บทที่ ๒

ความทั่วไปว่าด้วยแฮกเกอร์ (Hacker) และการเจาะระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาต

การศึกษาพฤติกรรมของบุคคลกับความรับผิดทางอาญา สิ่งที่จำเป็นจะต้องทราบในเบื้องต้นคือ บุคคลที่ทำการศึกษานั้นคือใครและมีพฤติกรรมหรือการกระทำอย่างไร มิเช่นนั้นแล้วการศึกษาจะเป็นไปในทางที่ไร้ความชัดเจนและผลสุดท้ายอาจก่อให้เกิดปัญหาความไม่เป็นเอกภาพในความเข้าใจของสังคมต่อพฤติกรรมนั้นๆ ด้วยเหตุนี้ในหัวข้อที่จะทำการศึกษาต่อไปจึงเป็นการอธิบายโดยมีจุดประสงค์ ๒ ประการคือ ประการแรกตอบคำถามที่ว่าผู้ที่ทำการศึกษาคือใครและประการที่สอง บุคคลผู้นี้มีพฤติกรรมหรือการกระทำอย่างไร

๑ คำนิยาม

๑.๑ แฮกเกอร์ (Hacker) คือใคร

พฤติกรรมมนุษย์ สามารถแบ่งได้เป็น พฤติกรรมที่แสดงออกให้บุคคลอื่นมองเห็นได้ (overt behavior) และพฤติกรรมที่เกิดขึ้นภายใน (covert behavior)[๑] ซึ่งเป็นสิ่งที่เหนือคาดหมายและยากที่จะจำกัดรูปแบบให้แน่นอน เนื่องจากพฤติกรรมมนุษย์เกิดจากกลไกที่ซับซ้อน และมีองค์ประกอบหลายอย่างเกี่ยวเนื่องสัมพันธ์กัน ซึ่งนอกจากการพิจารณาทางด้านร่างกายและจิตใจแล้ว สภาพสังคมที่มนุษย์อยู่อาศัยก็มีส่วนทำให้พฤติกรรมมนุษย์พัฒนาแตกต่างกัน

แฮกเกอร์เป็นตัวอย่างที่แสดงให้เห็นถึงพฤติกรรมของมนุษย์ที่มีวิวัฒนาการตามธรรมชาติ ซึ่งปรับเปลี่ยนไปตามสภาพแวดล้อมของสังคมในปัจจุบัน สังคมที่เต็มไปด้วยเครื่องมือทางอิเล็กทรอนิกส์ แฮกเกอร์เป็นคำที่ใช้เรียกแทนบุคคลซึ่งมีพฤติกรรมเกี่ยวข้องกับคอมพิวเตอร์ซึ่งเป็นอุปกรณ์ที่ได้รับความนิยมอย่างมากในปัจจุบัน และเป็นคำที่ใช้กันอย่างแพร่หลาย จนกระทั่งอาจกล่าวได้ว่าเป็นการคำที่ถูกใช้อย่างฟุ่มเฟือยโดยขาดหลักเกณฑ์ในการกำหนดคำนิยามที่แท้จริง บ่อยครั้งที่ผู้เขียนได้รับข่าวสารเกี่ยวกับการกระทำความผิดทางคอมพิวเตอร์ โดยเรียกผู้กระทำ

---

[๑] มนุษย์กับสังคม, พิมพ์ครั้งที่ ๒ (กรุงเทพมหานคร:มหาวิทยาลัยเกษตรศาสตร์,๒๕๔๒) หน้า ๒

ความผิดว่า"แฮกเกอร์" แต่ถ้าจะถามว่าแฮกเกอร์หมายความว่าอย่างไรก็คงจะเป็นเรื่องยากที่จะตอบได้ สาเหตุที่เป็นเช่นนี้ เนื่องจากคำว่าแฮกเกอร์เป็นคำที่กลุ่มผู้ใช้คอมพิวเตอร์ตั้งขึ้นจนเป็นที่เข้าใจกันหรือสื่อความหมายได้ภายในกลุ่ม[๒](Jargon) และแม้จะมีการริเริ่มที่จะกำหนดคำนิยามลงไว้ภายในพจนานุกรม ก็เป็นการบัญญัติคำนิยามที่ยังไม่เป็นที่ยอมรับโดยทั่วไป และยังไม่มีการกำหนด คำนิยามที่แน่นอนและสอดคล้องไปในทิศทางเดียวกันว่าการกระทำเช่นไรจึงเรียกผู้กระทำว่า"แฮกเกอร์"

ตัวอย่างที่แสดงให้เห็นถึงความไม่ชัดเจนของคำนิยาม อาจพิจารณาได้จากแบบสอบถามของบุคคลทั่วไปที่เข้าชม Web Site ของสถานีโทรทัศน์ CNN เพื่อให้แสดงความเห็นต่อคำนิยามคำว่าแฮกเกอร์ ของ พจนานุกรม เวบสเตอร์ (Webster 's New World College Dictionary) ที่ให้คำนิยามคำว่า "แฮกเกอร์" หมายถึง*นักคอมพิวเตอร์สมัครเล่นที่มีพรสวรรค์ ที่พยายามที่จะเข้าสู่แฟ้มข้อมูลในหลากหลายระบบโดยไม่ได้รับอนุญาต*[๓] และต่อพจนานุกรมแฮกเกอร์ (The New Hacker's Dictionary) ที่ให้ความหมายของแฮกเกอร์ หมายถึง *บุคคลที่มีความสุขกับการค้นหารายละเอียดเกี่ยวกับระบบของ Programs ต่างๆ และวิธีการที่จะพัฒนาความสามารถของตนเอง พร้อมทั้งเสริมว่า บุคคลที่บุกรุกเข้าสู่ระบบคอมพิวเตอร์คือ แครกเกอร์ (Cracker) ไม่ใช่ แฮกเกอร์ (Hacker)*[๔]

สำหรับคำถามที่ว่า "คุณจะให้คำนิยามของคำว่า"แฮกเกอร์"อย่างไร" (How do you define a hacker?) มีผู้แสดงความคิดเห็นที่หลากหลาย[๕] แต่โดยสรุปแล้วเห็นได้ว่าทุกคนมีความคิดเห็นที่ไม่สอดคล้องกันและเข้าใจความเป็น"แฮกเกอร์" ไม่เหมือนกัน จนกระทั่งไม่สามารถที่จะสรุปแนวทางของคำนิยามได้เป็นเอกฉันท์

---

[๒] โดยเริ่มใช้ในปี ค.ศ. ๑๙๖๐ ที่ สถาบันเทคโนโลยีแห่งเมสซาชูเซตส์ (Massachusetts Institute of Technology) หรือ MIT

[๓] A hacker is "a talented amateur of computers,specifically one who attempts to gain unauthorized access to files in various system

[๔] A person who enjoys exploring the details of programmable systems and how to stretch their capabilities,"adding that those who break into systems are actually "crackers" not "hackers"

[๕] ศึกษารายละเอียดการแสดงความคิดเห็นได้จาก www.cnn.com

๑.๒ สาเหตุที่ทำให้คำนิยามของคำว่าแฮกเกอร์แตกต่างกัน

สาเหตุที่ทำให้คำนิยามของคำว่าแฮกเกอร์แตกต่างกัน ผู้เขียนเห็นว่ามีปัจจัย ๒ ประการที่ทำให้เกิดกรณีดังกล่าว คือ

๑. รูปแบบและวิธีการกระทำความผิดเกี่ยวกับคอมพิวเตอร์มีแนวโน้มหลากหลายมากขึ้น ขณะที่การเรียกชื่อผู้กระทำความผิดยังไม่มีความชัดเจน เมื่อประกอบกับความนิยมในการใช้คำว่าแฮกเกอร์กับผู้มีพฤติกรรมในการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ จึงเป็นการง่ายที่จะถูกเสนอในนาม"แฮกเกอร์" โดยไม่พิจารณาว่าพฤติกรรมนั้นๆ ควรเรียกผู้กระทำว่าแฮกเกอร์หรือไม่ ซึ่งเป็นเหตุให้คำว่าแฮกเกอร์ถูกนำไปใช้ในหลายพฤติกรรมและมีความหมายแตกต่างกัน

๒. การเสนอข่าวของสื่อมวลชนซึ่งเป็นกลุ่มที่มีอิทธิพลต่อความคิดของประชาชนโดยทั่วไป จะใช้คำว่า"แฮกเกอร์"เรียกบุคคลที่มีความเกี่ยวข้องกับการกระทำความผิดทางคอมพิวเตอร์โดยไม่สนใจที่จะกล่าวถึงความหมาย ซึ่งเป็นสาเหตุให้ผู้บริโภคข่าวสารเข้าใจความหมายของคำโดยการอุปมาจากเนื้อความของข่าวขึ้นเองตามความเข้าใจ ส่งผลให้เกิดการแปลความหมายที่แตกต่างกัน

๑.๓ กลุ่มของคำนิยาม

โดยสรุป สาเหตุที่ทำให้เกิดปัญหาการให้คำนิยามที่แตกต่างกันคือความไม่ชัดเจนในความหมายของคำว่าแฮกเกอร์ เหตุนี้เพื่อประโยชน์ในการทำการศึกษาในหัวข้อต่อไป ในเบื้องต้นผู้เขียนจึงได้จัดแบ่งกลุ่มของคำนิยามที่ได้ศึกษามาเป็น ๓ กลุ่ม เพื่อใช้ในการพิจารณาหาความหมายที่เหมาะสม ดังนี้คือ

๑.๓.๑ การให้คำนิยามโดยอาศัยความเห็น

การกำหนดคำนิยามที่อยู่บนพื้นฐานของความคิดเห็นนั้น หากจะเปรียบเทียบเพื่อความเข้าใจก็จะคล้ายกับการออกสัมภาษณ์ผู้คนทั่วไปว่ามีความคิดเห็นต่อความหมายของคำว่าแฮกเกอร์อย่างไร ซึ่งเป็นที่คาดหมายได้ว่าจะได้รับคำตอบที่หลากหลายและมีความเป็นไปได้ที่บางส่วนขัดหรือแย้งกับคำตอบที่ผู้อื่นได้ให้ความหมายไว้ หรือถูกโต้แย้งโดยฝ่ายที่ไม่เห็นด้วย ซึ่งเป็นเรื่องปกติเพราะแต่ละคนอาศัยหลักในการพิจารณาและมีพื้นฐานความรู้แตกต่างกัน ดังเช่น

<u>การให้คำนิยามโดยอาศัยความเห็นว่าการกระทำของแฮกเกอร์ผิดหรือไม่</u>

๑. ฝ่ายที่เห็นว่า การกระทำของแฮกเกอร์เป็นสิ่งผิด จะกำหนดคำนิยามว่า แฮกเกอร์ หมายถึง อาชญากร ผู้บุกรุกเข้ามาในระบบคอมพิวเตอร์ และรวมความถึงผู้กระทำความผิดเกี่ยวกับคอมพิวเตอร์ทั้งปวง

๒. ฝ่ายที่เห็นว่าการกระทำของแฮกเกอร์เป็นเรื่องปกติธรรมดาของผู้ใช้คอมพิวเตอร์ ซึ่งจะพบเห็นคำนิยามในลักษณะนี้เป็นจำนวนมาก ดังเช่น

แฮกเกอร์ หมายถึง โปรแกรมเมอร์ระดับพระกาฬที่ชอบใช้เวลาส่วนใหญ่ไปกับการค้นหารายละเอียดของระบบคอมพิวเตอร์ หรือ เครือข่ายคอมพิวเตอร์[๖]

แฮกเกอร์ หมายถึง บุคคลที่มีความสนใจอย่างมากในระบบคอมพิวเตอร์ที่มีความซับซ้อน[๗]

แฮกเกอร์ หมายถึง ผู้ที่บอกผู้ดูแลระบบคอมพิวเตอร์ว่ามีข้อบกพร่องในระบบคอมพิวเตอร์ของเขาหรือไม่[๘]

แฮกเกอร์ หมายถึง คนธรรมดาที่ต้องการรู้ทุกสิ่งทุกอย่างที่เกี่ยวกับโลก[๙]

<u>การให้คำนิยามโดยอาศัยความเห็นโดยพิจารณาถึงจิตวิญญาณของบุคคล</u> เช่นการให้สัมภาษณ์ของ Emmanuel Glodstein[๑๐] ทางสถานีโทรทัศน์ CNN ที่กล่าวว่า

"การแฮก (Hacking) คือ การตั้งคำถามหลายๆข้อ และปฏิเสธที่จะหยุดตั้งคำถาม และนี่คือเหตุผลที่ทำไมคอมพิวเตอร์จึงเป็นสิ่งที่สมบูรณ์สำหรับผู้ที่ต้องการแสวงหาความรู้ คอมพิวเตอร์จะไม่บอกให้คุณหยุดพูดเมื่อคุณกำลังจะตั้งคำถามต่อไปหรือเมื่อกำลังป้อนคำถาม แต่ไม่อาจจะกล่าวได้ว่าการแฮกจะจำกัดเฉพาะคอมพิวเตอร์เท่านั้น ***บุคคลใดก็ตามที่มีจิตใจที่อยากรู้อยากเห็น จิตใจที่แสวงหาสิ่งท้าทายและความเชื่อในเสรีภาพในการแสดงความคิดเห็นและสิทธิที่จะรับรู้ สิ่งเหล่านี้ก็คือคำนิยามของบุคคลซึ่งมีจิตวิญญาณของความเป็นแฮกเกอร์"***

---

[๖] " แฮกเกอร์คอบ," Internet Tod@y ๒๖ (สิงหาคม ๒๕๔๐): ๕๖.

[๗] อ่านเพิ่มเติมได้ที่ " way to get into (and stay out of) trouble" ,University of Windsor 's websit

[๘] การแสดงความคิดเห็นของผู้ใช้นามว่า Michael Lawson ,ที่ http://www.cnn.com

[๙] ปรัชญญ์ เกิดรัตนชัย ,"Hacker ทำลายหรือสร้างสรรค์ ," BCM (กรกฎาคม ๒๕๔๐) : ๗๗.

[๑๐] editor-in-chief of 2600: The Hacker Quarterly and hosts a weekly radio program in New York called " off the Hood"

คำนิยามที่ได้จากความเห็นดังกล่าว แสดงให้เห็นถึงความเข้าใจของคำว่า แฮกเกอร์ที่แตกต่างและอยู่บนพื้นฐานของความคิดเห็นส่วนตัว ซึ่งเป็นไปได้ว่าคำนิยามที่ได้มีแนวโน้มที่จะขาดความเป็นกลางและโอนเอียงไปตามแนวความคิดของตนเป็นหลักใหญ่ คำนิยามที่ได้จึงไม่อาจยึดถือเป็นหลักในการพิจารณาหรือตัดสินได้ว่า แฮกเกอร์คือใคร เพราะมีโอกาสที่จะได้รับการคัดค้านจากฝ่ายตรงข้ามที่มีความคิดเห็นขัดแย้ง อีกทั้งไม่สามารถที่นำมาใช้ในการพิจารณาเรื่องความรับผิดในทางอาญา เนื่องจากความไม่ชัดเจนของความหมายและการกระทำ

๑.๓.๒ การให้คำนิยามที่กำหนดโดยอาศัยเจตนาของการกระทำ

การกำหนดคำนิยามในกลุ่มนี้จะกำหนดคำนิยามโดยแยกกันระหว่างแฮกเกอร์ที่มีเจตนาดีและเจตนาร้ายออกจากกันโดยสิ้นเชิง และจะไม่เรียกแฮกเกอร์ที่มีเจตนาดีว่าแฮกเกอร์แต่จะเรียกว่า แครกเกอร์ (Cracker) แทน

<u>แฮกเกอร์ที่มีเจตนาดี</u> หมายถึง แฮกเกอร์ที่เข้าสู่ระบบคอมพิวเตอร์ด้วยความตั้งใจที่จะปฏิบัติหน้าที่ที่ก่อให้เกิดคุณค่าแก่สังคม ประโยชน์สาธารณะ ซึ่งแฮกเกอร์เหล่านี้จะเป็นที่รู้กันในฐานะ "The Modern Day Robin Hood."[๙๙]

<u>แฮกเกอร์ที่มีเจตนาชั่วร้าย</u> หมายถึง แฮกเกอร์ที่เข้าสู่ระบบคอมพิวเตอร์ด้วยความตั้งใจที่จะลงโทษ ทำลาย ก่อวินาศกรรมต่อระบบคอมพิวเตอร์ และหรือ แฟ้มข้อมูลในระบบคอมพิวเตอร์

คำนิยามโดยอาศัยหลักเกณฑ์ข้อนี้ ถือว่าเป็นหลักเกณฑ์ที่แบ่งแยกได้ค่อนข้างชัดเจนว่าแฮกเกอร์คือบุคคลประเภทใด นอกจากนั้นยังได้รับการสนับสนุนจากผู้ที่เรียกตนเองว่าแฮกเกอร์ แต่เนื่องจากความนิยมในการที่จะใช้คำว่าแฮกเกอร์ ทำให้ปัจจุบันเกิดความสับสนในการใช้คำพูดในการเรียกบุคคล ซึ่งอาจจะเป็นเพราะขาดความเข้าใจในความหมายที่กำหนดไว้ เป็นเหตุให้บุคคลทั่วไปไม่ได้เรียกแฮกเกอร์ที่มีเจตนาชั่วร้ายว่า แครกเกอร์ แต่ยังคงเรียกติดปากกันว่าแฮกเกอร์ต่อไป หรืออาจกล่าวได้ว่าคนส่วนใหญ่ไม่ทราบว่าแครกเกอร์ต่างจากแฮกเกอร์อย่างไร แต่

---

[๙๙] Forester,Tom,&Perry Morrison,"Computer Ethics:Cautionary Tales and Ethical Dilemmas in Computing" (1990) :49-50 อ้างถึงใน Jeanie Konstantinou,"Computer Hacker:invasion of computer systems,computer and the law ," Friday,December 8 ,1995, INTERNET http://wing.buffalo.edu/law/complaw/complawpapers/konst.html

เรียกรวมการกระทำความผิดที่เกี่ยวข้องกับเครื่องคอมพิวเตอร์ว่าเป็นแฮกเกอร์รวมไปหมด นอกจากนั้นในการกำหนดคำนิยามโดยอาศัยหลักเกณฑ์นี้อาจก่อให้เกิดปัญหาได้ ๒ ประการคือ

๑. ถ้าบุคคลใดเริ่มเจาะเข้าระบบคอมพิวเตอร์ด้วยเจตนาดี ตั้งใจปฏิบัติหน้าที่เพื่อประโยชน์สาธารณะ (เจตนาดี) แต่ไม่ว่าด้วยเหตุใดก่อให้เกิดความเสียหาย (ซึ่งเป็นลักษณะของแครกเกอร์) หรือ ถ้าบุคคลใดเจาะระบบคอมพิวเตอร์โดยไม่ก่อให้เกิดคุณค่าแก่สังคมหรือประโยชน์แก่สาธารณะ (ซึ่งเป็นลักษณะของแฮกเกอร์)และขณะเดียวกันก็ไม่มีเจตนาชั่วร้ายที่จะตั้งใจทำลายหรือก่อวินาศกรรม เหตุดังนี้จะเรียกบุคคลดังกล่าวว่าแฮกเกอร์ หรือจะเรียกว่าแครกเกอร์

๒. เป็นการยากที่จะแยกให้เห็นโดยชัดแจ้งว่าแฮกเกอร์มีเจตนาเช่นไร เนื่องจากเป็นความรู้สึกภายในที่ไม่ได้แสดงออกมาภายนอก ดังเช่นหากกล่าวว่า นาย ก.คือแครกเกอร์ที่มีเจตนาชั่วร้าย นาย ก. อาจปฏิเสธได้ว่าตนไม่ได้มีเจตนาชั่วร้าย แม้ว่าผลที่เกิดจากการกระทำอาจก่อให้เกิดความเสียหาย

๓. ปัญหาเรื่องเจตนาทางด้านกฎหมายอาญา คำว่าเจตนาในมาตรา ๕๙ ไม่ได้ระบุว่าต้องเป็นเจตนาชั่วร้าย ดังนั้นจึงต้องเข้าใจให้ดีว่า เจตนาตามกฎหมายอาญา ตามมาตรา ๕๙ นี้เป็นเพียงเจตนากระทำความผิด (criminal intention) ตามที่กฎหมายบัญญัติซึ่งเป็นความไม่ดีอยู่ในตัวแล้ว เพราะกฎหมายมีไว้เพื่อความเป็นระเบียบของชุมชน และต้องแยกออกจากเรื่องของมูลเหตุชักจูงใจอันเป็นความสำนึกส่วนตัวซึ่งโดยทั่วไปไม่มีผลทางกฎหมาย เช่นจำเลยรับจ้างสีข้าวโดยคิดค่าจ้างเล็กน้อย เพื่อให้ชาวบ้านมีข้าวสารกิน ไม่เป็นข้อแก้ตัวให้พ้นความผิดตามพระราชบัญญัติค้าข้าวที่ต้องขออนุญาตก่อน[๑๒] ดังนั้นทางด้านกฎหมายเมื่อการกระทำของแฮกเกอร์ครบองค์ประกอบความผิดในส่วนเจตนาตามกฎหมายแล้ว ความผิดจึงอยู่ที่แฮกเกอร์กระทำโดยรู้สำนึกและประสงค์ต่อผลหรือเล็งเห็นผลของการกระทำนั้น ส่วนมูลเหตุจูงว่าจะกระทำเพราะมีเจตนาดีหรือเจตนาร้าย ไม่ทำให้การกระทำที่เป็นความผิดนั้นไม่เป็นความผิด การแยกแฮกเกอร์ว่าหมายถึงผู้กระทำที่มีเจตนาดีหรือเจตนาร้ายจึงไม่มีผลทางกฎหมาย

---

[๑๒] ทวีเกียรติ มีนะกนิษฐ,กฎหมายอาญา หลักและปัญหา (กรุงเทพมหานคร:สำนักพิมพ์นิติธรรม,๒๕๔๐),หน้า ๖๗.

๑.๓.๓ การให้คำนิยามโดยอาศัยลักษณะการกระทำ

จากการศึกษาเกี่ยวกับแฮกเกอร์นั้น จะพบว่าแฮกเกอร์ถูกนำมาใช้แทนลักษณะของการกระทำในหลายรูปแบบ ดังเช่น การปล่อยไวรัสคอมพิวเตอร์ การลักลอบใช้บริการโทรศัพท์ การเจาะระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาต เป็นต้น ดังนั้นผู้ให้คำนิยามในหมวดนี้จะกำหนดคำนิยามของแฮกเกอร์ตามลักษณะของการกระทำว่าหมายถึง ผู้ปล่อยไวรัสคอมพิวเตอร์ ผู้ลักลอบใช้บริการโทรศัพท์ หรือหมายถึงผู้เจาะระบบคอมพิวเตอร์ ตามลักษณะของการกระทำนั้นๆ หรืออาจจะมีการเรียกรวมกันว่าผู้ก่อกวนระบบคอมพิวเตอร์

ภายหลังจากทำการศึกษาคำนิยามทั้ง ๓ หมวดแล้ว เราไม่สามารถที่จะนำคำนิยามทั้ง ๓ ซึ่งมีความหลากหลายทางความคิดมากำหนดเป็นคำนิยามรวมกันได้ทั้งหมด เพราะคำนิยามนั้นต้องมีความชัดเจน โดยเฉพาะการศึกษาในส่วนที่เกี่ยวข้องกับวิธีการทางนิติบัญญัติ มิฉะนั้นแล้วจะส่งผลให้เกิดความยากลำบาก ดังคำกล่าวของท่านอาจารย์หยุด แสงอุทัยที่ว่า

"ในการบัญญัติกฎหมาย ถ้ากฎหมายใช้คำซึ่งมีความหมายตามที่เข้าใจกันอยู่ตามธรรมดาก็ไม่จำต้องมีบทนิยาม (definition) แต่ถ้ากฎหมายใดจะใช้ถ้อยคำให้มีความหมายแตกต่างกับที่เข้าใจกันอยู่โดยปกติแล้ว กฎหมายนั้นๆ ก็จะบัญญัติบทนิยามไว้โดยจำกัดความหมายของถ้อยคำที่ใช้เพื่อให้ตรงกับเจตนารมณ์ของกฎหมาย[๑๓]....."

ผู้เขียนในฐานะเป็นผู้ที่ทำการศึกษาในเรื่องความรับผิดของแฮกเกอร์ จึงจำเป็นต้องหาความเป็นหนึ่งเดียวของคำนิยาม ที่สร้างความกระจ่างแก่ผู้ต้องการศึกษาต่อไป และเมื่อพิจารณาถึงข้อบกพร่องในการกำหนดคำนิยามตามความคิดเห็นและการกำหนดคำนิยามโดยอาศัยเจตนาของการกระทำ หลักเกณฑ์การให้คำนิยามโดยอาศัยลักษณะการกระทำจึงเป็นหลักเกณฑ์ที่ผู้เขียนเห็นด้วยในการนำมาเป็นแนวทางในการกำหนดคำนิยามของคำว่าแฮกเกอร์ และมีความเป็นไปได้ในการนำมาพิจารณาประกอบกับขอบเขตของวิทยานิพนธ์ฉบับนี้ซึ่งมีสมมุติฐานในการกำหนดให้การแรกเข้าไปในระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาตเป็นความผิดอาญา ดังนั้น ผู้เขียนจึงกำหนดคำนิยามคำว่าแฮกเกอร์โดยพิจารณาลักษณะการกระทำของแฮกเกอร์เป็นหลัก ซึ่งคือกิริยา

---

[๑๓] หยุด แสงอุทัย ,กฎหมายอาญาภาค ๑ ,พิมพ์ครั้งที่ ๑๗ (กรุงเทพมหานคร: สำนักพิมพ์มหาวิทยาลัยธรรมศาสตร์,๒๕๔๐), หน้า ๒๕๕.

การเจาะระบบคอมพิวเตอร์ (Hacking) หรือเข้าสู่ระบบคอมพิวเตอร์ โดยเป็นการเจาะระบบคอมพิวเตอร์ที่กระทำโดยไม่ได้รับอนุญาตจากเจ้าของระบบคอมพิวเตอร์ เพราะหากการเข้าสู่ระบบคอมพิวเตอร์ได้รับอนุญาตโดยถูกต้องแล้ว ก็เปรียบเสมือนผู้ใช้เครื่องคอมพิวเตอร์ทั่วไปที่สามารถใช้เครื่องคอมพิวเตอร์ได้ตามปกติและคงไม่เรียกผู้ใช้คอมพิวเตอร์ทั่วไปว่าแฮกเกอร์เป็นแน่

ผู้เขียนเห็นว่าการให้คำนิยามคำว่าแฮกเกอร์ โดยพิจารณาจากการกระทำดังกล่าวนี้ จะเป็นหนทางที่ได้รับการยอมรับและสอดคล้องกับความเข้าใจของบุคคลทั่วไปเมื่อกล่าวถึงแฮกเกอร์ การให้คำนิยามในลักษณะเช่นนี้อาจไม่ครอบคลุมการกระทำทุกอย่างของแฮกเกอร์ที่ปรากฏขึ้นในปัจจุบัน แต่ถึงอย่างไรก็ตามต้องทำความเข้าใจเสียก่อนว่า การใช้คำว่าแฮกเกอร์ในปัจจุบันถือว่าเป็นการใช้คำที่แพร่หลายและกว้างจนเกินไป ดังนั้นจึงสมควรจำกัดการเรียกขานแฮกเกอร์ให้อยู่ภายในวงจำกัดของการเจาะระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาตเท่านั้น ไม่ควรจะนำเป็นเรียกให้รวมถึงการกระทำอื่นๆ เพียงเพราะว่าผู้กระทำมีความรู้คอมพิวเตอร์ หรือใช้คอมพิวเตอร์ได้อย่างเชี่ยวชาญ โดยถือว่าเป็นแฮกเกอร์รวมไปหมด ดังนั้นต่อจากนี้ไป ผู้เขียนจึงขอใช้คำว่าแฮกเกอร์ให้หมายถึง ***บุคคลผู้เจาะระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาต*** ซึ่งจะสอดคล้องกับการให้คำนิยามที่กล่าวถึงแฮกเกอร์ในพจนานุกรม เช่น

Hacker: a talented amateur of computers, specifically one who attempts to gain unauthorized access to files in various systems[๑๔] หรือ

Hacker

a: one who is proficient at using or programming a computer; a computer buff

b: one who illegally enters anothers electronic system,as to gain secret information.[๑๕]

เมื่อพิจารณาการให้คำนิยามต่างๆที่กล่าวมา จะทำให้เห็นความแตกต่างประการหนึ่งระหว่างพจนานุกรมฉบับต่างๆและผู้ใช้หรือผู้ที่เกี่ยวข้องกับคอมพิวเตอร์ในการกำหนดคำนิยามคือ ในพจนานุกรมต่างๆจะมองถึงลักษณะการกระทำที่แสดงออกมาภายนอกของบุคคลนั้นๆ ว่ากระทำอย่างไร ขณะที่ผู้ใช้หรือเกี่ยวข้องกับคอมพิวเตอร์จะให้คำนิยามโดยให้ความสำคัญที่จิตใจ จิตวิญญาณหรือความนึกคิดของผู้กระทำมากกว่าที่จะไปมอง ทางด้านผลที่ปรากฏออกมาจากการกระทำนั้นๆ

---

[๑๔] Webster 's New World College Dictionary

[๑๕] The American heritage college dictionary 3rd edition

๑.๔ ผู้เจาะระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาต

ภายหลังจากกำหนดให้แฮกเกอร์ซึ่งเป็นคำในภาษาต่างประเทศหมายถึง ผู้เจาะระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาตในภาษาไทยแล้ว เพื่อความเข้าใจที่ตรงกันเมื่อใช้คำว่าผู้เจาะระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาตแทนคำว่าแฮกเกอร์ จึงจำเป็นต้องพิจารณาความหมายภายในองค์ประกอบของคำ โดยแยกพิจารณาได้ดังนี้ คือ

๑.๔.๑ ระบบคอมพิวเตอร์ (Computer system)

ระบบคอมพิวเตอร์[๑๖] คือ องค์ประกอบทางคอมพิวเตอร์ที่ทำงานประสานกันเพื่อจัดการกับข้อมูลให้ได้ผลลัพธ์ออกมาในรูปแบบตามที่ต้องการ ประกอบด้วย[๑๗]

๑. ฮาร์ดแวร์ (Hardware) คือ ส่วนประกอบของเครื่องคอมพิวเตอร์ที่มองเห็นและสัมผัสได้ เช่น คีย์บอร์ด จอภาพ ตัวเครื่องคอมพิวเตอร์

๒. ซอฟต์แวร์ (Software) คือชุดคำสั่งงานให้เครื่องคอมพิวเตอร์ทำงานตามขั้นตอนที่วางไว้ เพื่อให้ได้ผลงานตามที่ผู้ใช้คอมพิวเตอร์ต้องการ

๓. ข้อมูล (Data) คือ ข้อเท็จจริงที่เกิดขึ้น และเป็นสิ่งที่ต้องการนำมาประมวลผลด้วยคอมพิวเตอร์เพื่อให้กลายเป็นสารสนเทศ (information)

๔. วิธีการปฏิบัติงาน (Procedure) คือ ขั้นตอนการทำงานซึ่งเราเป็นผู้กำหนดให้เครื่องคอมพิวเตอร์จัดการกับข้อมูล เช่น การกรอกข้อมูล

๕. บุคลากรทางคอมพิวเตอร์ (Peopleware) คือผู้ทำหน้าที่จัดการให้องค์ประกอบทั้ง ๔ ข้างต้นมาทำงานประสานกันจนได้ผลลัพธ์ออกมา หรืออาจกล่าวได้ว่าเป็นผู้ที่ทำงานทางด้านคอมพิวเตอร์โดยเฉพาะ ซึ่งมีหน้าที่แตกต่างกันไปตามลักษณะงาน

---

[๑๖] ฉัตรชัย กางกั้นและอรรณพ กางกั้น ,คอมพิวเตอร์ศาสตร์.(กรุงเทพมหานคร: บริษัท แคนเน็ดบุ๊ค จำกัด, ๒๕๔๐),หน้า ๗-๘.

[๑๗] โดยทั่วไปแล้วระบบคอมพิวเตอร์ประกอบไปด้วยองค์ประกอบใหญ่ ๓ องค์ประกอบคือ ฮาร์ดแวร์ ซอฟแวร์ และผู้ใช้ การแบ่งองค์ประกอบออกเป็น ๖ ประการดังแสดงไว้ เป็นการขยายการอธิบายองค์ประกอบของระบบคอมพิวเตอร์ให้แยกย่อยมากขึ้นเท่านั้นเอง

๖. เครือข่ายการสื่อสาร (Communication) คือการเชื่อมโยงคอมพิวเตอร์หลายๆ เครื่องให้สามารถใช้ข้อมูลร่วมกัน หรือถ่ายเทข้อมูลติดต่อถึงกันได้อย่างสะดวก เช่น อินเทอร์เน็ต (Internet) เป็นต้น

สำหรับผู้เจาะระบบคอมพิวเตอร์หรือแฮกเกอร์นั้น เมื่อกล่าวถึงระบบคอมพิวเตอร์ส่วนใหญ่จะหมายถึงระบบเครือข่ายของเครื่องขนาดใหญ่เช่น ระบบปฏิบัติการยูนิกส์ (UNIX) (Uniplexed Information and Computing System)[๙๕] ,MS Windows NT, VMS หรือ Mainframe

ระบบคอมพิวเตอร์ที่กล่าวได้ว่ามีความปลอดภัยจะต้องประกอบด้วยคุณสมบัติ ๓ ประการคือ

๑. มีความสามารถในการป้องกันข้อมูลที่เป็นความลับ (Data Confidentiality) ซึ่งจะช่วยรักษาข้อมูลไม่ให้ถูกเปลี่ยนแปลงหรือลักลอบนำไปใช้ ข้อมูลที่เป็นความลับเหล่านี้มีหลายประเภททั้งที่เป็นข้อมูลความลับของระบบและข้อมูลความลับของผู้ใช้งาน ข้อมูลความลับของระบบ ได้แก่บัญชีรายชื่อผู้ใช้และรหัสผ่าน สิทธิการเข้าใช้บริการต่างๆของระบบ รวมถึงสิทธิการจัดการระบบ ส่วนข้อมูลที่เป็นความลับของผู้ใช้งานทั่วไป ได้แก่ แฟ้มข้อมูลส่วนตัวของผู้ใช้แต่ละคน กุญแจส่วนตัวสำหรับการเข้ารหัสและถอดรหัสข้อมูลเป็นต้น

๒. สร้างความถูกต้องของการติดต่อสื่อสารข้อมูล (Data and Communication Integrity) เป็นวิธีการจัดการให้ข้อมูลที่ส่งผ่านกันในเครือข่ายคอมพิวเตอร์มีความถูกต้องและตรงกัน แอพพลิเคชันที่มีความจำเป็นต้องคำนึงถึงคุณสมบัติข้อนี้เป็นสำคัญ เช่นระบบจัดการฐานข้อมูลจากระยะไกล ข้อมูลที่ถูกส่งจากไคลเอนต์(Client)[๙๖]มักอยู่ในรูปของฐานข้อมูลที่มีการเปลี่ยนแปลงไปบางส่วนแล้ว ต้องการบันทึกลงในฐานข้อมูลกลาง หากข้อมูลที่ส่งผ่านเครือข่ายถูกดักจับและเปลี่ยนแปลงไประหว่างการส่งจะทำให้ฐานข้อมูลสองแหล่งไม่ตรงกัน ในกรณีนี้ผู้บริหารฐานข้อมูลจะไม่สามารถทราบได้หากไม่มีระบบป้องกันที่ดีพอ

---

[๙๕]UNIX หมายถึง ระบบปฏิบัติการที่พัฒนาโดยบริษัท Bell ซึ่งทำงานในลักษณะหลายๆโปรแกรมในสภาพแวดล้อมที่มีผู้ใช้หลายคน ยูนิกส์ถูกใช้เป็นเครื่องคอมพิวเตอร์แม่ข่ายหรือโฮสต์ (Hosts) ของเครือข่ายอินเทอร์เน็ตเป็นจำนวนมากในปัจจุบัน

[๙๖] คือ ซอฟต์แวร์ที่เป็นกระบวนงานในการขอบริการหรือข้อมูล

๓. มีการทำงานโดยปราศจากการบุกรุก (Assurance Against Denial-of-Services) ซึ่งได้แก่การรับประกันความถูกต้องของการทำงานโดยปราศจากการบุกรุกด้วยวิธีดอส (Dos:Denial-of-Services) การบุกรุกโดยวิธีนี้มักทำให้ระบบหยุดทำงานเนื่องจากทรัพยากรถูกใช้หมด ผู้บุกรุกจะอาศัยจุดอ่อนของโปรโตคอล(Protocols)[๒๐] และระบบปฏิบัติการเพื่อสร้างความเสียหาย เช่น สร้างแพ็กเกตไอซีเอ็มพี (ICMP)[๒๑]จำนวนมากโดยใช้คำสั่ง ping ซึ่งระบบไม่สามารถรองรับกับแพ็กเกตจำนวนมากเหล่านี้ได้[๒๒]

- **ระบบเครือข่าย** (Networks System)

เมื่อกล่าวถึงระบบคอมพิวเตอร์คงจะละเลยไม่ได้ที่จะกล่าวถึงคำว่า เน็ตเวิร์ค ซึ่งเป็นกลุ่มของเครื่องคอมพิวเตอร์ที่ต่อเข้าด้วยกัน เพื่อแลกเปลี่ยนข้อมูลหรือใช้อุปกรณ์ร่วมกันในแต่ละหน่วยงาน ไม่ว่าจะเป็นรัฐบาล บริษัทเอกชน หรือองค์กรอื่นๆ โดยแต่ละหน่วยงานต่างต้องรับผิดชอบเน็ตเวิร์คของตนเองในการป้องกันผู้บุกรุกเข้าระบบ ระบบเครือข่ายมีหลายประเภทดังเช่น ระบบ LAN (Local Area Network) ระบบ MAN (Metropolitan Area Network) ระบบ WAN (Wide Area Network) และระบบอินเทอร์เน็ต

- **อินเทอร์เน็ต** (Internet)

เมื่อใดก็ตามที่เน็ตเวิร์คเชื่อมต่อกับระบบเน็ตเวิร์คภายนอกเราจะเรียกว่า "อินเทอร์เน็ต" ซึ่งประกอบด้วยเน็ตเวิร์คนับพันที่ต่อเข้าด้วยกันรอบโลก หรืออาจเรียกว่าทางด่วนข้อมูล (Information Superhighway) หรือไซเบอร์สเปซ (Cyberspace)

อินเทอร์เน็ตได้ถูกพัฒนาสำหรับเพนตากอน(pentagon) ในปี ๑๙๖๐ เพื่อที่จะช่วยวิศวกรและนักวิจัยแลกเปลี่ยนข้อมูลในการพัฒนาอาวุธ ซึ่งนับแต่นั้นเป็นต้นมาอินเทอร์เน็ตก็เริ่มเกี่ยวข้อง

---

[๒๐] โปรโตคอล คือมาตรฐานขั้นตอนและวิธีการที่ใช้ในการติดต่อสื่อสารระหว่างระบบเครือข่ายคอมพิวเตอร์ โดยทั่วไปแล้วมาตรฐานที่เป็นที่นิยมใช้อย่างแพร่หลายคือ มาตรฐานขององค์การ International Standard organization (ISO)

[๒๑] ICMP คือ สัญญาณควบคุมการส่งข้อมูลผ่านโปรโตคอลทางอินเทอร์เน็ต

[๒๒] อุรุพงษ์ กัลยาสิริ และ สุรศักดิ์ สงวนพงษ์, "ระบบตรวจจับการบุกรุกทางเครือข่ายคอมพิวเตอร์," วารสารไมโครคอมพิวเตอร์," ปีที่ ๑๗ ฉบับที่ ๑๗๒ (พฤศจิกายน ๒๕๔๒) : ๑๒๔

กับเครือข่ายสาธารณะต่างๆ ในปี ๑๙๘๒ อินเทอร์เน็ตได้เชื่อมต่อกับระบบคอมพิวเตอร์ประมาณ ๕๐๐ เครื่องเข้าด้วยกันและเพิ่มขึ้นเรื่อยมา จนกระทั่งมากกว่า ๑ ล้านเครื่องทั่วโลก ซึ่งอินเทอร์เน็ตนี้เองที่มีความสัมพันธ์ต่อผู้เจาะระบบคอมพิวเตอร์หรือแฮกเกอร์ในแง่ที่เป็นเสมือนสนามที่ใช้ในการประลองฝีมือเพราะเมื่ออินเทอร์เน็ตสามารถติดต่อกันได้ทั่วโลก ผู้เจาะระบบคอมพิวเตอร์หรือแฮกเกอร์ก็จะสามารถไปสู่ที่ใดๆ ตามต้องการได้ทั่วโลกเช่นกัน

๑.๔.๒ การเจาะระบบคอมพิวเตอร์

การ "เจาะ" ระบบคอมพิวเตอร์นั้น เมื่อพิเคราะห์ถึงคำนี้ โดยทั่วไปสามารถเข้าใจได้ว่าคือการทะลุ ทะลวงผ่านสิ่งกีดขวางหรือการทำให้เป็นช่องเป็นรู[๒๓] โดยอาศัยเครื่องมือในการกระทำ ซึ่งการนำคำว่า "เจาะ" มาใช้กับระบบคอมพิวเตอร์นี้ ในเบื้องต้นผู้เขียนลังเลที่จะนำคำนี้มาใช้ เนื่องจากเมื่อพิเคราะห์โดยผิวเผินจะไม่แสดงถึงความเหมาะสมและสละสลวยตามภาษากฎหมายแม้แต่น้อย แต่จะโน้มเอียงไปในทางเป็นภาษาพูดมากกว่า อย่างไรก็ตามสาเหตุที่ผู้เขียนนำคำนี้มาใช้เนื่องจากได้รับการสนับสนุนจากท่านผู้รู้ว่า แม้คำว่า"เจาะ" จะไม่มีลักษณะเป็นภาษากฎหมายแต่หากพิจารณาถึงความเข้าใจโดยทั่วไปแล้ว การใช้คำว่า"เจาะ" สามารถสื่อให้เห็นภาพของการกระทำได้ดีกว่าการใช้คำว่า "เข้าสู่" ซึ่งเป็นคำแรกที่ผู้เขียนได้คิดไว้ และเมื่อพิจารณาในทางประวัติศาสตร์ ภาษาที่ใช้ในการบัญญัติกฎหมายก็มิได้มุ่งความสละสลวยมากกว่าความเข้าใจของผู้อ่านซึ่งคือประชาชนทั่วไปที่มีความเกี่ยวข้องกับการบังคับใช้กฎหมาย ตัวอย่างเช่น กฎหมายลักษณะโจรในกฎหมายตราสามดวง[๒๔] จะพบความผิดฐานโจรซุ่มซ่อน[๒๕] โจรล้วงลัก[๒๖] โจรฉกฉวย[๒๗]

---

[๒๓] พจนานุกรม ฉบับราชบัณฑิตยสถาน พ.ศ. ๒๕๒๕ พิมพ์ครั้งที่ ๓ (กรุงเทพมหานคร: สำนักพิมพ์อักษรเจริญทัศน์ ,๒๕๓๐),หน้า ๒๔๑.

[๒๔] หลวงสุทธิวาทนฤพุฒิ,ประวัติศาสตร์กฎหมาย ชั้นปริญญาโท.พิมพ์ครั้งที่ ๑ (กรุงเทพมหานคร: โรงพิมพ์มหาวิทยาลัยธรรมศาสตร์ ๒๕๑๖, หน้า ๔๑๕-๔๑๖.

[๒๕] "อันว่าโจรซุ่มซ่อนนั้นฤา คือคบกันไปคอยด้อมมอง ณ ทับราวป่าท่าน้ำสถานที่ใดๆ ก็ดี หมีให้เจ้าของรู้เหนเกบเอา ทรับ ช้างม้า เรือเกวียร ประการใดไป"

[๒๖] "อันว่าโจรล้วงลักนั้นฤา คือว่าโจรล้วง เรือ เรือน ร้าน เอาทรัพย์สิ่งของทังปวงไป"

[๒๗] "อันว่าโจรฉกฉวยนั้นฤา คือว่าหาเครื่องสาตราวุธหมีได้ ไปคอยอยู่ที่ถนนหนทางเปลี่ยวช่วงชิงเอาทรัพยสิ่งของเครื่องอัญมณีทังปวง"

นอกจากนี้กฎหมายป้องกันและปราบปรามการฟอกเงิน พ.ศ. ๒๕๔๒ คำว่า "ฟอก" เป็นคำที่แสดงให้เห็นกิริยาและเข้าใจได้ทันทีว่าคือการกระทำอันมีลักษณะทำให้สะอาดหมดจด เช่น ฟอกผ้า ฟอกจิตใจ[๒๘] เมื่อนำมาใช้กับการฟอกเงินจึงมีความหมายถึงการนำเงินที่ได้มาโดยไม่ชอบหรือเป็นเงินสกปรกมากระทำให้มีลักษณะสะอาดหมดจดเพื่อที่จะนำไปใช้ต่อไป ซึ่งหากตั้งคำถามว่ามีคำอื่นที่เหมาะสมกว่านี้หรือไม่ คำตอบคงเห็นได้จากผลลัพธ์ที่แสดงออกมาในชื่อของกฎหมายที่แสดงให้เห็นอยู่ในตัว

กิริยา ซุ่มซ่อน ล้วงลัก ฉกฉวยหรือฟอกเงิน เป็นสิ่งที่ผู้เขียนต้องการแสดงให้เห็นว่าการใช้คำกล่าวที่ง่ายแก่การเข้าใจอาจแสดงให้เห็นถึงเจตนารมณ์ของกฎหมายได้ดีกว่า ดังคำกล่าวของศาสตราจารย์หยุด แสงอุทัย ได้กล่าวถึงเรื่องภาษาในตัวบทกฎหมายไว้ตอนหนึ่งว่า *"ถ้อยคำที่ใช้ในตัวบทกฎหมายนั้น...ผู้ร่างกฎหมายจะต้องหาคำสามัญและเข้าใจง่าย ฯลฯ และ"อนึ่ง การที่จะร่างกฎหมายให้มีถ้อยคำชัดเจนพอที่บุคคที่สุจริตจะเข้าใจอย่างเดียวยังไม่เป็นการเพียงพอ เพราะยังมีบุคคลไม่สุจริตและไม่ปรารถนาจะปฏิบัติตามกฎหมายอยู่เป็นจำนวนมาก โดยเหตุนี้จึงต้องร่างกฎหมายให้ชัดเจนพอที่บุคคลที่ไม่สุจริตจะไม่เข้าใจผิดได้ ทั้งนี้คือจะต้องร่างอย่างไม่ยอมให้บุคคลที่ไม่สุจริตเช่นว่านี้เสแสร้งกล่าวอ้างได้ว่าเขาไม่เข้าใจกฎหมายนั้น...ทั้งนี้ คือผู้ร่างกฎหมายจะต้องคำนึงถึงการเลี่ยงกฎหมายที่อาจเกิดขึ้นได้ในอนาคตนั้นเองฯลฯ*[๒๙] การใช้คำซึ่งเข้าใจยากแม้จะสละสลวยแต่อาจก่อให้เกิดปัญหาเช่น การไม่เข้าใจของประชาชนหรือการแปลความหมายซึ่งอาจมีหลายนัย จึงเป็นการไม่สมควร

กิริยาการเจาะระบบคอมพิวเตอร์นี้ เราอาจได้ยินหรือพบเห็นการใช้คำนิยามที่มีความหมายที่ใกล้เคียงกัน ดังนี้คือ

๑. Break into ซึ่งเป็นคำที่ใช้เรียกกิริยาการเข้าสู่ การบุกรุก การเจาะ ที่มุ่งในการสื่อความหมายในลักษณะการทำลายสิ่งกีดขวางเพื่อเข้าไปในสิ่งใดๆ

๒. Hacking เป็นคำกิริยาที่แสดงถึงการกระทำของแฮกเกอร์ (Hacker) และนิยมใช้เมื่อกล่าวถึงการกระทำของแฮกเกอร์ ซึ่งมีการนำไปใช้ในหลายความหมาย ดังเช่น

---

[๒๘] พจนานุกรม ฉบับราชบัณฑิตยสถาน พ.ศ. ๒๕๒๕. หน้า ๖๐๘.

[๒๙] ธานินทร์ กรัยวิเชียร ภาษากฎหมายไทย. พิมพ์ครั้งที่ ๘ (กรุงเทพมหานคร:บริษัท เชเว่น พริ้นติ้ง กรุ๊ป จำกัด,๒๕๔๐), หน้า ๘๘.

Hacking basically means learning all there is to know about a system,becoming immersed in the system to the point of distraction ,and being able to fix the system if it breaks[๓๐]

Hacking คือการกระทำประเภทบุกรุก เจาะหรือหยั่ง เข้าไปในระบบคอมพิวเตอร์ เพื่อที่จะให้ได้มาซึ่งความรู้เกี่ยวกับระบบและการทำงานของมัน ซึ่งการกระทำที่ว่านี้เป็นเพราะว่าเราต้องการสิทธิที่จะจัดการข้อมูลทั้งหมดในระบบให้เป็นไปตามแบบที่ใจเราต้องการ[๓๑]

๓. Access เป็นคำที่มักจะใช้ในตัวบทกฎหมายในส่วนบทบัญญัติที่ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ โดยมีการให้คำนิยามในลักษณะขยายความซึ่งมีจุดประสงค์เพื่อให้ครอบคลุมถึงการกระทำหลายประการ ดังเช่นในกฎหมาย Federal computer law ของประเทศสหรัฐอเมริกา ที่ให้ความหมายไว้ว่า

Access หมายถึง เข้าไปสู่ สั่ง สื่อสารกับ ใส่ข้อมูลเข้าไปเก็บไว้ ล้วงข้อมูลมาจากเครื่องคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข่ายงานคอมพิวเตอร์ [๓๒]

แต่อย่างไรก็ตามแม้จะพบว่ามีการใช้คำกริยาที่แสดงถึงการเจาะระบบคอมพิวเตอร์ที่แตกต่างกัน แต่หากพิจารณาจุดมุ่งหมายของแต่ละคำแล้ว จะเห็นได้ว่ามีความมุ่งหมายไปในทิศทางเดียวกัน คือ การเจาะ หยั่ง เข้าไปสู่สิ่งที่ตนต้องการ เช่นกัน

---

[๓๐] Charles Zepp. Virtual community – Hackers Dr. Wood .Sociology and the Internet-Spring 1999 ,http:// camden-www.rutgers.edu/~wood/445/zepp.html

[๓๑] ทศพล กนกนุวัตร์ ,เจาะระบบ ถอดรหัส (How to Hack) (กรุงเทพมหานคร: บริษัท ซีเอ็ดยูเคชั่น จำกัด), หน้า ๑๑.

[๓๒] ภานุ รังสีสหัส,"การกระทำความผิดทางอาญาเกี่ยวกับคอมพิวเตอร์ " (วิทยานิพนธ์ปริญญานิติศาสตร์มหาบัณฑิต บัณฑิตวิทยาลัย จุฬาลงกรณ์มหาวิทยาลัย, ๒๕๓๓),หน้า ๕๓

๑.๔.๓ การกระทำโดยไม่มีอำนาจหรือไม่ได้รับอนุญาต

การกระทำโดยไม่ได้รับอนุญาตหรือไม่มีอำนาจ หมายถึงการกระทำใดๆ ที่กระทำต่อวัตถุ สิ่งของหรือสิทธิของผู้อื่น โดยไม่ได้รับอนุญาตจากบุคคลผู้มีสิทธิเหนือวัตถุ สิ่งของหรือสิทธินั้น หรือเป็นการกระทำโดยไม่ได้รับมอบอำนาจโดยชอบตามบทกฎหมาย ซึ่งอาจเป็นการกระทำโดยพลการหรือกระทำการเกินขอบเขตที่กำหนดไว้ สำหรับกรณีการเจาะระบบคอมพิวเตอร์นั้นสิ่งที่แสดงให้เห็นถึงการกระทำโดยไม่ได้รับอนุญาตอย่างชัดแจ้งคือ การผ่านระบบรักษาความปลอดภัยของระบบคอมพิวเตอร์เพื่อเข้าไปในระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาต ซึ่งการรักษาความปลอดภัยของระบบคอมพิวเตอร์นั้น มีหลายประเภท ดังเช่น

- *รหัสผ่าน (Passwords)* คือการเรียงกันของสัญลักษณ์ ซึ่งรู้โดยระบบคอมพิวเตอร์หรือผู้ใช้ สำหรับใช้ในการได้รับอนุญาตให้เข้าไปในระบบคอมพิวเตอร์และข้อมูลที่บรรจุอยู่ภายในไม่ว่าโดยสมบูรณ์หรือถูกจำกัดขอบเขต การผ่าน passwords มีความสำคัญมากในการที่จะพิสูจน์ว่าได้มีการเข้าสู่ระบบโดยมีอำนาจหรือไม่

- *Firewalls* เป็นอุปสรรคที่ใช้ในระบบรักษาความปลอดภัย โดยจะทำการตรวจสอบเพื่อบ่งชี้ว่าผู้ใดเป็นผู้ใช้คอมพิวเตอร์ ก่อนที่จะอนุญาตให้ผู้ใช้ดังกล่าวผ่านเข้าไปสู่ระบบเครือข่ายที่ใหญ่ขึ้น

๑.๔.๔ ความหมายของผู้เจาะระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาต

เมื่อพิจารณาความหมายจากองค์ประกอบของคำว่าผู้เจาะระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาตแล้ว ผู้เจาะระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาตจะหมายถึง ผู้ที่เจาะ หรือหยั่ง เข้าไปในองค์ประกอบทางคอมพิวเตอร์ที่ทำงานประสานกันเพื่อจัดการกับข้อมูลให้ได้ผลลัพธ์ออกมาในรูปแบบตามที่ต้องการ โดยปราศจากความยินยอมของผู้มีสิทธิในองค์ประกอบทางคอมพิวเตอร์ดังกล่าวหรือกระทำการเกินขอบอำนาจที่ได้รับมอบหมาย

การบุกรุกระบบคอมพิวเตอร์อาจเกิดทั้งจากบุคคลภายนอกและบุคคลภายในระบบ การบุกรุกที่เกิดจากบุคคลภายนอก (Outsider threat) เข้ามาทำลายระบบโดยวิธีการต่างๆ ได้แก่ การบุกรุกผ่านจุดอ่อนของบริการพื้นฐานของระบบ หรือการใช้โปรแกรมม้าโทรจัดเพื่อขโมยรหัสผ่าน

เป็นต้น นอกจากบุคคลภายนอกแล้วการบุกรุกอาจเกิดจากบุคคลภายในระบบ (Insider threat) ซึ่งใช้นอกขอบอำนาจโดยไม่หวังดี หรืออาจเกิดจากความรู้เท่าไม่ถึงการณ์[๓๓]

๒. การเจาะระบบคอมพิวเตอร์ทำได้อย่างไร

การเจาะระบบคอมพิวเตอร์ เป็นรูปแบบที่แสดงถึงความเป็นผู้เจาะระบบคอมพิวเตอร์หรือแฮกเกอร์อย่างแท้จริง การตอบคำถามที่ว่าการเจาะระบบทำอย่างไรคือการหาคำตอบว่าการเจาะระบบคอมพิวเตอร์มีวิธีการอย่างไร สาเหตุที่ต้องมีการเจาะระบบคอมพิวเตอร์เพราะไม่สามารถเข้าไปในระบบคอมพิวเตอร์ได้โดยวิถีทางปกติ แต่ต้องมีสิ่งที่แสดงให้เห็นถึงสิทธิหรือการได้รับอนุญาตเพื่อสามารถเข้าไปในระบบคอมพิวเตอร์นั้นๆ ถ้าจะเปรียบไปแล้วก็ดังเช่นการเข้าไปในสถานที่ใดๆ ที่มีรั้วรอบขอบชิดปิดประตูแน่นหนา ผู้เข้าไปได้จะต้องมีกุญแจซึ่งเจ้าของสถานที่ได้มอบให้ไว้อันเป็นการให้สิทธิหรืออำนาจที่จะเข้าไปในสถานที่ที่กำหนดไว้

ความสำคัญของการเจาะระบบคอมพิวเตอร์คือ จะทำอย่างไรจึงจะได้กุญแจเพื่อที่จะเข้าไปในระบบคอมพิวเตอร์นั้น ซึ่งระบบคอมพิวเตอร์หรือเป้าหมายของการเจาะระบบคอมพิวเตอร์ก็มีหลากหลายแบ่งแยกตามองค์ประกอบของระบบคอมพิวเตอร์ ดังเช่น ถ้าจะเจาะเวบเพจซึ่งเป็นระบบคอมพิวเตอร์จำพวกซอฟท์แวร์เราก็ต้องหากุญแจเพื่อที่จะเข้าไปในเวบเพจนั้นให้ได้เสียก่อน

การเจาะระบบคอมพิวเตอร์และเป้าหมายของการกระทำผิดทางคอมพิวเตอร์นี้ นายเดวิด ไอโคฟ อดีตหัวหน้าหน่วยไซเบอร์ ไครมินอล ของเอฟบีไอ แยกอาชญากรรมในคอมพิวเตอร์[๓๔]ออกเป็น ๔ จำพวกที่สำคัญได้แก่

---

[๓๓]อุรุพงษ์ กัลยาสิริ และ สุรศักดิ์ สงวนพงษ์, "ระบบตรวจจับการบุกรุกทางเครือข่ายคอมพิวเตอร์," วารสารไมโครคอมพิวเตอร์" : ๑๒๕.

[๓๔] ในที่นี้จะหมายถึงการแบ่งประเภทการกระทำในลักษณะการเจาะระบบคอมพิวเตอร์เท่านั้น เพราะในการแบ่งอาชญากรรมคอมพิวเตอร์โดยทั่วไปจะไม่จำกัดเฉพาะการเจาะระบบคอมพิวเตอร์ที่เป็นการกระทำของแฮกเกอร์เท่านั้น

๑. การเจาะระบบรักษาความปลอดภัยทางกายภาพ ได้แก่ตัวอาคาร อุปกรณ์ และสื่อต่างๆ เช่น การทำลายประตูอาคารที่เก็บรักษาระบบคอมพิวเตอร์ หรือการถอดรหัสผ่าน CMOS

๒. การเจาะเข้าไปในระบบการสื่อสารและการรักษาความปลอดภัยของซอฟต์แวร์ข้อมูลต่างๆ ดังเช่น การเจาะเว็บเพจ (Webpage)

๓. การเจาะเข้าสู่ระบบรักษาความปลอดภัยของระบบปฏิบัติการ ซึ่งรวมถึงการเจาะเข้าไปในกระบวนการรักษาความปลอดภัยที่ออกแบบไว้เพื่อแกะรอยและป้องกันอาชญากรคอมพิวเตอร์ เช่น การเจาะระหัสผ่านบน Windows NT, การเจาะระบบ UNIX, การแกะรหัสผ่านล็อกออน บน Windows

๔. การเจาะผ่านระบบรักษาความปลอดภัยส่วนบุคคล ทั้งจากภายในและภายนอกหน่วยงาน

เมื่อพิจารณาถึงเป้าหมายประกอบกับวิธีการเจาะระบบคอมพิวเตอร์ ซึ่งเป็นวิธีการทางเทคนิคแล้ว จึงเป็นที่คาดหมายได้ว่าจะมีวิธีการเจาะระบบคอมพิวเตอรที่ความหลากหลายและมีลักษณะเฉพาะ ดังนั้นการนำเสนอต่อๆไป จึงเป็นการแสดงตัวอย่างวิธีการหากุญแจที่จะใช้ในการเจาะระบบคอมพิวเตอร์เพียงบางส่วน สำหรับการศึกษาวิธีการกระทำโดยละเอียดซึ่งต้องอาศัยความเชี่ยวชาญพิเศษสามารถศึกษาเพิ่มเติมได้จากเอกสารทางคอมพิวเตอร์ได้โดยเฉพาะ

๒.๑ การเริ่มเจาะระบบคอมพิวเตอร์โดยทั่วไป

การเจาะระบบคอมพิวเตอร์นั้น ไม่จำเป็นว่าจะต้องหมุนโทรศัพท์เพื่อเข้าสู่ระบบคอมพิวเตอร์ทางเครือข่ายเท่านั้น การจู่โจมหรือการเข้าสู่ระบบคอมพิวเตอร์อาจจะกระทำทางกายภาพคือ การบุกรุกเข้าถึงตัวเครื่องคอมพิวเตอร์โดยตรง โดยเฉพาะเครื่องคอมพิวเตอร์ส่วนบุคคล ซึ่งเพียงไขควงที่สามารถเปิดฝาเครื่องก็สามารถเข้าถึงได้เช่นกัน ดังเช่นหากต้องการข้อมูลหรือไฟล์ทั้งหมดก็ทำการก๊อปปี้ฮาร์ดดิสก์ หรือทำการเคลียร์ข้อมูลในซีมอส เป็นต้น

ส่วนกรณีการเข้าสู่ระบบคอมพิวเตอร์โดยผ่านสายโทรศัพท์นั้น สิ่งแรกที่จะต้องมีคือเครื่องคอมพิวเตอร์และโมเด็ม โมเด็มเป็นเครื่องมือที่ทำให้เครื่องคอมพิวเตอร์สามารถสื่อสารกับคอมพิวเตอร์เครื่องอื่นๆ เมื่อมีเครื่องคอมพิวเตอร์และโมเด็มแล้ว อันดับต่อไปคือมองหาเครื่องคอมพิวเตอร์ที่เป็นเป้าหมายที่จะเข้าไป ซึ่งต้องอาศัยความรู้ในเรื่องชนิดของระบบคอมพิวเตอร์ที่เป็นเป้าหมาย เรียนรู้ระบบโทรศัพท์ ทำการเชื่อมต่อโมเด็มของตนเข้าสู่โมเด็มของระบบคอมพิวเตอร์ที่เป็นเป้าหมายและค้นรหัสผ่าน (passwords) หรือรหัสประจำตัวผู้ใช้ (user code)

ซึ่งเรื่องที่กล่าวมาแม้ฟังดูเป็นเรื่องเล็กน้อย แต่วิธีการที่กล่าวมาก็จำเป็นต้องอาศัยเวลา การอุทิศตนและความอดทน

วิธีการที่ผู้เจาะระบบคอมพิวเตอร์ใช้ในการเรียนรู้เกี่ยวกับระบบคอมพิวเตอร์นั้น ขึ้นอยู่กับชนิดของระบบคอมพิวเตอร์ที่ต้องการจะเข้าไป ในระบบคอมพิวเตอร์ที่มีขนาดเล็กสามารถทำการศึกษาจากหนังสือเพื่อทำความเข้าใจการทำงานทั่วไปของระบบว่าทำงานอย่างไร แต่เมื่อต้องการเข้าสู่ระบบคอมพิวเตอร์ที่มีขนาดใหญ่และซับซ้อนผู้เจาะระบบคอมพิวเตอร์จะใช้เวลานานขึ้นในการเรียนรู้เกี่ยวกับระบบคอมพิวเตอร์ ซึ่งนอกจากการพูดคุยกับแฮกเกอร์อื่นๆที่เคยเข้าในระบบคอมพิวเตอร์ที่เป็นเป้าหมายมาก่อนแล้ว ก็อาจใช้วิธีที่จะหาข้อมูลวิธีอื่นๆได้ ดังเช่น

๑. เข้าร่วมในงานแสดงคอมพิวเตอร์ต่างๆเพื่อหาข้อมูล เพราะเซลล์แมนหรือพนักงานขายอุปกรณ์ทางคอมพิวเตอร์นั้น มักจะยินดีและเต็มใจที่จะบอกทุกๆสิ่งที่ผู้ซื้อต้องการ

๒. เข้าไปในบริษัทซึ่งเป็นเป้าหมายของการเจาะระบบคอมพิวเตอร์ โดยเฉพาะบริเวณที่มีระบบคอมพิวเตอร์แล้วมองหาเอกสารที่วางอยู่รอบๆ เครื่องคอมพิวเตอร์นั้น เพราะอาจพบข้อมูลที่จำเป็นในการเจาะระบบคอมพิวเตอร์

๓. ค้นหาจากขยะของบริษัทที่เป็นเป้าหมายในการเจาะระบบคอมพิวเตอร์เพื่อหวังว่าจะพบคำบอกใบ้เกี่ยวกับระบบคอมพิวเตอร์ ซึ่งเราเรียกการกระทำเช่นนี้ว่า Dumpster Diving

๔. แสดงตัวโดยการแอบอ้างว่าเป็นช่างซ่อมระบบคอมพิวเตอร์ เพื่อขอเข้าไปในระบบคอมพิวเตอร์ที่มีการรักษาความปลอดภัยนั้น

ถ้าหากโชคดีข้อมูลที่ได้อาจเป็นเบอร์โทรศัพท์ ชนิดของโมเด็ม รหัสผ่านหรือรหัสผู้ใช้เครื่องคอมพิวเตอร์ แต่ถ้าหาข้อมูลดังกล่าวไม่พบผู้เจาะระบบคอมพิวเตอร์ก็จำต้องใช้ความพยายามในการค้นหาต่อไป

โดยสรุป ขั้นแรกของการเข้าสู่ระบบนั้น ผู้เจาะระบบคอมพิวเตอร์จะต้องมีเบอร์โทรศัพท์ที่จะใช้ในการติดต่อกับเครื่องคอมพิวเตอร์เป้าหมาย ส่วนวิธีที่จะได้เบอร์โทรศัพท์มานั้นก็แล้วแต่ว่าจะได้มาโดยวิธีใด ซึ่งหลังจากได้เบอร์โทรศัพท์แล้ว จะต้องเชื่อมต่อโมเด็มของตนเข้ากับโมเด็มของระบบคอมพิวเตอร์เป้าหมาย ซึ่งรวมถึงการทำให้แน่ใจว่าจะมีการสื่อสารและโต้ตอบกันระหว่างโมเด็มทั้งสอง ถ้าโมเด็มทั้งสองเข้ากันไม่ได้ก็จะต้องเปลี่ยนชนิดของโมเด็มและพยายามติดต่อกับโมเด็มอีกครั้ง ซึ่งเรื่องการเปลี่ยนชนิดของโมเด็มนี้เป็นเรื่องทางเทคนิค จึงจะไม่กล่าวในที่นี้

ขั้นตอนที่สอง หลังจากโมเด็มได้เชื่อมโยงเรียบร้อยแล้ว แฮกเกอร์จะต้องหารหัสผ่านและรหัสของผู้ใช้คอมพิวเตอร์ ซึ่งขั้นตอนนี้อาจใช้เวลามากในการค้นหาและลองเสี่ยง แต่อย่างไรก็ตามขั้นตอนนี้ก็ไม่ยากเกินไป สำหรับแฮกเกอร์ที่ฉลาด อดทนและมีความเชี่ยวชาญ

๒.๒ เครื่องมือที่นำมาสนับสนุนการเจาะระบบคอมพิวเตอร์

อาจมีผู้สงสัยว่าเหตุใดผู้เริ่มใช้คอมพิวเตอร์หรือเด็กที่เพิ่งเริ่มเรียนคอมพิวเตอร์ถึงได้เก่งกาจสามารถเจาะระบบคอมพิวเตอร์ของผู้อื่นได้ คำตอบก็คือ เพราะปัจจุบันมีเครื่องมือหรือโปรแกรมซึ่งมีวิธีการที่ไม่ยุ่งยากในการอำนวยความสะดวกหรือย่นระยะเวลาสำหรับผู้ที่คิดจะเจาะระบบคอมพิวเตอร์หลายชนิดด้วยกัน ดังเช่น

- โปรแกรม Sniffer เป็นโปรแกรมที่คอยดักเอาชื่อผู้ใช้และรหัสผ่านของทุกคนที่เข้ามาในระบบ[๓๕]

- โปรแกรม John the Ripper , Cracker Jack ,และ Pacecrack95 ซึ่งเป็นโปรแกรมที่จะนำ password file และไฟล์คำศัพท์ (wordlist) มาเปรียบเทียบกันเพื่อที่จะหาว่าชื่อผู้ใช้และพาสเวิร์ดคืออะไร

- โปรแกรม SATAN หรือ Security Administration Tool for Analyzing Networks เป็นอุปกรณ์ที่ใช้ในการวิเคราะห์ระบบคอมพิวเตอร์

- โปรแกรม War dialer เป็นโปรแกรมที่หมุนโทรศัพท์เพื่อใช้ในการค้นหาการเชื่อมต่อกับโมเด็ม

ตัวอย่างการเจาะเข้าสู่ระบบยูนิกซ์

เทคนิคการเจาะเข้าสู่ระบบยูนิกซ์มีตั้งแต่วิธีพื้นๆที่ไม่ได้ใช้เทคนิคหรือเครื่องมือใดๆ เรื่อยไปจนกระทั่งเทคนิคที่ซับซ้อน

---

[๓๕] **Network sniffer software**: scans TCP/IP packets for passwords that are sent while users log into a system

เดาสุ่ม

ด่านสำคัญในการเข้าสู่ยูนิกซ์คือรหัสผ่านซึ่งเก็บอยู่ในแฟ้ม /etc/passwd รหัสผ่านในแฟ้มนี้จะผ่านการเข้ารหัสลับทำให้ไม่ทราบถึงรหัสต้นฉบับได้ แต่แฟ้ม /etc/passwd ไม่ได้เป็นแฟ้มลับ แต่ในทางตรงข้ามกลับเปิดโอกาสให้ผู้ใช้ทุกคนเปิดอ่านได้ ผู้ซึ่งได้แฟ้มรหัสผ่านจะนำแฟ้มไปผ่านโปรแกรมวิเคราะห์หารหัส โดยตัวโปรแกรมจะสร้างรหัสต้นฉบับขึ้นมาจากพจนานุกรมคำศัพท์ (dictionary) ที่มีอยู่ในระบบ (เช่นในยูนิกซ์คือ /usr/dict) แล้วเข้ารหัสเพื่อนำผลที่ได้ไปเปรียบเทียบกับรหัสใน /etc/passwd โปรแกรมแกะรหัสผ่านเป็นโปรแกรมเขียนได้ง่าย ต้นฉบับโปรแกรมภาษาซีอาจมีความยาวเพียง ๖๐–๗๐ บรรทัด อีกทั้งยังมีโปรแกรมสำเร็จที่เผยแพร่ในอินเทอร์เน็ตอยู่แล้ว เช่น โปรแกรม Crack

Crack สร้างขึ้นเพื่อจุดประสงค์ให้ผู้ดูแลระบบคอมพิวเตอร์ใช้วิเคราะห์หาว่าผู้ใช้รายใดตั้งรหัสผ่านง่ายเกินไป แต่ก็มีผู้นำไปใช้ผิดวัตถุประสงค์ หนทางที่ป้องกันได้ส่วนหนึ่งก็คือผู้ใช้ทุกคนจะต้องเรียนรู้หลักการและตั้งรหัสผ่านที่คาดเดาได้ยาก เว้นแต่ยูนิกส์ในระบบ SystemV จะใช้วิธีแยกเอาส่วนของรหัสผ่านไปเก็บไว้ในแฟ้มต่างหากอีกแฟ้มหนึ่งที่ไม่อนุญาตให้ผู้ใช้ทั่วไปอ่านได้ กรรมวิธีแบบนี้เรียกว่าระบบ “shadow password”

สนิฟเฟอร์

สนิฟเฟอร์เป็นชื่อเครื่องหมายทางการค้าของระบบตรวจจับแพ็กเกตเพื่อนำมาวิเคราะห์และตรวจหาปัญหาในเครือข่าย ตัวระบบจะประกอบด้วยคอมพิวเตอร์ที่มีการ์ดเครือข่ายสมรรถนะสูงและซอฟต์แวร์ตรวจวิเคราะห์แพ็กเกต แต่ในปัจจุบันมีซอฟต์แวร์จำนวนมากที่มีขีดความสามารถระดับเดียวกับสนิฟเฟอร์ และทำงานได้โดยไม่ต้องพึ่งฮาร์ดแวร์โดยเฉพาะ อีกทั้งมีแพร่หลายในแทบทุกระบบปฏิบัติการ ชื่อสนิฟเฟอร์ในปัจจุบันจึงนิยมใช้เป็นชื่อเรียกของโปรแกรมใดๆ ที่สามารถตรวจจับและวิเคราะห์แพ็กเกตไปโดยปริยาย

ม้าโทรจัน

โปรแกรมม้าโทรจันเป็นโปรแกรมที่ลวงให้ผู้ใช้งานเข้าใจผิดว่าเป็นโปรแกรมปกติโปรแกรมหนึ่งที่ใช้งานอยู่เป็นประจำ แต่การทำงานจริงกลับเป็นการดักจับข้อมูลเพื่อส่งไปให้ผู้เจาะระบบคอมพิวเตอร์ ตัวอย่างเช่นโปรแกรมโทรจันที่ลวงว่าเป็นโปรแกรมล็อกอินเข้าสู่ระบบ เมื่อผู้ใช้ป้อนบัญชีและรหัสผ่านก็จะแอบส่งรหัสผ่านไปให้ผู้เจาะระบบแทน

ประตูกล

ผู้เจาะระบบคอมพิวเตอร์ใช้ ประตูลับ (backdoors) ซึ่งเป็นวิธีพิเศษเข้าสู่ระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาต ความหมายของประตูลับอาจรวมไปถึงวิธีการที่ผู้พัฒนาโปรแกรมทิ้งรหัสพิเศษหรือเปิดทางเฉพาะไว้ในโปรแกรมโดยไม่ให้ผู้ใช้ล่วงรู้ ผู้เจาะระบบคอมพิวเตอร์ส่วนใหญ่จะมีชุดซอฟต์แวร์ซึ่งสร้างขึ้นเพื่อเจาะเข้าสู่ระบบตามจุดอ่อนที่มีอยู่ด้วยวิธีการต่างๆ

ซอฟต์แวร์ตรวจช่องโหว่ระบบ

ในอินเทอร์เน็ตมีซอฟต์แวร์เป็นจำนวนมากที่ใช้ในการตรวจวิเคราะห์หารูโหว่ของระบบรักษาความปลอดภัยซอฟต์แวร์เหล่านี้เผยแพร่โดยไม่คิดมูลค่าและเป็นเสมือนดาบสองคมที่ทั้งผู้เจาะระบบคอมพิวเตอร์นำไปใช้ด้วยจุดประสงค์ที่ต่างกัน ซอฟต์แวร์ในกลุ่มนี้ซึ่งเป็นที่รู้จักแพร่หลายได้แก่ Internet Security Scanner, SATAN, COPS และTiger เป็นต้น