มูลนิธิศูนย์สารสนเทศเครือข่ายไทย
นายชยา ลิมจิตติ
ดร.ยรรยง เต็งอำนวย
นางเพ็ญศรี อรุณวัฒนามงคล
ดร.พจนันท์ รัตนไชยพันธ์

ความมั่นคงปลอดภัยของระบบชื่อโดเมน (Information Security in Domain Name System)

ปรับปรุง 5 มิถุนายน 2563

ระบบชื่อโดเมนคืออะไร

ก่อนจะทำความเข้าใจระบบชื่อโดเมน ต้องเริ่มด้วยการอธิบายเกี่ยวกับระบบอินเทอร์เน็ตโดยย่อเสียก่อน อินเทอร์เน็ตคือเครือข่ายคอมพิวเตอร์ที่เชื่อมต่อกันโดยใช้โปรโตรคอล TCP/IP อุปกรณ์ใด ๆ ที่จะรับส่ง ข้อมูลในระบบอินเทอร์เน็ตจะต้องมีหมายเลข โดยหมายเลขในเครือข่ายอินเทอร์เน็ตมีชื่อทางเทคนิคว่า หมายเลขไอพี อย่างไรก็ตามมนุษย์ซึ่งเป็นผู้ใช้งานอินเทอร์เน็ตนั้นไม่คุ้นเคยกับการจดจำหมายเลข ตัวอย่างเช่น ระบบโทรศัพท์จะอ้างอิงเครื่องโทรศัพท์ด้วยหมายเลข แต่ผู้ใช้งานจะคุ้นเคยกับชื่อบุคคล หรือสถานที่มากกว่า ดังนั้นจึงมีสมุดโทรศัพท์ (ที่เป็นกระดาษและไม่ใช่กระดาษ) ที่ช่วยให้ผู้ใช้งานบันทึก ชื่อกับหมายเลขโทรศัพท์ไว้ด้วยกัน ในระบบอินเทอร์เน็ตก็เช่นกัน ผู้ใช้งานอ้างอิงการติดต่อใน โลกอินเทอร์เน็ตด้วยชื่อ เช่น ชื่ออีเมล หรือชื่อเว็บ แต่อุปกรณ์ต่าง ๆ รับส่งข้อมูลโดยใช้หมายเลขไอพี ระบบที่อยู่เบื้องหลังและทำหน้าที่แปลงชื่อไปเป็นหมายเลขไอพีคือระบบชื่อโดเมน (Domain Name System: DNS)

“แม้ระบบชื่อโดเมนจะเป็นโปรแกรมที่ทำงานบนเครื่องคอมพิวเตอร์ แต่ระบบชื่อโดเมนมิใช่แอปพลิเคชันหนึ่งของอินเทอร์เน็ต แต่เป็นโครงสร้างพื้นฐานระดับสำคัญยิ่งยวดของอินเทอร์เน็ต”

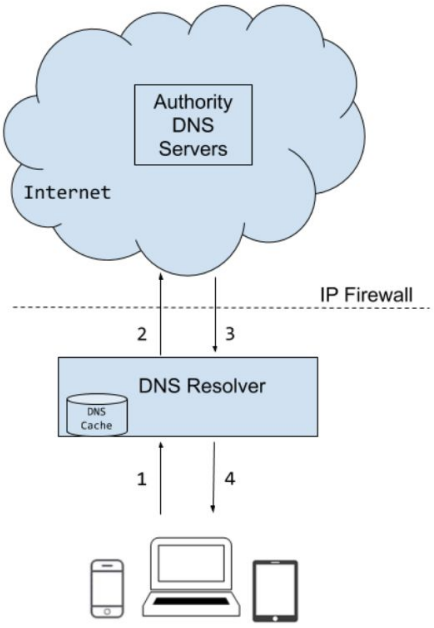
“Although Domain Name System is a software on computers, it is not an Internet application but critical Internet infrastructure.”

ระบบชื่อโดเมนเป็นส่วนประกอบที่สำคัญมากของระบบอินเทอร์เน็ต ทุกครั้งที่มีการใช้งานระบบใด ๆ บนอินเทอร์เน็ต เช่น พร้อมเพย์ LINE Facebook หรืออ่านเมล ระบบชื่อโดเมนจะเป็นขั้นตอนแรกที่ถูกเรียก ใช้งาน หากระบบชื่อโดเมนไม่สามารถทำงานได้ ผู้ใช้งานจะไม่สามารถใช้งานระบบใด ๆ บน อินเทอร์เน็ตได้เลย

นอกจากนี้ระบบค้นหาข้อมูลรายใหญ่ของโลก เช่น Google ก็ต้องอาศัยระบบชื่อโดเมนเช่นกัน เพราะ การเริ่มเก็บข้อมูล จากเว็บต่าง ๆ ทั่วโลกนั้นต้องเริ่มจากการแปลงชื่อเว็บเหล่านั้นไปเป็นหมายเลขไอพี เสียก่อน หากระบบชื่อโดเมนไม่สามารถทำงานได้ Google ก็ไม่สามารถเก็บข้อมูลได้ ดังนั้นจึงสามารถ สรุปได้ว่าระบบชื่อโดเมนเป็น โครงสร้างพื้นฐานที่สำคัญมากของระบบอินเทอร์เน็ต

การทำงานของระบบชื่อโดเมน

การทำงานของระบบชื่อโดเมน เริ่มจากการที่อุปกรณ์ของผู้ใช้งานอินเทอร์เน็ต ต้องแปลงชื่อไปเป็นหมายเลขไอพี (หรือสอบถามข้อมูลอื่น ๆ เช่น ต้องการทราบว่าควรส่งเมลสำหรับหน่วยงานนี้ ไปที่ไหน) โดยจะส่งคำถามไปยังคอมพิวเตอร์ที่ ทำหน้าที่เป็น DNS Resolver (หมายเลข 1) จากนั้น DNS Resolver ก็จะตรวจสอบจาก DNS Cache ว่าเคยมีใครเคยถามคำถามนี้หรือไม่ ถ้ามีก็ตอบ คำถามได้เลย (โดยใช้สำเนาคำตอบที่มีเก็บ ไว้แล้ว) หากไม่มีก็จะสอบถามไปยัง Authority DNS Server ต่าง ๆ ที่อยู่ในอินเทอร์เน็ต (หมายเลข 2) จนได้ คำตอบที่ต้องการ (หมายเลข 3) และส่งคำตอบ ที่ได้นั้นกลับไปยังอุปกรณ์ที่ถามมา (หมายเลข 4) พร้อมทั้งสำเนาคำตอบนั้นไว้ใน DNS Cache เพื่อใช้ตอบคำถามเดิมในครั้งถัดไป



รูปที่ 1 แสดงการทำงานของระบบชื่อโดเมนโดยย่อ

ความมั่นคงปลอดภัยของระบบชื่อโดเมน

จากที่กล่าวมาข้างต้นจะเห็นว่า ระบบชื่อโดเมนมีความสำคัญต่อการใช้งานอินเทอร์เน็ตมาก แต่ผู้ใช้งาน ทั่วไปอาจจะไม่ทราบว่ามีระบบชื่อโดเมนทำงานอยู่เบื้องหลัง หรือผู้ใช้บางกลุ่มอาจทราบว่ามีระบบชื่อโดเมน แต่อาจไม่เคยสงสัยว่าระบบชื่อโดเมนทำงานถูกต้องหรือไม่ เพราะผู้ใช้ส่วนใหญ่

เชื่อว่าระบบ โดเมนเนมทำงานถูกต้องเสมอ (ผู้คนทั่วไปจะมั่นใจว่าไฟฟ้าจากการไฟฟ้านครหลวงเชื่อถือได้) หรืออาจ เชื่อว่ามีความเสี่ยงน้อยมากที่ระบบชื่อโดเมนจะทำงานผิดพลาด

เพื่อให้เห็นภาพเกี่ยวกับความมั่นคงปลอดภัยของระบบชื่อโดเมน จึงขอเริ่มจากการวิเคราะห์ความมั่นคง ปลอดภัยของระบบโดยใช้หลัก 3 ประการด้านความมั่นคงปลอดภัยคือ Confidentiality Integrity และ Availabilty ดังนี้

1. **Confidentiality (ให้รู้เท่าที่ควรรู้) มีการรักษาความลับ มีการจำกัดการเข้าถึง**
   ซึ่งเมื่อนำหลักข้อนี้มาประยุกต์กับระบบชื่อโดเมน จะมีคำถามว่าข้อมูลในระบบโดเมนเนมเป็นความลับหรือไม่ ข้อมูลในระบบชื่อโดเมนควรปกปิดหรือเปิดเผยแค่ไหน กับใคร ทั้งนี้อาจเปรียบเทียบกับสมุดโทรศัพท์หน้าเหลืองและหน้าขาวที่มีการแจกจ่ายทั่วไปในอดีต คือควรแจกจ่ายสมุดโทรศัพท์ให้กับผู้ที่สนใจทั่วไปหรืออนุญาตเพียงแค่ให้สอบถามทีละชื่อเท่านั้น แต่ไม่ยอมให้สมุดทั้งเล่ม (โหลดข้อมูลทั้งหมด) นอกจากนี้เพื่อให้ระบบชื่อโดเมนมี Availability ที่ดี ระบบชื่อโดเมนจะมี Authority DNS Server มากกว่า 1 เครื่อง และ Authority DNS Server เหล่านั้นจะมีการถ่ายโอนข้อมูลชื่อโดเมนระหว่างกัน จึงควรป้องไม่ให้ผู้อื่นแอบสำเนาข้อมูลระหว่างการถ่ายโอนข้อมูลหรือไม่ อีกทั้งบางหน่วยงานจะแยกฐานข้อมูลชื่อโดเมน ในระบบอินเทอร์เน็ต (ภายนอกองค์กร) กับชื่อในระบบอินทราเน็ต (ภายในองค์กร์) ออกจากกัน ดังนั้นจึงต้องตรวจสอบว่าผู้สอบถามชื่อโดเมนมาจากภายในหรือภายนอกองค์กรเพื่อให้ข้อมูลชื่อโดเมนที่สอดคล้องกับนโยบายหน่วยงาน

2. **Integrity (ข้อมูลถูกต้องสมบูรณ์) เปลี่ยนแปลงได้เฉพาะผู้ที่มีสิทธิเท่านั้น**
   ซึ่งเมื่อนำหลักข้อนี้มาประยุกต์กับระบบชื่อโดเมน ประเด็นที่ต้องพิจารณาคือข้อมูลในระบบชื่อโดเมนถูกต้องสมบูรณ์หรือไม่ เช่นเมื่อ Authority DNS Server (รูปที่ 1) ซึ่งอยู่ในอินเทอร์เน็ตให้คำตอบแล้ว คำตอบนั้นไปถึง DNS Resolver และถูกส่งต่อไปยังผู้ใช้อย่างถูกต้องสมบูรณ์โดย ไม่มีการแก้ไขเปลี่ยนแปลงคำตอบ (ทั้งโดยเจตนาและความผิดพลาดทางเทคนิค) หรือไม่ และประเด็นที่สำคัญอีกประการหนึ่งคือข้อมูลชื่อโดเมนที่อยู่ที่ Authority DNS Server ถูกแก้ไขเปลี่ยนแปลงโดยผู้มีสิทธิ เท่านั้นหรือไม่

3. **Availability (มีใช้เมื่อต้องการ)**
   เนื่องจากระบบชื่อโดเมนจะต้องทำงานได้ทุกครั้งเมื่อผู้ใช้ เชื่อมต่ออินเทอร์เน็ต หรืออาจกล่าวได้ว่าระบบชื่อโดเมน ต้องทำงานได้ตลอดเวลา ซึ่งทำได้โดยมี DNS Resolver สำรอง

สำหรับผู้ใช้งาน และมี Authority DNS Server สำรองสำหรับทุกโดเมน รวมทั้ง Authority DNS Server หลักและสำรองไม่ควรอยู่ภายใน เครือข่ายคอมพิวเตอร์เดียวกัน

ความมั่นคงปลอดภัยของระบบชื่อโดเมนคือสภาวะที่ระบบชื่อโดเมนสามารถรักษาคุณสมบัติทั้ง 3 ประการไว้ได้ คือมีการรักษาความลับที่เหมาะสม ข้อมูลระบบชื่อโดเมนถูกต้องสมบูรณ์ และระบบชื่อโดเมนพร้อมใช้งาน ตลอดเวลา

ภัยคุกคามต่อระบบชื่อโดเมนและแนวทางการป้องกัน

เมื่อการใช้งานอินเทอร์เน็ตขยายจากหน่วยงานทางด้านการศึกษาและการวิจัยออกไปสู่หน่วยงานเอกชนและประชาชนทั่วไป อินเทอร์เน็ตจึงกลายเป็นสังคมที่มีผู้ใช้งานจากคนทุกประเภท สังคมของมนุษย์ประกอบด้วยคนดีและคนร้าย สังคมของผู้ใช้งานอินเทอร์เน็ตก็มีลักษณะเดียวกัน เมื่อคนร้ายใช้งานระบบอินเทอร์เน็ตจึงเกิดภัยคุกคามต่อระบบ

อินเทอร์เน็ตและระบบชื่อโดเมนส่งผลให้เกิดความเสียหายกับผู้ใช้งาน อินเทอร์เน็ต เช่น ผู้ร้ายแก้ไขข้อมูลระบบชื่อโดเมนทำให้ผู้ใช้ไปยัง เว็บของผู้ร้ายโดยผู้ใช้คิดว่ากำลังเชื่อมต่อกับเว็บที่ต้องการ หรือผู้ร้ายแก้ไขข้อมูลระบบชื่อโดเมนทำให้ผู้ร้ายสามารถอ่านจดหมายอิเล็กทรอนิกส์ทุกฉบับที่ส่งไปหน่วยงานนั้น ๆ ได้

การวิเคราะห์ภัยคุกคามต่อระบบชื่อโดเมนอาจจะแบ่งได้เป็น 3 ด้าน ดังนี้

1. **Disclosure** คือ ความพยายามที่จะเข้าถึงข้อมูลโดเมนของ หน่วยงานนั้น ๆ โดยไม่ได้รับอนุญาต เนื่องจากข้อมูลในระบบชื่อโดเมนเป็นข้อมูลที่ใช้งานจริงในระดับปฏิบัติการ หากผู้บุกรุกได้ข้อมูลชื่อโดเมนทั้งหมด ก็จะสามารถคาดเดาโครงสร้างของระบบสารสนเทศในหน่วยงานนั้น ๆ ได้ และอาจจะพยายามเข้าถึงระบบต่าง ๆ โดยไม่ได้รับอนุญาต หากหน่วยงานเห็นว่าควรจำกัดการเข้าถึง ข้อมูลชื่อโดเมน ก็ควรมีมาตรการป้องกันที่เหมาะสมเช่น การใช้ access control list, การใช้ transaction signature หรือการใช้เทคนิค split horizon dns เป็นต้น

2. **Destruction** คือ ความพยายามแก้ไขเปลี่ยนแปลงข้อมูลในระบบ ชื่อโดเมนโดยไม่ได้รับอนุญาต ความพยายามแก้ไขข้อมูลเกิดขึ้นได้ทั้งขณะที่ข้อมูล DNS ส่งผ่านระบบเครือข่ายคอมพิวเตอร์ (data in transit) และเกิดขึ้นได้โดยการแก้ไขข้อมูลที่ Authority DNS Server หรือ DNS Resolver โดยตรง เหตุการณ์ที่เกิดขึ้นจริงเช่น กรณี DNS Cache Poisoning หรือ DNSpionage เป็นต้น แนวทางการป้องกันที่เหมาะสมคือการใช้งาน DNSSEC ทั้งที่ Authority DNS server และ DNS resolver การใช้เทคนิค hidden master

รวมทั้งแนวปฏิบัติกรณีฉุกเฉินตาม Emergency Directive 19-01 ของ CISA ประเทศสหรัฐอเมริกา

3. **Denial** คือ การที่ระบบชื่อโดเมนไม่สามารถให้บริการได้ ซึ่งอาจจะเกิดขึ้นเนื่องจากเหตุหลายประการ เช่นเครื่องคอมพิวเตอร์ที่ให้บริการ DNS หยุดทำงาน หรือเกิดการโจมตีระบบโดเมนเนม เช่นกรณี Dyn DNS Attack ในปี 2559 แนวทางการป้องกันที่เหมาะสมคือการมี Authority DNS Server หลายเครื่องและอยู่คนละเครือข่ายคอมพิวเตอร์ หรือมี DNS Resolver มากกว่า 1 เครื่อง หรือกำหนดค่าต่างๆของ DNS Server/Resolver ให้เหมาะสมตามแนวปฏิบัติที่ดี รวมทั้งประสานงานกับ ISP ล่วงหน้าเพื่อวางแผนการบรรเทา เหตุหากเกิดกรณี DDoS DNS Attack

สรุป

ทุกคนที่ใช้งานอินเทอร์เน็ตจะต้องใช้งานระบบชื่อโดเมนร่วมด้วยเสมอ ความมั่นคงปลอดภัยของระบบชื่อโดเมนจึงมีความสำคัญมากต่อการใช้งานอินเทอร์เน็ต หากเกิดเหตุที่ทำให้สูญเสียความมั่นคงปลอดภัยของระบบชื่อโดเมน ก็จะเกิดผลกระทบกับความมั่นคงปลอดภัยของระบบสารสนเทศต่าง ๆ ได้

ข้อเสนอแนะ

1. ให้บังคับใช้ DNSSEC ทั้งที่ Authority Server และ DNS Resolver กับระบบชื่อโดเมนของหน่วยงานของรัฐ และหน่วยงานในกำกับของรัฐ
2. กำหนดมาตรฐานความมั่นคงปลอดภัยระบบชื่อโดเมนและบังคับใช้กับหน่วยงานของรัฐและหน่วยงานในกำกับของรัฐ เช่น การเข้ารหัสข้อมูลโดเมนระหว่าง Authority Server การป้องกันการเข้าถึงข้อมูลโดเมน หรือ การตรวจสอบการแก้ไขเปลี่ยนแปลงข้อมูลชื่อโดเมน เป็นต้น
3. ออกข้อกำหนดให้ ISP ต้องจัดให้มีบริการ DNS Resolver ภายในเครือข่ายของตนเอง และเปิดใช้งาน DNSSEC validation
4. กำหนดให้ DNS Resolver ที่มีจำนวน query เกินค่าที่กำหนดเป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศ