้เป็นประโยชน์ต่อโจทก์หรือจำเลย แต่พยานบุคคลให้การต่อศาลในฐานะผู้พบเห็นเหตุการณ์มาด้วยตนเองหรือผ่านการบอกเล่ามา พยานผู้เชี่ยวชาญอาจมีการนำสืบโดยอาศัยความเห็นของผู้เชี่ยวชาญคนใดคนหนึ่งก็ได้ แม้จะไม่ได้พบเห็นเหตุการณ์นั้นมา หรือไม่ได้ตรวจพิสูจน์พยานหลักฐาน

ชิ้นนั้นมาก็ได้ แต่สามารถอธิบายตามหลักวิชาการเกี่ยวกับเรื่องนั้น ๆ ก็ได้ หลักการในเรื่องการรับฟังพยานด้านนิติวิทยาศาสตร์นั้น ถูกยอมรับว่าน่าเชื่อถือและรับฟังได้พยานผู้เชี่ยวชาญที่พิสูจน์ข้อเท็จจริง

พยานหลักฐานทางด้านนิติวิทยาศาสตร์ เป็นพยานหลักฐานที่เกิดขึ้นจากการวิเคราะห์และวิจัยโดยอาศัยหลักวิทยาศาสตร์ ซึ่งในทางกฎหมายถือว่าพยานหลักฐานชนิดหนึ่งที่จะนำไปสู่กระบวนการศาลหรือจะนำเข้าสู่ความรู้ของศาล เพื่อให้ศาลวินิจฉัยว่าจำเลยมีความผิดหรือบริสุทธิ์ โดยกำหนดวิธีการนำสืบไว้กล่าวคือ หากคู่ความประสงค์จะอ้างหลักฐานทางนิติวิทยาศาสตร์เข้าสู่ศาล เพื่อนำสืบข้อเท็จจริง ให้นำสืบโดยผู้เชี่ยวชาญซึ่งได้ทำการตรวจวิเคราะห์หรือ ได้วิจัยสังเกตการณ์หรือสิ่งของต่าง ๆ ที่เกี่ยวข้องกับคดีนั้นมาแล้ว ฉะนั้นจึงกล่าวได้ว่าพยานหลักฐานทางนิติวิทยาศาสตร์นี้ก็คือพยานความเห็นของผู้เชี่ยวชาญตามกฎหมาย

การได้มาซึ่งพยานหลักฐานเพื่อเสนอในชั้นศาล มีขั้นตอน ดังนี้

1) กระบวนการค้นหรือการเข้าถึงข้อมูลอิเล็กทรอนิกส์ ต้องเข้าไปตรวจค้นให้เร็วที่สุดตามที่กฎหมายให้อำนาจ เพราะว่าถ้าล่าช้าพยานหลักฐานข้อมูลอิเล็กทรอนิกส์อาจสูญหาย หรือถูกทำลายหรือถูกแก้ไขเปลี่ยนแปลงไป ดังนั้นหลักการของพนักงานสืบสวนสอบสวน คือทำอย่างไรจึงจะ “เข้าถึง” หรือพบข้อมูลนั้นโดยวิธีการค้น และเมื่อพบข้อมูลแล้วต้องกักข้อมูลหรือล็อกข้อมูลให้อยู่ รูปแบบในการตรวจค้นข้อมูลอิเล็กทรอนิกส์ มี 2 รูปแบบ คือ

1.1) การค้นข้อมูลที่อยู่ในความครอบครองของมนุษย์ เช่น เครื่องคอมพิวเตอร์ที่เป็นแบบ Stand Alone หรือ แผ่น Diskette แผ่นซีดี ทรัมไดรฟ์ เป็นต้น ไม่ว่าจะใช้อยู่ในเคหสถาน หรือในสำนักงานที่พนักงานสืบสวนสอบสวนไม่อาจใช้เครื่องมือใด ๆ เชื่อมต่อเข้าไปในเครื่องคอมพิวเตอร์เพื่อเรียกดูข้อมูลที่เก็บอยู่ในฮาร์ดดิสก์ หรือสื่อต่าง ๆ ได้ นอกจากการเข้าไปค้นในที่รโหฐาน และเปิดเครื่องคอมพิวเตอร์ภายในเคหสถานหรือสำนักงานนั้นแล้วตรวจดู

1.2) การค้นข้อมูลที่อยู่ในเครือข่าย เช่น เครือข่ายในระบบ LAN (Local Area Network) หรือ WAN (Wide Area Network) ของสำนักงานหรือองค์กรเอกชนต่าง ๆ อันอาจมีข้อมูลที่เป็นความลับรวมอยู่ รวมถึงข้อมูลที่อยู่ในระบบเครือข่ายอินเทอร์เน็ต ซึ่งข้อมูลในรูปแบบนี้พนักงานสืบสวนสอบสวนอาจไม่มีความจำเป็นที่จะต้องเข้าไปในที่รโหฐาน แต่อาจใช้เครื่องมือหรือเครื่องคอมพิวเตอร์เชื่อมโยงไปยังเครื่องเป้าหมายในการตรวจค้นได้โดยใช้โปรแกรมบางอย่างในการดึงข้อมูลมาตรวจดู

2) กระบวนการยึด หรือการเก็บรักษาพยานหลักฐาน พนักงานสืบสวนสอบสวนจะต้องยึดและเก็บรักษาข้อมูลให้คงสภาพเดิมโดยไม่ถูกเปลี่ยนแปลง แก้ไข เพื่อให้พยานหลักฐานที่ได้มามีความน่าเชื่อถือมากที่สุดว่าไม่มีการแก้ไขเปลี่ยนแปลงใด ๆ ในข้อมูลอิเล็กทรอนิกส์ดังกล่าว

3) กระบวนการตรวจพิสูจน์หลักฐาน พนักงานสืบสวนสอบสวนจะต้องตระหนักถึงความไม่คงสภาพของพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์ ซึ่งสามารถแก้ไข เปลี่ยนแปลง

หรือถูกลบได้ง่าย ดังนั้นการตรวจพิสูจน์มิควรกระทำต่อพยานหลักฐานที่เป็นต้นฉบับ แต่ควรพิสูจน์หลักฐานจากสำเนาที่มาจากต้นฉบับเท่านั้น เพื่อมิให้พยานหลักฐานมีการปนเปื้อน หรือมีการเปลี่ยนแปลง

4) กระบวนการนำเสนอพยานหลักฐาน จะนำเสนอข้อมูลอิเล็กทรอนิกส์ในฐานะพยานวัตถุ หรือพยานเอกสาร และนำเสนออย่างไร เช่น ในรูป Printout เป็นต้น จึงจะทำให้ศาลเชื่อว่าเป็นข้อมูลที่แท้จริงถูกต้อง ไม่ถูกแก้ไขเปลี่ยนแปลง เพื่อให้พยานหลักฐานมีน้ำหนักน่าเชื่อถือ

จากขั้นตอนการให้ได้มาซึ่งพยานหลักฐานทางอิเล็กทรอนิกส์เพื่อใช้ในการเสนอต่อศาล จึงมีปัญหาว่าจะทำอย่างไรในการตรวจค้น ตรวจสอบ หรือตรวจยึดพยานหลักฐานทางดิจิทัล หรือพยานหลักฐานทางอิเล็กทรอนิกส์ จึงจะสามารถเก็บรักษาพยานหลักฐานคอมพิวเตอร์ หรือพยานหลักฐานอิเล็กทรอนิกส์ได้อย่างถูกต้องและถูกวิธีได้มาตรฐาน มีความน่าเชื่อถือ และเป็นที่ยอมรับในระบบของการบันทึก การสร้าง การขนย้ายและการเก็บรักษา เพื่อไม่ให้เกิดการเปลี่ยนแปลงในทุก ๆ ขั้นตอน

Chain of custody

คือกระบวนการในการปฏิบัติงานกับพยานหลักฐาน ในกรณีของการพิสูจน์หลักฐานทางดิจิทัล (Digital Forensics) จะเริ่มตั้งแต่ขั้นตอนการเก็บหลักฐาน การควบคุมการเข้าถึง การส่งต่อรับมอบในกรณีที่มีการปฏิบัติงานร่วมกับหน่วยงานอื่น ไปจนถึงการทำลายพยานหลักฐาน โดยในทุกขั้นตอนต้องมีการบันทึกการดำเนินงานอย่างละเอียด และมีการลงชื่อผู้รับผิดชอบเพื่อเป็นหลักฐาน ทั้งนี้เพื่อให้แน่ใจได้ว่า พยานหลักฐานทางดิจิทัลนั้น ได้รับการปฏิบัติอย่างถูกต้อง และไม่มีการเปลี่ยนแปลงหรือสูญหาย ซึ่งอาจทำให้เกิดความผิดพลาดของผลการตรวจพิสูจน์ได้

Chain of custody หรือ “ห่วงโซ่การคุ้มครองพยานหลักฐาน” คือ เอกสารแสดงลำดับการเกิดเหตุการณ์ หรือเอกสารแสดงทุกขั้นตอน ตั้งแต่การยึดเครื่องคอมพิวเตอร์ การดูแลรักษา การควบคุม การวิเคราะห์ และการจัดเก็บหลักฐานทางอิเล็กทรอนิกส์ เนื่องจากหลักฐานที่พบสามารถนำไปใช้ในยืนยันได้ในชั้นศาล หลักฐานเหล่านี้จึงจะต้องได้รับการจัดการอย่างระมัดระวังและรอบคอบ เพื่อหลีกเลี่ยงข้อกล่าวหาว่าเป็นหลักฐานที่ปลอมหรือทำขึ้นมาในการบันทึกจะไม่บันทึกเพียงแค่ว่าหลักฐานคือหลักฐานอะไรเท่านั้น แต่เรายังต้องบันทึกข้อมูลอื่น ๆ ด้วย เช่น ใครเป็นคนเก็บหลักฐาน เวลาที่เก็บหลักฐาน และรายละเอียดอื่น ๆ ที่เราพบขณะเก็บหลักฐาน กล่าวโดยสรุป คือ เอกสาร Chain of Custody จะประกอบด้วยข้อมูลที่เกี่ยวข้องกับ การรวบรวมหลักฐาน การขนย้ายหลักฐาน การจัดเก็บหลักฐาน และการจัดการกับหลักฐานทางอิเล็กทรอนิกส์

ข้อมูลในเอกสาร chain of custody มีดังนี้

วันและเวลาของการเก็บหลักฐาน

สถานที่ที่เก็บหลักฐาน

รายชื่อผู้เชี่ยวชาญ
รายชื่อเจ้าของเครื่องคอมพิวเตอร์
เหตุผลในการเก็บรวบรวมหลักฐาน
หมายเลขของคดี
ชนิดของอุปกรณ์
หมายเลข Serial Number ของอุปกรณ์ (ถ้ามี)
รุ่นของอุปกรณ์
ความจุของอุปกรณ์ หรือ Hard disk
คำอธิบาย ทางกายภาพของคอมพิวเตอร์ เช่น กำลังเปิดใช้งาน หรือปิดอยู่
ชื่อของไฟล์ทั้งหมดที่ถูกเก็บรวบรวม
ค่าแฮชของไฟล์ต้นฉบับ
ค่าแฮชของไฟล์ปลายทาง
ความคิดเห็น ข้อเสนอแนะ และปัญหาที่พบ
ลายเซ็นของบุคคลที่ดำเนินการกับหลักฐาน
รายละเอียดอื่น ๆ ที่เราพบขณะเก็บหลักฐาน (หากเป็นไปได้ให้บันทึกให้มากที่สุด)

4.2 เปรียบเทียบการคุ้มครอง ควบคุม การประกอบธุรกิจธนาคารที่บังคับใช้ตามกฎหมายไทย

4.2.1 พระราชบัญญัติธุรกิจสถาบันการเงิน พ.ศ. 2551 และที่แก้ไขเพิ่มเติม (ฉบับที่ 3) พ.ศ. 2561

พระราชบัญญัติธุรกิจสถาบันการเงิน พ.ศ. 2551 และที่แก้ไขเพิ่มเติม (ฉบับที่ 3) พ.ศ. 2561 [63] ความมุ่งหมายของกฎหมาย สถาบันการเงินเป็นธุรกิจที่มีบทบาทสำคัญในการขับเคลื่อนเศรษฐกิจของประเทศ โดยทำหน้าที่ในการระดมและจัดสรรเงินทุนแก่ภาคเศรษฐกิจ และมีความเกี่ยวข้องกับประชาชนจำนวนมาก การที่สถาบันการเงินประสบปัญหาย่อมส่งผลกระทบต่อเศรษฐกิจ ตลอดจนความเชื่อมั่นของประชาชนและผู้ฝากเงินที่มีต่อระบบสถาบันการเงินโดยรวมกฎหมายฉบับนี้ จึงกำหนดหลักเกณฑ์ในกำกับดูแลสถาบันการเงิน เพื่อให้สถาบันการเงินมีความมั่นคง และธรรมาภิบาลที่ดี ตลอดจนมีความเป็นธรรมต่อลูกค้าและประชาชน

สรุปสาระสำคัญของกฎหมาย

1) การจัดตั้งและการขอรับใบอนุญาต กำหนดว่าการที่บุคคลใดจะประกอบธุรกิจธนาคารพาณิชย์ ธุรกิจเงินทุน หรือธุรกิจ เครดิตฟองซิเอร์ หรือการที่ธนาคารพาณิชย์ต่างประเทศจะตั้งสาขาเพื่อประกอบธุรกิจธนาคารพาณิชย์ ในประเทศไทย จะต้องได้รับอนุญาตจากรัฐมนตรีว่าการกระทรวงการคลังโดยคำแนะนำของธนาคารแห่งประเทศไทย (มาตรา 9 มาตรา 10)

2) โครงสร้างสถาบันการเงิน (1) กำหนดว่าสถาบันการเงินต้องมีจำนวนหุ้นที่ถือโดยผู้มีสัญชาติไทยไม่ต่ำกว่า ร้อยละ 75 ของจำนวนหุ้นที่มีสิทธิออกเสียงและจำหน่ายได้ทั้งหมด และต้องมีกรรมการเป็นบุคคลผู้มีสัญชาติไทยไม่ต่ำกว่าสามในสี่ของจำนวนกรรมการทั้งหมด เว้นแต่ได้รับอนุญาตหรือได้รับการผ่อนผัน จากธนาคารแห่งประเทศไทยตามเงื่อนไขที่กฎหมายกำหนด (มาตรา 16) (2) กำหนดห้ามมิให้บุคคลใดถือหุ้นของสถาบันการเงินแห่งใดแห่งหนึ่งไม่ว่าโดยทางตรงหรือทางอ้อมเกินร้อยละ 10 ของจำนวนหุ้นที่จำหน่ายได้แล้วทั้งหมด เว้นแต่ได้รับอนุญาต จากธนาคารแห่งประเทศไทยหรือเป็นตามหลักเกณฑ์ที่ธนาคารแห่งประเทศไทยกำหนด (มาตรา 18) (3) กำหนดลักษณะต้องห้ามของกรรมการ ผู้จัดการ หรือผู้มีอำนาจในการจัดการ หรือที่ปรึกษาของสถาบันการเงิน (มาตรา 24) รวมทั้งกำหนดว่าการแต่งตั้งบุคคลดังกล่าว จะต้องได้รับความเห็นชอบจากธนาคารแห่งประเทศไทยก่อน (มาตรา 25)

3) การกำกับสถาบันการเงินกำหนดหลักเกณฑ์ในการกำกับสถาบันการเงิน เช่น การดำรงเงินกองทุนและสินทรัพย์ (มาตรา 29 ถึงมาตรา 32) การลงทุนในหลักทรัพย์ (มาตรา 33 ถึงมาตรา 35) ขอบเขตในการประกอบธุรกิจ (มาตรา 36) การทำนิติกรรมที่เกี่ยวข้องกับการประกอบธุรกิจของสถาบันการเงิน การตรวจสอบและการควบคุมภายใน ตลอดจนการบริหารและการจัดการของสถาบันการเงิน (มาตรา 41) การดำเนินการที่ต้องได้รับความเห็นชอบจากธนาคารแห่งประเทศไทย (มาตรา 43) ข้อห้ามในการให้สินเชื่อ (มาตรา 48 ถึงมาตรา 52) กลุ่มธุรกิจทางการเงิน (มาตรา 53 ถึงมาตรา 59) การจัดชั้นสินทรัพย์และการกันเงินสำรอง (มาตรา 60 ถึงมาตรา 62) การบริหารสินทรัพย์และการดำรงสินทรัพย์สภาพคล่อง (มาตรา 63 ถึงมาตรา 65) การจัดทำบัญชี การรายงาน ผู้สอบบัญชี (มาตรา 66 ถึงมาตรา 71) การควบ การโอน และเลิกกิจการ (มาตรา 72 ถึงมาตรา 79) ข้อห้ามมิให้สถาบันดำเนินการ (มาตรา 80) การจัดเก็บข้อมูล บัญชี เอกสาร หรือหลักฐานอื่นเกี่ยวกับกิจการ สินทรัพย์ และหนี้สิน (มาตรา 82)

4) การตรวจสอบสถาบันการเงินกำหนดให้ธนาคารแห่งประเทศไทยมีอำนาจแต่งตั้งพนักงานธนาคารแห่งประเทศไทยหรือบุคคลภายนอกเป็นผู้ตรวจการสถาบันการเงิน เพื่อทำหน้าที่ตรวจสอบกิจการ สินทรัพย์ และหนี้สินของสถาบันการเงิน บริษัทแม่ บริษัทลูก หรือบริษัทร่วม และบริษัทที่อยู่ในกลุ่มธุรกิจทางการเงิน ตลอดจนลูกหนี้และผู้ที่เกี่ยวข้องกับสถาบันการเงินนั้น (มาตรา 85)

5) การแก้ไขฐานะหรือการดำเนินงานของสถาบันการเงิน (1) กำหนดให้ธนาคารแห่งประเทศไทยมีอำนาจออกหนังสือเตือน คำสั่งห้าม หรือคำสั่งถอดถอนกรรมการ ผู้จัดการ หรือผู้มีอำนาจในการจัดการในกรณีที่สถาบันการเงิน กรรมการผู้จัดการ หรือผู้มีอำนาจในการจัดการฝ่าฝืนหรือไม่ปฏิบัติตามหลักเกณฑ์ที่กำหนดในกฎหมายฉบับนี้ (มาตรา 89) (2) กำหนดให้ธนาคารแห่งประเทศไทยมีอำนาจออกคำสั่งให้สถาบันการเงินแก้ไขฐานะหรือการดำเนินงาน เพิ่มทุน ลดทุน

ระงับการดำเนินการทั้งหมดหรือบางส่วนเป็นการชั่วคราวถอดถอนกรรมการ ผู้จัดการ หรือผู้มีอำนาจในการจัดการ ควบคุมสถาบันการเงิน หรือปิดกิจการสถาบันการเงิน ในกรณีที่สถาบันการเงินมีฐานะหรือการดำเนินงานอยู่ในลักษณะอันอาจเป็นเหตุให้เกิดความเสียหายแก่ประโยชน์ของประชาชน (มาตรา 90) (3) กำหนดมาตรการในการดำเนินการกับสถาบันการเงินที่มีเงินกองทุนต่ำกว่าที่กฎหมายกำหนด (มาตรา 95 ถึงมาตรา 99)

6) การเข้าควบคุมสถาบันการเงินกำหนดขั้นตอนการดำเนินการกรณีที่ธนาคารแห่งประเทศไทยมีคำสั่งควบคุมสถาบันการเงิน เช่น การแจ้งคำสั่งควบคุมแก่สถาบันคุ้มครองเงินฝากและตลาดหลักทรัพย์ (มาตรา 101) การแต่งตั้งและอำนาจหน้าที่ของคณะกรรมการควบคุมสถาบันการเงิน (มาตรา 102 ถึงมาตรา 109)

7) การกำกับสถาบันการเงินเฉพาะกิจ มาตรา 2(1) กำหนดให้รัฐมนตรีซึ่งรักษาการตามกฎหมายจัดตั้งสถาบันการเงินเฉพาะกิจสามารถมอบอำนาจให้ธนาคารแห่งประเทศไทยทำหน้าที่แทนได้ เช่น หน้าที่ในการกำกับดูแล หรือหน้าที่ในการกำหนดแนวนโยบาย เพื่อให้สถาบันการเงินเฉพาะกิจถือปฏิบัติ (มาตรา 120) (2) กำหนดให้ธนาคารแห่งประเทศไทย โดยความเห็นชอบของรัฐมนตรีว่าการกระทรวงการคลัง มีอำนาจออกประกาศกำหนดหลักเกณฑ์ให้สถาบันการเงินเฉพาะกิจปฏิบัติ เช่น หลักเกณฑ์เกี่ยวกับการจัดชั้นสินทรัพย์หรือการกันเงินสำรอง (มาตรา 120 วรรคสองและมาตรา 120/1)

8) บทกำหนดโทษ กำหนดโทษกรณีฝ่าฝืนหรือไม่ปฏิบัติตามหลักเกณฑ์ ที่กฎหมายฉบับนี้กำหนด และกรณีกรรมการ ผู้จัดการ หรือผู้มีอำนาจในการจัดการของสถาบันการเงิน หรือบุคคลใดกระทำความผิดโดยทุจริต (มาตรา 121 ถึงมาตรา 156)

บทบัญญัติที่คุ้มครองประชาชน

1) กำหนดให้สถาบันการเงินต้องประกาศข้อมูลในเรื่องอัตราดอกเบี้ย อัตราส่วนลดและค่าบริการต่าง ๆ ไว้ในที่เปิดเผย ณ สำนักงานของสถาบันการเงิน เพื่อให้ประชาชนและลูกค้าทราบข้อมูลดังกล่าว (มาตรา 38)

2) กำหนดให้ธนาคารแห่งประเทศไทยมีอำนาจออกประกาศกำหนดหลักเกณฑ์ในเรื่องต่าง ๆ เช่น การรับฝากเงิน การทำนิติกรรมหรือสัญญากับประชาชน เพื่อประโยชน์ในการคุ้มครองผู้บริโภค (มาตรา 39)

3) กำหนดให้สถาบันการเงินต้องแจ้งและแสดงวิธีการ ตลอดจนรายละเอียดในการคำนวณอัตราค่าบริการรายปีให้ประชาชนและลูกค้าผู้มาขอสินเชื่อทราบ (มาตรา 40)

4) กำหนดให้ธนาคารแห่งประเทศไทยมีอำนาจออกประกาศกำหนดหลักเกณฑ์เกี่ยวกับการเรียก/จ่าย ดอกเบี้ยหรือส่วนลด การเรียกค่าบริการ เงินมัดจำ หลักประกัน เบี้ยปรับ (มาตรา 46)

5) กำหนดให้ธนาคารแห่งประเทศไทย โดยความเห็นชอบของรัฐมนตรีว่าการกระทรวงการคลัง มีอำนาจออกประกาศกำหนดหลักเกณฑ์เกี่ยวกับการคุ้มครองผู้บริโภคให้สถาบันการเงินเฉพาะกิจปฏิบัติ (มาตรา 120/1 (4))

4.2.2 พระราชบัญญัติธนาคารแห่งประเทศไทย พุทธศักราช 2485 และที่แก้ไขเพิ่มเติม (ฉบับที่ 7) พ.ศ. 2561

<u>หมายเหตุ</u> ที่มา: [63] งานวิจัยที่อ้างถึง ได้สรุปสาระสำคัญของพระราชบัญญัตินี้ ดังต่อไปนี้

ความมุ่งหมายของกฎหมาย กฎหมายฉบับนี้มีขึ้นเพื่อจัดตั้งธนาคารแห่งประเทศไทยให้ทำหน้าที่เป็นธนาคารกลางของประเทศดูแล เสถียรภาพทางการเงิน เสถียรภาพของระบบสถาบันการเงิน และเสถียรภาพระบบการชำระเงินของประเทศ นอกจากนี้ ได้มีการจัดตั้งกองทุนเพื่อการฟื้นฟูและพัฒนาระบบสถาบันการเงินให้มีฐานะเป็นนิติบุคคลแยกต่างหากจากธนาคารแห่งประเทศไทย เพื่อทำหน้าที่ฟื้นฟูและพัฒนาระบบสถาบันการเงินให้มีความมั่นคงและมีเสถียรภาพ

สรุปสาระสำคัญของกฎหมาย

1) กำหนดวัตถุประสงค์ในการดำเนินงานของธนาคารแห่งประเทศไทยซึ่งต้องดำรงไว้ซึ่งเสถียรภาพทางการเงิน เสถียรภาพของระบบสถาบันการเงินและระบบการชำระเงิน (มาตรา 7) และอำนาจในการกระทำกิจการต่าง ๆ ของธนาคารแห่งประเทศไทยเพื่อให้บรรลุวัตถุประสงค์ (มาตรา 8) และกำหนดข้อห้ามมิให้ธนาคารแห่งประเทศไทยกระทำการในเรื่องต่าง ๆ (มาตรา 9)

2) กำหนดกระบวนการได้มา องค์ประกอบ คุณสมบัติและลักษณะต้องห้าม การประชุมและองค์ประชุม วาระในการดำรงตำแหน่ง อำนาจหน้าที่ และการพ้นจากตำแหน่งของคณะกรรมการชุดต่าง ๆ เพื่อทำหน้าที่ของธนาคารแห่งประเทศไทย (หมวด 4) ได้แก่ คณะกรรมการธนาคารแห่งประเทศไทย (มาตรา 24 ถึงมาตรา 28/5) คณะกรรมการนโยบายการเงิน (มาตรา 28/6 ถึงมาตรา 28/8) คณะกรรมการนโยบายสถาบันการเงิน (มาตรา 28/9 ถึงมาตรา 28/10) และคณะกรรมการระบบการชำระเงิน (มาตรา 28/11 ถึงมาตรา 28/12)

3) กำหนดกระบวนการคัดเลือก คุณสมบัติและลักษณะต้องห้าม วาระการดำรงตำแหน่งและการพ้นจากตำแหน่งของผู้ว่าการ รวมทั้งกำหนดให้ผู้ว่าการมีความเป็นอิสระในการบริหารจัดการกิจการของ ธปท. รวมทั้งข้อห้ามมิให้ผู้ว่าการซึ่งพ้นจากตำแหน่งไปดำรงตำแหน่งใดในสถาบันการเงินใดภายในระยะเวลา 2 ปีนับแต่พ้นจากตำแหน่ง (หมวด 5)

4) กำหนดสถานะ วัตถุประสงค์ ที่มาของแหล่งเงิน และอำนาจกระทำกิจการต่าง ๆ ของกองทุนเพื่อการฟื้นฟูและพัฒนาระบบสถาบันการเงิน องค์ประกอบ วาระการดำรงตำแหน่ง การพ้นจากตำแหน่ง การประชุมและองค์ประชุม อำนาจหน้าที่ของคณะกรรมการจัดการกองทุน (หมวด 5 ทวิ)

5) กำหนดหลักเกณฑ์เกี่ยวกับการดำเนินการตามอำนาจหน้าที่ของธนาคารแห่งประเทศไทยด้านต่าง ๆ ได้แก่ การออกธนบัตรของรัฐบาลและบัตรธนาคาร การดำเนินนโยบายการเงิน การบริหารจัดการสินทรัพย์ของธนาคารแห่งประเทศไทย การเป็นนายธนาคารและนายทะเบียนหลักทรัพย์ของรัฐบาล การเป็นนายธนาคารของสถาบันการเงิน การรักษาเสถียรภาพของระบบเศรษฐกิจและระบบการเงิน การจัดตั้งหรือสนับสนุนการจัดตั้งระบบการชำระเงิน (หมวด 6)

6) กำหนดข้อห้ามมิให้ผู้ว่าการ กรรมการ พนักงานและลูกจ้างกระทำการอันใดที่ขัดหรือแย้งระหว่างผลประโยชน์ของตนและผลประโยชน์ของ ธปท. หรือขัดแย้งกับการปฏิบัติหน้าที่ของตนเอง รวมทั้งให้พนักงานหรือลูกจ้างเปิดเผยข้อมูลส่วนได้เสียของตนในการปฏิบัติหน้าที่ และห้ามพนักงานหรือลูกจ้างที่มีส่วนได้เสียพิจารณาหรือเข้าร่วมการประชุมในเรื่องที่ตนมีส่วนได้เสีย และห้ามพนักงานและลูกจ้างดำรงตำแหน่ง รับจ้างหรือ ทำงานในสถาบันการเงิน เว้นแต่เป็นไปตามข้อบังคับของคณะกรรมการธนาคารแห่งประเทศไทย (มาตรา 46 ถึงมาตรา 48)

7) กำหนดให้รัฐมนตรีว่าการกระทรวงการคลังมีอำนาจหน้าที่กำกับดูแลโดยทั่วไปซึ่งกิจการของธนาคารแห่งประเทศไทย และให้ธนาคารแห่งประเทศไทยหารือเป็นครั้งคราวร่วมกับรัฐมนตรีว่าการกระทรวงการคลังเพื่อประโยชน์ในการรักษาเสถียรภาพทางเศรษฐกิจ การเงิน หรือระบบสถาบันการเงิน โดยกรณีมีเหตุอันอาจก่อให้เกิดผลกระทบหรือความเสียหายอย่างรุนแรง ให้ธนาคารแห่งประเทศไทยรายงานข้อเท็จจริงประเมินผลกระทบหรือความเสียหายที่อาจเกิดขึ้น วิเคราะห์ปัญหาและเสนอแนวทางแก้ไขต่อรัฐมนตรี หรือรัฐมนตรีอาจให้ธนาคารแห่งประเทศไทยรายงานข้อเท็จจริง วิเคราะห์ปัญหาและเสนอแนวทางแก้ไข เพื่อป้องกันเหตุการณ์ที่อาจก่อให้เกิดผลกระทบหรือความเสียหายอย่างรุนแรงก็ได้ รวมถึงให้ธนาคารแห่งประเทศไทย รายงานต่อรัฐมนตรีโดยเร็วในกรณีฐานะสุทธิของเงินสำรองระหว่างประเทศของทางการต่ำกว่าระดับที่จำเป็นต่อการรักษาเสถียรภาพทางการเงินและอัตราแลกเปลี่ยนเงินตรา (หมวด 8)

8) กำหนดให้การบัญชีของธนาคารแห่งประเทศจัดทำตามหลักการบัญชีที่รับรองทั่วไป เว้นแต่คณะกรรมการธนาคารแห่งประเทศไทยจะกำหนดเฉพาะเรื่องเป็นอย่างอื่นเพื่อให้สอดคล้องกับการปฏิบัติของธนาคารกลางอื่นได้ (มาตรา 54) และให้มีคณะกรรมการตรวจสอบเพื่อทำหน้าที่กำกับดูแลการตรวจสอบกิจการของธนาคารแห่งประเทศไทย (มาตรา 55)

9) กำหนดโทษสำหรับบุคคล สถาบันการเงิน ที่ฝ่าฝืนหรือไม่ปฏิบัติตามหลักเกณฑ์ที่กฎหมายฉบับนี้กำหนด กระทำความผิด (มาตรา 62 มาตรา 63 มาตรา 65) รวมถึงผู้ว่าการ กรรมการ พนักงานหรือลูกจ้างที่กระทำความผิดต่อตำแหน่งหน้าที่ หรือที่ฝ่าฝืนหรือไม่ปฏิบัติตามหลักเกณฑ์ที่กฎหมายฉบับนี้กำหนด (มาตรา 64 มาตรา 66 ถึง มาตรา 75)

บทบัญญัติที่คุ้มครองประชาชน (ไม่มี)

4.2.3 พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ. 2562

สาระสำคัญของกฎหมายนี้ [64] ที่เกี่ยวข้องกับงานวิจัย สรุปได้ดังนี้

มาตรา 3 “หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ” หมายความว่า หน่วยงานของรัฐหรือหน่วยงานเอกชน ซึ่งมีภารกิจหรือให้บริการโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

มาตรา 9 คณะกรรมการมีหน้าที่และอำนาจ ดังต่อไปนี้

(1) เสนอนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ ส่งเสริมและสนับสนุนการดำเนินการรักษาความมั่นคงปลอดภัยไซเบอร์ ตามมาตรา 42 และมาตรา 43 ต่อคณะรัฐมนตรีเพื่อให้ความเห็นชอบ ซึ่งต้องเป็นไปตามแนวทางที่กำหนดไว้ในมาตรา 42

(2) กำหนดนโยบายการบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

(3) จัดทำแผนปฏิบัติการเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์เสนอต่อคณะรัฐมนตรีสำหรับเป็นแผนแม่บทในการรักษาความมั่นคงปลอดภัยไซเบอร์ในสถานการณ์ปกติและในสถานการณ์ที่อาจจะเกิดหรือเกิดภัยคุกคามทางไซเบอร์ โดยแผนดังกล่าวจะต้องสอดคล้องกับนโยบาย ยุทธศาสตร์และแผนระดับชาติและกรอบนโยบายและแผนแม่บทที่เกี่ยวกับการรักษาความมั่นคง ของสภาความมั่นคงแห่งชาติ

(4) กำหนดมาตรฐานและแนวทางส่งเสริมพัฒนาระบบการให้บริการเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ สร้างมาตรฐานเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์และกำหนดมาตรฐานขั้นต่ำที่เกี่ยวข้องกับคอมพิวเตอร์ ระบบคอมพิวเตอร์ โปรแกรมคอมพิวเตอร์ รวมถึงส่งเสริมการรับรองมาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานเอกชน

(5) กำหนดมาตรการและแนวทางในการยกระดับทักษะความรู้และความเชี่ยวชาญในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของพนักงานเจ้าหน้าที่ เจ้าหน้าที่ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานเอกชนที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์

(6) กำหนดกรอบการประสานความร่วมมือกับหน่วยงานอื่นทั้งในประเทศและต่างประเทศที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์

(7) แต่งตั้งและถอดถอนเลขาธิการ

(8) มอบหมายการควบคุมและกำกับดูแล รวมถึงการออกข้อกำหนด วัตถุประสงค์ หน้าที่และอำนาจ และกรอบการดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ให้หน่วยงานควบคุมหรือกำกับดูแล หน่วยงานของรัฐ หรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

(9) ติดตามและประเมินผลการปฏิบัติตามนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ แผนปฏิบัติการเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์และการรักษาความมั่นคงปลอดภัยไซเบอร์ตามที่บัญญัติไว้ในพระราชบัญญัตินี้

(10) เสนอแนะและให้ความเห็นต่อคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ หรือคณะรัฐมนตรี เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์

(11) เสนอแนะต่อคณะรัฐมนตรีในการจัดให้มีหรือปรับปรุงกฎหมายที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์

(12) จัดทำรายงานสรุปผลการดำเนินงานของการรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีผลกระทบอย่างมีนัยสำคัญหรือแนวทางการพัฒนามาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ให้คณะรัฐมนตรีทราบ

(13) ปฏิบัติการอื่นใดตามที่บัญญัติไว้ในพระราชบัญญัตินี้ หรือคณะรัฐมนตรีมอบหมาย

มาตรา 22 ให้สำนักงานรับผิดชอบงานธุรการ งานวิชาการ งานการประชุม และงานเลขานุการของคณะกรรมการ และคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ (กกม.) และให้มีหน้าที่และอำนาจดังต่อไปนี้ด้วย

(1) เสนอแนะและสนับสนุนในการจัดทำนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ และแผนปฏิบัติการเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์ ตามมาตรา 9 ต่อคณะกรรมการ

...(3) ประสานงานการดำเนินการเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ตามมาตรา 53 และมาตรา 54

...(5) ดำเนินการและประสานงานกับหน่วยงานของรัฐและเอกชนในการตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์ตามที่ได้รับมอบหมายจากคณะกรรมการ

...(6) เฝ้าระวังความเสี่ยงในการเกิดภัยคุกคามทางไซเบอร์ ติดตาม วิเคราะห์และประมวลผลข้อมูลเกี่ยวกับภัยคุกคามทางไซเบอร์ และการแจ้งเตือนเกี่ยวกับภัยคุกคามทางไซเบอร์

... (8) ดำเนินการและให้ความร่วมมือหรือช่วยเหลือในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ โดยเฉพาะภัยคุกคามทางไซเบอร์ที่กระทบหรือเกิดแก่โครงสร้างพื้นฐานสำคัญทางสารสนเทศ

... (12) ทำความตกลงและร่วมมือกับองค์การหรือหน่วยงานทั้งในประเทศและต่างประเทศในกิจการที่เกี่ยวกับการดำเนินการตามหน้าที่และอำนาจของสำนักงาน เมื่อได้รับความเห็นชอบจากคณะกรรมการ

มาตรา 49 ให้คณะกรรมการมีอำนาจประกาศกำหนดลักษณะหน่วยงานที่มีภารกิจหรือให้บริการในด้าน ดังต่อไปนี้ เป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

(1) ด้านความมั่นคงของรัฐ

(2) ด้านบริการภาครัฐที่สำคัญ

(3) ด้านการเงินการธนาคาร

(4) ด้านเทคโนโลยีสารสนเทศและโทรคมนาคม

(5) ด้านการขนส่งและโลจิสติกส์

(6) ด้านพลังงานและสาธารณูปโภค

(7) ด้านสาธารณสุข

(8) ด้านอื่นตามที่คณะกรรมการประกาศกำหนดเพิ่มเติม

หมวด 4 บทกำหนดโทษ

มาตรา 70 ห้ามมิให้พนักงานเจ้าหน้าที่ตามพระราชบัญญัตินี้เปิดเผยหรือส่งมอบข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ ข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ หรือข้อมูลของผู้ใช้บริการที่ได้มาตามพระราชบัญญัตินี้ให้แก่บุคคลใด ผู้ใดฝ่าฝืนต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ...

มาตรา 71 พนักงานเจ้าหน้าที่ตามพระราชบัญญัตินี้ผู้ใดกระทำโดยประมาทเป็นเหตุให้ผู้อื่นล่วงรู้ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ ข้อมูลของผู้ใช้บริการหรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ที่ได้มาตามพระราชบัญญัตินี้ ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา 72 ผู้ใดล่วงรู้ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ ข้อมูลของผู้ใช้บริการหรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ที่พนักงานเจ้าหน้าที่ได้มาตามพระราชบัญญัตินี้ และเปิดเผยข้อมูลนั้นต่อผู้หนึ่งผู้ใดโดยมิชอบ ต้องระวางโทษจำคุกไม่เกินสองปี หรือปรับไม่เกินสี่หมื่นบาทหรือทั้งจำทั้งปรับ

มาตรา 73 หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศใดไม่รายงานเหตุภัยคุกคามทางไซเบอร์ ตามมาตรา 57 โดยไม่มีเหตุอันสมควร ต้องระวางโทษปรับไม่เกินสองแสนบาท

มาตรา 74 ผู้ใดไม่ปฏิบัติตามหนังสือเรียกของพนักงานเจ้าหน้าที่หรือไม่ส่งข้อมูลให้แก่พนักงานเจ้าหน้าที่ ตามมาตรา 62 (1) หรือ (2) โดยไม่มีเหตุอันสมควรแล้วแต่กรณี ต้องระวางโทษปรับไม่เกินหนึ่งแสนบาท

มาตรา 75 ผู้ใดฝ่าฝืนหรือไม่ปฏิบัติตามคำสั่งของคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ ตามมาตรา 65 (1) และ (2) โดยไม่มีเหตุอันสมควร ต้องระวางโทษปรับไม่เกินสามแสนบาท และปรับอีกไม่เกินวันละหนึ่งหมื่นบาท

มาตรา 76 ผู้ใดขัดขวาง หรือไม่ปฏิบัติตามคำสั่งของคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ หรือพนักงานเจ้าหน้าที่ซึ่งปฏิบัติการตามคำสั่งของคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ ตามมาตรา 66 (1) หรือไม่ปฏิบัติตามคำสั่งศาลตามมาตรา 66 (2)

(3) หรือ (4) โดยไม่มีเหตุอันสมควร ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา 77 ในกรณีที่ผู้กระทำความผิดตามพระราชบัญญัตินี้เป็นนิติบุคคล ถ้าการกระทำความผิดของนิติบุคคลนั้นเกิดจากการสั่งการหรือการกระทำของกรรมการหรือผู้จัดการหรือบุคคลใดซึ่งรับผิดชอบในการดำเนินงานของนิติบุคคลนั้น หรือในกรณีที่บุคคลดังกล่าวมีหน้าที่ต้องสั่งการหรือกระทำการและละเว้นไม่สั่งการหรือไม่กระทำการจนเป็นเหตุให้นิติบุคคลนั้นกระทำความผิด ผู้นั้นต้องรับโทษตามที่บัญญัติไว้สำหรับความผิดนั้น ๆ ด้วย

4.3 ข้อเท็จจริงที่ปรากฏขึ้นจริงบริบททางสังคมต่างประเทศ

Tesco Bank fined £16.4m by watchdog over cyber-attack

FCA says bank did not address warnings about 'deficiencies' until after attack started

▲ The FCA said the Tesco Bank fraud netted cyber-attackers £2.26m. Photograph: Andrew Milligan/PA

Tesco Bank has agreed to pay £16.4m as part of a settlement with the Financial Conduct Authority following a cyber-attack in 2016.

งานวิจัยนี้ได้ทำการวิเคราะห์กรณีศึกษาจากต่างประเทศ: Tesco Bank (UK) กับ Financial Conduct Authority [59] เมื่อ 1 ตุลาคม ค.ศ. 2018 Tesco Bank ของประเทศสหราชอาณาจักรโดนหน่วยงานรัฐชื่อว่า FCA (Financial Conduct Authority) ปรับ 16.4 ล้านปอนด์ เนื่องจากผิดพลาดหรือด้อยความสามารถในการปกป้องระบบ Debit Card จากการถูก hack เมื่อปี ค.ศ. 2016 โดยจากปัญหาดังกล่าว มีลูกค้าโดนแฮกทั้งหมด 34 รายการ เสียหายเป็นเงิน 2.26 ล้านปอนด์ ซึ่ง Tesco Bank ได้เร่งแก้ไข คืนให้ลูกค้าหมดแล้ว แต่ก็ยังถือว่าลูกค้าได้รับผลกระทบในการใช้บริการ

จะเห็นจากกรณีนี้ว่า ในต่างประเทศจะมีหน่วยงานอย่าง FCA คอยจัดการพวกธนาคาร หากปล่อยให้ระบบตัวเองมีจุดอ่อนโดน Hack แล้วกระทบต่อลูกค้าและต้องดูแลลูกค้าให้ดี ต้องแก้ไขระบบต่าง ๆ ให้ดี ไม่งั้น FCA เข้ามาตรวจสอบเพื่อลงโทษ ไม่ใช่แค่ต้องคืนเงินในรายการต่าง ๆ ที่โดนแฮกให้ลูกค้าสุดท้าย การผิดพลาดดังกล่าว ยังนำมาซึ่งการโดนปรับอีกด้วย กรณีนี้ โดนแฮก 2.26 ล้านปอนด์ ต้องคืนและรีบดูแลลูกค้า และยังโดนปรับอีก 16.4 ล้านปอนด์เพิ่มอีก ซึ่งจำนวนการปรับดังกล่าวสูงกว่ามูลค่าความเสียหายจากการโดนแฮกเสียอีก กรณีนี้ ยังดีที่ Tesco Bank ให้ความร่วมมืออย่างแข็งขันกับ FCA แสดงความเสียใจ และคืนเงินลูกค้าอย่างรวดเร็ว และรีบปิดจุดอ่อน ทำให้รอดจาก การปรับที่ตอนแรกตั้งไว้สูงถึง 33.56 ล้านปอนด์ เหลือแค่ปรับ 16.4 ล้าน ปอนด์ ในขั้นปรานี

หากมองกรณีกลับมาที่ธนาคารไทย จะเห็นว่าต่างกันอย่างมาก ที่มักปัดความรับผิดชอบไปให้กับลูกค้าธนาคารไว้ก่อน และไม่ยอมให้ความร่วมมือกับเจ้าหน้าที่รัฐ ในการสืบสวน สอบสวน โดยอ้างว่าธนาคารเป็นเหยื่อ ไม่ใช่จำเลยมีสิทธิ์ที่จะไม่ให้ข้อมูล จากนั้นมักมีการไปเสนอข้อเสนอให้ลูกค้าที่โดนแฮกว่าธนาคารจะช่วยคืนเงินให้ส่วนหนึ่งไม่เกินครึ่งหนึ่ง หรือหนึ่งในสามเพื่อเยียวยาและให้ลงชื่อในสัญญาไม่ดำเนินคดีใด ๆ อีก ซึ่งมีลูกค้าจำนวนมากจำยอมตามเงื่อนไขที่ธนาคารเหล่านี้เสนอ

ด้วยความแตกต่างในการบังคับให้ธนาคารต้องดูแลและรับผิดชอบต่อความมั่นคงของระบบ จะเห็นได้ว่า เมื่อเกิดรายการธุรกรรมฉ้อฉล (fraud transaction) หรือรายการแปลกปลอมที่เราไม่ใช้เกิดขึ้น หรือเมื่อมีประเด็นโดนแฮกระบบบัญชีธนาคารของลูกค้า ระบบของธนาคารในยุโรปทั่วไป ลูกค้าแค่ login เข้าระบบ แล้วส่ง instant message ผ่านระบบ chat รับเรื่อง ของระบบธนาคาร ก็มีคนรับเรื่องผ่าน chat คุยรายละเอียด ดำเนินการประสานงานให้แก้ไขปัญหาให้เรียบร้อย โดยเมื่อเกิดเหตุขึ้น ธนาคารจะรีบดูแลลูกค้าก่อน หากพบในภายหลังว่าเป็นความผิดลูกค้า จึงใช้กฎหมายดำเนินคดีกับลูกค้า คุณภาพบริการระดับนี้ถือว่าต่างกันอย่างมากกับคุณภาพการดูแลลูกค้าของธนาคารไทยโดยทั่วไป ที่เข้าถึง Call Center ยากมาก ยื่นเรื่องที่ธนาคารก็ต้องติดตาม วุ่นวาย ต้องทำการแจ้งความ สุดท้ายยังถูกบ่ายเบี่ยงเรื่องการชดใช้จากธนาคาร

4.4 เสนอแนะแนวทางแก้ไขปัญหาที่พบจากการวิเคราะห์ปัญหาด้านกฎหมาย

จากการวิเคราะห์ลักษณะการกระทำความผิด การศึกษาเปรียบเทียบกับคดีพิเศษที่ได้รับมอบหมายให้ทำการวิเคราะห์จุดอ่อน ปัญหาในการสืบสวนสอบสวน วิเคราะห์การรับฟังพยานหลักฐานที่เกี่ยวข้องกับประเด็นที่ทำการวิจัย วิเคราะห์เปรียบเทียบการคุ้มครอง ควบคุม การประกอบธุรกิจธนาคารที่มีการบังคับใช้ในกฎหมายไทย และกรณีข้อเท็จจริงที่เกิดในต่างประเทศ ข้างต้นทำให้ทราบถึงปัญหาที่เกิดขึ้น จึงเสนอแนวทางแก้ไขปัญหาที่เป็นรูปธรรม ดังนี้

แนวทางการแก้ไขปัญหา และข้อเสนอแนวทางบริหารจัดการที่เป็นรูปธรรม

1) กำหนดกฎ ระเบียบ และขั้นตอนการปฏิบัติของเจ้าหน้าที่หรือผู้ปฏิบัติงานที่มีอำนาจหน้าที่ในการสืบสวนสอบสวนรวบรวมพยานหลักฐานคดีอาชญากรรมทางเทคโนโลยีและสารสนเทศมีมาตรฐานในระดับสากล

2) กำหนดมาตรฐานรวมถึงการปรับปรุงกระบวนการทำงาน (Procedure) ข้อกำหนดในการดำเนินงาน (Work Instruction) และระบบการบริหารจัดการคุณภาพ (Quality Management System) ให้มีความเป็นระบบ และได้มาตรฐานตามหลักตรวจพิสูจน์พยานหลักฐานดิจิทัล และสอดคล้องกับมาตรฐาน ISO 17025:2005 หรือเป็นที่รู้จักตามมาตรฐาน มอก. 17025:2548 ที่มีการกำหนดในประเทศไทย การดำเนินการรวบรวมพยานหลักฐานการกระทำผิดที่เกี่ยวข้องกับเทคโนโลยีและสารสนเทศ ควรเป็นการร่วมการดำเนินการในลักษณะทีม (Work Shop) หรือมีการกำกับดูแลขณะปฏิบัติงานโดยประกอบด้วยผู้เชี่ยวชาญจากหน่วยงานต่าง ๆ ได้แก่ สำนักป้องกันและปราบปรามการกระทำความผิดทางเทคโนโลยีสารสนเทศและการสื่อสาร กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ สถาบันนิติวิทยาศาสตร์ กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (ปอท.) กลุ่มงานตรวจสอบและวิเคราะห์การกระทำความผิดทางเทคโนโลยี กองบังคับการสนับสนุนทางเทคโนโลยี (บก.สสท.) สำนักงานตำรวจแห่งชาติ กองคดีเทคโนโลยีและสารสนเทศ กองเทคโนโลยีและศูนย์ข้อมูลการตรวจสอบ กรมสอบสวนคดีพิเศษ สำนักงานอัยการสูงสุด และสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เพื่อให้ขั้นตอนการรับฟังพยานหลักฐานเกิดความน่าเชื่อถือขณะนำสืบพยานหลักฐานดังกล่าว

3) จัดตั้งคณะทำงานซึ่งประกอบด้วยผู้เชี่ยวชาญจากหน่วยงานต่าง ๆ ได้แก่ สำนักป้องกันและปราบปรามการกระทำความผิดทางเทคโนโลยีสารสนเทศและการสื่อสาร กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ สถาบันนิติวิทยาศาสตร์ กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (ปอท.) กลุ่มงานตรวจสอบและวิเคราะห์การกระทำความผิดทางเทคโนโลยี กองบังคับการสนับสนุนทางเทคโนโลยี (บก.สสท.) สำนักงานตำรวจแห่งชาติ กองคดีเทคโนโลยีและสารสนเทศ กองเทคโนโลยีและศูนย์ข้อมูลการตรวจสอบ กรมสอบสวนคดีพิเศษ

สำนักงานอัยการสูงสุด เพื่อ**พัฒนาระบบการแสวงหาข้อเท็จจริงและการรวบรวมพยานหลักฐานที่เกี่ยวข้องกับพยานหลักฐานอิเล็กทรอนิกส์** ซึ่งพนักงานสอบสวนได้ทำไปเกี่ยวกับความผิดที่กล่าวหา เพื่อที่จะทราบข้อเท็จจริงหรือพิสูจน์ความผิด เพื่อจะเอาตัวผู้กระทำผิดมาฟ้องลงโทษ และรู้ตัวผู้กระทำผิดและพิสูจน์ให้เห็นความผิดหรือความบริสุทธิ์ของผู้ต้องหา รวมถึงขั้นตอนการเก็บรวบรวมและตรวจพิสูจน์พยานหลักฐาน และการนำสืบพยานหลักฐานทางดิจิทัลในชั้นศาล

4) เสนอให้มีการนำบทบัญญัติตามพระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 และที่แก้ไขเพิ่มเติม ว่าด้วยการแต่งตั้งที่ปรึกษาในคดีพิเศษ ตามมาตรา 30 ในกรณีมีเหตุจำเป็นต้องใช้ผู้เชี่ยวชาญ มาปรับใช้ในการร่วมปฏิบัติงานดำเนินการรวบรวมพยานหลักฐานการกระทำผิดที่เกี่ยวข้องกับเทคโนโลยีและสารสนเทศ หรือตามมาตรา 33 ในกรณีที่มีความจำเป็น เพื่อประโยชน์ในการสืบสวนและสอบสวนคดีพิเศษเรื่องใดเรื่องหนึ่งโดยเฉพาะ รัฐมนตรีอาจเสนอให้นายกรัฐมนตรีในฐานะหัวหน้ารัฐบาล มีคำสั่งตามกฎหมายว่าด้วยระเบียบบริหารราชการแผ่นดิน ให้เจ้าหน้าที่ของรัฐในหน่วยงานอื่นมาปฏิบัติหน้าที่มาปรับใช้ในการร่วมปฏิบัติงานดำเนินการรวบรวมพยานหลักฐานการกระทำผิดที่เกี่ยวข้องกับเทคโนโลยีและสารสนเทศดังกล่าว

5) จัดตั้งหน่วยงานกลาง โดย**พัฒนาบุคลากร**ที่มีอำนาจหน้าที่ควบคุมการรวบรวมพยานหลักฐานที่เกี่ยวข้องกับอาชญากรรมทางเทคโนโลยีและสารสนเทศให้เกิดความเชี่ยวชาญและมี**มาตรฐานการตรวจพิสูจน์พยานหลักฐานให้มีระดับสากลโดยให้มีความเชี่ยวชาญ หรือมีทักษะเฉพาะด้าน 2 ทาง คือ (1) ด้านเทคโนโลยีและสารสนเทศ (2) ด้านกฎหมาย เพื่อให้ผลปฏิบัติงานในการรวบรวมพยานหลักฐานสามารถพิสูจน์ และรับฟังในกระบวนพิจารณาได้**

6) เสนอให้คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ใช้อำนาจตามมาตรา 22 แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562 เช่น ทำความตกลงและร่วมมือกับองค์การหรือหน่วยงานทั้งในประเทศและต่างประเทศในกิจการที่เกี่ยวกับการดำเนินการตามหน้าที่และอำนาจของสำนักงานในการกำกับดูแล หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ Critical Information Infrastructure (CII) ด้านการเงินการธนาคาร โดยอาจเสนอให้มีการปรับปรุงกฎหมายให้การไม่ปฏิบัติตามถือเป็นการละเว้น ที่มีโทษทางอาญาในอนาคตต่อไปด้วย

7) เสนอให้มีการจัดตั้งศาลชำนัญพิเศษ เพื่อให้มีอำนาจพิจารณาพิพากษาคดีอาญาที่เกี่ยวข้องกับอาชญากรรมทางคอมพิวเตอร์ โดยให้ศาลชำนัญพิเศษดังกล่าว มีอำนาจหน้าที่ทำการไต่สวนหรือมีคำสั่งใด ๆ ซึ่งคดีที่มีความผิดอาญาที่มีความจำเป็นต้องใช้ความชำนาญพิเศษ ในการพิจารณาและพิพากษาคดี

จากการเสนอแนวทางในการบริหารจัดการเพื่อแก้ไขปัญหาดังกล่าว ทำให้เห็นปัญหาในการควบคุมการประกอบธุรกิจหรือการให้บริการธนาคารอิเล็กทรอนิกส์ในประเทศไทย ในประเด็นสำคัญที่ประเทศไทย ไม่มีและแตกต่างกับต่างประเทศ คือ กรณีเกิดปัญหาหรืออาชญากรรมทางไซเบอร์ต่อ

บริการธนาคารอิเล็กทรอนิกส์ กฎหมายในประเทศไทย ยังไม่มีอำนาจในการลงโทษ (Sanction) สถาบันการเงินหรือธนาคารที่จงใจปล่อยปละ ละเว้น หรืออาจกระทำการโดยประมาทเลินเล่ออย่างร้ายแรง ในฐานะเป็นผู้ประกอบการที่ควรต้องมีความรอบคอบ ยิ่งกว่าวิญญูชนในวิชาชีพทั่วไปควรจะต้องมี

4.5 ผลการวิเคราะห์เทคนิควิธีที่เกี่ยวข้องกับการโจมตี HTTPS, PKI

4.5.1 ผลการวิเคราะห์ตรวจสอบ HTTP Response Header

การวิเคราะห์ตรวจสอบการตั้งค่ากลไก HSTS ในกลุ่มเว็บไซต์ที่ใช้ในการทดลอง ประกอบด้วยเว็บไซต์ที่ให้บริการธนาคารออนไลน์ในไทย จำนวน 11 เว็บ, เว็บไซต์ที่ให้บริการ E-commerce จำนวน 5 เว็บ ซึ่งสามารถตรวจสอบการตั้งค่า Header HSTS โดยการ Request เว็บไซต์ผ่าน Web Browser จากนั้น Inspect Network แล้วเลือกดูข้อมูลในหัวข้อ Response Headers ก็จะพบ Header HSTS ดังภาพที่ 4.1

ภาพที่ 4.1 ผลการตรวจสอบการตั้งค่ากลไก HSTS

4.5.2 ผลการตรวจสอบการตั้งค่ากลไก HSTS ของเว็บไซต์ธนาคารออนไลน์ในประเทศไทย

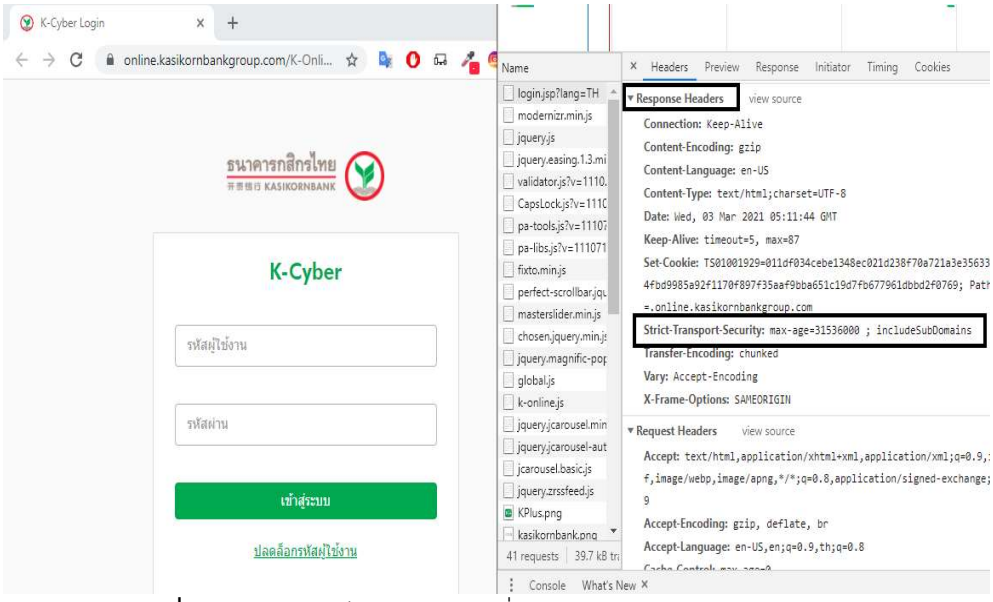
ผลการตรวจสอบ HTTP Header HSTS ของเว็บไซต์ที่ให้บริการธนาคารออนไลน์ในประเทศไทย จำนวน 11 เว็บ พบว่ามีการปรับแต่งค่าตามค่ามาตรฐาน 4 ธนาคาร (ค่าที่แนะนำโดย Google คือ **Strict-Transport-Security: max-age=31536000; includeSubDomains) และมี 3 ธนาคาร ที่มีการตั้งค่า Max-Age Configuration ไม่เหมาะสม (ค่าที่แนะนำโดย Google คือ 31536000 ขึ้นไป) และไม่พบการ Configure HSTS จำนวน 4 ธนาคาร ซึ่งธนาคารออนไลน์ดังกล่าวน่าจะโดนโจมตีด้วย SSL Stripping Attack ได้ และมีเพียง 1 ธนาคาร ที่มีการตั้งค่ากลไก HSTS แบบ Preload ซึ่งน่าจะเป็นค่าที่เหมาะสมที่สุดในการป้องกัน SSL Stripping Attack ดัง**

ตารางที่ 4.1

ตารางที่ 4.1 ผลการตรวจสอบการตั้งค่ากลไก HSTS ของเว็บไซต์ธนาคารออนไลน์ในประเทศไทย

ระบบธนาคารออนไลน์ในไทย*	HSTS			
	Header	IncludeSubdomains	Max-Age	Preload
A	Yes	Yes	31536000	No
B	Yes	Yes	31536000	Yes
C	Yes	Yes	31536000	No
D	Yes	Yes	31536000	No
E	Yes	Yes	12051306	No
F	Yes	Yes	15552000	No
G	Yes	No	No	No
H	ไม่พบการ Configure HSTS			
I	ไม่พบการ Configure HSTS			
J	ไม่พบการ Configure HSTS			
K	ไม่พบการ Configure HSTS			

** เพื่อสงวนชื่อเว็บไซต์ธนาคารออนไลน์ในประเทศไทย จึงใช้อักษรย่อแทน*



ภาพที่ 4.2 ตัวอย่างเว็บไซต์ธนาคารที่ Configuration Max-Age HSTS เหมาะสม

4.5.3 ผลการตรวจสอบการตั้งค่ากลไก HSTS ของเว็บไซต์ E-commerce

ผลการตรวจสอบ HTTP Header HSTS ของเว็บไซต์ที่ให้บริการระบบ E-commerce จำนวน 5 เว็บ พบว่ามีการ Configuration ตามค่ามาตรฐาน 4 เว็บ และมีเพียง 1 เว็บ ที่มีการตั้งค่ากลไก HSTS แบบ Preload ซึ่งน่าจะเป็นค่าที่เหมาะสมที่สุด ดังตารางที่ 4.2

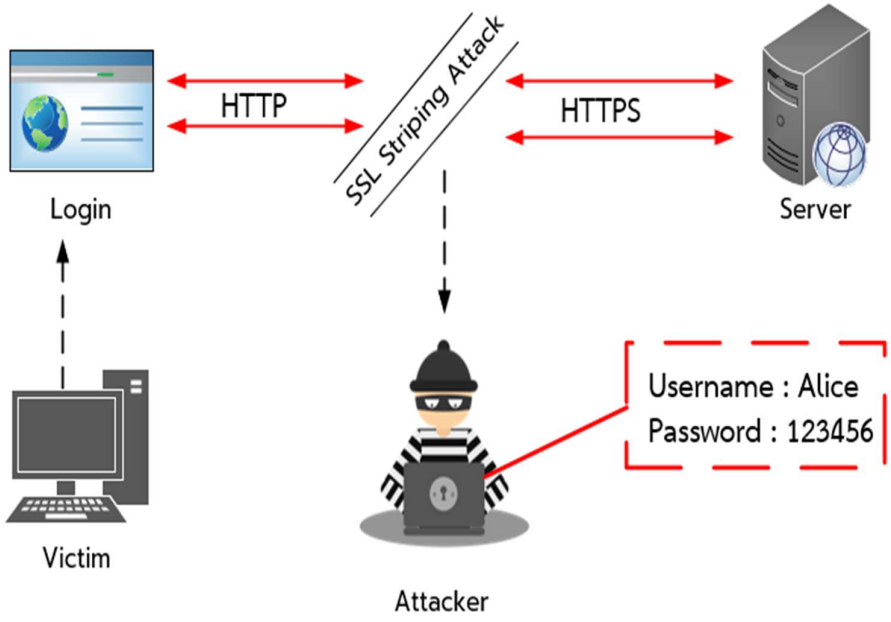
ตารางที่ 4.2 ผลการตรวจสอบการตั้งค่ากลไก HSTS ของเว็บไซต์ E-commerce

เว็บไซต์ E-commerce*	HSTS			
	Header	IncludeSubdomains	Max-Age	Preload
L	Yes	Yes	47474747	Yes
M	Yes	Yes	31536000	No
N	Yes	Yes	31536000	No
O	Yes	Yes	31536000	No
P	Yes	Yes	31536000	No

** เพื่อสงวนชื่อเว็บไซต์ E-commerce จึงใช้อักษรย่อแทน*

4.6 ผลการทดลองโจมตี SSL Stripping Attack

ผลการทดลองโจมตีเว็บไซต์ด้วย SSL Stripping Attack จากกลุ่มตัวอย่าง เพื่อให้ทราบผลการโจมตีว่าเป็นไปตามความคาดหวังหลังอ่านค่า HSTS Response Header หรือไม่ จึงทำการทดลอง Strip และ Sniff ในหน้าเข้าสู่ระบบ (Login) บนเว็บเบราว์เซอร์ Google Chrome, Safari, Internet Explorer, Mozilla Firefox และ Opera ในการทดสอบพบว่า หากการโจมตีด้วยเทคนิค SSL Stripping Attack สามารถทำการทำลายระบบป้องกัน SSL/TLS ได้สำเร็จ โพรโทคอลเดิมที่เป็น HTTPS จะถูกบังคับให้ใช้เป็น HTTP แทน ทำให้สามารถดักจับข้อมูล (Data Sniff) ของชื่อผู้ใช้และรหัสผ่านออกมาได้ ซึ่งมีรูปแบบการโจมตี ดังภาพที่ 4.3



ภาพที่ 4.3 รูปแบบการโจมตีด้วย SSL Stripping Attack

4.6.1 ผลการโจมตีเว็บไซต์ธนาคารออนไลน์ในประเทศไทยด้วยวิธี SSL Stripping Attack

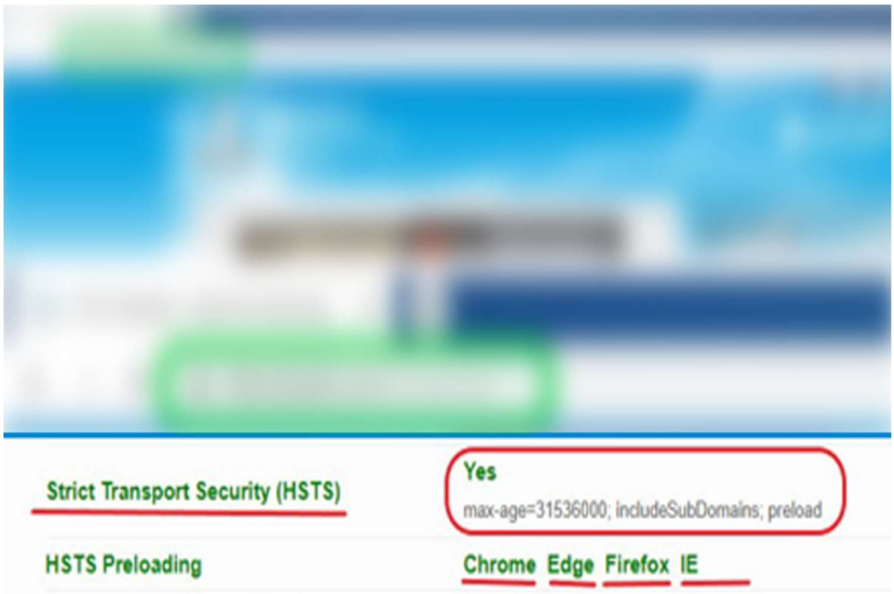
จากการทดลองโจมตีเว็บไซต์ธนาคารออนไลน์ในประเทศไทย จำนวน 11 เว็บ ด้วยวิธี SSL Stripping Attack จากผลลัพธ์ในการทดลอง จะเห็นได้ว่ามีเพียงหนึ่งธนาคารที่รอดจากการถูกโจมตีด้วย SSL Strip และ Sniff ดักจับข้อมูล และพบว่าเป็นเพียงธนาคารเดียวที่มีการตั้งค่า HSTS แบบ Preload ดังตารางที่ 4.3 และผลการทดลอง มี 10 ใน 11 ธนาคาร ที่สามารถทำลายระบบป้องกันปลด HTTPS เป็น HTTP ได้ แม้มีการตั้งค่า HSTS Config ด้วยค่า Max-age ที่เหมาะสม เมื่อดูจาก HTTP Response Header โดยใน 10 ธนาคาร ที่ถูก Strip มี 9 ธนาคารที่ถูก Sniff ได้ด้วย ทำให้สามารถดักจับข้อมูลรหัสผ่านของเหยื่อได้ ดังตารางที่ 4.3 ทั้งนี้ มีเพียงหนึ่งธนาคารที่ถึงแม้สามารถโจมตี SSL Strip ได้ แต่กลับไม่สามารถนำข้อมูลไปใช้ประโยชน์ได้ เนื่องจากข้อมูลรหัสผ่านมีการแฮชหรือใช้การส่งรหัสผ่านบนอินเทอร์เน็ตโดยแปลงรูปให้เป็น Salted-hash password (SHP) ก่อน ดังภาพที่ 4.6

ตารางที่ 4.3 ผลการโจมตีเว็บไซต์ธนาคารออนไลน์ในประเทศไทยด้วยวิธี SSL Stripping **Attack**

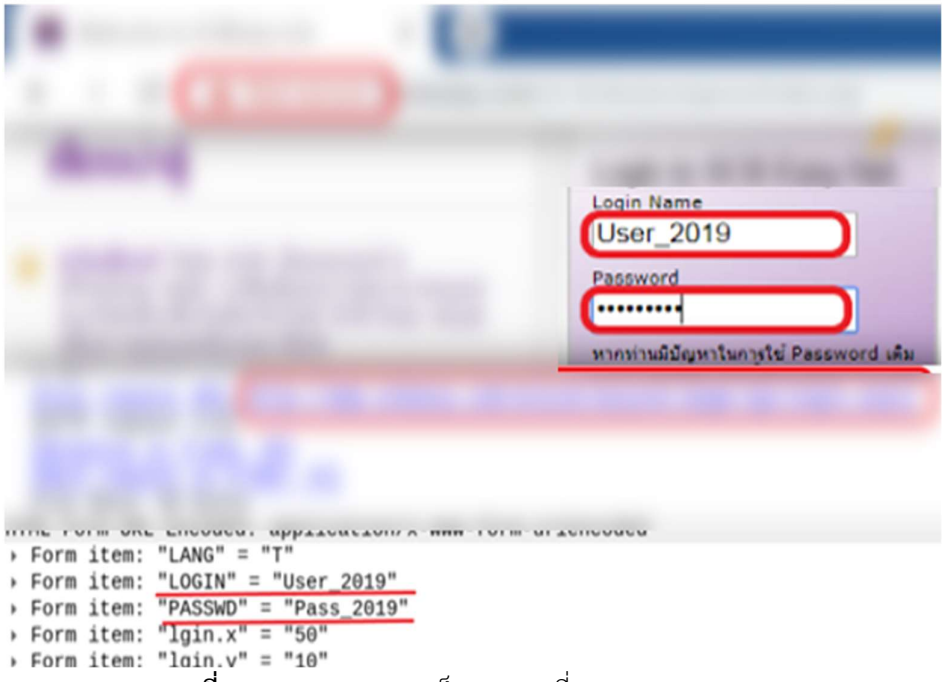
เว็บไซต์*	HSTS		SSL Strip Attack	
	Max-Age	Preload	SSL Strip	Data Sniff
A	31536000	No	✓	✓
B	31536000	Yes	×	×
C	31536000	No	✓	✓
D	31536000	No	✓	✓
E	12051306	No	✓	×
F	15552000	No	✓	✓
G	No	No	✓	✓
H	ไม่พบการ Configure HSTS		✓	✓
I	ไม่พบการ Configure HSTS		✓	✓
J	ไม่พบการ Configure HSTS		✓	✓
K	ไม่พบการ Configure HSTS		✓	✓

** เพื่อสงวนชื่อเว็บไซต์ธนาคารออนไลน์ในไทย จึงใช้อักษรย่อแทน*

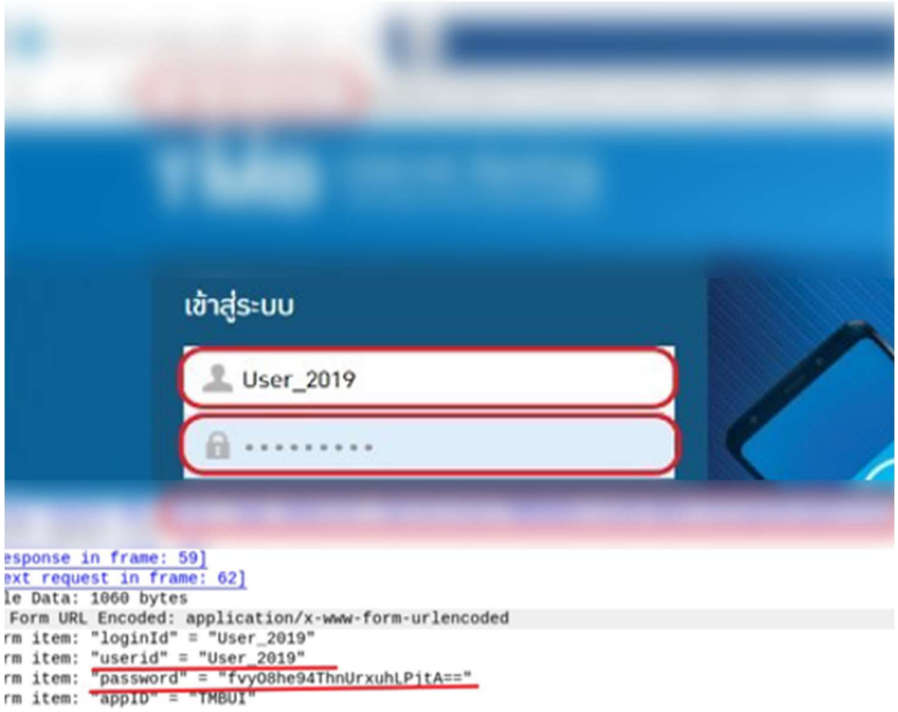
✓ : สามารถโจมตีได้ × : ไม่สามารถโจมตีได้



ภาพที่ 4.4 ผลการทดลองเว็บธนาคารที่มีการตั้งค่า HSTS แบบ Preload



ภาพที่ 4.5 ผลการทดลองเว็บธนาคารที่ถูก SSL Strip และ Sniff



ภาพที่ 4.6 ผลการทดลองเว็บธนาคารที่มีการปรับใช้ Salted-hash password

ตารางที่ 4.4 สรุปผลการโจมตีเว็บไซต์ธนาคารออนไลน์ในประเทศไทย

Web Browser	SSL Strip Attack		
	โจมตีได้	โจมตีไม่ได้	ดักจับข้อมูลไม่ได้
Google Chrome	10	1	2
Safari	10	1	2
Internet Explorer	10	1	2
Mozilla Firefox	10	1	2
Opera	10	1	2

4.6.2 ผลการโจมตีเว็บไซต์ E-commerce ด้วยวิธี SSL Stripping Attack

จากการทดลองโจมตีเว็บไซต์ E-commerce จำนวน 5 เว็บ ด้วยวิธี SSL Stripping Attack ได้ผลลัพธ์ในการทดลองและรายละเอียดดังนี้ จาก

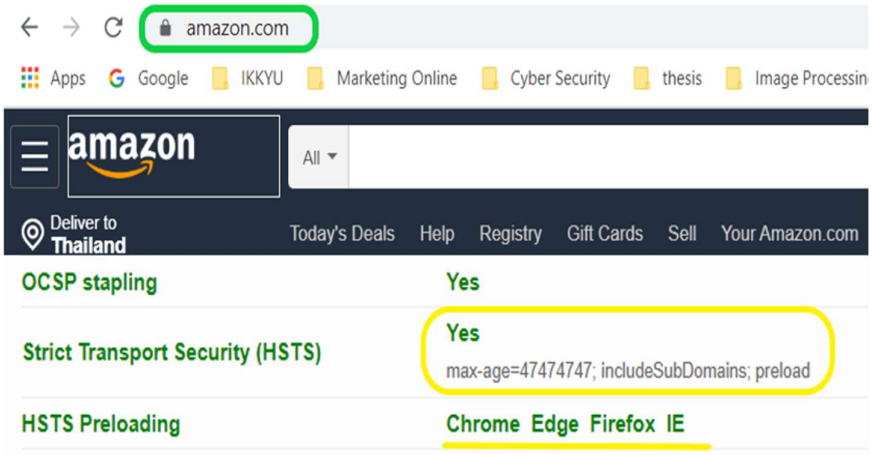
ตารางที่ 4.5 จะเห็นได้ว่า มีเพียงหนึ่ง E-commerce ที่รอดจากการถูกโจมตี SSL Strip และ Sniff ดักจับข้อมูล เนื่องจากมีการตั้งค่า HSTS แบบ Preload ดังภาพที่ 4.7 และใน E-commerce Web 4 sites ผลการทดลองสามารถทำลายระบบป้องกันปลด HTTPS ไปเป็น HTTP ได้ แม้มีการตั้งค่า HSTS Config ด้วยค่า Max-age ที่เหมาะสมเมื่อดูจาก HTTP Response Header แต่กลับสามารถโจมตี Strip และ Sniff ดักจับข้อมูลรหัสผ่านของเหยื่อได้ ดังภาพที่ 4.8

ตารางที่ 4.5 ผลการโจมตีเว็บไซต์ E-commerce ด้วยวิธี SSL Stripping Attack

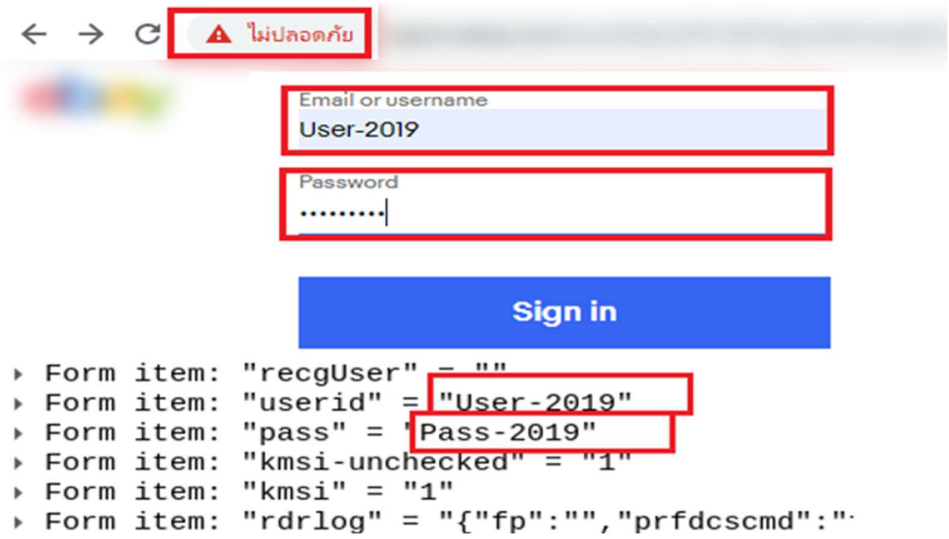
เว็บไซต์*	HSTS		SSL Strip Attack	
	Max-Age	Preload	SSL Strip	Data Sniff
L	47474747	Yes	×	×
M	31536000	No	✓	✓
N	31536000	No	✓	✓
O	31536000	No	✓	✓
P	31536000	No	✓	✓

** เพื่อสงวนชื่อเว็บไซต์ E-commerce จึงใช้อักษรย่อแทน*

✓ : สามารถโจมตีได้ × : ไม่สามารถโจมตีได้



ภาพที่ 4.7 ผลการทดลองเว็บ E-commerce ที่มีการตั้งค่า HSTS แบบ Preload



ภาพที่ 4.8 ผลการทดลองเว็บ E-commerce ที่ถูก SSL Strip และ Sniff

4.6.3 ผลสรุปการโจมตีเว็บไซต์กลุ่มตัวอย่าง

ตารางที่ 4.6 สรุปผลการโจมตีเว็บไซต์กลุ่มตัวอย่าง

เว็บไซต์	SSL Strip Attack		
	โจมตีได้	โจมตีไม่ได้	ดักจับข้อมูลไม่ได้
เว็บไซต์ธนาคารออนไลน์ ในประเทศไทย 11 เว็บ	10	1	2
เว็บไซต์ E-commerce 5 เว็บ	4	1	1

ผลการทดลองโจมตีเว็บไซต์กลุ่มตัวอย่างของระบบ ที่ให้บริการ Online Banking และ E-commerce พบว่า ทั้งสคริปต์การโจมตีแบบใหม่ของแฮกเกอร์ที่ใช้ Bettercap Script และสูตรการโจมตีแบบเก่าของ Moxie Marlinspike ก็ให้ผลการโจมตีเหมือนกัน ซึ่งหากสามารถทำการจู่โจมด้วย SSL Stripping Attack ได้สำเร็จ คือสามารถเปลี่ยนการใช้โพรโทคอล HTTPS เป็น HTTP ได้แล้ว ผู้โจมตีจะสามารถทำการโจมตีต่อเพื่อดักจับ (sniff) ข้อมูลสำคัญต่าง ๆ ของเหยื่อได้ไม่ว่าจะเป็น ชื่อผู้ใช้ รหัสผ่าน หรือข้อมูลอื่น ๆ ที่ถูกส่งไปยัง Server ซึ่งหากบนเว็บไซต์ที่ถูกโจมตีใช้ SSL/TLS เพียงอย่างเดียวในการป้องกันระบบ จะทำให้ผู้โจมตีสามารถดักจับข้อมูลออกมาได้ ในรูปของ Clear Text แต่ในกรณีของบางเว็บไซต์ หากมีการใช้ทั้ง SSL/TLS และการเข้า Hash รหัสผ่านช่วยเสริมอีกด้วย จะทำให้ผลของการโจมตีของ Hacker จะได้ข้อมูลออกมาในลักษณะของ Hashed Text ที่ไม่สามารถนำไปใช้งานได้โดยตรง ซึ่งสามารถสรุปเพิ่มเติมได้ดังนี้

1) การโจมตี HTTPS ด้วยวิธีการ SSL Stripping Attack พบว่า ถึงแม้จะมีการใช้งาน SSL/TLS ในรูปแบบตลอดขบวนการ หรือเฉพาะหน้า Login ยังเกิดปัญหาการโจมตีจากการจู่โจมด้วยเทคนิค SSL Stripping Attack ได้

2) การโจมตีด้วยเทคนิค SSL Stripping Attack ทั้งการโจมตีด้วย Bettercap ที่เป็นรูปแบบใหม่ และการโจมตีแบบเก่าของ Moxie Marlinspike พบว่าถึงแม้มีการ Configuration ปรับใช้กลไก HSTS ตามสูตรที่รู้กัน HSTS กลับไม่ประสบผลสำเร็จในการป้องกัน

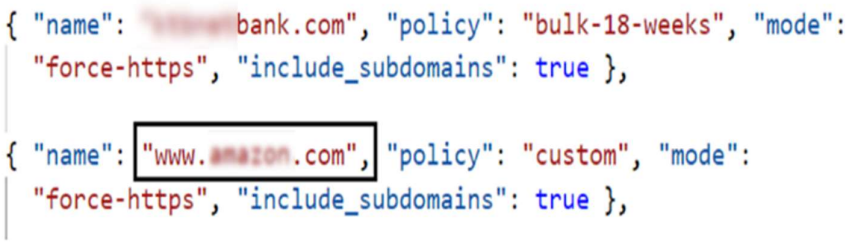
3) การโจมตีด้วยเทคนิค SSL Stripping Attack สามารถทำการโจมตีได้บนทุกแพลตฟอร์มของฮาร์ดแวร์ ระบบปฏิบัติการ และเว็บเบราว์เซอร์

4.6.4 ผลการวิเคราะห์ HSTS Preload List

จากการศึกษาเว็บไซต์ที่มีการตั้งค่ากลไก HSTS Preload List พบว่า จะถูกบรรจุไว้ใน List ที่

https://chromium.googlesource.com/chromium/src/net/+/master/http/transport_security_state_static.json

และเมื่อเว็บเบราว์เซอร์มีการ Update จะมีการดึงเอา List นี้ไปเก็บไว้ในเว็บเบราว์เซอร์ ผลการทดลองเว็บไซต์ที่มีการปรับใช้ HSTS แบบ Preload ที่ไม่สามารถโจมตีได้ มีธนาคารออนไลน์ในไทย 1 ธนาคาร และเว็บไซต์ E-commerce ต่างประเทศ 1 เว็บไซต์ ที่มีการจดทะเบียน HSTS Preload และถูกลิสต์ไว้ใน transport_security_state_static.json ดังภาพที่ 4.9

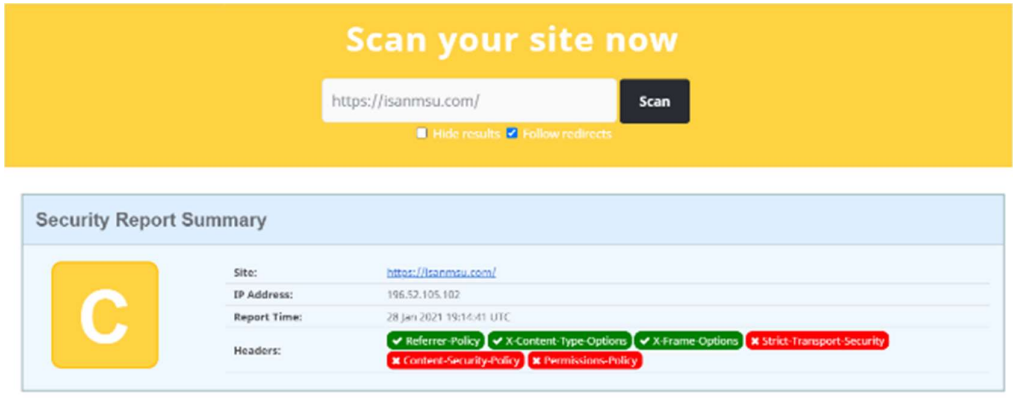


ภาพที่ 4.9 HSTS Preload List ในเว็บกลุ่มตัวอย่าง

เพื่อให้เห็นผลการทดลองในมิติอื่น ๆ จึงนำเว็บไซต์อาสาสมัคร isanmsu.com มาทำการทดสอบ โดยเริ่มจากการ Inspect Network เพื่อเช็คค่า HTTP Response Header ได้ผลคือไม่พบการตั้งค่า HSTS หลังจากนั้นทำการโจมตีด้วย SSL Stripping Attack ผลเป็นที่น่าแปลกใจคือไม่สามารถ SSL Strip HTTPS ของเว็บไซต์อาสาสมัครได้ ดังนั้นจึงทำการตรวจสอบ HSTS Preload List ดังภาพที่ 4.10 ทำให้รู้ว่าเว็บไซต์ isanmsu.com มีการปรับใช้ความมั่นคง HSTS แบบ Preload ซึ่งก่อนหน้านี้ที่เช็คค่า Header ไม่พบการตั้งค่า HSTS เพราะว่าหลังลงทะเบียนเสร็จแล้ว เจ้าของเว็บไซต์ได้ลบค่า Header HSTS ออก ทำให้รู้ว่าถึงลบค่าคอมฟิก HSTS หลังจากลงทะเบียน Preload สำเร็จแล้ว ก็ไม่ส่งผลกระทบในการป้องกันแต่อย่างใด

ภาพที่ 4.10 HSTS Preload ของเว็บไซต์ isanmsu.com

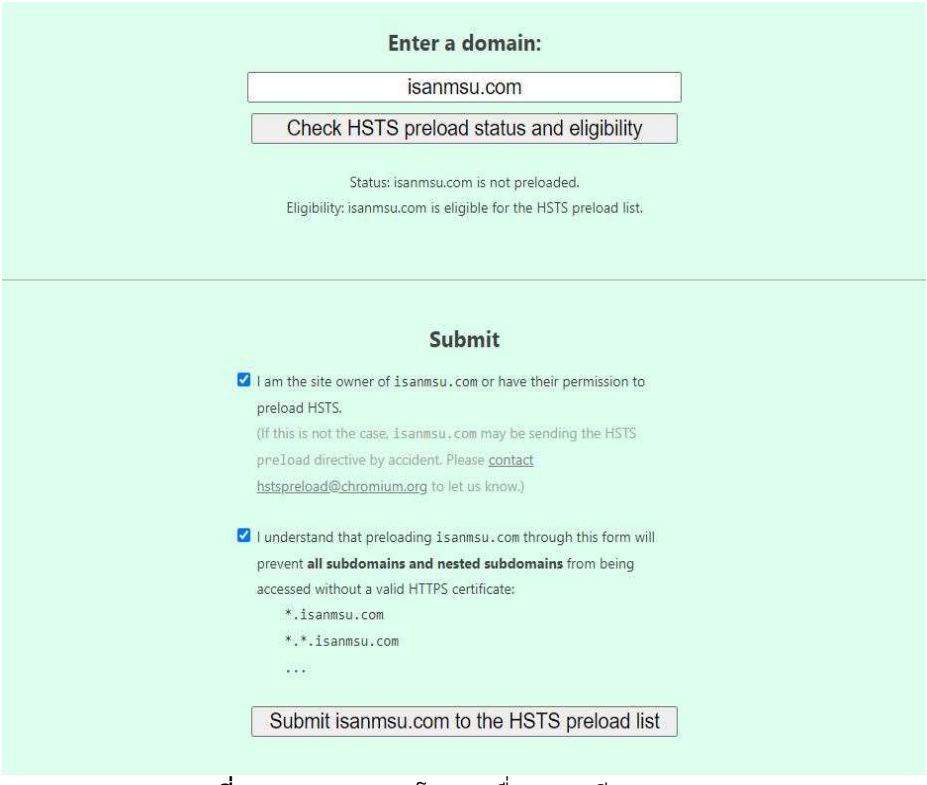
จากการทดสอบเว็บไซต์ที่จัดอันดับให้คะแนนความมั่นคงปลอดภัยของเว็บไซต์หลายบริการ เช่น https://securityheaders.com, www.serpworx.com และ ssllabs.com พบว่ามีข้อผิดพลาดในการประเมินผล HSTS ดังตัวอย่าง แสดงในภาพที่ 4.11 ที่ให้คะแนนความมั่นคงปลอดภัยไม่ผ่านในด้านการป้องกัน SSL Stripping Attack เพียงเพราะเช็คจากค่า HTTP Response Header เพียงอย่างเดียว ทั้งที่เว็บไซต์ isanmsu.com มีความมั่นคงปลอดภัยจากการถูกโจมตีดังกล่าว เพราะทำการตั้งค่า HSTS แบบ Preload และถูกเก็บไว้ใน Preload List เรียบร้อยแล้ว การค้นพบนี้เป็นองค์ความรู้สำคัญที่ควรนำไปปรับวิธีให้คะแนนความมั่นคงปลอดภัยเว็บไซต์ใหม่



ภาพที่ 4.11 ผลการ Scan Website isanmsu.com

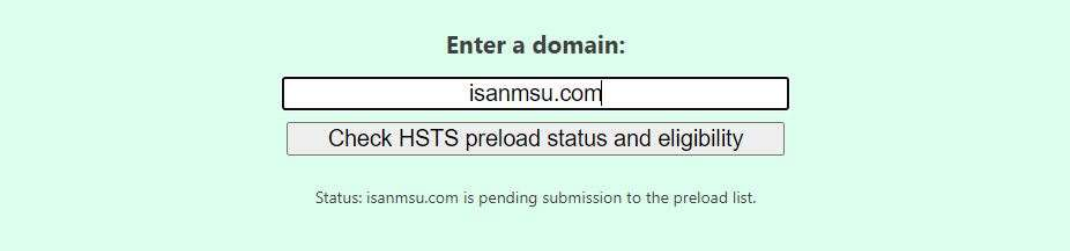
4.6.5 ผลการแนะนำการตั้งค่า HSTS แบบ Preload

HSTS Preload ได้รับการดูแลในโครงการ Chromium ที่ถูกพัฒนาโดย Google มีเป้าหมายเพื่อสร้างกลไกต่าง ๆ ให้มีความมั่นคงปลอดภัยและมีเสถียรภาพในการใช้งาน ผู้ดูแลระบบตั้งค่า HTTP Header ให้เป็น Strict-Transport-Security: maxage=31536000;includeSub Domains; preload และนำโดเมนเนม (Domain Name) เข้าตรวจสอบและลงทะเบียนใช้งานได้ที่เว็บไซต์ hstspreload.org ดังภาพที่ 4.12



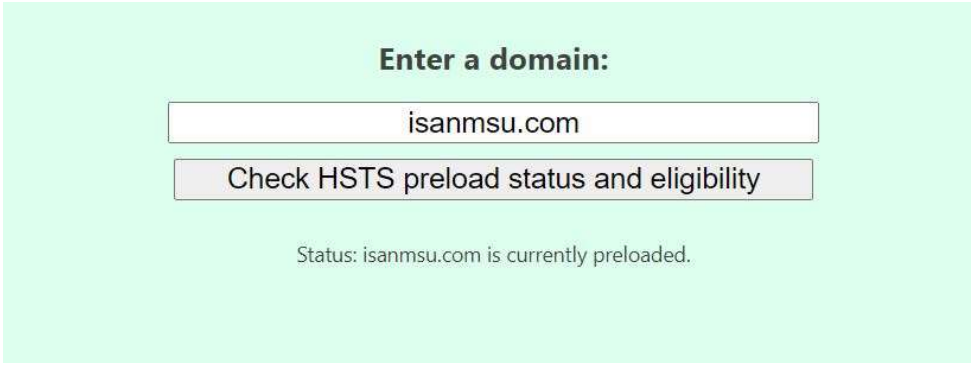
ภาพที่ 4.12 ตรวจสอบโดเมนเพื่อลงทะเบียน HSTS Preload

หลังจากนำโดเมนเนมลงทะเบียนสำเร็จระบบจะแสดงสถานะบอกให้รู้ว่ามีการส่งไปยัง Preload List เพื่อเตรียมความพร้อมในการอัพโหลดเข้าฐานข้อมูล HSTS Preload ในเว็บเบราว์เซอร์ ดังภาพที่ 4.13



ภาพที่ 4.13 สถานะการส่งคำร้อง HSTS Preload ลงทะเบียนสำเร็จ

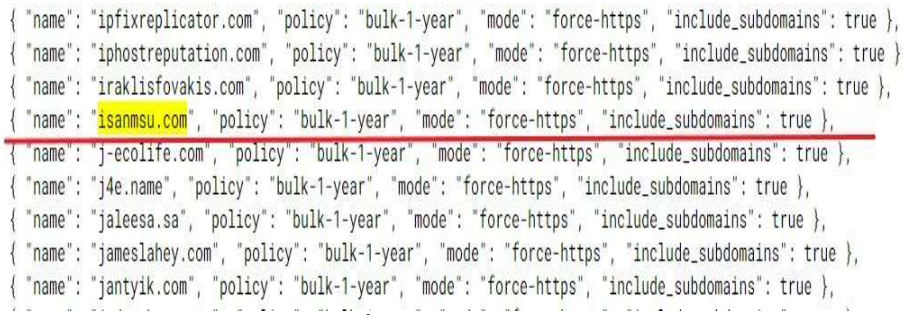
การลงทะเบียน HSTS Preload ที่สามารถป้องกันการถูกโจมตีได้ ต้องรอให้ Google ในโครงการ Chromium นำข้อมูลโดเมนอัพโหลดเข้าฐานข้อมูลเพื่อบรรจุลงในเบราว์เซอร์ จึงจะสามารถทำงานได้อย่างสมบูรณ์ โดยสามารถเข้าเช็คสถานะดังกล่าวได้ที่ hstspreload.org ดังภาพที่ 4.14



ภาพที่ 4.14 สถานะการทำงาน Preload HSTS

HSTS Preload ที่ได้รับการ Submission จะมีการฝังอยู่ที่เว็บเบราว์เซอร์ สามารถเช็คข้อมูลได้ที่ Chromium HSTS Preload List:

https://cs.chromium.org/chromium/src/net/http/transport_security_state_static.json



ภาพที่ 4.15 HSTS Preload List

4.7 ผลการวิเคราะห์ปัญหากลไก HSTS และการกลับมาจู่โจมได้ใหม่ของ SSL Stripping Attack

เพื่อให้เข้าใจผลการทดลองในเชิงลึกยิ่งขึ้น จึงได้ทำการศึกษาเครื่องมือที่ใช้ในการโจมตีด้วย SSL Stripping Attack ทั้ง Ettercap ที่เป็นแบบเดิมของ Marlinspike และแบบใหม่ของผู้โจมตีที่ใช้ Bettercap จากการศึกษา Script แบบใหม่ของ Bettercap พบการโจมตีที่เรียกว่า HSTS Hijack ที่ทำให้ทราบสาเหตุการล้มเหลวของกลไก HSTS ซึ่งจะได้แสดงผลการทดลอง ดังนี้

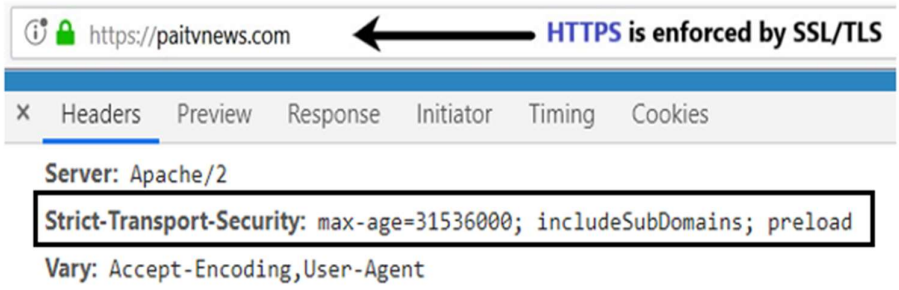
4.7.1 ผลการทดลอง HSTS Directive

การทดลองครั้งนี้เลือกเว็บไซต์อาสาสมัคร paitvnews.com ที่มีการปรับใช้ HTTPS ร่วมกับ HSTS ในการป้องกัน SSL Stripping Attack ในการทดลองได้ศึกษาการทำงานของกลไก HSTS ซึ่งมีรูปแบบการ Request – Response ที่ทำงานในฝั่ง Server ผ่าน HTTP Header การโจมตีจึงทำการแก้ไขโค้ดภาษา JavaScript ของ Bettercap ชื่อไฟล์ hstshijack.js ดังภาพที่ 4.16 เพิ่มเข้าไปในไฟล์ที่ใช้ในการติดต่อไปยังเซิร์ฟเวอร์ของ Bettercap ที่ติดตั้งใน Kali Linux 2020.1

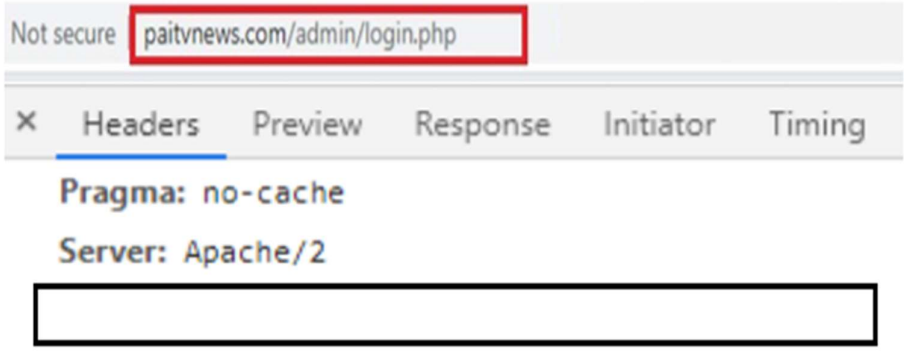
```
function onRequest(req, res) {
    res.Status      = 200;
    res.ContentType = "text/html";
    res.Body        = readFile("caplets/www/index.html");
    headers         = res.Headers.split("\r\n")
    for (var i = 0; i < headers.length; i++) {
        header_name = headers[i].replace(/:.*/, "")
        res.RemoveHeader(header_name);
    }
    res.SetHeader("Connection", "close");
}
```

ภาพที่ 4.16 รูปแบบโค้ด JavaScript ใน Bettercap ที่ใช้ในการโจมตี HSTS

เพื่อให้เข้าใจผลการโจมตีของ Module Bettercap จึงทำการแก้ไข Script ที่ใช้ในการโจมตีโดยลบ HSTS Header ที่ตั้งค่ามาจากฝั่ง Server ดังภาพที่ 4.17 และทำการโจมตีเปลี่ยนค่า Header HSTS เข้าไปใหม่โดยที่ไม่เคยมีการตั้งค่ามาก่อน ดังภาพที่ 4.18 – 4.20 ซึ่งสรุปได้ว่าการโจมตีดังกล่าวสามารถเพิ่มและลบการตั้งค่ากลไก HSTS ได้อย่างง่ายดาย โดยไม่มีการแจ้งเตือนความผิดปกติใด ๆ จาก Web Browser

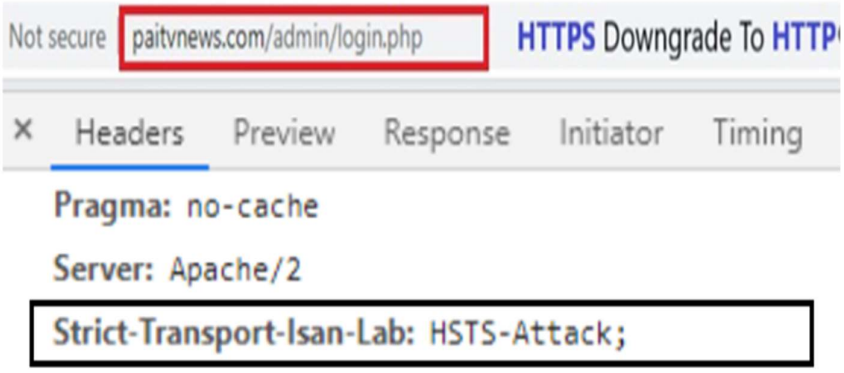


ภาพที่ 4.17 ก่อนถูกโจมตียังเห็นค่า Header HSTS ปกติ



ภาพที่ 4.18 หลังถูกโจมตีค่า Header HSTS จะถูกปลดออก

ภาพที่ 4.19 ก่อนถูกโจมตี inject HSTS header



ภาพที่ 4.20 หลังจากถูกโจมตี inject HSTS header

4.7.2 ผลการทดลอง HSTS Preload

การทดลองโจมตีได้เลือกเว็บไซต์ facebook.com จากการศึกษาพบว่าการปรับใช้ HSTS แบบ Preload ดูมีความมั่นคงปลอดภัยกว่า HSTS แบบธรรมดา เนื่องจากมีการบังคับเชื่อมต่อ HTTPS ตั้งแต่เริ่มต้นการสื่อสาร แต่การที่จะบอกให้เว็บเบราว์เซอร์เชื่อมต่อ HTTPS ตั้งแต่เริ่มต้นการสื่อสารได้ก็จำเป็นต้องมีข้อมูลเว็บไซต์เหล่านั้นอยู่ในฐานข้อมูล Web Browser เสียก่อน เหตุนี้เอง งานวิจัยนี้ จึงเสนอแนวคิดการทดสอบ โดยใช้เทคนิคการโจมตีที่เรียกว่า Homograph Attack โดยอาศัยความสามารถ Bettercap ใน Kali Linux 2020.1 ซึ่งมีรูปแบบโค้ดคำสั่งที่ใช้โจมตีดังภาพที่ 4.21

```
set hstshijack.targets          facebook.com, *.facebook.com
set hstshijack.replacements     facebook.corn, *.facebook.corn

set http.proxy.script  ********************************

set dns.spoof.domains           facebook.corn, *.facebook.corn
http.proxy  on
dns.spoof   on
```

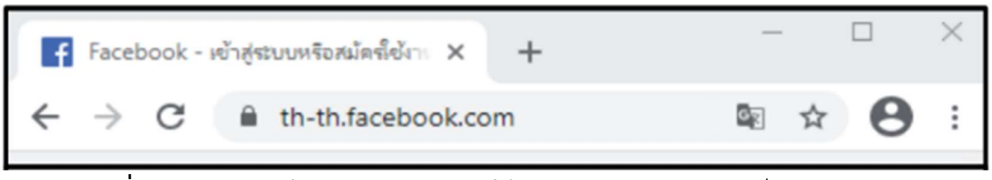
ภาพที่ 4.21 คำสั่งของเทคนิค Homograph Attack ที่ใช้ในการโจมตี HSTS Preload

เพื่อให้ทราบผลการโจมตี facebook.com จึงทำการเช็ค HSTS Preload List ในฐานข้อมูลของไฟล์ transport_security_state_static.json พบว่า facebook.com มีการปรับใช้ HSTS Preload

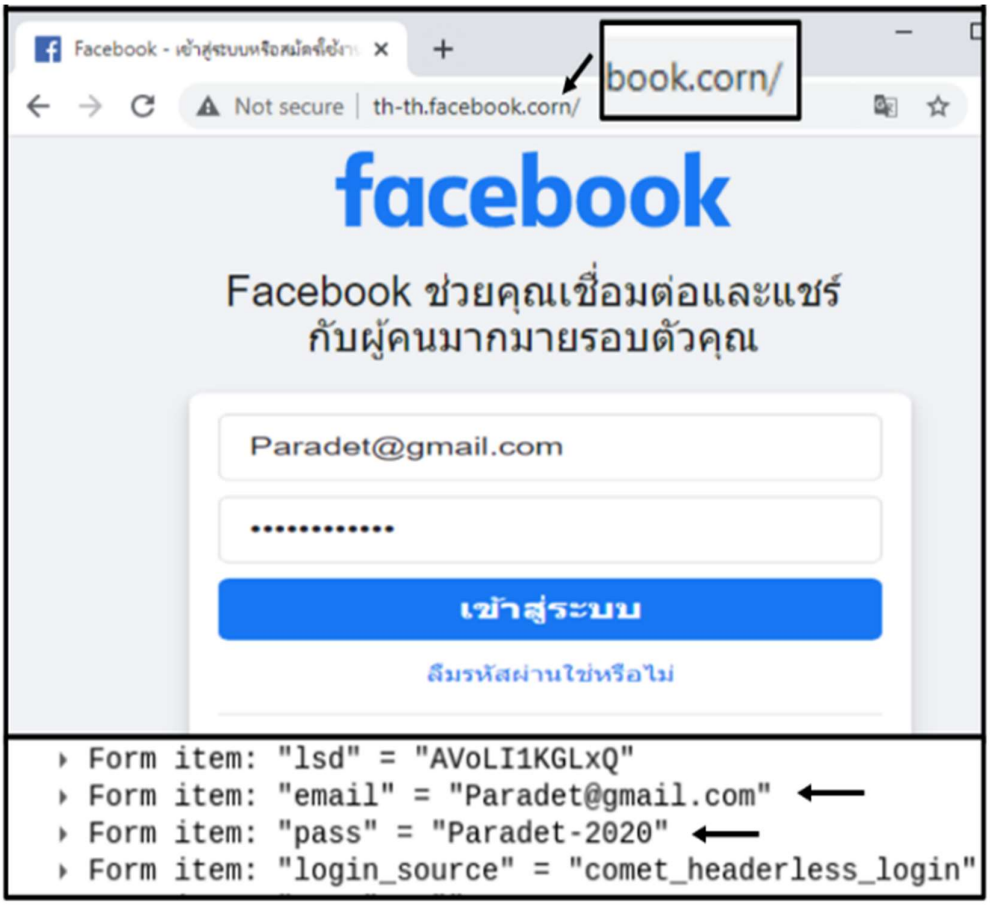
ดังภาพที่ 4.22 เพื่อการป้องกันการถูกโจมตี SSL Stripping Attack จากการจู่โจมด้วยเทคนิค Homograph Attack ได้ทำการปลอมแปลงโดเมน (DNS Spoof) ในระดับการโจมตี Top-Level Domain (TLD) แปลงจาก .com เป็น .corn ผลการโจมตีพบว่า สามารถปลดระบบป้องกันออกได้อย่างสมบูรณ์ และทำการดักจับข้อมูลของเหยื่อได้อย่างง่ายดาย ดังภาพที่ 4.23 – 4.24


```
{
  "name": "facebook.com", "policy": "custom",
  "mode": "force-https", "pins": "facebook", "include_subdomains_for_pinning": true
},
{ "name": "www.facebook.com", "policy": "custom", "mode": "force-https", "include_subdomains": true, "pins": "facebook" },
{ "name": "m.facebook.com", "policy": "custom", "mode": "force-https", "include_subdomains": true, "pins": "facebook" },
{ "name": "tablet.facebook.com", "policy": "custom", "mode": "force-https", "include_subdomains": true, "pins": "facebook" },
{ "name": "secure.facebook.com", "policy": "custom", "mode": "force-https", "include_subdomains": true, "pins": "facebook" },
{ "name": "pixel.facebook.com", "policy": "custom", "mode": "force-https", "include_subdomains": true, "pins": "facebook" },
{ "name": "apps.facebook.com", "policy": "custom", "mode": "force-https", "include_subdomains": true, "pins": "facebook" },
{ "name": "upload.facebook.com", "policy": "custom", "mode": "force-https", "include_subdomains": true, "pins": "facebook" },
{ "name": "developers.facebook.com", "policy": "custom", "mode": "force-https", "include_subdomains": true, "pins": "facebook" },
{ "name": "touch.facebook.com", "policy": "custom", "mode": "force-https", "include_subdomains": true, "pins": "facebook" },
{ "name": "mbasic.facebook.com", "policy": "custom", "mode": "force-https", "include_subdomains": true, "pins": "facebook" },
{ "name": "code.facebook.com", "policy": "custom", "mode": "force-https", "include_subdomains": true, "pins": "facebook" },
{ "name": "t.facebook.com", "policy": "custom", "mode": "force-https", "include_subdomains": true, "pins": "facebook" },
{ "name": "mtouch.facebook.com", "policy": "custom", "mode": "force-https", "include_subdomains": true, "pins": "facebook" },
{ "name": "business.facebook.com", "policy": "custom", "mode": "force-https", "include_subdomains": true, "pins": "facebook" },
{ "name": "research.facebook.com", "policy": "custom", "mode": "force-https", "include_subdomains": true, "pins": "facebook" },
{
  "name": "messenger.com", "policy": "custom",
  "mode": "force-https", "pins": "facebook", "include_subdomains_for_pinning": true
},
{ "name": "www.messenger.com", "policy": "custom", "mode": "force-https", "include_subdomains": true, "pins": "facebook" },
```


ภาพที่ 4.22 facebook.com ที่อยู่ใน HSTS Preload List



ภาพที่ 4.23 ก่อนถูกโจมตียังมีการบังคับใช้ HTTPS และ TLD ยังเป็น .com อยู่



ภาพที่ 4.24 หลังจากถูกโจมตีการบังคับใช้ HTTPS จะถูกปลดออก และ TLD จะเป็น .corn

4.8 ออกแบบและพัฒนาต้นแบบด้านซอฟต์แวร์ และเทคนิควิธีในการป้องกัน

จากแนวคิดที่ต้องการรักษาข้อมูลในระหว่างการสื่อสารเว็บไซต์ จึงทำการปรับใช้ Salted Hash Password (SHP) เพื่อเสริมสร้างเกราะป้องกันซ้อนทับ SSL/TLS อีกชั้น หากถูกโจมตีแบบ SSL Striping Attack หรือโพรโทคอลมาตรฐานทำงานผิดพลาด ไม่ได้รับการป้องกัน แต่หากมีการเข้ารหัส Message Encryption ที่ดี ถึงแม้ว่าถูกดักจับข้อมูลระหว่างการสื่อสารก็อยู่ในรูป Cipher Text การออกแบบระบบครั้งนี้ ได้พัฒนาเว็บไซต์ต้นแบบคือ isan-banking ทำงานร่วมกับ Mobile OTP ซึ่งจะได้แสดงผลลัพธ์ในการทดลอง ดังนี้

4.8.1 ผลการทดลอง isan-banking ร่วมกับ Mobile OTP

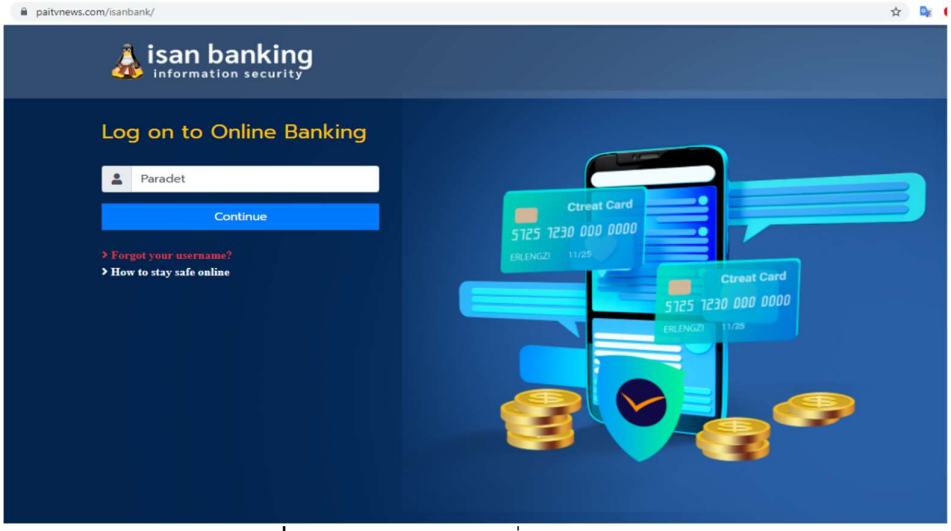
1) การทำงานของ Mobile OTP

การแสดงรหัส OTP ของทางฝั่ง Mobile OTP เมื่อผู้ใช้งานต้องการเข้าสู่ระบบเพื่อใช้งานเว็บไซต์ isan-banking ต้องใช้รหัส OTP ที่ได้จาก Mobile OTP ในการยืนยันเข้าสู่ระบบ ซึ่งรหัส OTP จะถูกสร้างขึ้นใหม่ในทุก ๆ 30–60 วินาทีแล้วแต่การตั้งค่าดังภาพที่ 4.25

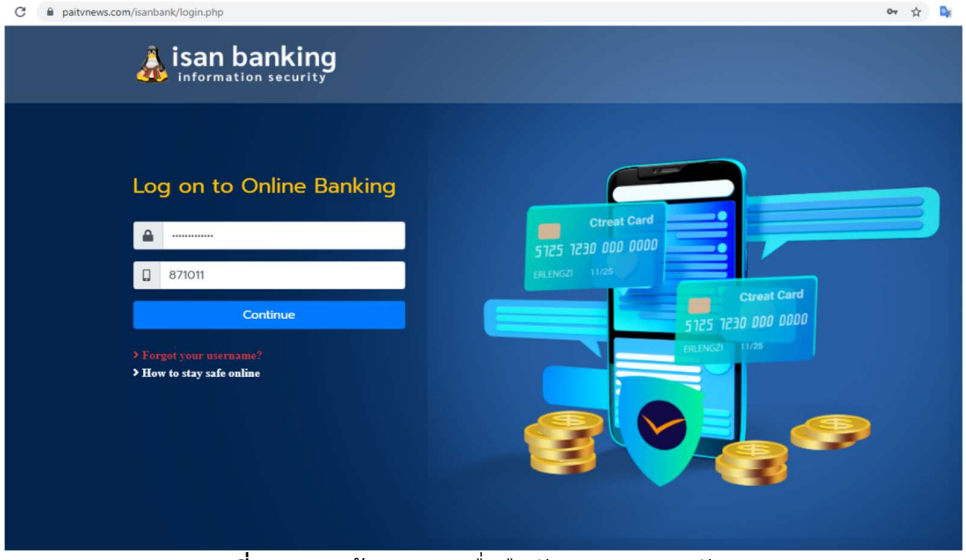
ภาพที่ 4.25 รหัส OTP จาก Mobile-OTP

2) หน้า Login เข้าสู่ระบบ isan-banking

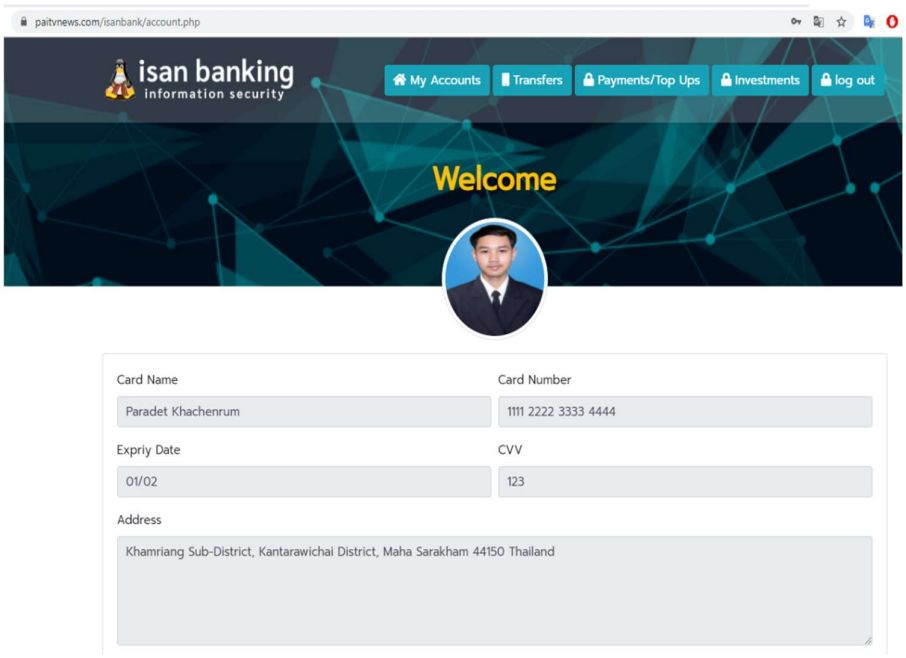
เริ่มแรกระบบจะให้ผู้ใช้งานกรอก Username เพื่อพิสูจน์ตัวตน ดังภาพที่ 4.26 ถ้าตรวจสอบแล้วถูกต้อง ก็จะเข้าสู่หน้าถนัดไปเพื่อทำการ Login ในหน้า Password และ OTP หลังจากทำการยืนยันข้อมูล ดังภาพที่ 4.27 หากข้อมูลถูกต้องทั้งหมดก็จะสามารถเข้าสู่ระบบ isan-banking ได้สำเร็จ ดังภาพที่ 4.28



ภาพที่ 4.26 หน้า Login เพื่อยืนยัน Username



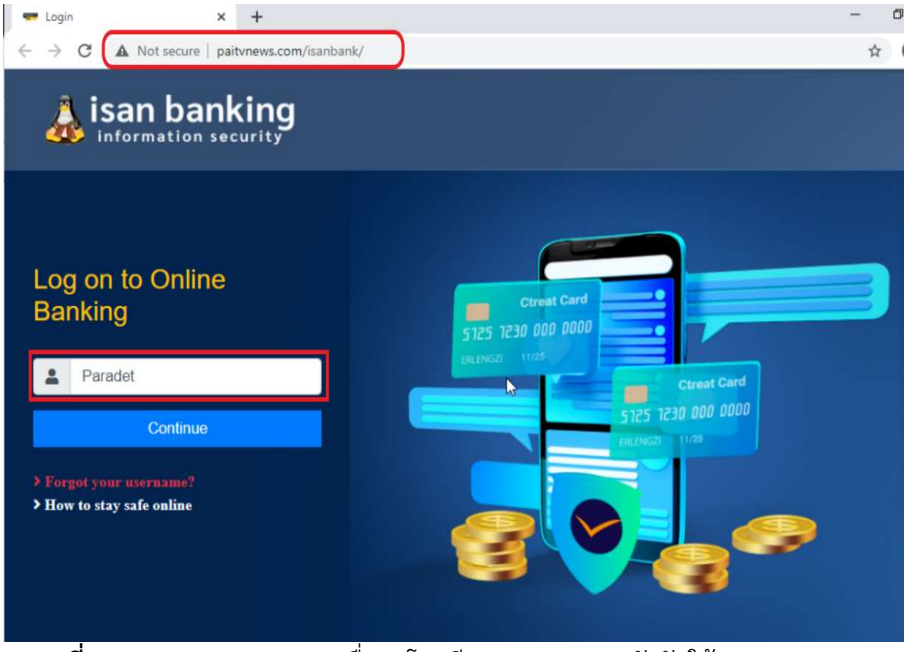
ภาพที่ 4.27 หน้า Login เพื่อยืนยัน Password กับ OTP



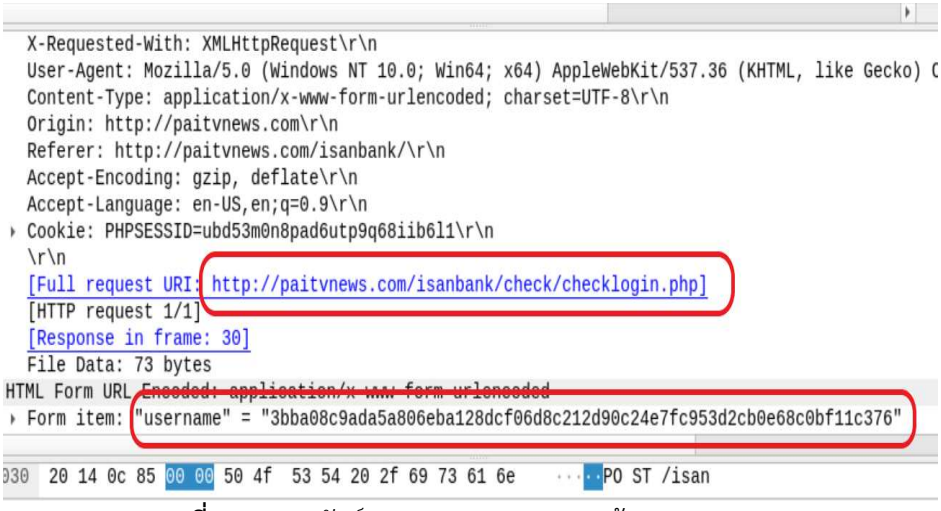
ภาพที่ 4.28 ผลการ Login เข้าสู่ระบบสำเร็จ เว็บ isan-banking

4.8.2 ผลการทดสอบความมั่นคง isan-banking ด้วยวิธี SSL Stripping Attack

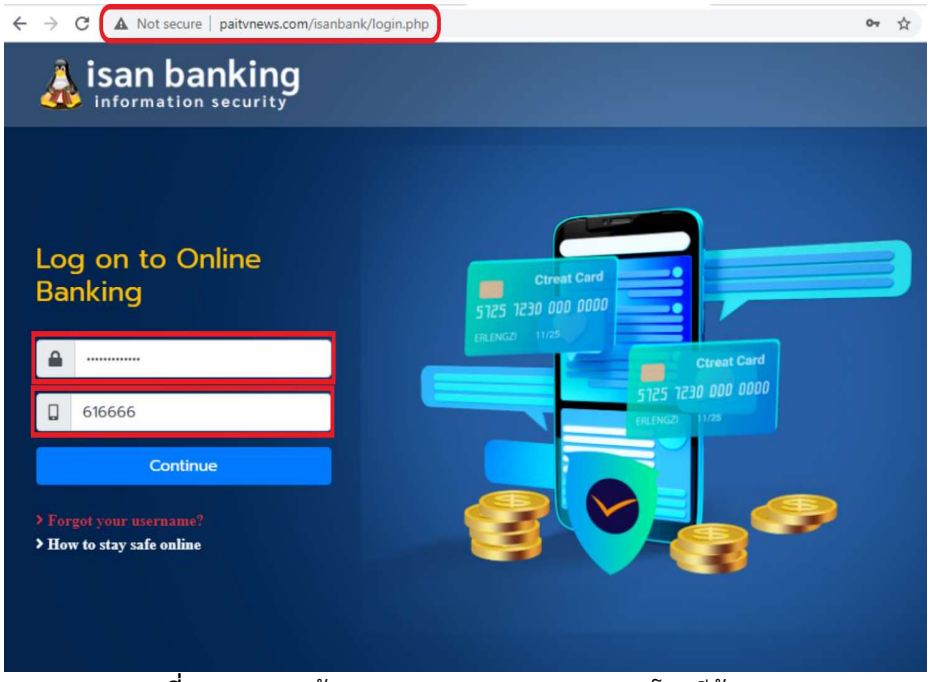
การทดสอบ isan-banking โจมตีด้วยเทคนิค SSL Stripping Attack พบว่าเมื่อสามารถทำลายโพรโทคอล SSL/TLS เปลี่ยนการสื่อสารจาก HTTPS เป็น HTTP ได้ จะส่งผลให้สามารถดักสกัดข้อมูล Username, Password และ OTP ระหว่างการสื่อสารบนระบบเครือข่ายได้ ดังภาพที่ 4.29 – 4.33 แต่จากผลการทดลองดังกล่าว ก็ยังไม่สามารถหาประโยชน์จากข้อมูลที่ดักจับได้ เนื่องจากระบบที่พัฒนาขึ้นมีการนำ Username, Password เข้ากระบวนการ Hash ด้วยภาษา JavaScript ที่มีการประมวลผลที่ฝั่งไคลเอนต์ ก่อนที่จะถูกส่งผ่านไปยังเครื่อง Server ทำให้ถึงแม้มีการดักจับข้อมูล แต่ข้อมูลก็จะอยู่ในรูปแบบที่โดน Hash ที่ไม่สามารถนำมาถอดรหัสย้อนกลับเพื่อหาข้อมูลที่แท้จริงได้ และในส่วน OTP ถึงแม้จะอยู่ในรูป Clear text แต่ค่า OTP ก็จะมีอายุใช้งานเพียง 30 - 60 วินาที และจะไม่มีการใช้ซ้ำ โดยจะมีสร้าง OTP ใหม่ เพื่อนำมาใช้งานครั้งถัดไปเรื่อย ๆ ทำให้แม้ดักจับ OTP ไปได้ ก็จะไม่สามารถนำไปใช้งานกับการ login ครั้งถัดไปได้



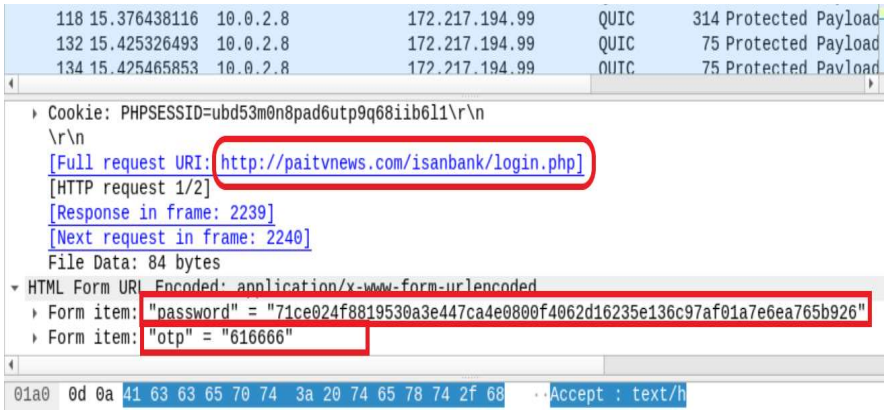
ภาพที่ 4.29 ผล Login User เมื่อถูกโจมตี SSL Strip การบังคับใช้ HTTPS จะถูกปลดออก



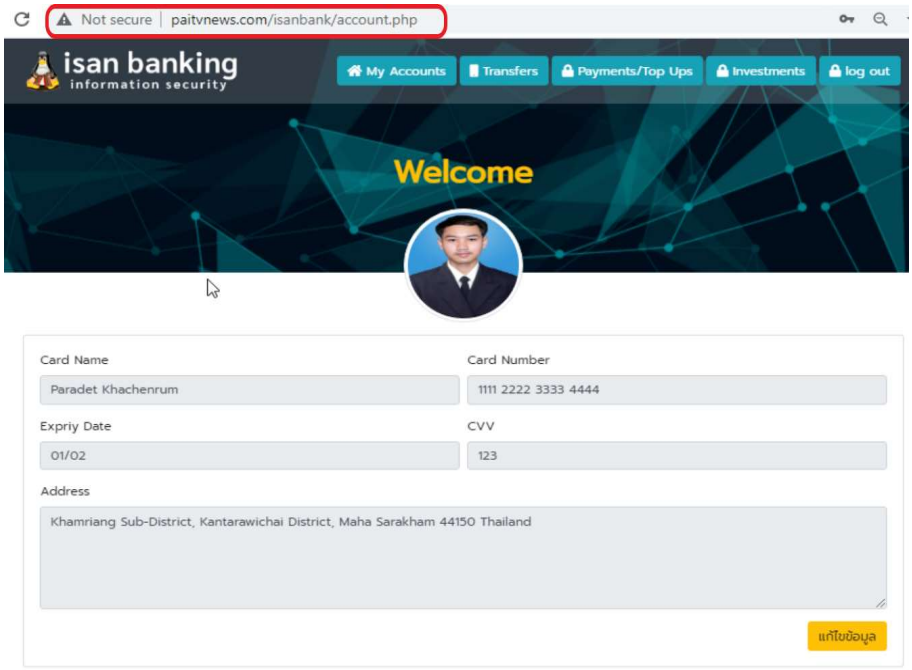
ภาพที่ 4.30 ผลลัพธ์การ Strip และ Sniff หน้า Login Username



ภาพที่ 4.31 ผลหน้า Login Password และ OTP โจมตีด้วย SSL Strip



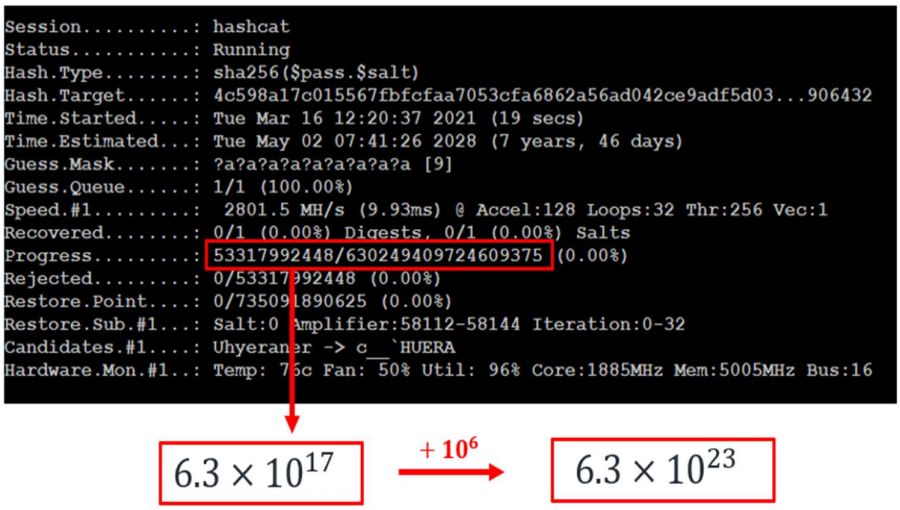
ภาพที่ 4.32 ผลลัพธ์การ Strip และ Sniff หน้า Login Password และ OTP



ภาพที่ 4.33 ผลการ Login เข้าสู่ระบบสำเร็จ

4.8.3 การทดสอบ Brute Force Attack ระบบ ISAN Banking

จากการทดสอบ Brute Force Attack ระบบ ISAN Banking เพื่อถอดค่า Hash ต้องทำการบวกค่า Salt เท่ากับ 10^6 และบวกเข้ากับค่า Hash เดิมจะได้เท่ากับ 10^{23} ดังภาพที่ 4.34 อุปกรณ์ที่ใช้ในการทดลอง Windows 10, CPU Core i5 2320, Ram 4 GB, NVIDIA GeForce GTX 1080 Ti ความเร็วในการถอดรหัสที่ 2801.5 MH/s และใช้โปรแกรม Hashcat ในการ Brute Force Attack จากการคำนวณเพื่อหาระยะเวลาที่ใช้ในการถอดค่า Hash พบว่าต้องใช้เวลาโดยประมาณ 7,130,884 ปี ดังการคำนวณ



ภาพที่ 4.34 ค่า Hash + Salt ของระบบ ISAN Banking

วิธีการคำนวณให้นำค่า Hash and Salt decryption process ÷ Speed of decryption of GTX1080 × SEC × MIN × Hour × Year แทนค่าตามสูตร ดังภาพที่ 4.35

$$\frac{6.3 \times 10^{23}}{2801500000 \times 60 \times 60 \times 24 \times 365} = 7{,}130{,}883.08041$$

ภาพที่ 4.35 เวลาคำนวณถอดค่า hash ระบบ ISAN Banking ด้วย NVIDIA GTX 1080 Ti

จากการศึกษา GPU Farms ของ University of Hong Kong [52] ที่ใช้การ์ดจอ NIVIDA GeForce RTX 2080 Ti ถึง 100 เท่า ซึ่งแต่ละตัวมีความเร็วในการถอดรหัสที่ 5519.1 MH/s นำมาคิดเป็น 100 เท่าจะได้ 5519.1 x 100 = 551,910 MH/s จากการคำนวณตามสเปคดังกล่าว โดยเอาค่า Hash ที่ทดลองก่อนหน้านี้มาเป็นตัวตั้ง จะได้เท่ากับ 6.3×10^{23} นำมาหารกับความเร็วของอุปกรณ์เพื่อหาเวลาที่ใช้ในการ Brute Force Attack ดังตัวอย่างที่แสดงต่อไปนี้

$$\frac{6.3 \times 10^{23}}{551{,}910{,}000{,}000 \times 60 \times 60 \times 24 \times 365} = 36196.4245517$$

ผลปรากฏว่า NIVIDA GeForce RTX 2080 Ti ที่ 100 เท่า จากการคำนวณต้องใช้เวลาในการถอดค่า Hash ประมาณ 36,197 ปี ผลการเปรียบเทียบนี้ชี้ให้เห็นว่าผู้โจมตีที่ใช้อุปกรณ์ดังกล่าวไม่สามารถถอดรหัสได้ทันภายในเวลา 30-60 วินาที ของค่า OTP ที่มีการเปลี่ยนใหม่ไปเรื่อย ๆ

ในการทดสอบเพื่อให้เห็นผลแตกต่างยิ่งขึ้นจึงนำสเปคซุปเปอร์คอมพิวเตอร์จาก IBM [53] คือ IBM Power System AC922, IBM POWER9 22C 3.07GHz, NVIDIA Volta GV100, Dual-rail Mellanox EDR InfiniBand มี 2.28 ล้านคอร์ และความเร็ว 122.3 Petaflop แทนค่าตามสูตรจะได้ดังนี้

$$\frac{6.3 \times 10^{23}}{122.3 \times 10^{15} \times 60 \times 60 \times 24} = 59.6211501772$$

จากผลการคำนวณของซุปเปอร์คอมพิวเตอร์ของ IBM ในการ Brute Force Attack เพื่อถอดค่า hash จะใช้เวลาโดยประมาณ 60 วัน ซึ่งก็ยังไม่สามารถถอดค่า Hash ได้ทันภายในเวลา 30-60 วินาที ของค่า OTP ที่มีการเปลี่ยนใหม่ไปเรื่อย ๆ จึงทำให้การใช้งาน Mobile OTP มีความมั่นคง

สรุปผลการทดสอบจู่โจม Brute Force Attack ต่อรหัสผ่านในรูปแบบ salted-hash password ที่ออกแบบและใช้ในงานวิจัยนี้ พบว่าการโจมตีแม้ใช้คอมพิวเตอร์ที่มีความเร็วสูงมากๆ ก็ต้องใช้เวลานานมากเป็นเดือน เพื่อทำการค้นหารหัสผ่านที่ดักจับได้ ซึ่งประสิทธิภาพที่เพิ่มมานี้ของ salt ทำให้ hashed password ที่ได้ มีความแข็งแกร่งกว่า hashed password ทั่วไปที่อาจถูก Brute Force Attack ด้วย rainbow crack ได้

บทที่ 5
บทสรุป

5.1 สรุปผลการวิจัย

โครงการวิจัยนี้ได้บรรลุวัตถุประสงค์ที่ได้กำหนดไว้ครบทุกประการดังต่อไปนี้

1) วิเคราะห์ปัญหาอาชญากรรม กรณีการกระทำความผิดอาญาในรูปแบบต่าง ๆ ต่อระบบธนาคารอิเล็กทรอนิกส์ที่เกิดขึ้น ทั้งทางเทคนิคความมั่นคงเทคโนโลยีสารสนเทศ และเทคนิคทางกฎหมายที่เกี่ยวกับการสืบสวนสอบสวน

2) วิเคราะห์กฎหมาย ระเบียบ ที่เกี่ยวข้องกับการบริการธนาคารอิเล็กทรอนิกส์ และคดีเทคโนโลยีสารสนเทศ ในประเทศไทยที่มีอยู่ในปัจจุบัน

3) วิเคราะห์เทคนิควิธีทางด้านความมั่นคงเทคโนโลยีสารสนเทศ ที่เกี่ยวข้องกับการโจมตี HTTPS และ PKI

4) บูรณการผลที่ได้ในข้อที่ 1 ถึง 3 เพื่อออกแบบ แนวทางในการติดตาม ตรวจสอบ การกระทำผิดอาญาต่อระบบธนาคารอิเล็กทรอนิกส์

5) ออกแบบและพัฒนาต้นแบบระบบและเทคนิควิธี เพื่อการป้องกันปัญหาอาชญากรรมต่อระบบธนาคารอิเล็กทรอนิกส์

5.2 ผลที่ได้จากการวิจัย

5.2.1 องค์ความรู้ใหม่ที่ได้

1) ในแง่เทคนิคทาง Cyber Security เพื่อการป้องกันระบบ e-banking

1.1) ผลการตรวจสอบการใช้งานกลไก HSTS ที่เป็นเทคโนโลยีที่ใช้ในการป้องกัน SSL Stripping Attack พบว่า เว็บไซต์ธนาคารออนไลน์ในประเทศไทย เว็บไซต์ E-commerce ที่ให้บริการในประเทศไทย หลายแห่งยังมีการปรับใช้กลไก HSTS ไม่ถูกต้อง เนื่องจากทำการตั้งค่า HSTS แบบ None Preload ที่เว็บเซิร์ฟเวอร์แบบเดิมที่ไม่ได้รับการสนับสนุนแล้ว และบางเว็บไซต์แย่ถึงขั้นไม่มีการ Configuration กลไก HSTS เลย ซึ่งจากผลการทดลอง พบมีเพียง 1 เว็บไซต์ธนาคารออนไลน์ในประเทศไทย และ 1 เว็บไซต์ E-commerce ที่มีการ Preload HSTS อย่างถูกต้อง

1.2) การทำงานที่ Web Browser ในปัจจุบัน ไม่สนับสนุนการตั้งค่า HSTS ที่รับค่าจาก HTTP Response Header ที่ส่งผ่านอินเทอร์เน็ตอีกแล้ว เนื่องจากการโจมตีด้วย HSTS Hijacking สามารถทำลายการตั้งค่าของกลไก HSTS ออกได้

1.3) การปรับใช้กลไก HSTS ที่เหมาะสมเพื่อช่วยป้องกัน SSL Stripping Attack ต้องทำการตั้งค่า HSTS แบบ Preload เท่านั้น ซึ่งการตั้งค่า HSTS Configuration ที่ Web Server ไม่มีประโยชน์อีกต่อไป เพราะฝ่าย Hacker สามารถปลดค่า Header HSTS ออกได้

1.4) เว็บไซต์ที่มีการตั้งค่า HSTS แบบ Preload จากผลการทดสอบถึงแม้สามารถป้องกันการโจมตีด้วย SSL Stripping Attack ได้ แต่หากผู้โจมตีในระดับ Professional Hacker ที่มีความเชี่ยวชาญทำการจู่โจมด้วยเทคนิค Homograph Attack ก็ย่อมที่จะสามารถปลดค่ากลไก HSTS แบบ Preload ออกได้

1.5) ระบบตรวจสอบความมั่นคงปลอดภัยของเว็บไซต์ที่ Scan Website เพื่อเช็คว่าป้องกัน SSL Stripping Attack ได้หรือไม่ ใช้วิธีตรวจสอบแค่ HTTP Response Header HSTS จะไม่สามารถเชื่อถือได้ ต้องทำการตรวจสอบในฐานข้อมูล HSTS Preload List เท่านั้น จึงจะได้ผลที่ถูกต้อง

1.6) นอกจากการพึ่งโพรโทคอล HTTPS แล้ว ระบบ online banking web ควรจะต้องมีกลไกชั้นที่สองในการป้องกันการ sniff ข้อมูล ดังจะเห็นได้จากการจู่โจม HTTPS ที่วนเกิดปัญหาขึ้น แก้ไขได้แล้วก็วนกลับมาถูกจู่โจมได้อีกเรื่อยๆ โดยงานวิจัยนี้ได้เสนอกลไกเสริม โดยใช้ Client-Side Script ของเว็บไซต์ในการสร้าง Salted Hash Password โดยร่วมกับการใช้ Mobile OTP บน Mobile Banking App เป็น salt เพื่อช่วยในการ hash รหัสผ่านของ online banking ที่อยู่บนเว็บ

2) ในแง่กฎหมาย คดีและแนวทางการสืบสวนสอบสวนคดี e-banking

ในรายงานได้วิเคราะห์ปัญหาในการสืบสวน สอบสวนคดีทำนองนี้ และได้สรุปแนวทางในการใช้กฎหมายเพื่อการสืบสวนสอบสวนไว้แล้ว (รายละเอียดในบทที่ 4)

หมายเหตุ ทั้งนี้องค์ความรู้ใหม่ได้รับการตีพิมพ์เป็นบทความวิจัยในวารสารวิชาการระดับชาติในฐานข้อมูล Thai Citation Index (TCI) ตามที่กำหนดเป้าหมายไว้แล้ว ดังภาคผนวกที่ 2

5.2.2 ต้นแบบระบบทาง IT

ในงานวิจัยนี้ได้พัฒนาระบบต้นแบบเว็บไซต์ ISAN Banking ที่รักษาความมั่นคงปลอดภัยของข้อมูลด้วย Salted Hash Password ร่วมกับ Mobile OTP เพื่อช่วยป้องกันการถูกดักจับข้อมูลระหว่างการสื่อสารในอินเทอร์เน็ต จากการทดสอบโจมตีด้วยวิธี SSL Striping Attack ที่มีลักษณะการทำงานคือจะบังคับเปลี่ยนแปลงโพรโทคอลในการสื่อสารจาก HTTPS เป็น HTTP ซึ่งทำให้ไม่มั่นคงปลอดภัยระหว่างการสื่อสาร ผลการทดลองพบว่าเว็บไซต์ต้นแบบที่พัฒนาขึ้นสามารถป้องกันการโจมตีดังกล่าวได้ โดยให้ผลลัพธ์คือแฮกเกอร์ที่ทำการโจมตีดักจับข้อมูลจะได้ค่า Hash ที่ไม่สามารถนำไปใช้ประโยชน์ได้

จึงทำให้การสื่อสารของระบบเว็บไซต์ ISAN Banking มีความมั่นคงปลอดภัยจากการถูกโจมตีด้วยวิธี SSL Striping Attack

โดยระบบต้นแบบธนาคารออนไลน์ที่มีการเสริมสร้างความมั่นคงติดตั้งอยู่ที่ https://isanmsu.com/isanbank/

และมีการพัฒนาต้นแบบ Mobile OTP ที่ใช้ร่วมกับระบบนี้ในรูปแบบ Smartphone Application ที่ใช้ระบบปฏิบัติการ Android

ซึ่งระบบดังกล่าวนี้สามารถใช้เป็นต้นแบบสำหรับธนาคารและหน่วยงานต่าง ๆ ในประเทศไทย

5.2.3 แผนการนำไปใช้ประโยชน์จริง

1) แนวทางในการสืบสวน สอบสวน สามารถนำไปใช้ในงานของกองคดีเทคโนโลยีและสารสนเทศ กรมสอบสวนคดีพิเศษ กระทรวงยุติธรรม และหน่วยงานอื่น ๆ ที่เกี่ยวข้องกับคดีการบริการธนาคารอิเล็กทรอนิกส์

2) ภาควิชาวิทยาการคอมพิวเตอร์ คณะวิทยาการสารสนเทศ มหาวิทยาลัยมหาสารคาม ซึ่งเป็นผู้ร่วมวิจัย สามารถนำผลการวิจัยที่เกิดขึ้นไปใช้ประโยชน์ในการสอนในหลายวิชาที่เกี่ยวข้อง เช่น วิชาความมั่นคงไซเบอร์ วิชาความมั่นคงเทคโนโลยีสารสนเทศขั้นสูง และยังใช้ในการวิจัย รวมถึงการให้คำปรึกษากับนิสิตระดับปริญญาตรี โท และเอก โดยงานวิจัยนี้ได้เป็นส่วนหนึ่งในการให้คำปรึกษาและงานวิทยานิพนธ์ระดับปริญญาโทของนายภารเดช คะเชนรัมย์ (นิสิตปริญญาโท วิทยาการคอมพิวเตอร์ มหาวิทยาลัยมหาสารคาม) ซึ่งเป็นผู้ช่วยวิจัยของโครงการวิจัยนี้ด้วย และงานวิจัยต่อยอดจากโครงการวิจัยนี้ ได้ใช้เป็นแนวทางวิทยานิพนธ์ระดับปริญญาเอกของนายคธาวุฒิ จันบัวลา (นิสิตปริญญาเอก หลักสูตรเทคโนโลยีสารสนเทศ มหาวิทยาลัยมหาสารคาม) ซึ่งเป็นผู้ช่วยวิจัยของโครงการวิจัยนี้ด้วย

3) ประชาชนทั่วไป สามารถใช้ประโยชน์จากงานวิจัยนี้ เพื่อตระหนักถึงความมั่นคงปลอดภัยของระบบ e-banking

4) ผลการวิเคราะห์ปัญหา และแนวทางในการป้องกันปัญหาทางเทคนิคความมั่นคงเทคโนโลยีสารสนเทศ และต้นแบบระบบที่สร้างขึ้นในการป้องกัน สามารถนำไปใช้ประโยชน์สำหรับธนาคารและหน่วยงานต่าง ๆ ในประเทศไทย

5.3 แนวทางการวิจัยต่อในอนาคต

แม้ว่างานวิจัยนี้จะประสบผลสำเร็จในการวิเคราะห์ทั้งปัญหาในแนวทางการสืบสวนสอบสวนคดีด้านธนาคารอิเล็กทรอนิกส์ และช่วยแก้ปัญหาทางเทคนิคที่เกี่ยวข้องกับคดีดังกล่าว โดยป้องกันการถูกดักจับข้อมูลที่ถูกโจมตีด้วยวิธี SSL Stripping Attack ที่มิจฉาชีพมักใช้ แต่ก็ยังมีบางประเด็นถึงแม้จะไม่ได้อยู่ในขอบเขตของงานวิจัยนี้ และเป็นแนวทางในการศึกษาวิจัยต่อไปได้ เช่น

1) มาตรฐานความมั่นคงต่าง ๆ ไม่ว่าจะเป็น PKI หรือ TLS ยังมีการเปลี่ยนแปลง ถูกคุกคามโดย Hacker และถูกพัฒนาเพื่อปรับปรุงอยู่ตลอดเวลา ทำให้เมื่อเวลาเปลี่ยนไป Hacker มักหาทางจู่โจมได้อีก ต้องมีการทวนสอบทางเทคนิคเป็นระยะ และมีการติดตามการเปลี่ยนแปลงของเทคโนโลยี รวมถึงวิเคราะห์ระบบ online banking และระบบอื่น ๆ ของทั้งหน่วยงานรัฐและเอกชนในประเทศว่ามีโอกาสถูกโจมตีอีกหรือไม่

2) สิ่งสำคัญที่สุดในทางเทคนิคของการปกป้องระบบที่ศึกษา ยังคงขึ้นอยู่กับ PKI ซึ่งยังมีปัญหาการแทรกแซงของ Evil Certificate Authority ได้ แนวทางที่จะแก้ปัญหาได้ทางหนึ่งคืออาจศึกษาวิจัยเพื่อสร้างระบบ Blockchain ของธนาคารต่าง ๆ ในประเทศไทย หรือของกลุ่มเว็บไซต์ที่ต้องการความมั่นคงปลอดภัยในประเทศไทย เพื่อเข้ามาช่วยเสริมสร้างความมั่นคงปลอดภัย แทนการเชื่อถือ Certificate Authority ในต่างประเทศที่พบว่ามีปัญหา แนวคิดนี้ต้องอาศัยการออกแบบ Distributed Trust Consensus Algorithm ที่เหมาะสมทั้งด้านประสิทธิภาพในการคำนวณและด้านความมั่นคงปลอดภัย เป็นประเด็นวิจัยที่น่าท้าทายอย่างหนึ่งในอนาคต

3) ควรมีการศึกษาข้อกฎหมายต่างประเทศด้าน e-banking ในเชิงเปรียบเทียบกับกฎหมายของไทย เพื่อปรับปรุงกฎหมายไทย หรือนำแนวคิดมาปรับให้เข้ากับบริบทข้อกฎหมายของประเทศไทยต่อไป และอาจพิจารณาความเป็นไปได้ในการจัดให้มีหน่วยงานคล้าย Financial Conduct Agency (FCA) ของยุโรป และแนวคิดในการจัดการที่คล้ายคลึงกัน ในการจัดการปัญหาต่าง ๆ ของ e-banking

บรรณานุกรม

บรรณานุกรมภาษาไทย

[7] ประพจน์ ธรรมศิรารักษ์, สมนึก พ่วงพรพิทักษ์. การวิเคราะห์ปัญหาและทดสอบความมั่นคงของเทคโนโลยีรหัสผ่านแบบใช้ครั้งเดียว. วารสารวิทยาศาสตร์และเทคโนโลยีมหาวิทยาลัยมหาสารคาม มีนาคม–เมษายน 2558; ปีที่ 34 ฉบับที่ 2: หน้า 10-24;

[10] “ธุรกรรมการชำระเงินผ่านบริการ Mobile banking และ Internet banking”. [สืบค้นเมื่อ 24 ตุลาคม 2564]; ได้จาก: http://www2.bot.or.th/statistics/ReportPage.aspx?reportID =688&language=TH.

[25] สมนึก พ่วงพรพิทักษ์, ณัฐวุฒิ ศรีวิบูลย์, อภิรักษ์ ทูลธรรม. การประเมินปัญหาและพัฒนาวิธีแก้ไขปัญหาการโจมตีระบบเว็บไซต์ที่ให้บริการธนาคารทางอินเทอร์เน็ต. งานวิจัยงบประมาณแผ่นดิน: มหาวิทยาลัยมหาสารคาม; 2557.

[34] สมนึก พ่วงพรพิทักษ์, อภิรักษ์ ทูลธรรม. การประเมินวิธีแก้ไขปัญหาการโจมตีด้วยการเปลี่ยนเอสเอสแอล. วารสารเทคโนโลยีสารสนเทศ มกราคม - มิถุนายน 2557; 10[1]: 37-47.

[44] it24hrs.com. “ผู้ใช้มือถือต้องระวัง! ถูกจารกรรมเงินในบัญชีได้ จากการรับ SMS”. [สืบค้นเมื่อ 15 ตุลาคม 2562]; http://www.it24hrs.com.

[45] สมนึก พ่วงพรพิทักษ์. “ระบบรหัสผ่านแบบใช้ครั้งเดียวที่เสริมสร้างความมั่นคง”. รายงานวิจัยสถาบันเทคโนโลยีป้องกันตนเอง (องค์การมหาชน) พ.ศ. 2560.

[53] 10 ซุปเปอร์คอมพิวเตอร์ที่เร็วที่สุดในโลกในปี 2018. [online]. June 2018 [cited 5 October 2021]; https://www.enterpriseitpro.net/world-s-10-fastest-supercomputers/.

[54] คดีพิเศษที่ 74/2559 กรมสอบสวนคดีพิเศษ กระทรวงยุติธรรม

[55] คดีพิเศษที่ 142/2561 กรมสอบสวนคดีพิเศษ กระทรวงยุติธรรม

[56] คดีพิเศษที่ 117-119/2561 กรมสอบสวนคดีพิเศษ กระทรวงยุติธรรม

[60] คณาธิป ทองรวีวงศ์, กฎหมายความผิดเกี่ยวกับคอมพิวเตอร์ เล่ม 1, 2563

[61] กิตติยา พรหมจันทร์ คณะนิติศาสตร์ ม.สงขลานครินทร์ | กฎหมาย 4.0, 28 ตุลาคม 2564 https://www.bangkokbiznews.com/blogs/columnist/968445

[62] สาวตรี สุขศรี, กฎหมายว่าด้วยอาชญากรรมคอมพิวเตอร์และอาชญากรรมไซเบอร์, 2564

[63] พระราชบัญญัติธนาคารแห่งประเทศไทย พุทธศักราช 2485 และที่แก้ไขเพิ่มเติม (ฉบับที่ 7) พ.ศ.2561. [สืบค้นเมื่อ 26 พฤศจิกายน 2564]; https://www.bot.or.th/Thai/AboutBOT/LawsAndRegulations/Pages/Law05.aspx

[64] พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ. 2562. [สืบค้นเมื่อ 26 พฤศจิกายน 2564]; http://www.ratchakitcha.soc.go.th/DATA/PDF/2562/A/069/_____T_0020.PDF

บรรณานุกรมภาษาต่างประเทศ

[1] Rescorla E. HTTP Over TLS. IETF, RFC 2818, May 2000.

[2] Marlinspike M. New Tricks For Defeating SSL In Practice. [online]. 2009 [cited 14 September 2021]; https://www.blackhat.com/presentations/bh-dc-09/Marlinspike/BlackHat-DC-09-Marlinspike-Defeating-SSL.pdf.

[3] Cross-protocol attack on TLS using SSLv2 (DROWN) (CVE-2016-0800). [online]. [cited 1 March 2022]; https://www.openssl.org/news/secadv/20160301.txt.

[4] POODLE: SSLv3 vulnerability (CVE-2014-3566). [online]. [cited 1 October 2021]; https://access.redhat.com/articles/1232123.

[5] Zheng X. Phishing with Unicode Domains. [online]. 14 April 2017 [cited 14 September 2021]; https://access.redhat.com/articles/1232123.

[6] Arnbak A, Asghari H, Eeten M, Eijk N. Security Collapse in the HTTPS Market. Journal of ACM Queue; September 2014; pp. 11–15.

[8] Mulliner C, Borgaonkar R, Stewin P, et al. “SMS-Based One-Time Passwords: Attacks and Defense”. Proceedings of Detection of Intrusions and Malware, and Vulnerability Assessment (DIMVA); 17-19 July 2013; Berlin, Germany. Springer. pp. 150-159.

[9] Perlner P, Fenton J, Burr W, Richer J, Leftkovitz N, Danker J, et al. Digital Identity Guidelines: Authentication and Lifecycle Management. NIST, SP 800-63B, June 2017.

[11] Dierks T, Rescorla E. The Transport Layer Security (TLS) Protocol Version 1.2. IETF, RFC 5246, August 2008.

[12] "PKI System". [cited 10 March 2018]; http://www.cipher.risk.tsukuba.ac.jp/wordpress/wp/content/uploads/2012/02/pki_e.png.

[13] Durumeric Z, Kasten J, Bailey M, J. H. "Analysis of the HTTPS Certificate ecosystem". Proceedings of the conference on Internet Measurement Conference (IMC); New York, USA, 2013.

[14] Hodges J, Jackson C, Barth A. HTTP Strict Transport Security (HSTS). IETF, RFC 6797, November 2012.

[15] Browser Support HSTS. [online]. 1 June 2020 [cited 14 December 2021]; https://caniuse.com/#search=hsts.

[16] HTTP Strict Transport Security. [online]. 2019 [cited 17 September 2021]; https://www.acunetix.com/wp-content/uploads/2019/05/hsts.png.

[17] Burkholder P. SSL Man-in-the-Middle Attacks. [online]. 2002 [cited 25 September 2021]; https://www.sans.org/reading-room/whitepapers/threats/ssl-man-in-the-middle-attacks-480.

[18] Callegati F, Cerroni W, Ramilli M. "Man-in-the-Middle Attack to the HTTPS Protocol". IEEE Security & Privacy Magazine. 7: 78–81.

[19] Driftnet. [computer program]. Version 1.1.5. doko@debian.org; 2015.

[20] Dsniff. [computer program]. Version 2.3. monkey.org; December 2000.

[21] Bettercap. [computer program]. Version 2.26.1. bettercap.org; 2019.

[22] Ettercap. [computer program]. Version 0.8.3. Alberto Ornaghi; July 2019.

[23] Wireshark. [computer program]. Version 3.0.6. Wireshark Foundation; April 2016.

[24] TCPDump. [computer program]. Version 4.9.2.5072. Microolap Technologies LTD; June 2019.

[26] Steube J, Gristina G. Hashcat. [online]. 2020 [cited 14 February 2021]; https://hashcat.net/hashcat/.

[27] transport_security_state_static. [online]. 2019 [cited 4 November 2021]; https://cs.chromium.org/chromium/src/net/http/transport_security_state_static.json.

[28] Fairweather D, Mozer H, Rinehart S, Shin D. "An enhanced approach to preventing the SSLstripping attack". Proceedings of the International Conference on Information and Communication Technology Convergence (ICTC); Jeju, South Korea, 2015; pp. 339-343.

[29] Selvi J. "Bypassing HTTP Strict Transport Security". Proceedings of Black Hat Europe, 14-17 October 2014; Amsterdam, the Netherlands.

[30] Fung A, Cheung K. "SSLock: sustaining the trust on entities brought by SSL". Proceedings of the ACM Symposium on Information, Computer, and Communications Security; 13-16 April 2010; Beijing, China. pp. 204-213.

[31] Fung A, Cheung K. "HTTPSLock: Enforcing HTTPS in Unmodified Browsers with Cached JavaScript". Proceedings of the Network and System Security; 1-3 September 2010; Melbourne, Australia. pp. 269-274.

[32] Puangpronpitag S, Masusai N. "An Efficient and Feasible Solution to ARP Spoof Problem". Proceedings of the 6th International Conference on Electrical Engineering/ Electronics, Computer, Telecommunications, and Information Technology (ECTI-CON); 6-9 May 2009; Pattaya, Chonburi, Thailand. pp. 910-913.

[33] Puangpronpitag S, Sriwiboon N. "Simple and Lightweight HTTPS Enforcement to Protect against SSL Stripping Attack". Proceedings of International Conference on Computational Intelligence, Communication Systems and Networks. 24-27 July 2012; Phuket, Thailand. pp. 229-234.

[35] Sriwiboon N, Puangpronpitag S. Detection & Protection Mechanisms Against SSL Strip Attacks. Proceedings of International Joint Conference on Computer Science and Software Engineering; 30 May-1 June 2012; Bangkok, Thailand. pp. 25-30.

[36] Adams C, Lloyd S. "Understanding PKI: concepts, standards, and deployment considerations". Addison Wesley Professional. 2003; pp. 11-15.

[37] Nikiforakis N, Younan Y, Joosen W. "HProxy: client-side detection of SSL stripping attacks". Proceedings of the international conference on Detection of intrusions and malware, and vulnerability assessment; 8-9 July 2010; Bonn, Germany.
pp. 200-218.

[38] Tooltham A, Puangpronpitag S. Click2Enforce: a Browser Extension to Protect against SSL Stripping Attacks. Information Technology Journal, Vol. 9, No. 2 July - December 2013; pp. 7-13.

[39] Puangpronpitag S. Information Security and Advanced Networks (ISAN). Faculty of Informatics, Mahasarakham University. [online]. 2019 [https://isanmsu.com.

[40] Bank of Thailand. Internet Banking. [online]. [cited 18 November 2021]; https://www.bot.or.th/Thai/Pages/default.aspx.

[41] Kaspersky Lab. ZeuS-in-the-Mobile – Facts and Theories. [online]. 6 October 2011 [cited 24 June 2021]; https://www.securelist.com/en/analysis/204792194/ZeuS_in_the_Mobile_Facts_and_Theories.

[42] Kaspersky Lab. Android Trojan Found in Targeted Attack. [online]. 26 March 2013 [cited 24 October 2021]; https://securelist.com/blog/incidents/35552/android-trojan-found-in-targeted-attack-58.

[43] Mimoso M. Android Banking Trojan Svpeng Goes Phishing. [online]. 5 November 2013 [cited 24 October 2021]; http://threatpost.com/android-banking-trojan-svpeng-goes-phishing/102822.

[46] Google Chrome. [computer program]. Version 79. Google Incorporation; 2020.

[47] Microsoft Edge. [computer program]. Version 85. Microsoft; 2020.

[48] Mozilla Firefox. [computer program]. Version 72. mozilla.org; 2020.

[49] Internet Explorer. [computer program]. Version 11. Microsoft Corporation; 2020.

[50] Safari. [computer program]. Version 13. Apple Incorporate; 2020.

[51] Market Share Statistics for Internet Technologies. [online]. February - September 2020 [cited 14 September 2021]; https://netmarketshare.com.

[52] The University of Hong Kong. HKU CS GPU Farm. [online]. 2021 [cited 25 October 2021]; https://www.cs.hku.hk/gpu-farm/home.

[57] https://www.accenture.com/us-en/insights/financial-services/cost-cybercrime-study-financial-services. [online] [cited 5 December 2021]

[58] https://www.pages.clearswift.com/rs/591-QHZ-135/images/csw-the-unknown-threat-report-guide.pdf?_ga=2.154910584.1515187320.1601680767-547152612.1601680762. [online] [cited 5 December 2021]

[59] “Tesco Bank fined £16.4m by watchdog over cyber-attack”, The Guardian, October 2018. https://www.theguardian.com/business/2018/oct/01/tesco-bank-fined-cyber-attack-fca?fbclid=IwAR2eR1B-Fl1LRObKlUWuF1K6_MrcjZcVTQt4lhLytHqjzDe bhJ2kcZ72S88. [online] [cited 5 December 2021]

ภาคผนวก

ภาคผนวก ก ผลการตีพิมพ์

บทความวิจัย

การวิเคราะห์ปัญหาการทำงานผิดพลาดของกลไกเอชเอสทีเอสและการจู่โจมด้วยการเปลือยเอสเอสแอล

ภารเดช คะเชนรัมย์ ดรุณี พ่วงพรพิทักษ์ และ สมนึก พ่วงพรพิทักษ์*
กลุ่มวิจัยความมั่นคงสารสารสนเทศและเครือข่ายขั้นสูง มหาวิทยาลัยมหาสารคาม
เอกชัย พ่วงพรพิทักษ์
กรมสอบสวนคดีพิเศษ กระทรวงยุติธรรม

* ผู้นิพนธ์ประสานงาน โทรศัพท์ 08 9453 2159 อีเมล: somnuk.p@msu.ac.th DOI: 10.14416/j.kmutnb.2021.07.007
รับเมื่อ 9 มีนาคม 2564 แก้ไขเมื่อ 8 มิถุนายน 2564 ตอบรับเมื่อ 17 มิถุนายน 2564 เผยแพร่ออนไลน์ 29 กรกฎาคม 2564
© 2021 King Mongkut's University of Technology North Bangkok. All Rights Reserved.

บทคัดย่อ

การโจมตีด้วยการเปลือยเอสเอสแอลเป็นหนึ่งในเทคนิคที่รู้จักกันอย่างแพร่หลาย เพื่อโจมตีเว็บไซต์ที่ใช้เอชทีทีพีเอส ดังนั้นกลไกเอชเอสทีเอสจึงได้ถูกนำเสนอและใช้งานเพื่อสยบการโจมตีดังกล่าว แต่อย่างไรก็ตาม จากการศึกษาเมื่อไม่นานมานี้หลายงาน ได้แสดงให้ว่าการโจมตีด้วยการเปลือยเอสเอสแอลเดิมสามารถนำมาใช้โจมตีระบบธนาคารออนไลน์ และเว็บอีคอมเมิร์ซได้ผลอีกครั้งแม้มีการตั้งค่าเอชเอสทีเอสแล้วก็ตาม ดังนั้นงานวิจัยนี้จึงทำการตรวจสอบ และวิเคราะห์หาเหตุผลเบื้องหลังการทำงานล้มเหลวของกลไกเอชเอสทีเอส และการกลับมาโจมตีได้ใหม่ของการโจมตีด้วยการเปลือยเอสเอสแอล เพื่อวิเคราะห์ปัญหาได้ทำการทดลองบนเครือข่ายเพื่อการทดสอบต่อเว็บธนาคารออนไลน์ของไทย 11 ธนาคาร ระบบเว็บอีคอมเมิร์ซ 4 เว็บ และเว็บอาสาสมัครอีก 2 เว็บ และยังมีการวิเคราะห์เอชทีทีพีเรสพอนซีพเฮดเดอร์ และวิเคราะห์สคริปต์ที่แฮกเกอร์ใช้ในการจู่โจม ในที่สุดสาเหตุของปัญหาก็ได้รับการวิเคราะห์และแนวทางในแก้ปัญหาได้ถูกเสนอแนะ

คำสำคัญ: กลไกเอชเอสทีเอส การจู่โจมด้วยการเปลือยเอสเอสแอล ความมั่นคงเว็บ

การอ้างอิงบทความ: ภารเดช คะเชนรัมย์, ดรุณี พ่วงพรพิทักษ์, สมนึก พ่วงพรพิทักษ์ และ เอกชัย พ่วงพรพิทักษ์, "การวิเคราะห์ปัญหาการทำงานผิดพลาดของกลไกเอชเอสทีเอสและการจู่โจมด้วยการเปลือยเอสเอสแอล," *วารสารวิชาการพระจอมเกล้าพระนครเหนือ*, 2564, doi: 10.14416/j.kmutnb.2021.07.007.

วารสารวิชาการพระจอมเกล้าพระนครเหนือ, 2564
The Journal of KMUTNB., 2021

Research Article

Problem Analysis of HSTS Malfunction and SSL Stripping Attack

Paradet Khachenrum, Darunee Puangpronpitag and Somnuk Puangpronpitag*
Information Security & Advanced Network (ISAN) Research Group, Mahasarakham University, Maha Sarakham, Thailand
Egachai Puangpronpitag
Department of Special Investigation (DSI), Ministry of Justices, Bangkok, Thailand

* Corresponding Author, Tel. 08 9453 2159, E–mail: somnuk.p@msu.ac.th
DOI: 10.14416/j.kmutnb.2021.07.007
Received 9 March 2021; Revised 8 June 2021; Accepted 17 June 2021; Published online: 29 July 2021
© 2021 King Mongkut's University of Technology North Bangkok. All Rights Reserved.

Abstract

SSL stripping attack was one of the most notorious techniques to hack HTTPS websites. So, HTTP Strict Transport Security (HSTS) mechanism had been proposed and deployed to subdue the attack. However, a few recent studies have shown that the old SSL stripping attack could be deployed to effectively attack several on-line banking and e-commerce web sites again even with HSTS configuration. Hence, this paper investigates and analyzes reasons behind the malfunction of HSTS and the return of SSL stripping attacks. To analyze the problem, testbed experiments on 11 Thai online banking, 4 e-commerce websites and 2 volunteer websites, an analysis of HTTP response headers and hacker's scripts are done. The cause of problems has finally been analyzed and the solutions are suggested.

Keywords: HTTP Strict Transport Security (HSTS) Mechanism, SSL Stripping Attack, Web Security

Please cite this article in press as: P. Khachenrum, D. Puangpronpitag, S. Puangpronpitag, and E. Puangpronpitag, "Problem analysis of HSTS malfunction and SSL stripping attack," *The Journal of KMUTNB*, 2021 (in Thai), doi: 10.14416/j.kmutnb.2021.07.007.

1. บทนำ

การให้บริการต่างๆ ผ่านเว็บไซต์มีประเด็นที่ต้องให้ความสำคัญ คือ ข้อมูลที่สื่อสารกันระหว่างผู้ใช้งานกับผู้ให้บริการ หรือเว็บเบราว์เซอร์กับเว็บเซิร์ฟเวอร์จำเป็นต้องถูกเข้ารหัสเพื่อป้องกันการถูกดักจับข้อมูล โดยในปัจจุบันเทคโนโลยีสำคัญที่ใช้ คือ HTTPS (Hypertext Transfer Protocol Secure) [1] ซึ่งอาศัยโพรโทคอล HTTP ร่วมกับโพรโทคอล TLS (Transport Layer Security) [2] เพื่อปกป้องข้อมูลระหว่างการสื่อสาร ซึ่ง HTTPS จะอาศัยโครงสร้างพื้นฐานกุญแจสาธารณะ (Public Key Infrastructure: PKI) [3] การเข้ารหัสแบบสมมาตร (Symmetric) และอสมมาตร (Asymmetric) ทำให้ข้อมูลอยู่ในรูปแบบ Cipher Text ที่สามารถป้องกันการถูกดักจับได้

อย่างไรก็ตาม ได้มีเทคนิคที่ใช้โจมตี HTTPS ถูกพัฒนาขึ้นโดยเฉพาะอย่างยิ่งการโจมตีด้วยการเปลือยเอสเอสแอล (SSL Stripping Attack) ซึ่งถูกเสนอโดย Marlinspike และคณะ [4] ตั้งแต่ ค.ศ 2009 โดยจะทำให้การทำงานของโพรโทคอล HTTPS ถูกเปลี่ยนไปเป็น HTTP ที่ไม่มีการเข้ารหัส ผู้โจมตีจึงสามารถดักจับข้อมูลสำคัญ เช่น ชื่อผู้ใช้ และรหัสผ่านได้โดยเทคนิคการโจมตีนี้ มีมิจฉาชีพทั่วโลกรวมถึงในประเทศไทย ได้นำไปใช้ในการก่ออาชญากรรมเพื่อโจมตีระบบธนาคารออนไลน์ (Internet Banking) ระบบการค้าอิเล็กทรอนิกส์ (E-Commerce) และบริการอื่นๆ ที่สำคัญ

ดังนั้น SSL Stripping Attack จึงถือเป็นภัยคุกคามร้ายแรงที่สร้างปัญหาให้กับบริการผ่านเว็บไซต์มายาวนาน มีหลายงานวิจัยได้เสนอแนวทางแก้ไขแต่จากการศึกษาพบว่ายังขาดประสิทธิภาพในการป้องกัน เช่น SSLock [5] พบปัญหาในมาตราฐานการพัฒนาระบบและมีความยุ่งยากในการปรับใช้กับเว็บไซต์ HProxy [6] และ HTTPSLock [7] ทำได้เพียงตรวจสอบการโจมตีไม่อาจป้องกันได้ ระบบ ISAN-HTTPS Enforcer [8] เป็น JavaScript API สำหรับเว็บเซิร์ฟเวอร์เพื่อบังคับการสื่อสารให้เป็น HTTPS ที่ฝั่ง Client โดยเสมือนผู้ใช้พิมพ์ https:// เข้าไปเอง ซึ่งสามารถป้องกันการโจมตีด้วย SSL Stripping Attack ได้ แต่จากงานวิจัย [9] พบว่า ยังถูกโจมตีได้ด้วยการปรับ Python Script ของ SSL Stripping Attack เพื่อปลด JavaScript Tag ของระบบป้องกันนี้ออกได้ และระบบ Click2Enforce [10] เป็น Extension ของ Google Chrome ที่ให้ผู้ใช้เพิ่ม Domain Name ที่ต้องการลงใน List เพื่อบังคับใช้ HTTPS ในการสื่อสารในภายหลัง แต่วิธีนี้ต้องอาศัยความร่วมมือจากผู้ใช้งานมากเกินกว่าที่จะเป็นไปได้โดยทั่วไป ซึ่งหากผู้ใช้งานมีความระวังอยู่แล้ว ก็ย่อมสังเกตตัวสัญลักษณ์กุญแจล็อกของ HTTPS ได้เอง ดังนั้น SSL Stripping Attack ก็ย่อมไม่ใช่ปัญหากับกลุ่มผู้ใช้ดังกล่าว

ปัจจุบันกลไกที่ถูกเสนอให้ใช้ในการป้องกัน SSL Stripping Attack คือ กลไก HSTS (HTTP Strict Transport Security) [11] และยังเป็นหนึ่งในมาตรฐานของ IETF ตามเอกสาร RFC 6797 ซึ่งกลไก HSTS ทำหน้าที่เป็นกลไกส่วนเสริมของโพรโทคอล HTTPS ที่เปิดให้เว็บเซิร์ฟเวอร์ “บังคับ” ให้เว็บเบราว์เซอร์เชื่อมต่อผ่าน HTTPS เท่านั้น แม้ผู้ใช้จะไม่ระบุว่าต้องการใช้ HTTPS ก็ตาม ทำให้เว็บไซต์ที่ต้องการความมั่นคงสูง เช่น ระบบธนาคารออนไลน์ ระบบการค้าอิเล็กทรอนิกส์ มีการปรับใช้อย่างแพร่หลาย

ด้วยการตั้งค่าเพื่อใช้กลไก HSTS ของหลายเว็บไซต์ โดยเฉพาะอย่างยิ่งธนาคารออนไลน์ในประเทศไทย ทำให้ปัญหาการโจมตีด้วย SSL Stripping Attack ดูจะสิ้นสุดลงแล้ว กระทั่งเมื่อเดือนตุลาคม พ.ศ 2562 มีหลายกลุ่มวิจัย เช่น [12] ได้ทำการวิเคราะห์ปัญหาความมั่นคงของเว็บไซต์ทั้งในและนอกประเทศไทย โดยสำรวจเว็บไซต์ที่ให้บริการธนาคารออนไลน์ รวมถึงระบบเซอร์วิสที่สำคัญต่างๆ พบว่า ระบบเว็บไซต์หลายแห่ง โดยเฉพาะอย่างยิ่งธนาคารออนไลน์ ที่ดูเหมือนจะได้รับการป้องกันด้วยกลไก HSTS ไปแล้ว แต่กลับถูกโจมตีได้อีกครั้งทั้งสคริปต์การจู่โจมแบบใหม่ของแฮกเกอร์ที่มีการเผยแพร่ และวิธีการโจมตีด้วยสคริปต์เดิมของ Moxie Marlinspike (ที่ไม่น่าจะได้ผลแล้ว) ดังนั้น SSL Stripping Attack จึงยังกลับมาเป็นภัยคุกคามต่อความมั่นคงของบริการผ่านเว็บไซต์ แม้จะมีการตั้งค่ากลไก HSTS เพื่อป้องกันตามเอกสารต่างๆ [13], [14] ที่มีการเผยแพร่ในอินเทอร์เน็ต

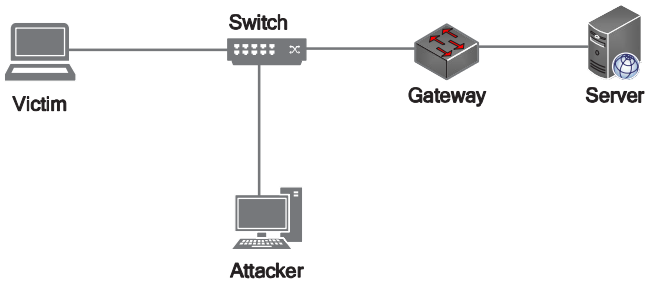
งานวิจัยนี้เป็นความร่วมมือระหว่างทีมผู้วิจัยกับฝ่ายคดีเทคโนโลยีสารสนเทศ กรมสอบสวนคดีพิเศษ กระทรวงยุติธรรม โดยมีจุดมุ่งหมายดังนี้ 1) ตรวจสอบเว็บไซต์ธนาคาร

ออนไลน์ในประเทศว่ายังถูกโจมตีด้วยการเปลือยเอสเอสแอลอยู่หรือไม่? 2) วิเคราะห์ปัญหาความผิดปกติ/ความล้มเหลวของกลไก HSTS และวิเคราะห์การโจมตีของแฮกเกอร์ โดยอาศัย SSL Stripping Attack ด้วยสคริปต์การโจมตีแบบเดิม และใหม่ เพื่อให้เข้าใจสาเหตุที่ SSL Stripping Attack กลับมาโจมตีได้ใหม่อีกครั้ง และ 3) เพื่อเสนอแนวทางการแก้ไขปัญหาป้องกันการถูกโจมตีดังกล่าว โดยผลลัพธ์จากงานวิจัยนี้ จะเป็นส่วนช่วยป้องกันอาชญากรรมทางคอมพิวเตอร์ต่อเว็บไซต์ที่ให้บริการสำคัญต่างๆ ทั้งระบบธนาคารออนไลน์ ระบบการค้าอิเล็กทรอนิกส์ และระบบเซอร์วิสที่สำคัญที่ให้บริการประชาชนอื่นๆ ซึ่งมีความสำคัญต่อเศรษฐกิจ สังคม และการบริหารประเทศในยุคดิจิทัล

2. วัสดุ อุปกรณ์และวิธีการวิจัย

2.1 แรงจูงใจของงานวิจัยนี้

SSL Stripping Attack เป็นภัยคุกคามร้ายแรงที่สร้างปัญหาให้กับระบบเว็บไซต์มายาวนาน มีหลายงานวิจัยที่พยายามเข้ามาแก้ไขปัญหาดังกล่าว จนกระทั่ง HSTS ได้ถูกเลือกใช้เป็นมาตรฐานในการป้องกัน และดูเหมือนว่าปัญหาจะจบลงแล้ว แต่จากการตรวจสอบของหลายงานวิจัยเช่น [12] ในช่วง พ.ศ 2562 พบว่า การโจมตีด้วย SSL Stripping Attack ผ่าน Bettercap Script [15] สามารถโจมตีเว็บไซต์ธนาคารออนไลน์ในประเทศไทยหลายแห่งได้ แม้เว็บไซต์ดังกล่าวมีการปรับใช้กลไก HSTS ในการบังคับการเชื่อมต่อ HTTPS ก็ตาม นอกจากนี้ SSL Stripping Scripts แบบเดิมของ Marlinspike ที่เคยจู่โจมไม่ได้ผลจากการตั้งค่า HSTS ตามคำแนะนำของหลายแหล่ง เช่น [8], [9] ก็กลับมาโจมตีได้ผลอีกครั้ง กอปรกับคดีที่มีการโจมตีระบบธนาคารออนไลน์ได้เกิดขึ้นในประเทศไทยหลายคดี ในช่วงหลายปีที่ผ่านมามีบางคดีได้ถูกกำหนดให้เป็นคดีพิเศษ ทั้งนี้เพราะมูลค่าความเสียหาย ความซับซ้อนของทั้งเทคนิควิธีในการโจมตี และวิธีทางกฎหมายในการสืบสวนสอบสวนคดี ดังนั้น ฝ่ายคดีเทคโนโลยีสารสารสนเทศ กรมสอบสวนคดีพิเศษ กระทรวงยุติธรรม จึงได้ร่วมมือกับทีมวิจัยเพื่อวิเคราะห์ปัญหาดังกล่าวอย่างละเอียด เพื่อเข้าใจปัญหา และเสนอวิธีการแก้ไขทั้งทางเทคนิควิธี และทางกฎหมาย โดยงานวิจัยนี้เป็นส่วนหนึ่งของความร่วมมือดังกล่าวที่มองด้านเทคนิควิธี



รูปที่ 1 Experimental Environment

2.2 เครื่องมือที่ใช้ในการวิจัย

เครื่องเหยื่อ (Victim) ใช้ CPU Intel i5 RAM 8GB โดยมี MS Windows 10 เป็นระบบปฏิบัติการ และใช้ Google Chrome เป็นเว็บเบราว์เซอร์ เครื่องของผู้โจมตี (Attacker) ใช้ CPU Intel i5 RAM 8GB โดยใช้ Kali Linux 2020.1 เป็นระบบปฏิบัติการ พร้อมติดตั้งโปรแกรม Bettercap, Ettercap, ARP Spoofing Tools และสคริปต์ในการจู่โจม SSL/TLS ของ Hacker แบบใหม่ที่แพร่หลายในอินเทอร์เน็ตในช่วง ค.ศ. 2019 และสคริปต์ SSL Strip Attack เดิมของ Marlinspike เพื่อใช้ในการโจมตี

การทดลองทำบน Test-bed มีสภาพแวดล้อมในการทดลองแสดงดังรูปที่ 1 ทั้งแบบ Wireless และ Wired Networks โดยเครื่องผู้โจมตี และเครื่องเหยื่ออยู่ในวง LAN เดียวกัน เครื่องเหยื่อใช้ Google Chrome Browser เพื่อเข้าสู่หน้า Login ของเว็บไซต์ปลายทาง และเครื่องผู้โจมตีทำการแทรกกลางการสื่อสาร ด้วยเทคนิค ARP Poisoning และทำการ SSL Stripping Attack ด้วยสคริปต์ 2 แบบ คือ แบบใหม่ที่ Hacker สร้างขึ้นและแจกใน ค.ศ. 2019 และแบบเดิมของ Marlinspike ที่มีมาตั้งแต่ ค.ศ. 2009 และดักจับข้อมูลด้วย Wireshark

2.3 เว็บที่ใช้ในการทดลอง

เว็บไซต์ที่นำมาทดลองประกอบด้วย เว็บไซต์ธนาคารออนไลน์ในประเทศไทย จำนวน 11 เว็บ เว็บไซต์ที่ให้บริการ

ระบบ E-Commerce 4 เว็บ เว็บไซต์ที่อาสาสมัครร่วมทดสอบ 2 เว็บ (โดยเป็นเว็บไซต์ของกลุ่มวิจัย และทีวีออนไลน์) โดยเว็บไซต์ธนาคารในประเทศไทยทั้ง 11 เว็บ เป็นการเลือกแบบเจาะจงตามความต้องการของกรมสอบสวนคดีพิเศษ เพื่อทราบสถานะภาพความมั่นคงปลอดภัยของธนาคารไทย ณ ปัจจุบันต่อปัญหาภัยคุกคามดังกล่าว และเว็บ E-Commerce ทั้ง 4 เว็บ ก็ถูกเลือกอย่างเจาะจง เนื่องจากเป็นเว็บไซต์ที่มีลูกค้าเป็นคนไทยจำนวนมาก ซึ่งเป็นไปตามความต้องการของกรมสอบสวนคดีพิเศษเช่นกัน เพื่อทราบสถานะการณ์ความมั่นคงปลอดภัยและใช้เป็นข้อมูลในการหาแนวทางการป้องปรามคดีที่จะเกิดในประเทศไทยต่อไป สำหรับเว็บอาสาสมัคร 2 เว็บ ที่ร่วมทดสอบเป็นเว็บของพันธมิตรของกลุ่มวิจัยที่เจาะจงนำมาใช้ทดสอบ เพราะมีความพยายามตั้งค่าเพื่อป้องกันขั้นสูงและใส่กลไกการป้องกันเพิ่มเติม ซึ่งจะสามารถนำมาวิเคราะห์เปรียบเทียบเพื่อเรียนรู้ปัญหา

ทั้งนี้การทดลองกระทำภายใต้การกำกับของนิติกรจากส่วนคดีเทคโนโลยีสารสนเทศ กรมสอบสวนคดีพิเศษ เพื่อไม่ให้ผิดจรรยาบรรณและกฎหมาย โดยไม่มีวัตถุประสงค์เจาะเข้าไปในระบบผู้ให้บริการ หรือก่อให้เกิดผลกระทบต่อการทำงานของระบบผู้ให้บริการแต่อย่างใด เพียงแต่เป็นการทดลองดักจับข้อมูลระหว่างการสื่อสารเท่านั้น โดยใช้เหยื่อที่สมมุติขึ้นและข้อมูลชื่อผู้ใช้และรหัสผ่านที่ทำการทดสอบเป็นของผู้ทดลองเอง หรือเป็นเพียงค่าปลอมที่ตั้งขึ้นที่ไม่ใช่ของจริง

2.4 การวิเคราะห์กลไก HSTS

นอกจากการทดลอง SSL Stripping Attack ในกลุ่มตัวอย่างเว็บไซต์แล้ว เพื่อเข้าใจปัญหาอย่างแท้จริง งานวิจัยนี้ยังทำการ 1) ตรวจสอบและวิเคราะห์ HTTP Response Header ของเว็บไซต์ที่นำมาทดลองว่ามีการตั้งค่ากลไก HSTS หรือไม่อย่างไร 2) ตรวจสอบและวิเคราะห์ HSTS Preload List และ 3) ตรวจสอบและวิเคราะห์ Hacker Scripts ที่ใช้ในการโจมตี

3. ผลการทดลอง

3.1 ผลการตรวจสอบการตั้งค่ากลไก HSTS

การตรวจสอบการตั้งค่ากลไก HSTS ของเว็บไซต์ที่ใช้ในการทดลองทั้ง 17 เว็บไซต์ สามารถทำได้โดยการ Request เว็บไซต์ผ่านเว็บเบราว์เซอร์ จากนั้น Inspect Network แล้วเลือกดูข้อมูล Response Headers ก็จะพบ HSTS Header ดังแสดงรูปที่ 2

รูปที่ 2 ตัวอย่าง HSTS Config. ใน HTTP Header

ตารางที่ 1 ผลการตั้งค่า HSTS ของเว็บธนาคารในไทย

เว็บไซต์*	HSTS		
	Header	Max-Age	Preload
A	Yes	31536000	No
B	Yes	31536000	Yes
C	Yes	31536000	No
D	Yes	31536000	No
E	Yes	16070400	No
F	Yes	15552000	No
G	Yes	No	No
H	ไม่พบ HSTS config.		No
I	ไม่พบ HSTS config.		No
J	ไม่พบ HSTS config.		No
K	ไม่พบ HSTS config.		No

* เพื่อสงวนชื่อธนาคาร จึงใช้อักษรย่อแทนชื่อของธนาคาร

จุดประสงค์ของการตรวจสอบค่า HTTP Header นี้เพื่อดูว่ามีเว็บไซต์ที่หน่วยงานของรัฐต้องการให้สำรวจ ทั้งธนาคารออนไลน์ และ E-Commerce มีการตั้งค่า HSTS เพื่อป้องกันการโจมตีหรือไม่ และตั้งค่าเหมาะสมหรือไม่?

จากตารางที่ 1 หากดูจาก HTTP Header พบว่า 11 เว็บไซต์ของธนาคารออนไลน์ในไทยที่ทดสอบ มี 4 เว็บ ที่ใน Header ไม่พบการตั้งค่า HSTS ซึ่งน่าจะทำให้โดน SSL Stripping Attack ได้โดยง่าย เห็นได้ว่าทั้ง 4 ธนาคาร ในไทยไม่มีการปรับปรุงกลไกการป้องกันโจมตีตามมาตรฐานขั้นต้น ส่วนอีก 3 เว็บ

ธนาคารมีการตั้งค่า HSTS แต่ค่า Max Age Configuration ไม่เหมาะสม (ค่าที่แนะนำโดย Google คือ 31536000 วินาทีขึ้นไป [16]) ซึ่งน่าจะโดนโจมตีได้ และมีเพียง 1 ธนาคาร ที่เหมือนจะตั้งค่า HSTS เป็นแบบ Preload (ที่น่าจะเหมาะสมที่สุด ซึ่งจะได้แสดงผลต่อไป)

ตารางที่ 2 ผลการตั้งค่า HSTS ของเว็บ E-Commerce

เว็บไซต์*	HSTS		
	Header	Max-Age	Preload
L	Yes	47474747	Yes
M	Yes	31536000	No
N	Yes	31536000	No
O	Yes	31536000	No

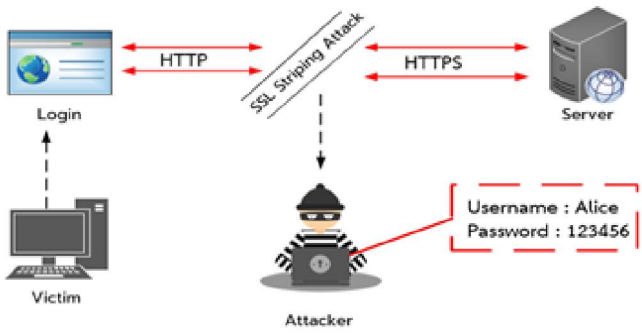
* เพื่อสงวนชื่อ E-commerce Websites จึงใช้อักษรย่อแทน

จากตารางที่ 2 หากดูจาก HTTP Header พบว่า 4 E-Commerce Web Sites มีการตั้งค่า HSTS ทั้ง 4 เว็บ และมีค่า Max-Age ที่เหมาะสม โดยมีเพียง 1 เว็บ คือ L ที่ตั้งค่า HSTS เป็นแบบ Preload (ที่น่าจะเหมาะสมที่สุด)

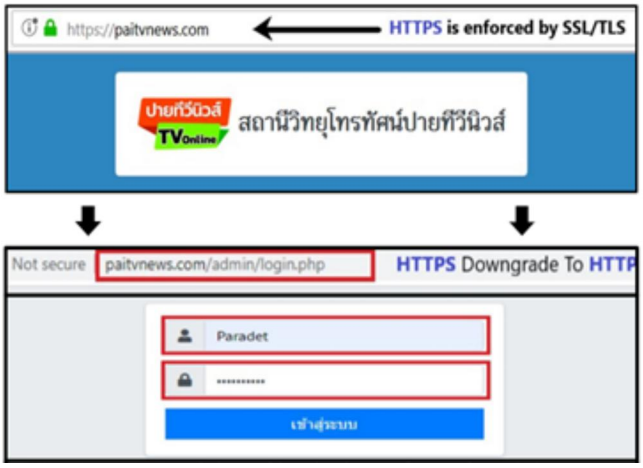
ตารางที่ 3 ผลการตั้งค่า HSTS ของเว็บที่อาสาให้ทดสอบ

เว็บไซต์	HSTS		
	Header	Max-Age	Preload
isanmsu.com	ไม่พบ HSTS config.		No
paitvnews.com	Yes	31536000	Yes

จากตารางที่ 3 หากดูจาก HTTP Header ใน 2 เว็บที่อาสาให้ทดสอบ พบว่า isanmsu.com ใน Response Header ไม่มีการตั้งค่า HSTS config และน่าจะถูก SSL Strip Attack ได้ ส่วน paitvnews.com พบมีการตั้งค่า HSTS เป็นแบบ Preload (ที่น่าจะเหมาะสมที่สุด) และไม่น่าจะถูก SSL Strip Attack ได้ ในขั้นตอนนี้การวิเคราะห์ในเบื้องต้นจะดูเหมือนว่า isanmsu.com ไม่มั่นคงปลอดภัย แต่ paitvnews.com มั่นคงปลอดภัย ซึ่ง 2 เว็บอาสาสมัครนี้ เป็นส่วนที่ร่วมมือกับทีมวิจัย เพื่อจะได้นำไปสู่การวิเคราะห์ในขั้นตอนต่อไปว่าการอ่านค่า Response Header ไม่ใช่วิธีการวิเคราะห์ที่ถูกต้องสมบูรณ์ (ซึ่งจะได้กล่าวต่อไป)



รูปที่ 3 รูปแบบการโจมตีด้วย SSL Stripping Attack



รูปที่ 4 ตัวอย่างผลการ Strip และ Sniff

3.2 ผลการทดลองโจมตีด้วย SSL Stripping Attack

เพื่อให้ทราบว่าการโจมตีด้วย SSL Stripping Attack ต่อกลุ่มตัวอย่างเว็บไซต์ ทั้ง 17 เว็บ มีผลเป็นอย่างไร เป็นไปตามความคาดหวังหลังอ่านค่า HSTS Response Header หรือไม่ จึงได้ทำการทดลอง Strip และดักจับข้อมูล (Sniff) ในหน้า Login เพื่อเก็บชื่อผู้ใช้และรหัสผ่านโดยจำลองการโจมตีบน Test-bed แสดงดังรูปที่ 3 และตัวอย่างผลการโจมตีจริงของเว็บไซต์ paitvnews.com แสดงดังรูปที่ 4

ในการทดลองได้ใช้เครื่องมือโจมตีทั้งสองแบบ คือ SSL Strip Script ดั้งเดิมของ Marlinspike หรือ Ettercap และ Bettercap Script ใหม่ที่ Hacker มีการเผยแพร่ในช่วงประมาณ ค.ศ. 2019 ผลปรากฏว่าทั้งสองสคริปต์ให้ผลลัพธ์ของการทดลองเหมือนกัน ดังแสดงในตารางที่ 4–6

ตารางที่ 4 ผลการโจมตีเว็บไซต์ธนาคารออนไลน์ในไทย

เว็บไซต์*	HSTS		SSL Strip Attack	
	Max-Age	Preload	SSL Strip	Sniff
A	31536000	No	✓	✓
B	31536000	Yes	×	×
C	31536000	No	✓	✓
D	31536000	No	✓	✓
E	16070400	No	✓	×
F	15552000	No	✓	✓
G	Yes	No	✓	✓
H	ไม่พบ HSTS config.		✓	✓
I	ไม่พบ HSTS config.		✓	✓
J	ไม่พบ HSTS config.		✓	✓
K	ไม่พบ HSTS config.		✓	✓

* เพื่อสงวนชื่อธนาคาร จึงใช้อักษรย่อแทนชื่อของธนาคาร

จากตารางที่ 4 จะเห็นว่ามีเพียง 1 ธนาคาร ที่ตั้งค่า HSTS เป็นแบบ Preload ที่ไม่โดน SSL Strip ทำให้ไม่สามารถ Sniff ข้อมูลได้ และมี 10 ใน 11 ธนาคาร ที่หน้าเว็บโดน SSL Stripping Attack ปลด HTTPS ไปเป็น HTTP ได้ โดยใน 10 ธนาคาร ที่ถูก Strip ได้นี้มี 9 ธนาคาร ที่ถูก Sniff รหัสผ่านได้โดยง่าย ดังตัวอย่างแสดงในรูปที่ 5 ทั้งนี้มี 1 ธนาคาร ที่แม้ป้องกัน SSL Strip Attack ไม่ได้ แต่จากการตรวจสอบพบว่า มีกลไกการ Hash Password ทำให้แม้จะโดน Sniff ก็ไม่รู้ว่ารหัสผ่านคืออะไร

ตารางที่ 5 ผลการโจมตีเว็บไซต์ E-Commerce

เว็บไซต์*	HSTS		SSL Strip Attack	
	Max-Age	Preload	SSL Strip	Sniff
L	47474747	Yes	×	×
M	31536000	No	✓	✓
N	31536000	No	✓	✓
O	31536000	No	✓	✓

* เพื่อสงวนชื่อ E-commerce Websites จึงใช้อักษรย่อแทน

จากตารางที่ 5 สำหรับเว็บ E-Commerce จะเห็นว่า 3 ใน 4 เว็บ แม้มีการตั้งค่า HSTS config ด้วยค่า Maxage ที่เหมาะสมเมื่อดูจาก HTTP Response Header แต่ก็โดน

รูปที่ 5 ผลการโจมตี SSL Strip และ Sniff

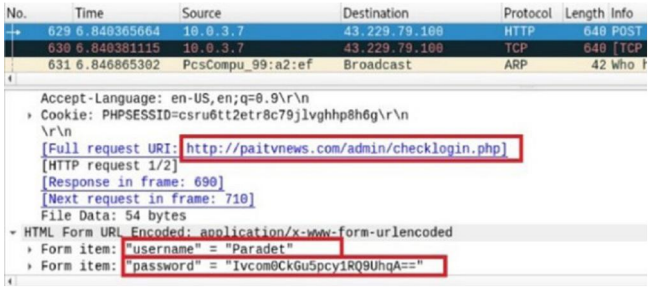
SSL Strip ปลด HTTPS ไปเป็น HTTP ได้ และถูก Sniff รหัสผ่านได้โดยง่าย มีเพียง E-commerce Web L ที่มีการตั้งค่า HSTS Configuration เป็นแบบ Preload ที่ไม่โดน Strip จึงทำให้ไม่สามารถ Sniff รหัสผ่านได้

ตารางที่ 6 ผลการโจมตีเว็บอาสาสมัคร

เว็บไซต์	HSTS		SSL Strip Attack	
	Max-Age	Preload	SSL Strip	Data Sniff
paitvnews.com	31536000	Yes	✓	×
isanmsu.com	ไม่พบ HSTS config.		×	×

จากตารางที่ 6 แสดงผลการโจมตีต่อเว็บอาสาสมัคร 2 เว็บ ได้ผลลัพธ์คือ paitvnews.com ที่เมื่อดูจาก HTTP Response Header เหมือนจะมีการตั้งค่า HSTS แบบ Preload ไว้ซึ่งน่าจะไม่สามารถ Strip ได้ แต่กลับสามารถ Strip HTTPS ไปเป็น HTTP ได้ แต่ที่น่าแปลกใจคือในทางตรงข้าม คือ isanmsu.com ซึ่งเมื่อดูจาก HTTP Response Header เหมือนไม่มีการตั้งค่า HSTS ไว้เลยกลับไม่สามารถ Strip และ Sniff ได้ ซึ่งจะได้วิเคราะห์ในการตรวจสอบขั้นต่อไป

ที่น่าสังเกตอีกอย่างคือ paitvnews.com แม้โดน Strip ได้ แต่มีการแฮชค่ารหัสผ่านไว้ด้วยเทคนิค Salted-Hash Password (SHP) ทำให้ผลการ Sniff ไม่อาจได้ค่ารหัสผ่านไปใช้ประโยชน์ได้ แสดงดังในรูปที่ 6 ซึ่งเหมือนกับเว็บ Online Banking ของธนาคารแห่งหนึ่งในไทยที่แสดงไว้ในตารางที่ 4



รูปที่ 6 Salted-Hash Password

ซึ่งถือเป็นแนวทางป้องกันที่ดี ในกรณีโพรโทคอล HTTPS หลุด รหัสผ่านก็ยังได้รับการป้องกันชั้นที่ 2

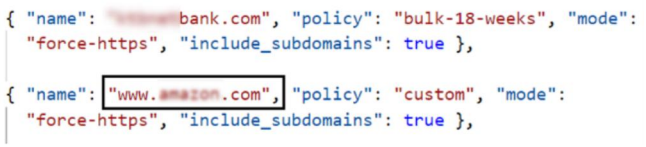
ตารางที่ 7 สรุปผลการโจมตีกลุ่มตัวอย่างทั้ง 17 เว็บ

เว็บไซต์	SSL Strip Attack		
	โจมตีได้	โจมตีไม่ได้	ดักจับไม่ได้
เว็บไซต์ธนาคารในไทย	10	1	2
เว็บไซต์ E-Commerce	3	1	1
เว็บไซต์วิจัยและเว็บไซต์ทีวีออนไลน์	1	1	2

สรุปผลการโจมตีเว็บกลุ่มตัวอย่างที่ใช้ทดลองเป็นไปดังตารางที่ 7 พบว่า SSL Strip Script ใหม่ของ Hacker หรือ Script เดิมของ Marlinspike ก็ให้ผลการโจมตีเหมือนเดิม แต่เป็นที่น่าแปลกใจเพราะเคยมีผลการวิจัย [8], [9] ที่แสดงให้เห็นว่าหลังมีกลไก HSTS เกิดขึ้น SSL Strip เดิมของ Marlinspike ถูกนำมาทดสอบแล้วไม่สามารถเปลือย SSL เปลี่ยน HTTPS ไปเป็น HTTP ได้ และผลของกลุ่มเว็บอาสาสมัคร ยิ่งดูน่าสงสัยเพราะ isanmsu.com ที่ดูจาก HTTP Response Header เหมือนจะไม่มีการคอนฟิก HSTS กลับไม่อาจ Strip ได้ และส่วน paitvnews.com ในทางตรงข้ามที่เหมือนมีการคอนฟิก HSTS แบบ Preload กลับโดน Strip ได้

3.3 ผลการวิเคราะห์ HSTS Preload List

จากประเด็นปัญหาที่พบในตอนท้ายของหัวข้อ 3.2 ผู้วิจัยจึงได้ทำการตรวจสอบข้อมูลเกี่ยวกับการ Preload HSTS และพบว่า เว็บไซต์ที่มีการตั้งค่า HSTS แบบ Preload จะถูกบรรจุไว้ใน List ที่ https://chromium.go oglesource.



รูปที่ 7 List HSTS แบบ Preload ส่วนที่ 1

รูปที่ 8 isanmsu.com อยู่ใน Preload List

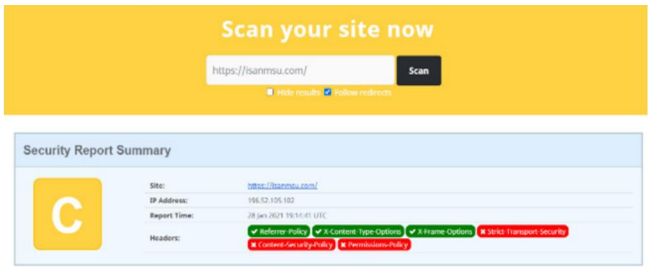
com/chromium/src/net/+/master/http/transport_security_state_static.json และเมื่อเว็บเบราว์เซอร์มีการ Update จะมีการดึงเอา List นี้ไปเก็บไว้ในเบราว์เซอร์

ผลการตรวจสอบ List ดังกล่าวพบว่า เว็บธนาคารออนไลน์ B (ที่มีการตั้งค่าแบบ Preload และไม่ถูก Strip จากการทดลอง) E-commerce Web L (ที่มีการตั้งค่าแบบ Preload และไม่ถูก Strip จากการทดลอง) ล้วนถูกลิสต์ไว้อยู่ใน transport_security_state_static .json ดังแสดงรูปที่ 7 ส่วน paitvnews.com แม้ใน HTTP Response Header เหมือนมีการตั้งค่า HSTS แบบ Preload แต่กลับถูก SSL Strip ได้นั้น ไม่พบชื่อเว็บใน List แต่อย่างใด จึงสรุปได้ว่าแม้มีการตั้งค่า HTTP Header ให้ HSTS เป็น Preload แต่หากไม่ได้ทำการ Preload เข้า List จริง ก็ยังคงถูก SSL Strip ได้

สำหรับ isanmsu.com แม้ไม่พบการตั้งค่า HSTS ใน HTTP Response Header แต่กลับไม่โดน SSL Strip เพราะจากการตรวจสอบ Preload List ดังรูปที่ 8 พบว่า มีการทำ HSTS Preload ไว้

โดยการทดลองก่อนหน้านี้ที่ไม่พบ Header HSTS ของเว็บไซต์ isanmsu.com เพราะหลังลงทะเบียน HSTS Preload เสร็จแล้ว ได้ทำการลบค่า Header HSTS ออก ทำให้สรุปได้ว่า แม้จะลบ HSTS Header หลัง Preload ก็ไม่มีผลในการป้องกัน SSL Strip เพราะ HSTS Header เหมือนจะไม่ได้รับการสนใจเลยด้วยซ้ำจากเว็บเบราว์เซอร์ แต่ดูเหมือนจะอาศัย Preload List แทน

จากการทดลองเว็บที่บริการให้คะแนนความมั่นคงปลอดภัยของเว็บไซต์หลายบริการ เช่น https://security



รูปที่ 9 ผลการ Scan เว็บไซต์ isanmsu.com

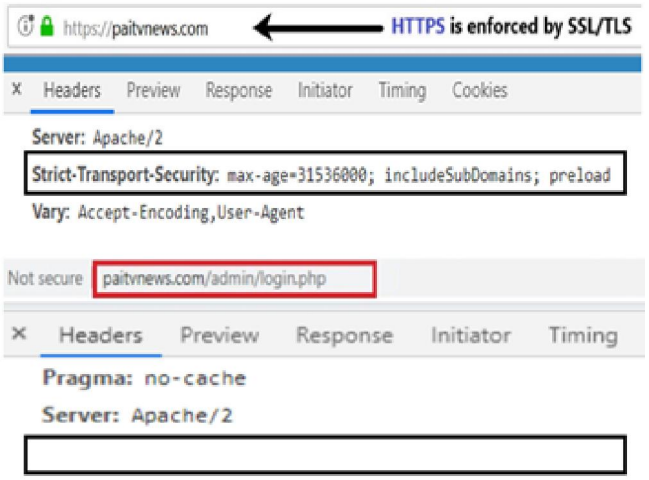
headers.com, www.serpworx.com และ ssllabs.com พบว่า มีข้อผิดพลาดในการวิเคราะห์ HSTS ดังตัวอย่างรูปที่ 9 ที่ให้คะแนน isanmsu.com ว่าไม่ผ่านเรื่อง HSTS เพียงเพราะดูค่าจาก Response Header ทั้งที่เว็บนี้มีความมั่นคงปลอดภัยจาก SSL Stripping Attack ที่ได้ทำ HSTS Preload ไว้และอยู่ใน Preload List เรียบร้อยแล้ว การค้นพบนี้เป็นความรู้สำคัญที่ควรนำไปปรับวิธีการให้คะแนนความมั่นคงปลอดภัยของเว็บไซต์ใหม่

3.4 ผลการวิเคราะห์ Hacker Scripts

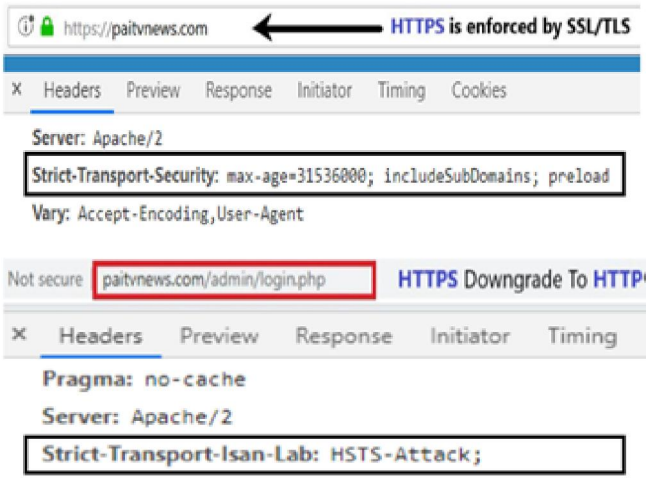
เพื่อให้เข้าใจมากขึ้น จึงได้ทำการตรวจสอบ Scripts ของ Hackers ทั้งแบบเดิมของ Marlinspike และแบบใหม่ของผู้โจมตีที่ใช้ Bettercap จากการศึกษากลไก Script แบบใหม่ พบ Module ที่ชื่อว่า HSTS Hijack ที่ทำให้เข้าใจถึงสาเหตุการล้มเหลวของกลไก HSTS อธิบายดังนี้

HSTS Hijack Module สามารถใช้โจมตีเพื่อลบ HSTS Header ที่ถูกตั้งค่ามาจากเซิร์ฟเวอร์ออกได้ และยังสามารถใช้เพิ่มค่า HSTS Header ตามแต่ Hacker ต้องการหลังแทรกกลางการสื่อสารได้แล้ว

เพื่อให้เข้าใจผลการโจมตีของ Module ดังกล่าว ได้ทำการปรับ Script เพื่อทดลองโจมตี paitvnews.com โดยลบ HSTS Header ที่ตั้งค่ามาจากฝั่งเซิร์ฟเวอร์ออก (ดังแสดงรูปที่ 10) และเพิ่ม HSTS Header เข้าไปโดยที่ไม่มีการตั้งค่ามาก่อนในฝั่งของเซิร์ฟเวอร์ (ดังแสดงรูปที่ 11) สรุปผลได้ว่า Module ดังกล่าวสามารถใช้เพิ่มและลบ HSTS Configuration ได้อย่างง่ายดาย โดยไม่พบว่ามีการแจ้งเตือนความผิดปกติใดๆ จากเว็บเบราว์เซอร์



รูปที่ 10 ผลการ Remove HSTS Header



รูปที่ 11 ผลการ Inject HSTS Header

จากผลการทดลอง โดย Module HSTS Hijacking ทำให้เข้าใจได้ชัดเจนว่า Script ของการจู่โจม SSL Strip Attack แบบใหม่ที่มีการเผยแพร่ในกลุ่ม Hacker ในช่วง ค.ศ. 2019 สามารถนำมาใช้ปรับเปลี่ยนค่าคอนฟิกของกลไก HSTS ที่ตั้งค่ามาจากฝั่งเซิร์ฟเวอร์แล้วส่งผ่านเครือข่ายมายังเว็บเบราว์เซอร์ปลายทางได้หมด ทำให้ส่งผลลบได้ 2 ประการ คือ 1) การตั้งค่า HSTS จากเซิร์ฟเวอร์จะไม่มีประโยชน์อะไรเพราะถูก Hacker ลบออกได้ และ 2) Hacker ยังสามารถจู่โจมโดยการเพิ่มค่า HSTS Configuration ตามที่ตัวเองต้องการเข้าไป ซึ่งสามารถนำไปใช้บังคับให้เว็บไซต์ที่ไม่ใช้และไม่ได้สนับสนุน https ถูกบังคับเป็น https และก่อให้

เกิดการล้มเหลวในการเข้าสู่เว็บไซต์นั้นได้ หรือก็คือ Denial of Service (DoS) Attack เว็บไซต์นั้นได้

ด้วยเหตุนี้ จะเห็นได้จากผลการทดลองก่อนหน้านี้ เว็บเบราว์เซอร์ต่างๆ ได้ทำการยกเลิกการสนับสนุนการทำงานของ HSTS Configuration ที่อยู่ใน HTTP Header ที่ตั้งค่าจากเซิร์ฟเวอร์แล้วส่งผ่านเครือข่ายมายังเว็บเบราว์เซอร์ปลายทางทั้งหมด ดังนั้นแม้มีการตั้งค่าใดๆ ก็ไม่มีผล และจากผลการทดลองและตรวจสอบ Response Header จะเห็นว่ามีเว็บไซต์จำนวนมากยังไม่ทราบปัญหานี้ ซึ่งยังอาศัยการตั้งค่า HSTS ให้ทำงานในฝั่งเซิร์ฟเวอร์ที่ไม่ได้ผลในการป้องกัน

แนวทางที่ถูกต้องในปัจจุบัน คือ หากเว็บใดต้องการบังคับใช้ HSTS เพื่อต่อต้าน SSL Stripping Attack จะต้องทำการ Preload โดยตั้งค่า HSTS Header เป็น Preload แล้วทำการลงทะเบียนกับ https://hstspreload.org เมื่อดำเนินการเรียบร้อยแล้วต้องรอจนเว็บเบราว์เซอร์ Update Version ถึงจะทำการดึงฐานข้อมูล HSTS Preload List ลงมาและสนับสนุนการบังคับใช้ https ของเว็บที่ทำการ Preload ทั้งนี้ HSTS Header ที่ตั้งค่าไว้หลังจากนั้น จะลบออกก็ได้ไม่ได้มีผลต่อการบังคับใช้ https แต่อย่างใด

4. สรุป

จากการทดลองวิเคราะห์ปัญหาการทำงานที่ผิดปกติของกลไก HSTS และการกลับมาโจมตีได้ใหม่ของ SSL Stripping Attack ในการทดลองสามารถสรุปผลได้ดังนี้

1) เว็บไซต์ธนาคารออนไลน์ และเว็บไซต์ E-Commerce หลายแห่งยังใช้งานกลไก HSTS ที่เป็นเทคโนโลยีในการใช้ป้องกัน SSL Stripping Attack ยังไม่ถูกต้อง เนื่องจากตั้งค่า HSTS ที่เว็บเซิร์ฟเวอร์แบบเดิมที่ไม่ได้รับการสนับสนุนแล้ว และบางเว็บไซต์แย่ถึงขั้นไม่มีการ Configuration กลไก HSTS เลย มีเพียง 1 เว็บธนาคารออนไลน์ในประเทศไทยจาก 11 แห่ง และ 1 เว็บ E-commerce จาก 4 แห่ง ที่ทดสอบพบมีการ Preload HSTS อย่างถูกต้อง

2) การจัดการ HSTS ที่เหมาะสมเพื่อช่วยป้องกัน SSL Stripping Attack ต้องทำการ Preload เว็บไซต์ว่าใช้ Strict HTTPS ที่ hstspreload.org ซึ่งการตั้งค่า HSTS Configuration ที่เว็บเซิร์ฟเวอร์ไม่มีประโยชน์อีกต่อไป เพราะฝ่าย Hacker สามารถใช้เทคนิค HSTS Hijacking ในการปลดค่าออกได้

3) เว็บเบราว์เซอร์ในปัจจุบัน ไม่สนับสนุนการตั้งค่า HSTS จาก HTTP Response Header ที่ส่งผ่านอินเทอร์เน็ตอีกแล้ว เนื่องจากเทคนิค HSTS Hijacking สามารถก่อปัญหา DoS ต่อเว็บที่ไม่ใช่ HTTPS ได้ ด้วยเหตุนี้เอง จึงทำให้ SSL Stripping Attack Script เดิมของ Marlinspike ที่ใช้ไม่ได้ผลกลับมาใช้ได้ผลอีกครั้ง

4) ระบบ Scan Website ที่ใช้ตรวจสอบการป้องกัน SSL Stripping Attack ว่าป้องกันได้หรือไม่ ใช้วิธีเช็คแค่ HTTP Header HSTS ไม่ได้ผลอีกอีกต่อไป ต้องทำการตรวจสอบในฐานข้อมูล HSTS Preload List จึงจะได้ผลที่ถูกต้อง

5) จากการทดลอง พบว่ามีบางเว็บไซต์ที่ทำการปรับใช้กลไกป้องกันชั้นที่ 2 คือ Salted-hash password (SHP) ซึ่งเป็นกลไกที่ดีช่วยทำให้ข้อมูลที่ Hacker ดักจับ เช่น รหัสผ่านไม่อยู่ในรูปแบบ Clear Text แม้ Hacker จะ Strip HTTPS เป็น HTTP ได้ ซึ่งวิธีนี้น่าจะเป็นแนวทางที่ควรทำควบคู่ไปกับการ Preload HSTS

ในส่วนของ SHP แม้จะเป็นแนวทางที่ดี แต่ยังมีโอกาสโดนโจมตีด้วย Rainbowcrack [17] ได้ งานวิจัยที่จะทำต่อไปในอนาคต จะได้มีการเสนอวิธีการที่เหมาะสมในการแก้ปัญหาต่อไป

5. กิตติกรรมประกาศ

ขอขอบพระคุณ กรมสอบสวนคดีพิเศษ (DSI) กระทรวงยุติธรรม ในการร่วมวิจัย งานวิจัยนี้ได้รับทุนสนับสนุนส่วนหนึ่งจากทุนวิจัยรายได้ คณะวิทยาการสารสนเทศ มหาวิทยาลัยมหาสารคาม

เอกสารอ้างอิง

[1] E. Rescorla. (2000). *HTTP Over TLS*. [Online]. Available: https://www.rfc-editor.org/info/rfc2818/

[2] E. Rescorla. (2018). *The Transport Layer Security (TLS) Protocol Version 1.3*. [Online]. Available:

https://www.rfc-editor.org/info/- rfc8446/

[3] C. Adams and S. Lloyd, *Understanding PKI: Concepts Standards and Deployment Con Siderations*, Addison Wesley, 2002, pp. 11–15.

[4] M. Marlingspike. (2009, August). New Tricks for Defeating SSL in Practice. Black Hat, USA. [online]. Available: https://www.blackhat.com /presentations/bh-dc-09/Marlinspike/BlackHat-DC-09-Marlinspike-Defeating-SSL.pdf

[5] A. Fung and K. Cheung, "SSLock: Sustaining the trust on entities brought by SSL," in *Proceedings of the ACM Symposium on Information*, 2010, pp. 204–213.

[6] N. Nikiforakis, Y. Younan, and W. Joosen, "HProxy: Client-side detection of SSL stripping attack," in *Proceedings of International Conference on Detection of Intrusions*, 2010, pp. 200–218.

[7] A. P. H. Fung and K. W. Cheung, "HTTPSLock: Enforcing HTTPS in unmodified browsers with cached Javascript," in *Proceedings of Fourth International Conference on Network and System Security*, 2010, pp. 269–274.

[8] S. Puangpronpitag and N. Sriwiboon, "Simple and lightweight HTTPS enforcement to protect against SSL striping attack," in *Proceedings of International Conference on Computational Intelligence, Communication Systems and Networks*, Phuket, Thailand, 2012, pp. 229–234.

[9] S. Puangpronpitag and A. Tooltham "Experimental evaluation of SSL stripping attack solutions," *Information Technology Journal*, vol. 10, no. 1, pp. 37–47, 2014 (in Thai).

[10] A. Tooltham and S. Puangpronpitag, "Click2-Enforce: A browser extension to protect against SSL stripping attacks," *Information Technology Journal*, vol. 9, no. 2, pp. 7–13, 2013 (in Thai).

[11] J. Hodges, C. Jackson, and A. Barth. (2012). *HTTP Strict Transport Security (HSTS)*. [Online]. Available: https://datatracker.ietf.org/doc/html/rfc6797/

[12] S. Puangpronpitag, "Surveys of e-banking web security," Information Security & Advanced Network Research Group, Tech. Rep. 2019-1005, Oct. 2019.

[13] W. Jacqueem. (2021, January). Force HSTS Using htaccess. InMotion Hosting, Virginia Beach. [Online]. Available: https://www.in-motionhosting.com/support/website/force-hsts-using-htaccess/

[14] T. Griffin. (2020, December). How to Enable HTTP Strict Transport Security (HSTS) in WordPress, Griffin Media LLC, United States. [Online]. Available: https://thomasgriffin.com/enable-http-strict-transport-security-hsts-wordpress/

[15] Bettercap. (2019). bettercap Version 2.26.1. [Online]. Available: https://bettercap.org

[16] Google Inc. (2020). *Chromium HSTS*. [Online]. Available: https://hstspreload.org/

[17] RainbowCrack Project. (2020). *RainbowCrack*. [Online]. Available: http://project-rainbowcrack .com/

ประวัติหัวหน้าโครงการวิจัย

นายเอกชัย พ่วงพรพิทักษ์

กองคดีเทคโนโลยีและสารสนเทศ กรมสอบสวนคดีพิเศษ กระทรวงยุติธรรม

E-mail: egachai_p@dsi.go.th **Mobile Phone Number:** 085-951 9898

ประวัติการศึกษา

ที่	เดือน/ปี	วุฒิ/สาขา	สถาบันที่สำเร็จการศึกษา
1	ส.ค. 2550	Certificate Training on Biometrics and Technology Surveillance	The Investigation Bureau Ministry of Justice, Taiwan.
2	พ.ค. 2550	นิติศาสตรมหาบัณฑิต Master of Laws (LL.M.), สาขากฎหมายเอกชนและธุรกิจ	มหาวิทยาลัยธุรกิจบัณฑิตย์
3	มิ.ย. 2548	เนติบัณฑิตไทย สมัยที่ 57	สำนักอบรมศึกษากฎหมายแห่งเนติบัณฑิตยสภา
4	พ.ค. 2544	นิติศาสตรบัณฑิต เกียรตินิยมอันดับหนึ่ง (เหรียญทอง)	มหาวิทยาลัยภาคตะวันออกเฉียงเหนือ

ประสบการณ์การทำงาน

ที่	ปีทำงาน	ตำแหน่ง	สถานที่ทำงาน
1	2547-ปัจจุบัน	พนักงานสอบสวนคดีพิเศษ ระดับชำนาญการพิเศษ	กองคดีเทคโนโลยีและสารสนเทศ กรมสอบสวนคดีพิเศษ กระทรวงยุติธรรม
2	2547-ปัจจุบัน	ที่ปรึกษากฎหมาย	Information Security & Advanced Network (ISAN) Research Group, Mahasarakham University

ที่	ปีทำงาน	ตำแหน่ง	สถานที่ทำงาน
3	2549-2550	อาจารย์บรรยายพิเศษ	วท.ม. เทคโนโลยีสารสนเทศ คณะวิทยาการสารสนเทศ มหาวิทยาลัยมหาสารคาม
4	2546-2547	นิติกรระดับปฏิบัติการ	สำนักความรับผิดทางแพ่ง กรมบัญชีกลาง กระทรวงการคลัง

ประสบการณ์ทำงานที่เกี่ยวข้อง

- ปฏิบัติงานและทำหน้าที่รับผิดชอบงานด้านสืบสวน สอบสวน อาชญากรรมทางด้านเทคโนโลยีและสารสนเทศ เป็นเวลา 18 ปี

- ปฏิบัติงานและทำหน้าที่เกี่ยวข้องกับงานกฎหมาย ระเบียบ ข้อบังคับ โดยเฉพาะกฎหมายที่เกี่ยวข้องกับเทคโนโลยีและสารสนเทศ เป็นเวลา 18 ปี

- (อดีต)ปฏิบัติหน้าที่อีกหน้าที่หนึ่ง สำนักงานรองเลขาธิการคณะกรรมการป้องกันและปราบปรามการทุจริตในภาครัฐ (พันตำรวจเอก ญาณพล ยั่งยืน)

- ปัจจุบันได้รับคำสั่งปฏิบัติหน้าที่เป็นผู้ช่วยเลขานุการคณะอนุกรรมการป้องกันทางเทคโนโลยีสารสนเทศ ตามคำสั่งคณะกรรมการป้องกันและแก้ไขปัญหาคดีความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร ที่ 2/2561 ลงวันที่ 11 พฤษภาคม 2561

ผลงานวิชาการ

- ปัญหาอำนาจไต่สวน และวินิจฉัย ระหว่างสำนักงานคณะกรรมการ ป.ป.ช. กับสำนักงานคณะกรรมการ ป.ป.ท. ภายใต้สังกัดกระทรวงยุติธรรม, บทความวิชาการ, พ.ศ. 2552

- อาชญากรรมทางคอมพิวเตอร์กับบทกฎหมายที่ใช้สำหรับลงโทษผู้กระทำความผิด, วารสารคณะนิติศาสตร์, มหาวิทยาลัยภาคตะวันออกเฉียงเหนือ, มกราคม พ.ศ. 2551

- ปัญหาพนักงานสอบสวนผู้รับผิดชอบในกรณีเกิดการกระทำความผิดเกี่ยวกับคอมพิวเตอร์, บทความวิชาการ พ.ศ. 2551

- ปัญหากฎหมายในการคุ้มครองการทำงาน และผลประโยชน์ตอบแทนของผู้ปฏิบัติงานในสถาบันอุดมศึกษาเอกชน, วิทยานิพนธ์สาขานิติศาสตรมหาบัณฑิต, พ.ศ. 2550

- คู่มือการบริหารจัดการในการเข้าตรวจสถานที่เกิดเหตุคดีเกี่ยวกับอาชญากรรมคอมพิวเตอร์ พ.ศ. 2548, งานวิชาการ สำนักคดีเทคโนโลยีและสารสนเทศ กรมสอบสวนคดีพิเศษ

ประวัตินักวิจัยร่วม

ผู้ช่วยศาสตราจารย์ ดร.สมนึก พ่วงพรพิทักษ์
ภาควิชาวิทยาการคอมพิวเตอร์ คณะวิทยาการสารสนเทศ มหาวิทยาลัยมหาสารคาม
E-mail: somnuk.p@msu.ac.th **Mobile Phone Number: 089-4532159**

ประวัติการศึกษา

ที่	ปี	วุฒิ/สาขา	สถาบันที่สำเร็จการศึกษา
1	ค.ศ. 2003	PhD Computer Networking (ทุน กพ)	University of Leeds, UK
2	ค.ศ. 1999	MSc. Distributed Multimedia System (Distinction), (ทุนรัฐบาลอังกฤษ Chevening Scholarship)	University of Leeds, UK
3	พ.ศ. 2538	วท.บ. วิทยาการคอมพิวเตอร์ (เกียรตินิยม) (ทุน A&H Fujimoto Foundation)	มหาวิทยาลัยขอนแก่น
4	ค.ศ. 2015	Graduate Certification in Tertiary Education Management (ทุนจาก Sweden International Development Agency: SIDA)	LH Martin Institute, University of Melbourne, Australia.

ประสบการณ์การทำงาน

ที่	ปีทำงาน	ตำแหน่ง	สถานที่ทำงาน
1	2541-ปัจจุบัน	อาจารย์และประธานหลักสูตร วท.ม. วิทยาการคอมพิวเตอร์	คณะวิทยาการสารสนเทศ มหาวิทยาลัยมหาสารคาม
2	2547-ปัจจุบัน	หัวหน้ากลุ่มวิจัย	Information Security and Advanced Network (ISAN) Research Group มหาวิทยาลัยมหาสารคาม

ที่	ปีทำงาน	ตำแหน่ง	สถานที่ทำงาน
3	2563-ปัจจุบัน	กรรมการประจำ (ผู้ทรงคุณวุฒิ)	คณะครุศาสตร์ มหาวิทยาลัยนครพนม
4	2557-ปัจจุบัน	กองบรรณาธิการ	วารสารวิทยาศาสตร์ คชสาส์น มหาวิทยาลัยราชภัฏสุรินทร์
5	2552-ปัจจุบัน	กองบรรณาธิการ	วารสารวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยมหาสารคาม
6	2560-2561	Visiting Researcher	School of Computing, Faculty of Engineering, University of Leeds
7	2554-2556	รองคณบดีฝ่ายวิจัยและวิเทศสัมพันธ์	คณะวิทยาการสารสนเทศ มหาวิทยาลัยมหาสารคาม
8	2550-2554	ประธานหลักสูตร วท.ม. เทคโนโลยี สารสนเทศ	คณะวิทยาการสารสนเทศ มหาวิทยาลัยมหาสารคาม
9	2552-2554	ผู้ช่วยคณบดีฝ่ายเทคโนโลยี สารสนเทศ และคณะกรรมการ บริหาร	คณะวิทยาการสารสนเทศ มหาวิทยาลัยมหาสารคาม
10	2551-2554	กรรมการบริหารประจำสำนัก วิทยบริการและเทคโนโลยีสารสนเทศ	มหาวิทยาลัยราชภัฏสุรินทร์
11	2547-2550	ผู้ช่วยผู้อำนวยการด้านวิจัยและ เครือข่าย	สำนักคอมพิวเตอร์ มหาวิทยาลัย มหาสารคาม
12	2547-2550	รองคณบดีฝ่ายวิจัยและวิเทศสัมพันธ์ และคณะกรรมการบริหาร	คณะวิทยาการสารสนเทศ มหาวิทยาลัยมหาสารคาม
13	2547-2554	อาจารย์พิเศษด้านเครือข่ายและความ มั่นคงเทคโนโลยีสารสนเทศ	คณะวิทยาศาสตร์ มหาวิทยาลัยขอนแก่น
14	2538 -2540	วิศวกรระบบคอมพิวเตอร์	บริษัทเงินทุนภัทรธนกิจ (มหาชน) จำกัด

ความเชี่ยวชาญพิเศษ

Cyber Security, Computer Network, Future Internet, IT Crimes, Blockchain and Applied Cryptography

โครงการวิจัยที่เคยได้รับทุนบางส่วน

ชื่อโครงการวิจัย	แหล่งทุนวิจัย
Security Analysis and Performance Enhancement of Software-Defined Network and Named Data Network	The Newton Mobility Grant, UK Royal Academy, UK Government ค.ศ. 2016 – 2018
One Time Password System with Enhanced Security	สำนักงานเทคโนโลยีป้องกันตนเอง (สทป) กระทรวงกลาโหม พ.ศ. 2559-2560
Security Enhancement of One Time Password Technology	วช 2558
MOODLE Extended Development to Enhance the Efficiency of E-learning Systems	วช 2557
Security Enchantment of Open Source IP telephony Packages and Quality Evaluation	วช 2556
Network Access Control for campus	ทุนวิจัยจากบริษัท North East IT พ.ศ. 2554
KhonKaen One Stop Services	ศูนย์ส่งเสริมอุตสาหกรรมซอฟต์แวร์ พ.ศ. 2552-2553
Multicast Reliable Transport Design	ทุนนักวิจัยรุ่นกลาง สำนักงานกองทุนส่งเสริมการวิจัย (สกว.) พ.ศ. 2551-2553
The Design of Multicast Congestion Control: Application to Multimedia and Distributed Databases	ทุนนักวิจัยรุ่นใหม่ สกว. สำนักงานกองทุนส่งเสริมการวิจัย (สกว.) พ.ศ. 2547-2549
Automated Obscenity Web Sites Filtering Systems for Schools	National Electronic & Computer Technologies Center (NECTEC) Grant ค.ศ. 2004-2006

ผลการตีพิมพ์บทความวิจัยบางส่วน

N. Sriwiboon, **S. Puangpronpitag**. “A Novel Access Control Scheme with Immediate Revocation of Access Privileges for Named Data Networking” ICIC Express Letters, Vol. 17, No. 1, January 2023.

T. Chuachan, K. Djemame and **S. Puangpronpitag**, "Solving MTU Mismatch and Broadcast Overhead of NDN over Link-layer Networks", International Journal of Networked and Distributed Computing, Vol. 8, No. 2, March 2020, pp. 67-75.

P. Kasabai, K. Djemame and **S. Puangpronpitag**, "Priority-based Scheduling Policy for OpenFlow Control Plane," KSII Transactions on Internet and Information Systems, vol. 13, no. 2, pp. 733-750, 2019. DOI: 10.3837/tiis.2019.02.04.

S. Puangpronpitag. "One Time Password System with Enhanced Security", Defence Technology Academic Journal. Vol. 1, No. 1, January - April 2019, pp.75-86.

A. Suwannasa, **S. Puangpronpitag**, W. Phongsiri, "A Novel Authentication Scheme for V2I Communication Based on WAVE Unicast Services", International Journal of Distributed Sensor Networks (IJDSN), Volume 2013, Article ID 827084, 2013. doi:10.1155/2013/827084.

S. Puangpronpitag and W. Phongsiri. "Khonkaen One Stop Services: a Thai-Triple-Helix-based project in Taking University Expertise to Serve Provincial ICT Strategies and Promote Software Industry", Procedia - Social and Behavioral Sciences. Vol. 52, 2012, pp. 246-252.

S. Puangpronpitag, T. Chuachan, and P. Pawara. “Classifying Peer-to-peer Traffic using Protocol Hierarchy”, Proceedings of the International Conference on Computer and Information Sciences, Malaysia. June 2014.

R. Sok and **S. Puangpronpitag.** "A Comparative Study on the Safety of Internet Banking Systems between Cambodia and Thailand", MSU Journal of Science and Technology, 35(5):596-608, September-October 2016.