1. การสร้าง dependable system ต้องการสี่สิ่งที่จำเป็น นอกจากสามสิ่งที่เราได้เรียนรู้กันในชั้นเรียน คือ policy mechanism และ assurance แล้วอีกสิ่งหนึ่งคืออะไร และสิ่งนี้จำเป็นอย่างไร

   คำตอบ จากบทที่ 1 หัวข้อย่อย 1.2 ได้กล่าวไว้ว่าอีกสิ่งที่สำคัญคือ Incentive ซึ่งหมายถึงแรงจูงใจที่จะป้องกันและบำรุงรักษาระบบให้ทำงานได้อย่างถูกต้อง โดยสิ่งนี้จำเป็นเป็นอย่างมาก เนื่องจากไม่มีระบบใดในโลกนี้ที่จะปลอดภัยในทุกด้าน ทุกระบบล้วนแล้วแต่จะมีช่องโหว่ ซึ่งในปัจจุบันช่องโหว่จากระบบรักษาความปลอดภัยอาจจะยังไม่โผล่ แต่ก็ไม่ได้มีการันตีว่าในอนาคตจะไม่มีโผล่ออกมา เช่นช่องโหวใน Google drive ที่สามารถทำให้ผู้โจมตีหลอกให้ผู้ใช้งานติดตั้งมัลแวร์ได้ [1] ซึ่งส่วนหนึ่งมาจาก Policy ของทาง Google เองที่ไม่เว็บเบราว์เซอร์อย่าง Google Chrome จะเชื่อถือไฟล์ที่มาจากทาง Google เอง ซึ่งในที่นี้คือ Google drive

2. การนำมีดขึ้นเครื่องบินได้ใน **สมัยก่อนเกิดเหตุการณ์ 9/11** เกิดจาก policy ที่ผิดพลาดหรือ mechanism ที่มีช่องโหว่

   คำตอบ เกิดจาก policy ที่ผิดพลาด

3. นำมีดขึ้นเครื่องบินได้ใน **สมัยปัจจุบัน** เกิดจาก policy ที่ผิดพลาดหรือ mechanism ที่มีช่องโหว่

   คำตอบ mechanism ที่มีช่องโหว่

4. “Security Theatre” คืออะไร ยกตัวอย่างกรณีที่นิสิตเคยประสบ เคยได้ยินมา ที่บ่งบอกถึงความเป็น “Security Theatre” (คำตอบของแต่ละคนไม่ควรจะเหมือนกัน)

   คำตอบ Security Theatre คือมาตรการที่ทำให้ดูเหมือนปลอดภัยมากกว่าความเป็นจริง โดยที่ผมเคยประสบมาคือ ระบบตรวจวัดไข้เพื่อป้องกันผู้ติดเชื้อ COVID-19 ก่อนเข้าสู่พื้นที่ต่าง ๆ ซึ่งการวัดไข้ที่เรามักจะเห็นตามห้างสรรพสินค้าเป็นการทำเพื่อให้คนรู้สึกสบายใจมากขึ้นโดยจริง ๆ แล้วไม่สามารถเพิ่มความปลอดภัยได้มากขึ้นเสียเท่าไร เนื่องจากการวัดด้วยปืนวัดอุณหภูมิ ไม่สามารถวัดได้อย่างแม่นยำเสียเท่าไร โดยจะคลาดเคลื่อนได้ง่ายตามสภาพแวดล้อม เช่นก่อนหน้านี้อยู่ในห้องแอร์ ก็จะทำให้วัดค่าได้ต่ำลง หรือถ้าเดินตากแดดมา ก็จะทำให้วัดค่าได้สูงขึ้น ซึ่งการที่วัดได้อย่างแม่นยำเราอาจจะต้องใช้ปรอทวัดไข้วัดเป็นคน ๆ ไป แต่วิธีนี้กินเวลาเป็นอย่างมาก

5. Threat model ที่ดีของตู้ ATM ควรจะพิจารณาใครบ้างเป็นผู้โจมตีและพิจารณาอะไรบ้างเป็นสิ่งที่ต้องปกป้อง

   คำตอบ ผู้โจมตีที่เป็นไปได้ทั้งบุคคลภายใน เช่น พนักงานธนาคาร และ บุคคลภายนอก ซึ่งสำหรับการป้องกันบุคคลภายในจะต้องปกป้องเรื่องการเข้าถึงระบบ และการให้สิทธิ์พนักงานในการแก้ไข ซึ่งควรจะปกป้องโดยการทำ Policy ให้แน่นหนา ไม่ว่าจะเป็นเรื่องของความสามารถในการเข้าถึงไฟล์หรือโครงสร้างการจัดเก็บข้อมูล ส่วนการป้องกันสำหรับบุคคลภายนอกจะแบ่งเป็น 2 ประเภทคือ Remote Attack กับ Local Attack ซึ่ง Remote Attack ควรจะพิจารณาเกี่ยวกับ Network เป็นหลัก เช่นพวก Connection to bank ต้องดูว่าได้ Encrypt ข้อมูลดีแล้วหรือไม่ ส่วน Local Attack จะต้องพิจารณาสามส่วนหลัก ๆ ของ ตู้ ATM โดยส่วนแรกคือ Computer ของตู้ ต้องตรวจสอบว่ามี USB/HDD แปลกปลอมถูกต่อไว้หรือไม่ รวมถึงดู Boot file ด้วย ส่วนต่อมาคือ Card Reader กับแป้นตัวเลข ต้องดูว่ามีใครมาติดตั้งชุดดักข้อมูลบัตรหรือไม่ ส่วนสุดท้ายคือช่องรับธนบัตร ต้องดูว่ามีอุปกรณ์แปลกปลอมที่ช่วยให้เครื่องจำหนายธนบัตรผิดพลาดหรือไม่

6. ธนาคารให้ความสำคัญกับคุณสมบัติทางด้าน security (secrecy integrity availability) ด้านใดมากที่สุด รองลงมา และน้อยที่สุด เพราะเหตุใด

   คำตอบ จาก Example case แล้ว ธนาคารให้ความสำคัญกับ Integrity มากที่สุดเนื่องจากทุกเคสล้วนแล้วแต่จะโจมตีทางด้าน Secrecy เพราะว่าข้อมูลของธนาคารนั้น ล้วนแล้วแต่จะเป็นเรื่องเงิน การที่ข้อมูลถูกแก้ไขแบบไม่ถูกต้องแม้แต่น้อย ก็จะเป็นเรื่องร้ายแรงมาก ส่วนรองลงมาที่ธนาคารให้ความสำคัญคือ Secrecy เนื่องจากเป็นทางหลัก ๆ ที่ผู้ไม่ประสงค์ดีนำมาโจมตี ส่วนเรื่อง Availability น้อยที่สุดเนื่องจากระบบล่มก็ยังมีผลกระทบน้อยเมื่อเทียบกับสองประการแรก

7. ค่ายทหารให้ความสำคัญกับคุณสมบัติทางด้าน security (secrecy integrity availability) ด้านใดมากที่สุด รองลงมา และน้อยที่สุด เพราะเหตุใด

   คำตอบ จาก Example case แล้ว ค่ายทหารให้ความสำคัญกับด้าน Secrecy มากที่สุดเนื่องจากข้อมูลทางการทหารเป็นเรื่องที่ Sensitive คนที่ไม่ควรรู้จะต้องไม่รู้ ส่วนรองลงมาคือ Integrity เนื่องจากการติดต่อทางการทหารไม่ควรจะถูกดักแก้ไข ส่วนเรื่อง Availability น้อยสุดถึงแม้ว่าทางค่ายทหารจะต้องการให้สื่อสารกันได้ แต่ก็ต้องการให้คนที่ไม่เกี่ยวข้องไม่สามารถเข้าถึงได้แม้ว่าคนที่ควรเข้าถึงได้ควรจะเข้าถึงได้ แต่เพื่อความปลอดภัย จะเข้าไม่ได้บางเวลาก็มิเป็นไร

8. โรงพยาบาลให้ความสำคัญกับคุณสมบัติทางด้าน security (secrecy integrity availability) ด้านใดมากที่สุด รองลงมา และน้อยที่สุด เพราะเหตุใด

   คำตอบ จาก Example case แล้ว โรงพยาบาลให้ความสำคัญกับ Secrecy มากที่สุดเพราะว่า ข้อมูลการรักษาของคนไข้แต่ละคนเป็นข้อมูลที่ต้องรักษา Privacy เป็นอย่างมาก ส่วนรองลงมาคือ Integrity เนื่องจากข้อมูลที่โรงพยาบาลเก็บไว้คือข้อมูลการรักษาของคนไข้ ทำให้ถ้าถูกแก้ไขจะทำให้เกิดความเสียหาย โดยอาจจะทำให้การรักษาผิดพลาดได้ ส่วนเรื่อง Availability น้อยที่สุด

9. ทำไมระบบคอมพิวเตอร์ในยุคก่อนจึงมีความปลอดภัยมากกว่าในยุคปัจจุบัน

   คำตอบ คอมพิวเตอร์สมัยก่อนไม่มี Resource Sharing จึงทำให้การโจมตีเป็นไปได้ลำบากเพราะทุก ๆ ช่วงเวลามีการรันแค่ Process เดียว อีกทั้งคอมพิวเตอร์สมัยก่อนยังไม่มีการเชื่อมต่อ Network ทำให้ปลอดภัยไปอีกขั้นหนึ่ง

10. ทำไมเราจึงสร้างระบบคอมพิวเตอร์ที่ปลอดภัยอย่างสมบูรณ์แบบไม่ได้

    คำตอบ เพราะว่าการที่สมบูรณ์แบบแล้วจะทำให้คอมพิวเตอร์ใช้งานยากและลำบากมาก เลยทำให้ไม่ค่อยมีผู้ที่พัฒนาคอมพิวเตอร์ไปสู่จุดที่ปลอดภัยอย่างสมบูรณ์ อีกทั้งบางทีเราก็ไม่รู้ว่าตรงไหนไม่ปลอดภัยจนกระทั่งเราทำการใช้ระบบอย่างจริงจัง

11. เราควรจะลงทุนกับระบบความปลอดภัยของคอมพิวเตอร์มากน้อยเพียงใด

    คำตอบ ควรที่จะลงทุนกับระบบความปลอดภัยให้น้อยกว่าหรือเทียบเท่ากับมูลค่าความเสียหายที่เกิดขึ้นเมื่อระบบหรือข้อมูลถูกผู้ไม่ประสงค์ดีนำไปใช้งาน (ซึ่งในทางปฏิบัติอาจจะยากเล็กน้อยเพราะมีบางอย่างประเมินเป็นมูลค่ามิได้)

12. ในสถานการณ์ต่อไปนี้ อธิบายว่ามีการฝ่าฝืนคุณสมบัติความปลอดภัยในด้านใดบ้าง secrecy หรือ integrity หรือ availability ในแต่ละข้ออาจมีการฝ่าฝืนมากกว่าหนึ่งคุณสมบัติ

    - นายดำลอกการบ้านของนายแดง

      คำตอบ ฝ่าฝืนด้าน Secrecy เพราะนายด าไม่ควรจะเข้าถึงการบ้านนายแดงได้

    - นายดำทำให้คอมพิวเตอร์ของนายแดงล่มสลาย

คำตอบ ฝ่าฝืนด้าน Integrity เพราะนายดำไม่ควรที่จะเข้าถึงคอมพิวเตอร์ของนายแดงเพื่อทำให้ล่มได้และฝ่าฝืนด้าน Availability เพราะทำให้นายแดงไม่สามารถเข้าถึงคอมตัวเองได้

- นายดำแปลงเช็คที่จ่ายให้นายแดงจากจำนวนเงิน 100,000 บาท เป็น 10,000 บาท

  คำตอบ ฝ่าฝืนด้าน Integrity เนื่องจากนายดำไม่ควรที่จะแก้ไขข้อมูลของนายแดงได้

- นายดำปลอมลายเซ็นต์นายแดงที่ใช้เซ็นสัญญาการก่อสร้างมูลค่า 100 ล้านบาท

  คำตอบ ฝ่าฝืนด้าน Secrecy เนื่องจากนายด าไม่ควรที่เข้าไปจะปลอมแปลงข้อมูลของนายแดงได้

- นายดำและนายแดงจดทะเบียนเว็บ paruj.com แล้วปฏิเสธข้อเสนอซื้อของภารุจที่ต้องการเป็นเจ้าของเว็บชื่อนี้

  คำตอบ ผมคิดว่าไม่ฝ่าฝืนนะครับ เพราะการจดทะเบียนโดเมนขึ้นอยู่กับว่าใครจดก่อน แล้วถ้าผู้ที่มาตอนหลังจะมาขอซื้อ ผู้จดทะเบียนก่อนก็ควรจะมีสิทธิ์ปฏิเสธ

- นายดำได้รับรู้เบอร์บัตรเครดิตของนายแดง ทำการยกเลิกบัตรของนายแดง และทำให้บริษัทเครดิตการ์ดส่งบัตรใบใหม่มาให้กับนายดำที่ที่อยู่ของนายดำ

คำตอบ ฝ่าฝืนด้าน Secrecy เพราะว่านายดำไม่ควรจะที่จะเข้าถึงข้อมูลของนายแดงได้ และ ฝ่าฝืนด้าน Integrity เพราะว่านายดำไม่ควรจะแก้ไขที่อยู่ของนายแดงได้

13. แนวทางในการสร้างระบบให้ปลอดภัยมี 5 แนวทางได้แก่อะไรบ้างและแนวทางใดปลอดภัยที่สุด

คำตอบ มีดังนี้

1. Isolate คือการทำให้ทุกคนทำงานอย่างไม่เกี่ยวเนื่องกัน (ปลอดภัยสุดเนื่องจากทุกคนไม่ Share resource กันเลย)
2. Exclude คือการไม่ให้ผู้ไม่ประสงค์ดีเข้ามาในระบบ
3. Restrict คือการที่ให้ผู้ไม่ประสงค์ดีเข้ามาในระบบ แต่ไม่สามารถเข้ามาทำอะไรได้
4. Recover คือการย้อนระบบมาในจุดก่อนได้รับความเสียหาย
5. Punish คือจับผู้ไม่ประสงค์ดีและนำมาทำการลงโทษ

14. ทำไมเราไม่เลือกสร้างระบบคอมพิวเตอร์โดยใช้แนวทางที่ปลอดภัยที่สุด

คำตอบ การที่ระบบคอมพิวเตอร์ถูกออกแบบมาเพื่อสร้างความปลอดภัยมากเท่าใด การใช้งานยิ่งลำบากขึ้นเท่านั้น เช่นการที่จะให้ระบบปลอดภัยที่สุด เราอาจจะต้องย้อนกลับไปใช้คอมพิวเตอร์สมัยโบราณที่ไม่มี Resource Sharing เนื่องจากอาจจะโดนโจมตีข้าม Process ซึ่งจะทำให้ระบบทำงานช้าลงเป็นอย่างมาก รวมถึงอาจจะต้องทำให้ระบบเข้าถึงไม่ได้จากภายนอก ซึ่งก็จะหมายความว่า Service ต่าง ๆ จะไม่สามารถใช้ได้เลย เช่น Social media, E-mail และเกมต่าง ๆ ดังนั้นต่อให้ปลอดภัยเพียงใด แต่ไม่มีคนใช้ ก็ไร้ประโยชน์ ไม่คุ้มค่าพัฒนา

15. ทำไม security policy กับ mechanism จึงควรเป็นอิสระต่อกันให้มากที่สุด (กล่าวคือไม่ให้มีการระบุ policy ที่ผูกติดกับตัว mechanism ใด ๆ)

คำตอบ เนื่องจากการผูกกันระหว่าง Security policy กับ Mechanism จะทำให้ Policy หย่อนไปตาม Mechanism ถ้าเทียบแล้วก็คล้าย ๆ กับการสร้าง Algorithm (เทียบเป็น policy) ซึ่งการสร้าง Algorithm ควรจะทำให้รันได้ในทุก ๆ Programming language (เทียบเป็น mechanism)

16. จุดประสงค์หลักของการสร้างระบบ access control หรือ information flow control คืออะไร

คำตอบ Access control เป็นการมุ่งเน้นไปทางด้านการพิจารณาว่าจะทำอย่างไรไม่ให้ผู้ไม่มีสิทธิ์อ่านข้อมูลได้ ส่วน information flow control เป็นการมุ่งเน้นไปทางด้านการพิจารณาว่าจะทำอย่างไรไม่ให้ข้อมูลเดินทางไปถึงคนที่ไม่มีสิทธิ์ได้

17. แนวทางในการทำ assurance ที่เหมาะสมเป็นอย่างไรบ้าง

คำตอบ แนวทางการทำ assurance ควรจะทำให้สามารถเช็คได้จากหลาย ๆ mechanism เพื่อที่จะเช็คให้ครบถ้วนที่สุด แต่ทว่าการเช็คหลาย ๆ ที่ก็เป็นการกระทำที่ซับซ้อนเป็นอย่างมาก แม้อาจจะไม่ยากสำหรับ Administrator แต่กับ Users ที่มีความสามารถไม่สูงอาจจะเป็นเรื่องที่ยากมาก ดังนั้นควรจะต้องทำให้ใช้ได้ง่ายทั้ง Administrator และ Users

18. แนวทางการทำ Defense in depth ที่บทความนี้กล่าวถึงมีกี่ชั้น รายละเอียดเป็นอย่างไร

คำตอบ สามขั้นคือ

1. Network level security จะถูก Implement โดยใช้พวก Firewall เพื่อกันไม่ให้ผู้ที่ไม่ควรเข้ามาได้เข้ามาได้

2. OS security ควรจะทำใน Sandbox เพื่อ Isolate การทำงานให้แยกกัน เพื่อให้มีการโจมตีข้าม process ให้น้อยที่สุด
3. Application security จะใช้วิธีเช็ค Authorization โดยตรง เพื่อป้องกับให้ผู้ที่ไม่มีสิทธิใช้งานได้

References

[1] R. Lakshmanan, "A Google Drive 'Feature' Could Let Attackers Trick You Into Installing Malware," 22 August 2020. [Online]. Available: https://thehackernews.com/2020/08/google-drive-file-versions.html. [Accessed 1 September 2020].