ใบรับรองวิทยานิพนธ์

บัณฑิตวิทยาลัย มหาวิทยาลัยเกษตรศาสตร์

วิทยาศาสตรมหาบัณฑิต (วิทยาการคอมพิวเตอร์)

ปริญญา

วิทยาการคอมพิวเตอร์ | วิทยาการคอมพิวเตอร์

สาขา | **ภาควิชา**

เรื่อง ความพร้อมในการให้บริการดีเอ็นเอสเซคของไอเอสพีในประเทศไทย

DNSSEC Readiness of Thai ISPs

นามผู้วิจัย นายสัญชัย นิจวิภากุล

ได้พิจารณาเห็นชอบโดย

อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก .....

(ผู้ช่วยศาสตราจารย์สุขุมาล กิติสิน, Ph.D.)

อาจารย์ที่ปรึกษาวิทยานิพนธ์ร่วม .....

(ผู้ช่วยศาสตราจารย์ชวลิต ศรีสถาพรพัฒน์, Ph.D.)

หัวหน้าภาควิชา .....

(ผู้ช่วยศาสตราจารย์ศิริกร จันทร์นวล, M.Sc.)

บัณฑิตวิทยาลัย มหาวิทยาลัยเกษตรศาสตร์รับรองแล้ว

.....

(รองศาสตราจารย์กัญจนา ธีระกุล, D.Agr.)

คณบดีบัณฑิตวิทยาลัย

วันที่ ..... **เดือน** ..... **พ.ศ.** .....

วิทยานิพนธ์

เรื่อง

ความพร้อมในการให้บริการดีเอ็นเอสเซคของไอเอสพีในประเทศไทย

DNSSEC Readiness of Thai ISPs

โดย

นายสัญชัย นิจวิภากุล

เสนอ

บัณฑิตวิทยาลัย มหาวิทยาลัยเกษตรศาสตร์
เพื่อความสมบูรณ์แห่งปริญญาวิทยาศาสตรมหาบัณฑิต (วิทยาการคอมพิวเตอร์)
พ.ศ. 2557

สัญชัย นิจวิภากุล 2557: ความพร้อมในการให้บริการดีเอ็นเอสเซคของไอเอสพีในประเทศไทย ปริญญาวิทยาศาสตรมหาบัณฑิต (วิทยาการคอมพิวเตอร์) สาขาวิทยาการคอมพิวเตอร์ ภาควิชาวิทยาการคอมพิวเตอร์ อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก: ผู้ช่วยศาสตราจารย์สุขุมาล กิติสิน, Ph.D. 102 หน้า

โดเมนเนมเซอร์วิสเป็นบริการที่เป็นหัวใจสำคัญของการให้บริการโปรแกรมผ่านเครือข่ายทุกประเภท เนื่องจากมีการโจมตีช่องโหว่ของดีเอ็นเอสทำให้มีการเสนอการปรับปรุงดีเอ็นเอสเพื่อเพิ่มความปลอดภัยและยืนยันผู้ให้บริการที่เรียกว่าดีเอ็นเอสเซค อีกทั้งมีการประกาศนโยบายโดยรัฐบาลกลางของสหรัฐอเมริกาให้ปรับเปลี่ยนการใช้งานทุกโดเมนภายใต้โดเมน gov เพื่อให้รองรับการบริการดีเอ็นเอสเซคภายใน ธันวาคม พ.ศ. 2552 อันมีผลให้รูทเนมเซิร์ฟเวอร์ทั้งหมดและเนมเซิร์ฟเวอร์ในระดับ Top-Level ต้องปรับตัวตามมาให้บริการดีเอ็นเอสเซค ดังนั้นผู้ให้บริการเครือข่าย (ISPs) ทั่วโลกจึงควรต้องปรับตามนโยบายอันส่งผลต่อโครงสร้างเครือข่ายอินเทอร์เน็ตนี้ด้วย ผู้วิจัยจึงทำการสำรวจความพร้อมในการให้บริการดีเอ็นเอสเซคของผู้ให้บริการเครือข่าย (ISPs) ในประเทศไทยเพื่อความปลอดภัยในการใช้งานอินเทอร์เน็ตในระดับสากล โดยทำการทดลองตั้งแต่เดือนมีนาคม พ.ศ. 2556 ถึงเดือนพฤศจิกายน พ.ศ. 2556 พบว่าผู้ให้บริการ 4 ใน 6 รายที่เนมเซิร์ฟเวอร์มีการสนับสนุนการทำงานของดีเอ็นเอสเซค และจากแนวโน้มเชื่อว่าผู้ให้บริการอื่นๆจะปรับตัวตามในไม่ช้า

_____ _____ __ / __ / __

ลายมือชื่อนิสิต ลายมือชื่ออาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก

Sunchai Nijvipakul 2014: DNSSEC Readiness of Thai ISPs. Master of Science (Computer Science), Major Field: Computer Science, Department of Computer Science. Thesis Advisor: Assistant Professor Sukumal Kitisin, Ph.D. 102 pages.

Domain Name Service is a core service to all services provided through the Internet. Because of the vulnerabilities of the DNS has been increasingly major concerned. Researchers had proposed an extension in order to add security and the identity validation to the conventional DNS called DNSSEC. Additionally, federal government of the US recognized the importance of DNSSEC; therefore, issued a policy that all domain names under gov domain must be modified to incorporate DNSSEC to their name servers by December of 2009. This has resulted in the DNSSEC adoption by the ISP worldwide. Therefore, our experiments were carried in order to survey on the availability DNSSEC service in Thai ISPs to ensure international standard security of the Internet usage. The experiments was done during March 2013 until November 2013 and it was found that four out of six ISPs are equipped with name servers supporting DNSSEC and the trends showed that the rests would continue to improve their service to support DNSSEC soon.

_____ _____ __ / __ / __

Student's signature Thesis Advisor's signature

กิตติกรรมประกาศ

วิทยานิพนธ์ฉบับนี้สำเร็จลุล่วงได้ดี ด้วยความช่วยเหลืออย่างดียิ่งของอาจารย์ ผศ.ดร. สุขุมาล กิติสิน ประธานกรรมการที่ปรึกษา ที่กรุณาช่วยให้คำแนะนำขั้นตอนวิธีในการดำเนินงาน ชี้แนะแนวทางแก้ไขปัญหาและตรวจสอบแก้ไขข้อบกพร่องในงานวิจัยมาโดยตลอด รวมถึงอาจารย์ ผศ.ดร.ชวลิต ศรีสถาพรพัฒน์ และอาจารย์ ดร.เสฏฐวิทย์ เกิดผล ที่ช่วยให้คำแนะนำเรื่องต่างๆ มาโดยตลอด

ขอขอบคุณผู้จัดการฝ่ายสื่อสารข้อมูล นาย วสัน เสนาะกรรณ์ และ นางสาว สุนีรัตน์ ใจหาร สำหรับความกรุณาให้เข้าทดสอบอินเทอร์เน็ตของ CAT และ ขอขอบคุณผู้ที่ให้ความอนุเคราะห์ในการใช้งานอินเทอร์เน็ตของ 3BB JINET TOT และ TRUE

ขอกราบขอบพระคุณ คุณพ่อสง่า นิจวิภากุลและคุณแม่ผ่องศรี นิจวิภากุล ที่ให้กำลังใจในการเรียน ให้การสนับสนุนและให้ความช่วยเหลืออย่างที่สุดมาโดยตลอดจนสำเร็จการศึกษา

ขอขอบพระคุณคณาจารย์ทุกท่านที่ให้การอบรม สั่งสอนวิชาความรู้ต่างๆมาจนสำเร็จการศึกษา

ขอขอบคุณบัณฑิตวิทยาลัยและภาควิชาวิทยาการคอมพิวเตอร์ ที่ได้สนับสนุนด้านอุปกรณ์ด้านเงินทุนนำเสนองานในประเทศ และสถานที่ตลอดระยะเวลาในการทำวิทยานิพนธ์

ขอขอบคุณเพื่อนๆปริญญาโททุกคนที่ให้คำแนะนำการเขียนวิทยานิพนธ์ และความช่วยเหลืออำนวยความสะดวกในการสอบปากเปล่าขั้นสุดท้าย

คุณค่าและประโยชน์อันพึงมีจากวิทยานิพนธ์นี้ ขอมอบแด่ผู้มีพระคุณทุกท่าน

สัญชัย นิจวิภากุล

มิถุนายน 2557

สารบัญ

หน้า

สารบัญตาราง

สารบัญตาราง (ต่อ)

ตารางผนวกที่ **หน้า**

สารบัญภาพ

สารบัญภาพ (ต่อ)

ภาพที่ **หน้า**

ความพร้อมในการให้บริการดีเอ็นเอสเซคของไอเอสพีในประเทศไทย

DNSSEC Readiness of Thai ISPs

คำนำ

ระบบชื่อโดเมน (Domain Name System) หรือดีเอ็นเอส (DNS) อ้างอิงจาก RFC1034 (1987), RFC1035 (1987) และ Paul and Cricket (2001) เป็นระบบที่ "สำคัญ" และเป็นหัวใจของการให้บริการอื่นของอินเทอร์เน็ต (Internet) เนื่องจากดีเอ็นเอสทำหน้าที่แปลงชื่อโดเมน (Domain Name) ที่ใช้ในการติดต่อเป็นหมายเลขไอพี (IP address) จึงทำให้อุปกรณ์ต่างๆ ในอินเทอร์เน็ตสามารถสื่อสารและรับส่งข้อมูลถึงกันได้ตัวอย่างเช่น หากผู้ใช้งานต้องการเปิดเว็บ (web) www.ku.ac.th จำเป็นต้องทราบหมายเลขไอพีของเครื่องบริการ (server) ที่ให้บริการข้อมูลของเว็บ www.ku.ac.th จากนั้นจึงดำเนินกระบวนการในการติดต่อได้ หากได้รับหมายเลขไอพีของเครื่องบริการที่ให้บริการข้อมูลของเว็บ www.ku.ac.th มาผิด อาจเนื่องด้วยช่องโหว่ของดีเอ็นเอสต่างๆ ทำให้ข้อมูลความลับ เช่น รหัสในการเข้าระบบของเรารั่วไหลได้

จากเหตุดังกล่าวข้างต้นเป็นที่มาของดีเอ็นเอสเซค (DNSSEC) อ้างอิงจาก RFC4033 (2005), RFC4034 (2005), RFC4035(2005) ซึ่งเป็นส่วนขยายของดีเอ็นเอสเกี่ยวกับความปลอดภัย สามารถทำงานร่วมกับดีเอ็นเอสได้ โดยอาศัยหลักวิทยาการเข้ารหัสลับด้วยกุญแจไม่สมมาตร (Asymmetric Key) และลายเซ็นดิจิทัล (Digital Signature) เพื่อให้บริการในการรับรองความถูกของข้อมูลที่ได้รับจากแหล่งกำเนิดของแต่ละชื่อโดเมน (Data Origin Authentication) ข้อมูลไม่ถูกเปลี่ยนแปลงระหว่างการรับส่ง (Data Integrity) และรับรองคำตอบที่ว่าไม่มีชื่อโดเมนหรือชนิดของระเบียนทรัพยากร (Resource Record) ที่ร้องขอนั้นจริงๆ (Authenticating Name and Type Non-Existence) แต่อย่างไรก็ดีเอ็นเอสเซคไม่สามารถป้องกันการโจมตีเพื่อให้ระบบไม่สามารถให้บริการได้ (Denial-of-Service) และไม่รองรับการเข้ารหัส-ถอดรหัสข้อความที่รับและส่ง

การใช้บริการเอ็นเอสเซคนั้น คำตอบที่ได้รับจากเนมเซิร์ฟเวอร์ สามารถมีขนาดใหญ่กว่าเดิมเมื่อเทียบกับดีเอ็นเอส เนื่องจากการเพิ่มกระบวนการด้านความปลอดภัย ทำให้อุปกรณ์เครือข่ายบางอุปกรณ์ทำการโยนทิ้ง (discard) ข้อมูลนั้น ซึ่งสาเหตุอาจมาจากเหตุผลด้านความปลอดภัย ทำให้ผู้ร้องขอข้อมูลไม่ได้รับคำตอบ หรือหมายเลขไอพีที่ต้องการ ซึ่งเป็นสาเหตุให้ไม่สามารถใช้งานอินเทอร์เน็ตได้

การพบช่องโหว่ดีเอ็นเอสของ Dan Kaminsky ในปี พ.ศ. 2551 อ้างอิงจาก (Matthew Olney.,2008) และการประกาศนโยบายโดยรัฐบาลกลางของสหรัฐอเมริกาให้ปรับเปลี่ยนการใช้งานทุกโดเมนภายใต้โดเมน gov ให้รองรับการบริการดีเอ็นเอสเซคภายใน ธันวาคม พ.ศ. 2552 อ้างอิงจาก Karen Evans (2008) มีผลทำให้รูทเนมเซิร์ฟเวอร์และเนมเซิร์ฟเวอร์ในระดับ Top-Level ต้องปรับตัวตามมาให้บริการดีเอ็นเอสเซค วิทยานิพนธ์นี้เป็นการสำรวจความพร้อมในการให้บริการเอ็นเอสเซคของไอเอสพี (ISPs) ในประเทศไทย รวมทั้งเสนอรูปแบบการเข้าถึงบริการเอ็นเอสเซคผ่านแต่ละไอเอสพี และแนวทางในการทดสอบเครือข่ายว่ารองรับการทำงานของเอ็นเอสเซคหรือไม่ โดยทำการทดลองตั้งแต่เดือนมีนาคม พ.ศ. 2556 ถึงเดือนพฤศจิกายน พ.ศ. 2556 พบว่าผู้ให้บริการ 4 ใน 6 รายที่เนมเซิร์ฟเวอร์มีการสนับสนุนการทำงานของดีเอ็นเอสเซค และจากแนวโน้มเชื่อว่าผู้ให้บริการอื่นๆจะปรับตัวตามในไม่ช้า

วัตถุประสงค์

1. เพื่อศึกษาและสำรวจความพร้อมในการให้บริการดีเอ็นเอสเซคของไอเอสพีในประเทศไทย

2. เพื่อศึกษาการทำงานของดีเอ็นเอสเซค

3. เสนอแนวทางในการทดสอบเครือข่ายสำหรับการใช้งานดีเอ็นเอสเซค

ประโยชน์ที่คาดว่าจะได้รับ

1. ไอเอสพีสามารถใช้กระบวนการของวิธีการสำรวจเป็นแนวทางในการตรวจสอบเครือข่ายของไอเอสพีเอง

2. ผู้ดูแลเครือข่ายสามารถใช้กระบวนการของวิธีการสำรวจในการตรวจสอบเครื่อข่ายของตัวเองได้

3. ช่วยเป็นแรงผลักดันให้ไอเอสพีหรือองค์กรธุรกิจต่างๆ เล็งเห็นความสำคัญของการใช้งานดีเอ็นเอสเซค

ขอบเขตและข้อจำกัด

1. ไอเอสพีในประเทศไทยมีจำนวนมาก และมีบริการหลากหลาย ซึ่งทำให้ไม่สามารถทดสอบได้ทุกไอเอสพี

2. การใช้งานอินเตอร์เน็ทอาจจะเสียค่าบริการเป็นรายปี หรือทำสัญญาเป็นปีจึงอาจไม่สามารถทดสอบได้ทุกไอเอสพี

3. การทดสอบกับเนมเซิร์ฟเวอร์ของทางไอเอสพี 1 เครื่อง อาจเป็นการไม่ยุติธรรมในการสรุปผล

การตรวจเอกสาร

ทฤษฎีที่เกี่ยวข้อง

การรับและส่งข้อมูลบนอินเทอร์เน็ต อุปกรณ์ต้นทางจำเป็นต้องรู้หมายเลขไอพีของอุปกรณ์ปลายทางถึงจะสามารถส่งข้อมูลถึงกันได้ ด้วยการเติบโตของอินเทอร์เน็ตทำให้มีอุปกรณ์เที่เชื่อต่ออินเทอรเน็ตจำนวนมากมายมหาศาล และการท่องจำหมายเลขไอพีซึ่งเป็นเลขฐานสองจำนวน 32 บิต นั้นเป็นเรื่องยาก จึงมีระบบที่ทำการกำหนดชื่อให้กับอุปกรณ์ในอินเทอร์เน็ต ซึ่งเป็นชื่อที่มนุษย์เข้าใจและจดจำง่าย โดยระบบนี้เรียกว่าดีเอ็นเอส

ระบบชื่อโดเมน (Domain Name System)

ระบบชื่อโดเมน หรือ ดีเอ็นเอสซึ่งให้บริการแปลงชื่อโดเมนเป็นหมายเลขไอพี (IP address) หรือหมายเลขไอพีเป็นชื่อโดเมน มีโครงสร้างแบบลำดับขั้น หรือแบบต้นไม้ ไม่มีศูนย์กลาง

องค์ประกอบ และ คำศัพท์ที่เกี่ยวข้อง

1. โดเมนเนมสเปซ (Domain Name Space)

คือโครงสร้างต้นไม้ ใช้ในการตั้งชื่อโดเมน โดยแต่ละโหนดมีป้าย (label) กำกับไว้ ซึ่งอาจจะว่างป่าวได้

ภาพที่ 1 โดเมนเนมสเปซ

ที่มา: Paul and Cricket (April 2001)

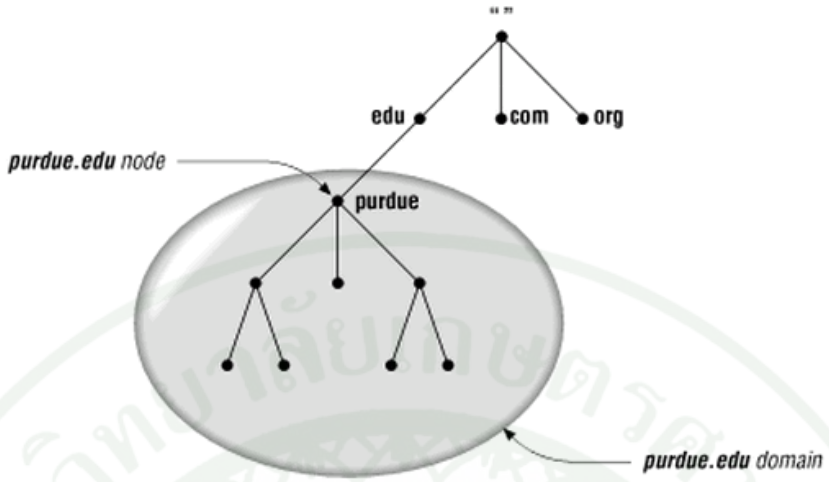
2. ป้าย (Label)

โหนดแต่ละโหนดจะมีป้ายซึ่งมีความยาวตั้งแต่ 0 ถึง 63 ตัวอักษร โดยโหนดในระดับเดียวกัน หรือโหนดพี่น้อง ไม่สามารถมีป้ายเหมือนกันได้ โหนดคนละระดับสามารถมีป้ายที่ซ้ำกับโหนดอื่นได้

ป้ายที่มีความยาวเท่ากับ 0 ถูกสงวนไว้สำหรับ โหนดรากที่อยู่บนสุดของต้นไม้หรือลำดับขั้น โดย arpa, com, edu, gov, mil และ org คือป้ายของแต่ละโหนดดังภาพที่ 1

3. ชื่อโดเมน (Domain Name)

ชื่อโดเมนของแต่ะละโหนด คือการนำป้ายของแต่ละโหนดมาต่อกัน ซึ่งเริ่มต้นจากโหนดนั้นไปถึงโหนดราก โดยไม่สนใจตัวอักษรว่าเป็นพิมพ์ใหญ่หรือตัวอักษรพิมพ์เล็ก ซึ่งคั่นแต่ละป้ายด้วยจุด (".") และมีความยาวไม่เกิน 255 ตัวอักษร สามารถดูตัวอย่างเช่น จากภาพที่ 2 ชื่อโดเมนของโหนดที่ป้ายเป็น purdue คือ purdue.edu



ภาพที่ 2 โดเมน pudue.edu

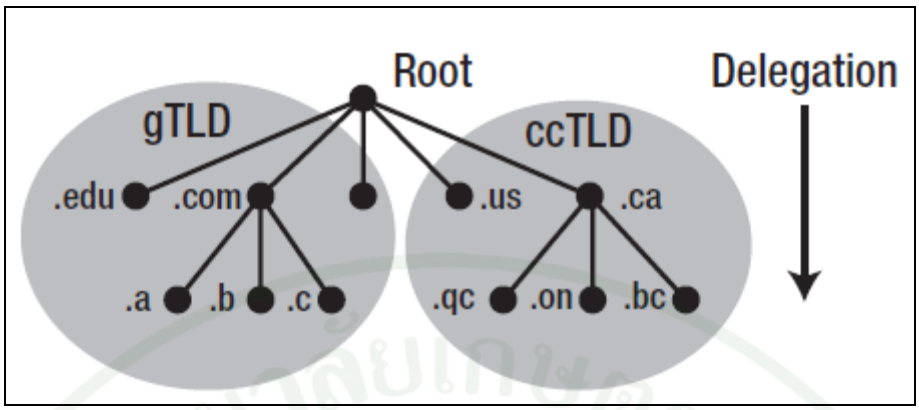
ที่มา: Paul and Cricket (April 2001)

4. โดเมน (Domain)

คือ โครงสร้างต้นไม้ส่วนย่อยของโดเมนเนมสเปซ ครอบคลุมส่วนของโหนดลูกทั้งหมด ดังแสดงในภาพที่ 2 โดยโดเมนเป็นการกำหนดขอบเขตของการบริหารและจัดการโดเมนให้องค์กรดูแล

4.1. โดเมนระดับ Top-Level

โดเมนระดับ Top-Level หรือ TLD คือโดเมนที่อยู่ระดับสูงสุดซึ่งรองจากโหนดราก แบ่งเป็น 2 ชนิด ได้แก่โดเมนระดับ Top-Level ทั่วไป (generic Top-Level Domains) หรือ gTLD และโดเมนระดับ Top-Level รหัสประเทศ (country-code Top-Level Domains) หรือ ccTLD ดังแสดงในภาพที่ 3 โดย edu และ com เป็นโดเมนระดับ Top-Level ทั่วไป ส่วน us และ ca เป็นโดเมนระดับ Top-Level รหัสประเทศ



ภาพที่ 3 โดเมนระดับ Top-Level

ที่มา: Ron Aitchison (2011)

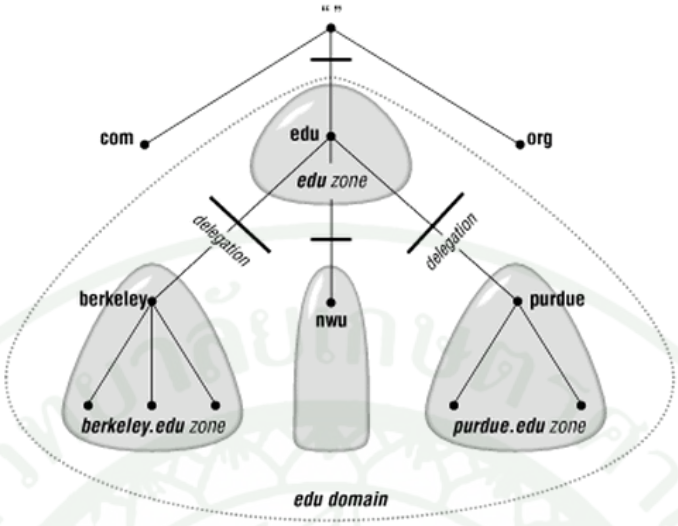
4.2. เจ้าของโดเมน (Domain Authority) และ การมอบหน้าที่ (Delegation)

เจ้าของโดเมนคือองค์กรที่บริหารจัดการโดเมนนั้นๆ และเจ้าของโดเมนสามารถทำการมอบหน้าที่การบริหารจัดการโดเมนในระดับล่างให้แก่องค์กรอื่น ซึ่งเป็นไปตามโครงสร้างลำดับขั้นของดีเอ็นเอส

ตัวอย่าง เช่น ICANN (Internet Corporation for Assigned Numbers) เป็นองค์กรที่ไม่แสวงหากำไรในประเทศสหรัฐอเมริกาบริหารจัดการโดเมน root ซึ่ง ICANN บริหารจัดการโดเมนระดับ Top-Level ทั่วไป โดยมีการมอบหน้าที่ให้แก่องค์กรอื่นที่ทำการลงทะเบียนและทำตามข้อตกลงของ ICANN และ ICANN ทำการกำหนดโดเมนระดับ Top-Level รหัสประเทศ ให้องค์กรของแต่ละประเทศ อ้างอิงจาก Ron Aitchison (2011:6)

5. โซน (Zone) และแฟ้มข้อมูลโซน (Zone File)

โซนคือส่วนของโดเมนเนมสเปซ ซึ่งต้องต่อเนื่องกัน โดยบ่งบอกถึงการแบ่งการบริหารจัดการข้อมูลของดีเอ็นเอสออกเป็นส่วนๆ ในการใช้งานจริงแฟ้มข้อมูลโซนจะเป็นตัวแทนของโซนที่เนมเซิร์ฟเวอร์ใช้ในการทำงานเกี่ยวกับดีเอ็นเอส โดยแฟ้มข้อมูลโซนจะประกอบไปด้วยระเบียนทรัพยากรชนิดต่างๆ ที่เนมเซิร์ฟเวอร์ใช้เป็นข้อมูลในการแปลงชื่อโดเมนเป็นหมายเลขไอพี



ภาพที่ 4 โซนและโดเมน

ที่มา: Paul and Cricket (April 2001)

6. ระเบียนทรัพยากร (Resource Record)

ข้อมูลในดีเอ็นเอสจะถูกเก็บในรูปแบบระเบียนทรัพยากร โดยข้อมูลในแต่ละระเบียนทรัพยากรจะแตกต่างกันไป ขึ้นอยู่กับว่าระเบียนทรัพยากรเป็นระเบียนทรัพยากรชนิดใด ใช้ในระบบใด ซึ่งระเบียนทรัพยากรมีโครงสร้างดังแสดงในภาพที่ 5 และสามารถดูรายละเอียดส่วนต่างๆ ของโครงสร้างระเบียนทรัพยากรได้จากตารางที่ 1

Name	Type	Class	TTL	RDLength	RDATA

ภาพที่ 5 โครงสร้างระเบียนทรัพยากร

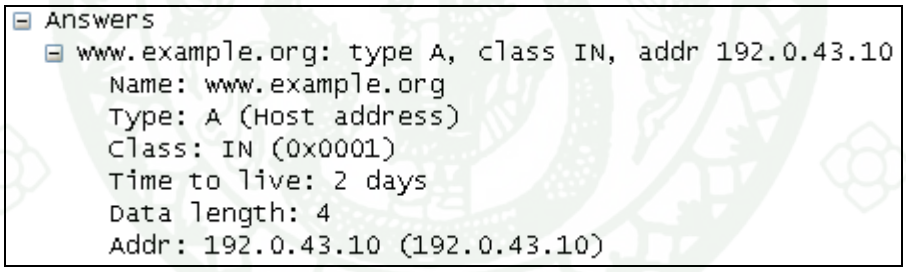
ตารางที่ 1 รายละเอียดของส่วนต่างๆ ในระเบียนทรัพยากร

ส่วน	รายละเอียด	ความยาว
Name	แสดงชื่อโดเมนของระเบียนทรัพยากร	ชื่อโดเมน

ตารางที่ 1 (ต่อ)

ส่วน	รายละเอียด	ความยาว
Type	แสดงชนิดของระเบียนทรัพยากร	2 ไบต์
Class	ระบุว่าระเบียนทรัพยากรทำงานบนระบบใด เช่น ในอินเทอร์เน็ตส่วนนี้มีค่าเท่ากับ 1	2 ไบต์
TTL	แสดงช่วงเวลาวินาทีที่ระเบียนทรัพยากรจะสามารถอยู่ในแคชของเนมเซิร์ฟเวอร์ได้	4 ไบต์
RDLength	แสดงความยาวของส่วน RData	2 ไบต์
Rdata	แสดงข้อมูลของระเบียนทรัพยากรตาม Type และ Class	ตามข้อมูล

สามารถดูตัวอย่างชนิดระเบียนทรัพยากรและรายละเอียดได้จากตารางที่ 2 และภาพตัวอย่างระเบียนทรัพยากรที่ได้จากโปรแกรมดักจับแพ็กเก็ต (packet) ชื่อว่า Wireshark จากภาพที่ 6



ภาพที่ 6 ตัวอย่างระเบียนทรัพยากรที่ได้จากโปรแกรม Wireshark

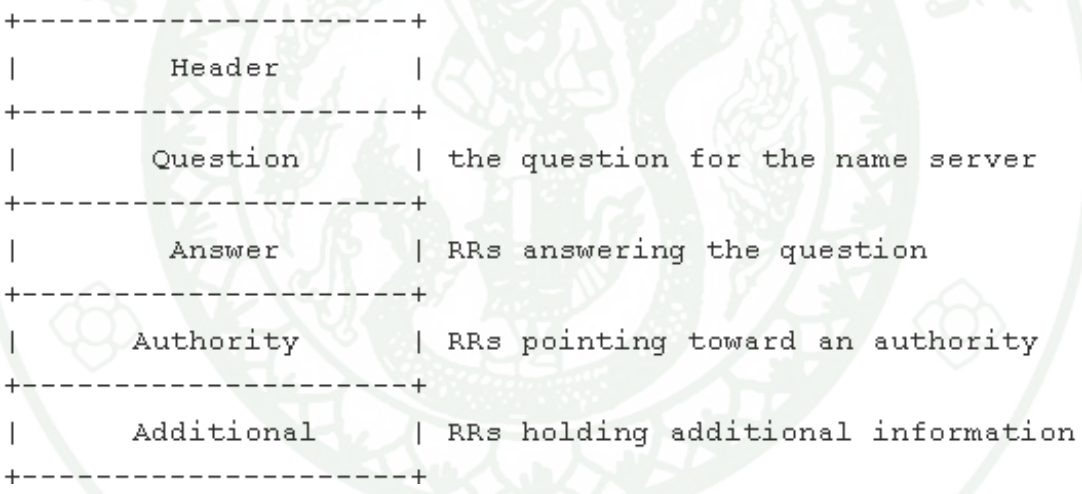
ตารางที่ 2 ตัวอย่างชนิดระเบียนทรัพยากรและรายละเอียด

ชนิดของระเบียนทรัพยากร	รายละเอียด
A	หมายเลขไอพีเวอร์ชั่น 4
AAAA	หมายเลขไอพีเวอร์ชั่น 6
NS	เนมเซิร์ฟเวอร์
CNAME	ผูกชื่อโดเมนหนึ่งกับอีกชื่อโดเมนหนึ่ง

ตารางที่ 2 (ต่อ)

ชนิดของระเบียนทรัพยากร	รายละเอียด
SOA	แสดงรายละเอียดชื่อโซน เนมเซิร์ฟเวอร์หลักที่จัดการข้อมูลของโซน อีเมล์ของผู้ดูแล และรายละเอียดเกี่ยวกับวันในการปรับให้เป็นปัจจุบัน
PTR	ตัวชี้ชื่อโดเมนใช้ในการเปลี่ยนหมายเลขไอพีเป็นชื่อโดเมน
MX	ชื่อโดเมนของเครื่องบริการอีเมล์
TXT	ข้อความที่เป็นตัวอักษร

7. ข้อความดีเอ็นเอส (DNS messages)



ภาพที่ 7 โครงสร้างข้อความดีเอ็นเอส

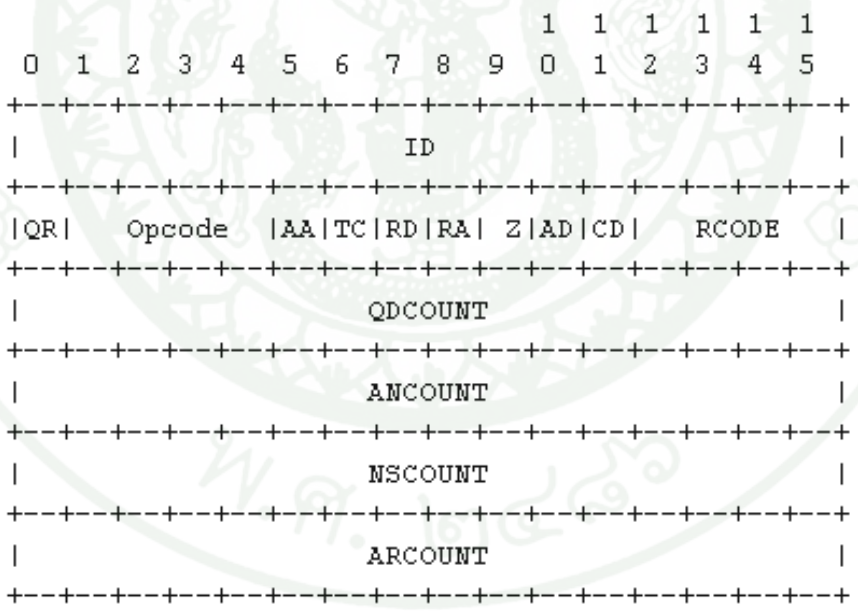
ที่มา: RFC1034 (1987)

ในการรับและส่งข้อมูลของดีเอ็นเอส ใช้โครงสร้างเดียวกัน ซึ่งเรียกว่าข้อความ (message) แบ่งได้เป็น 2 แบบคือ query โดยเนมเซิร์ฟเวอร์หรือไคลเอนต์ (client) ใช้สำหรับสอบถามข้อมูลเกี่ยวกับดีเอ็นเอส และ response โดยเนมเซิร์ฟเวอร์ใช้สำหรับตอบคำถามเกี่ยวกับดีเอ็นเอส ซึ่งโครงสร้างของข้อความดีเอ็นเอสแบ่งเป็นส่วนต่างๆ ดังภาพที่ 7

ตารางที่ 3 รายละเอียดของส่วนต่างๆ ในโครงสร้างข้อความดีเอ็นเอส

ส่วนโครงสร้างข้อความดีเอ็นเอส	รายละเอียด
Header	แบ่งเป็นตัวบ่งชี้ (flag) เพื่อระบุค่าต่างๆ เกี่ยวกับข้อความ
Question	ส่วนที่เป็นคำถาม แบ่งเป็น 3 ส่วนได้แก่ QNAME, QTYPE และ QCLASS
Answer	ส่วนที่บรรจุระเบียนทรัพยากรสำหรับคำตอบ
Authority	ส่วนที่บรรจุระเบียนทรัพยากรของเนมเซิร์ฟเวอร์ที่เกี่ยวข้องกับชื่อโดเมนที่สอบถาม
Additional	ส่วนที่บรรจุระเบียนทรัพยากรที่เกี่ยวข้องกับ ระเบียนทรัพยากรในส่วน Answer และ Authority

7.1. โครงสร้างส่วนหัว (header) ของข้อความดีเอ็นเอส



ภาพที่ 8 โครงสร้างส่วนหัวของข้อความดีเอ็นเอส

ที่มา: RFC2535 (1999)

ตารางที่ 4 รายละเอียดของส่วนต่างๆ ในส่วนหัวของข้อความดีเอ็นเอส

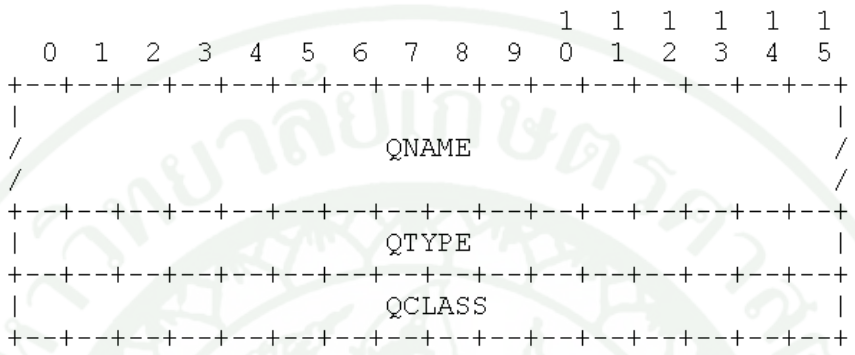
ส่วนและตัวบ่งชี้	รายละเอียด
ID	ตัวเลขที่ใช้ระบุ query และถูกคัดลอกลงใน response ที่เกี่ยวข้องกัน
QR	ถ้าเป็น query มีค่าเป็น 0 หรือ response มีค่าเป็น 1
Opcode	แสดงชนิดของ query ค่าเป็น 0 เป็น query ธรรมดา ค่าเป็น 1 เป็น query แบบผกผัน (inverse) ค่าเป็น 2 เป็น query ใช้สอบถามสถานะของเครื่องบริการ ค่าเป็น 3-15 สงวนไว้ใช้ในอนาคต
AA (Authoritative Answer)	มีค่าเป็น 1 ใน response ที่มากจากเครื่องบริการเจ้าของชื่อโดเมน (Authoritative Name Server)
TC (Truncation)	มีค่าเป็น 1 ใน response ที่มีขนาดใหญ่เกิดกว่าที่จะส่งด้วยโพรโทคอล UDP ในครั้งเดียว
RD (Recursion Desired)	หากค่าเป็น 0 ใน query เครื่องบริการที่ได้รับ query จะทำการส่ง response โดยใช้ข้อมูลภายในแคชของตนเอง หากค่าเป็น 1 ใน query เครื่องบริการที่ได้รับ query จะทำการส่ง response โดยใช้ข้อมูลภายในแคชของตนเอง และหากไม่มีข้อมูลในแคชของตนเอง เครื่องบริการจะทำกระบวนการหาคำตอบ (Resolution) จนได้คำตอบจึงจะทำการส่ง response กลับไป
RA (Recursion Available)	มีค่าเป็น 0 ใน response แสดงว่า เนมเซิร์ฟเวอร์ที่ได้รับ query นั้น ไม่รองรับการทำงานแบบเรียกซ้ำ (recursive) มีค่าเป็น 1 ใน response แสดงว่า เนมเซิร์ฟเวอร์ที่ได้รับ query นั้น รองรับการทำงานแบบเรียกซ้ำ (recursive)
Z	สำรองไว้ใช้ในอนาคต มีค่าเป็น 0

ตารางที่ 4 (ต่อ)

ส่วนและตัวบ่งชี้	รายละเอียด
AD (Authenticated Data)	มีค่าเป็น 1 ใน response แสดงข้อมูลใน response ปลอดภัย เชื่อถือได้
CD (Checking Disabled)	มีค่าเป็น 1 ใน query เพื่อแจ้งเครื่องบริการโดเมนที่ได้รับ query นั้นไป ไม่ต้องดำเนินการตรวจสอบข้อมูล (validation)
RCODE (Response code)	แสดงสถานะของ response ค่าเป็น 0 ไม่มีข้อผิดพลาดเกิดขึ้น ค่าเป็น 1 เครื่องบริการไม่สามารถตีความ query ที่ได้รับมาได้ (FORMERR) ค่าเป็น 2 เครื่องบริการไม่สามารถดำเนินการตาม query ได้ เนื่องจากเครื่องบริการมีปัญหา (SERVFAIL) ค่าเป็น 3 แสดงว่าไม่มีชื่อโดเมนหรือชนิดของระเบียนทรัพยากรตามที่ query สอบถามมา (NXDOMAIN) ค่าเป็น 4 แสดงว่าเครื่องบริการนี้ไม่สนับสนุนชนิดของ query ที่ได้รับ ค่าเป็น 5 เครื่องบริการปฏิเสธการดำเนินตาม query (REFUSED) ค่าเป็น 6 ถึง 15 สำรองไว้ใช้ในอนาคต
QDCOUNT	บอกจำนวนของคำถามในส่วน question ของข้อความดีเอ็นเอส
ANCOUNT	บอกจำนวนของระเบียนทรัพยากรในส่วน Answer ของข้อความดีเอ็นเอส
NSCONUT	บอกจำนวนของระเบียนทรัพยากรในส่วน Authority ของข้อความดีเอ็นเอส
ARCOUNT	บอกจำนวนของระเบียนทรัพยากรในส่วน Additional ของข้อความดีเอ็นเอส

7.2. โครงสร้างของส่วนคำถาม (Question) ของข้อความดีเอ็นเอส

สามารถดูโครงสร้างของส่วนคำถามของข้อความดีเอ็นเอสได้จากภาพที่ 9 และรายละเอียดของส่วนต่างๆ แสดงในตารางที่ 5



ภาพที่ 9 โครงสร้างส่วนคำถามของข้อความดีเอ็นเอส

ที่มา: RFC1035 (1987)

ตารางที่ 5 รายละเอียดโครงสร้างของส่วนคำถามของข้อความดีเอ็นเอส

โครงสร้างของส่วนคำถามของข้อความดีเอ็นเอส	รายละเอียด
QNAME	ชื่อโดเมนใน query ที่ต้องการทราบ
QTYPE	ชนิดของระเบียนทรัพยากรที่ต้องการทราบ
QCLASS	ทำงานระบบใด

8. อีดีเอ็นเอส (Extension Mechanisms for DNS)

เนื่องจากข้อความในดีเอ็นเอสถูกจำกัดขนาดอยู่ที่ 512 ไบต์ สำหรับการใช้โพรโตคอล UDP ในการรับส่งข้อมูล ซึ่งการเติบโตของอินเทอร์เน็ต ทำให้มีชื่อโดเมนเกิดขึ้นมากมาย หรือบริการดีเอ็นเอสเซคทำให้ขนาดของ response มีขนาดใหญ่ขึ้นเกิน 512 ไบต์ ดังนั้นกระบวนการอีดีเอ็นเอสเวอร์ชัน 0 หรือ EDNS0 ซึ่งคือกระบวนการที่ ไคลเอนต์และเนมเซิร์ฟเวอร์ ทำการประกาศ

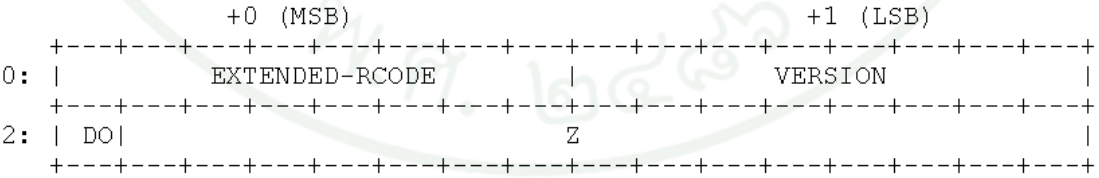
ว่ามีบัฟเฟอร์ขนาดเท่าไหร่ไปกับ query และ response ทำให้ไคลเอนต์และเครื่องบริการต่างๆ สามารถรับส่งข้อมูลดีเอ็นเอสที่ขนาดเกิน 512 ไบต์ได้ โดยทำการเพิ่มระเบียนทรัพยากรที่กำหนดขึ้นมาใหม่ที่เรียกว่า Pseudo-RR ชนิด OPT (option) เพิ่มในส่วนของ Additional ของข้อความดีเอ็นเอส อ้างอิงจาก RFC6891 (2013)

ระเบียนทรัพยากร Pseudo-RR เป็นระเบียนทรัพยากรที่ RDLength มีค่าเป็น 0 ทำให้ RData ไม่มีข้อมูล สามารถดูรายละเอียดต่างๆของ Pseudo-RR ได้จากตารางที่ 6

ตารางที่ 6 โครงสร้างระเบียนทรัพยากร Pseudo-RR

โครงสร้างระเบียนทรัพยากร	รายละเอียด
Name	แสดงเป็นชื่อโดเมนราก
Type	มีค่า 41 สำหรับ OPT
Class	ระบุขนาดบัฟเฟอร์ที่ใช้ในการรับส่งข้อมูลได้
TTL	แสดงโครงสร้างตามภาพที่ 10
RDLength	ความยาวเป็น 0 เนื่องจากไม่มีข้อมูลใน Rdata
Rdata	ไม่มี

โครงสร้างของส่วน TTL ของระเบียนทรัพยากร pseudo-RR ดังภาพที่ 10 ซึ่งประกอบไปด้วยส่วน EXTENDEN-RCODE, VERSION, DO และ Z สามารถดูรายละเอียดได้จากตารางที่ 7



ภาพที่ 10 โครงสร้างของส่วน TTL ของระเบียนทรัพยากร Pseudo-RR

ที่มา: RFC6891 (2013)

ตารางที่ 7 รายละเอียดส่วนต่างๆ ของโครงสร้าง TTL ของระเบียนทรัพยากร Pseudo-RR

รายการ	รายละเอียด
EXTENDEN-RCODE	ใช้ร่วมกับ RCODE ที่อยู่ในส่วนหัวของข้อความดีเอ็นเอส ซึ่งรวมเป็น 12 bit (8 EXTENDEN-RCODE +4 RCODE)
VERSION	มีค่า 41 สำหรับ OPT pseudo-RR
DO (DNSSEC OK)	มีค่าเป็น 1 ใน query แบบดีเอ็นเอสเซค
Z	มีค่าเท่ากับ 0 สำรองไว้ใช้ในอนาคต

จากภาพที่ 11 ผู้วิจัยได้ใช้ไคลเอนต์ทำการทดสอบส่ง query ไปยังเนมเซิร์ฟเวอร์ b.nic.io โดยระบุขนาดบัฟเฟอร์ที่ไคลเอนต์จัดการได้ที่ 1000 ไบต์ และได้รับ response กลับมาจาก ซึ่งขนาดไม่เกิน 1000 ไบต์ และตัวบงชี้ TC มีค่าเท่ากับ 1 โดยปกติแล้วหากระบุขนาดบัฟเฟอร์เป็น 4096 ไบต์จะได้รับ response ที่มีขนาดประมาณ 2500 ไบต์

```
C:\>
C:\>dig +nodnssec +norec +retry=0 +ignore +qr +bufsize=1000 any ac. @b.nic.io.

; <<>> DiG 9.8.4 <<>> +nodnssec +norec +retry=0 +ignore +qr +bufsize=1000 any ac
. @b.nic.io.
;; global options: +cmd
;; Sending:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 46276
;; flags:; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1000
;; QUESTION SECTION:
;ac.                            IN      ANY

;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 46276
;; flags: qr aa tc; QUERY: 1, ANSWER: 16, AUTHORITY: 0, ADDITIONAL: 3

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;ac.                            IN      ANY

;; ANSWER SECTION:
ac.                     86400   IN      A       193.223.78.210
ac.                     86400   IN      NS      a.nic.ac.
qdplaYmKef5SpXBpZveyFpNGhJMV01PN om1Z9/1f1RwEPRGZ9NK9r1abRwXykVK8d0aGrsHf1kJbaE/
ZL0PBMWBt KZ5nCQm8LFNwueGYYL/hiLiIDenD1hHSARCyO03P0nPnUUoHrYLXulfm NWFeUDs3EWk=
ac.                     86400   IN      RRSIG   A 8 1 86400 20140817012654 20140
712171441 15896 ac. UW2tjIJHhymYy0ZylwDO1M50UUDhp6xWvXc/oVr8aseNEt5tQOCvkgjl 5Jc
s5YYGNBKWkLOORX6uIVsINdYmCPMMz3nWH/oA3U6CbU0Cmm4bz4Zi YQvCqCCzOAFns5sRY9a3q8hImt
FT/cZnuP76tH3holj8/dKcgcGlpQoS F/k=

;; ADDITIONAL SECTION:
b.nic.ac.               172800  IN      A       78.104.145.37
a.nic.ac.               172800  IN      A       64.251.31.177

;; Query time: 343 msec
;; SERVER: 194.0.2.1#53(194.0.2.1)
;; WHEN: Mon Jul 14 19:48:56 2014
;; MSG SIZE  rcvd: 893
```

ภาพที่ 11 ผลลัพธ์ที่ได้จากการปรับขนาดบัฟเฟอร์

9. เนมเซิร์ฟเวอร์ (Name Server)

คือเครื่องบริการที่มีโปรแกรมจัดการข้อมูลเกี่ยวกับชื่อโดเมน ซึ่งเนมเซิร์ฟเวอร์จะตอบการร้องขอโดยใช้ข้อมูลตัวเอง หรือส่งคำร้องไปยังเนมเซิร์ฟเวอร์อื่น ขึ้นอยู่กับชนิดของเนมเซิร์ฟเวอร์นั้นๆ แบ่งเป็น 3 ชนิดดังนี้

9.1. เครื่องบริการเจ้าของชื่อโดเมน (Authoritative Name Servers)

ถ้าเนมเซิร์ฟเวอร์ บริหารจัดการข้อมูลเกี่ยวกับชื่อโดเมนที่สอบถามมา ไม่ได้รู้จากแคช หรือจากกระบวนการหาคำตอบ แสดงว่าเครื่องบริการนั้นเป็นเครื่องบริการเจ้าของชื่อโดเมน ซึ่งบริหารจัดการข้อมูลของชื่อโดเมนนั้นๆ

9.2. รีโซลเวอร์ (Resolver)

คือเครื่องบริการที่ทำการหาชื่อโดเมน จากการสอบถามของไคลเอนต์ หรือเนมเซิร์ฟเวอร์ต่างๆ ซึ่งจะบันทึกข้อมูลที่ได้จากกระบวนการหาคำตอบ (Resolution) ลงในแคช (cache) จนข้อมูลนั้นหมดอายุ และทำการตอบคำถามจากข้อมูลในแคชก่อนที่จะไปสอบถามจากเนมเซิร์ฟเวอร์อื่น

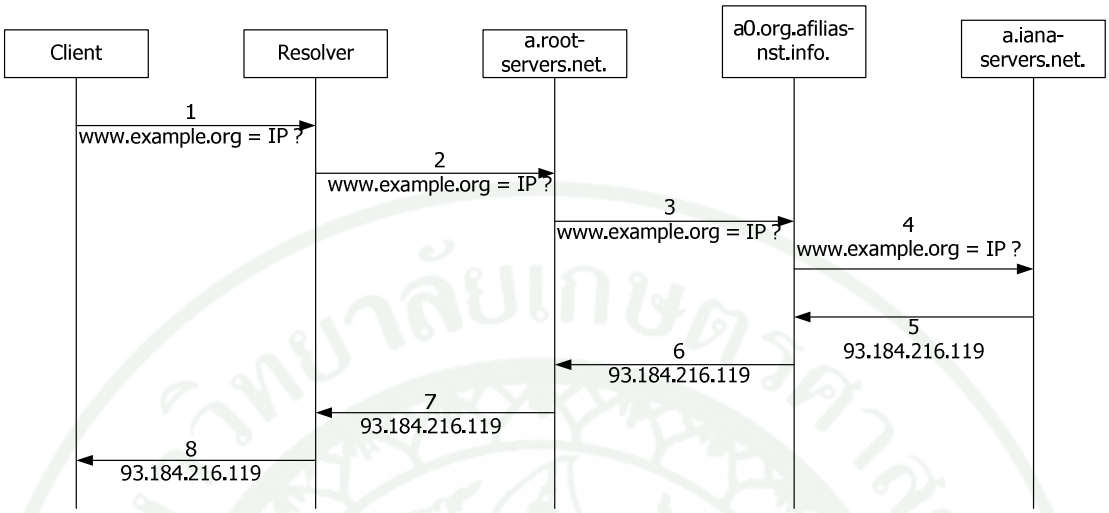
9.3. เนมเซิร์ฟเวอร์เรียกซ้ำ (Recursive Name Server)

คือเครื่องบริการที่ทำหน้าที่ทั้ง เครื่องบริการเจ้าของชื่อโดเมน และรีโซลเวอร์ในเครื่องเดียวกัน

10. กระบวนการหาคำตอบ (Resolution)

คือกระบวนการในการหาคำตอบของรีโซลเวอร์ โดยปกติจะเริ่มจากการที่ไคลเอนต์ส่ง query ไปยังที่รีโซลเวอร์ที่ถูกตั้งค่าไว้ จากนั้นรีโซลเวอร์ จะทำการส่ง query ไปยังเนมเซิร์ฟเวอร์อื่นๆ จนได้รับ response รีโซลเวอร์จึงทำการตอบกลับไปยังไคลเอนต์ที่ส่ง query มา โดยมีการทำงานอยู่สองแบบ

10.1. กระบวนการหาคำตอบแบบเรียกซ้ำ (Recursive Resolution)



ภาพที่ 12 กระบวนการหาคำตอบแบบเรียกซ้ำ

จากภาพที่ 12 แสดงกระบวนการหาคำตอบแบบเรียกซ้ำ โดยไคลเอนต์ทำการส่ง query สอบถามหมายเลขไอพีของชื่อโดเมน www.example.org ไปยังรีโซลเวอร์ที่ทำการตั้งค่าไว้ สามารถดูรายละเอียดของกระบวนการได้จากตารางที่ 8

ตารางที่ 8 รายละเอียดการทำงานของกระบวนการหาคำตอบแบบเรียกซ้ำ

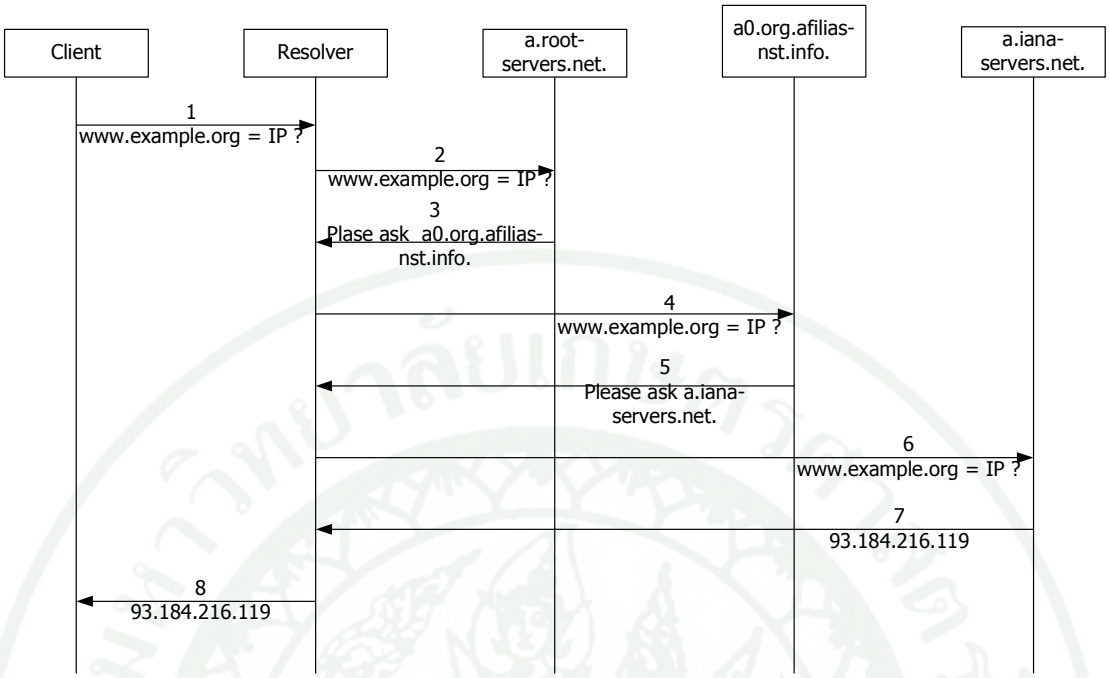
กระบวนการที่	รายละเอียด
1	ไคลเอนต์ทำการส่ง query สอบถามหมายเลขไอพีของชื่อโดเมน www.example.org ไปยังรีโซลเวอร์ที่ทำการตั้งค่าไว้
2	รีโซลเวอร์ทำการส่ง query สอบถามหมายเลขไอพีของชื่อโดเมน www.example.org ไปยังเครื่องบริการ a.root-servers.net ซึ่งคือเครื่องบริการเจ้าของชื่อโดเมน root
3	เครื่องบริการ a.root-servers.net ทำการส่ง query สอบถามหมายเลขไอพีของชื่อโดเมน www.example.org ไปยังเครื่องบริการ a0.org.afilias-nst.info ซึ่งคือเครื่องบริการเจ้าของชื่อโดเมน org

ตารางที่ 8 (ต่อ)

กระบวนการที่	รายละเอียด
4	เครื่องบริการ a0.org.afilias-nst.info ทำการส่ง query สอบถามหมายเลขไอพีของชื่อโดเมน www.example.org ไปยังเครื่องบริการ a.iana-servers.net ซึ่งคือเครื่องบริการเจ้าของชื่อโดเมน example.org
5	เครื่องบริการ a.iana-servers.net ซึ่งคือเครื่องบริการเจ้าของชื่อโดเมน example.org ทำการส่ง response หมายเลขไอพีของชื่อโดเมน www.example.org ไปยังเครื่องบริการ a0.org.afilias-nst.info
6	เครื่องบริการ a0.org.afilias-nst.info ทำการส่ง response หมายเลขไอพีของชื่อโดเมน www.example.org ไปยังเครื่องบริการ a.root-servers.net
7	เครื่องบริการ a.root-servers.net ทำการส่ง response หมายเลขไอพีของชื่อโดเมน www.example.org ไปยังรีโซลเวอร์
8	รีโซลเวอร์ทำการส่ง response หมายเลขไอพีของชื่อโดเมน www.example.org ไปยังไคลเอนต์

10.2. กระบวนการหาคำตอบแบบทำซ้ำ (Iterative Resolution)

กระบวนการหาคำตอบแบบทำซ้ำแตกต่างจากกระบวนการหาคำตอบแบบเรียกซ้ำ ที่รีโซลเวอร์จะทำการหาคำตอบเองทั้งหมดดังแสดงในภาพที่ 13 และสามารถดูรายละเอียดการทำงานได้จากตารางที่ 9



ภาพที่ 13 กระบวนการหาคำตอบแบบทำซ้ำ

ตารางที่ 9 รายละเอียดการทำงานของกระบวนการหาคำตอบแบบทำซ้ำ

กระบวนการที่	รายละเอียด
1	ไคลเอนต์ทำการส่ง query สอบถามหมายเลขไอพีของชื่อโดเมน www.example.org ไปยังรีโซลเวอร์ที่ทำการตั้งค่าไว้
2	รีโซลเวอร์ทำการส่ง query สอบถามหมายเลขไอพีของชื่อโดเมน www.example.org ไปยังเครื่องบริการ a.root-servers.net ซึ่งคือเครื่องบริการเจ้าของชื่อโดเมน root
3	เครื่องบริการ a.root-servers.net ทำการส่ง response กลับมาว่าไม่มีข้อมูลชื่อโดเมน www.example.org ให้ไปสอบที่เครื่องบริการ a0.org.afilias-nst.info แทน
4	รีโซลเวอร์ทำการส่ง query สอบถามหมายเลขไอพีของชื่อโดเมน www.example.org ไปยังเครื่องบริการ a0.org.afilias-nst.info ซึ่งคือเครื่องบริการเจ้าของชื่อโดเมน org

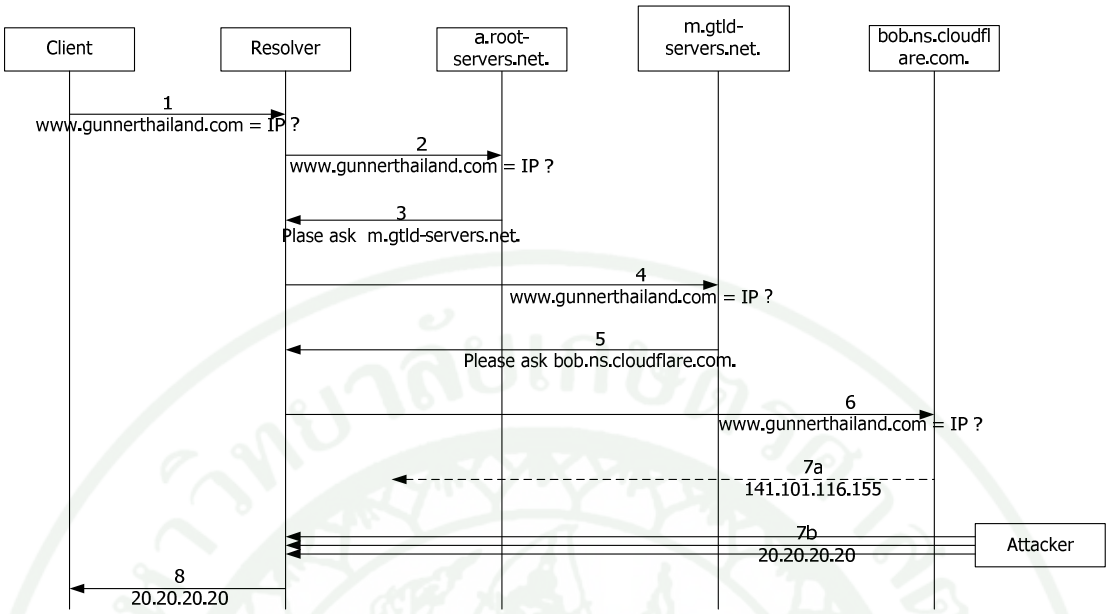
ตารางที่ 9 (ต่อ)

กระบวนการที่	รายละเอียด
5	เครื่องบริการ a0.org.afilias-nst.info ทำการส่ง response กลับมาว่าไม่มีข้อมูลชื่อโดเมน www.example.org ให้ไปสอบที่เครื่องบริการ a.iana-servers.net แทน
6	รีโซลเวอร์ทำการส่ง query สอบถามหมายเลขไอพีของชื่อโดเมน www.example.org ไปยังเครื่องบริการ a.iana-servers.net ซึ่งคือเครื่องบริการเจ้าของชื่อโดเมน example.org
7	เครื่องบริการ a0.org.afilias-nst.info ทำการส่ง response กลับมาหมายเลขไอพีของชื่อโดเมน www.example.org คือ 93.184.216.119
8	รีโซลเวอร์ทำการส่ง response ที่มีรายละเอียดหมายเลขไอพีของชื่อโดเมน www.example.org ไปยังไคลเอนต์

ช่องโหว่ของดีเอ็นเอส

1. การโจมตีแบบ Cache Poisoning

คือ การที่ผู้โจมตีพยายามส่งคำตอบปลอมให้กับรีโซลเวอร์ที่เป็นเป้าหมาย ก่อนที่ รีโซลเวอร์เป้าหมายจะได้รับคำตอบจริงๆ จากเครื่องบริการเจ้าของชื่อโดเมน โดยจะใช้ไอดี หมายเลขไอพี และพอร์ต (port) ที่รีโซลเวอร์ที่เป็นเป้าหมายใช้ในการหาคำตอบ หากไอดี หมายเลขไอพี และพอร์ตที่ผู้โจมตีส่งคำตอบปลอมให้กับรีโซลเวอร์เป้าหมายตรงกัน รีโซลเวอร์เป้าหมายก็จะรับคำตอบปลอมพร้อมกับทำการเก็บข้อมูลลงแคชของตัวเอง จนกระทั่งหมดช่วงเวลา TTL ดังนั้นหากมีไคลเอนต์ ที่ใช้งานรีโซลเวอร์นั้นก็จะได้รับข้อมูลที่ผิดพลาดไป อ้างอิงจาก Sainstitute (2003)



ภาพที่ 14 การโจมตีแบบ Cache Poisoning

ตารางที่ 10 กระบวนการโจมตีแบบ Cache Poisoning

กระบวนการที่	รายละเอียด
1	ไคลเอนต์ทำการส่ง query สอบถามหมายเลขไอพีของชื่อโดเมน www.gunnerthailand.com ไปยังรีโซลเวอร์ที่ทำการตั้งค่าไว้
2	รีโซลเวอร์ทำการส่ง query สอบถามหมายเลขไอพีของชื่อโดเมน www.gunnerthailand.com ไปยังเครื่องบริการ a.root-servers.net ซึ่งคือเครื่องบริการเจ้าของชื่อโดเมน root
3	เครื่องบริการ a.root-servers.net ทำการส่ง response กลับมาว่าไม่มีข้อมูลชื่อโดเมน www.gunnerthailand.com ให้ไปสอบที่เครื่องบริการ m.gtld-servers.net แทน
4	รีโซลเวอร์ทำการส่ง query สอบถามหมายเลขไอพีของชื่อโดเมน www.gunnerthailand.com ไปยังเครื่องบริการ m.gtld-servers.net ซึ่งคือเครื่องบริการเจ้าของชื่อโดเมน com
5	เครื่องบริการ m.gtld-servers.net ทำการส่ง response กลับมาว่าไม่มีข้อมูลชื่อโดเมน www.gunnerthailand.com ให้ไปสอบที่เครื่องบริการ bob.ns.cloudflare.com แทน

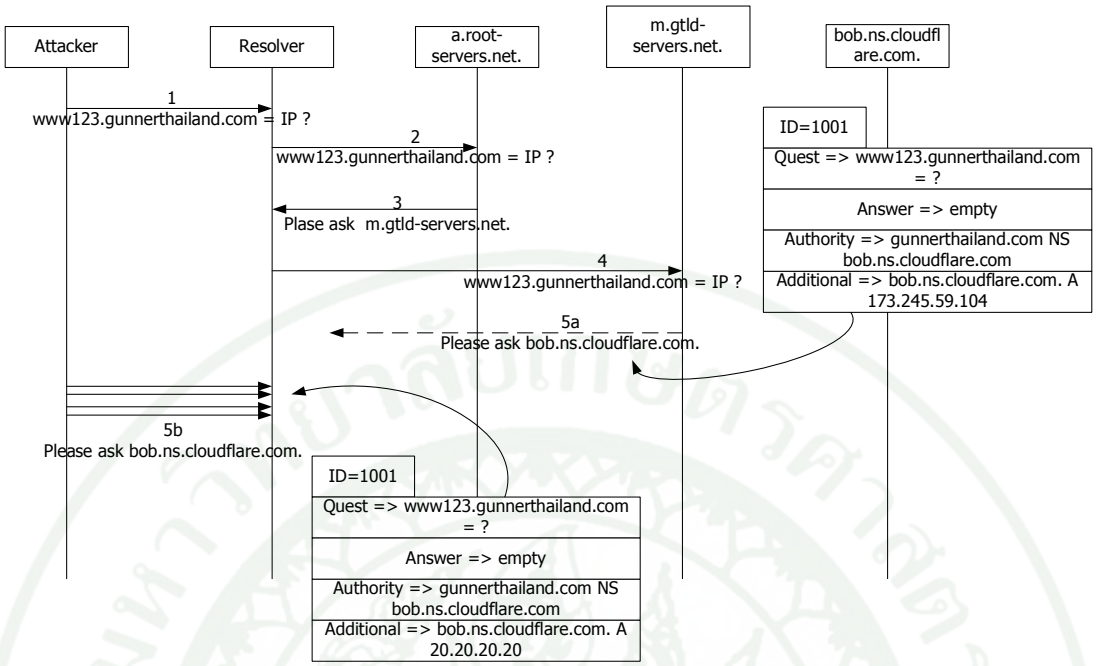
ตารางที่ 10 (ต่อ)

กระบวนการที่	รายละเอียด
6	รีโซลเวอร์ทำการส่ง query สอบถามหมายเลขไอพีของชื่อโดเมน www.gunnerthailand.com ไปยังเครื่องบริการ bob.ns.cloudflare.com ซึ่งคือเครื่องบริการเจ้าของชื่อโดเมน gunnerthailand.com
7a	เครื่องบริการ bob.ns.cloudflare.com ทำการส่ง response กลับมาหมายเลขไอพีของชื่อโดเมน www.gunnerthailand.com คือ 141.101.116.155
7b	ผู้โจมตีทำการส่ง response ปลอมจำนวนมากโดยมีข้อมูลของชื่อโดเมน www.gunnerthailand.com คือ 20.20.20.20 ก่อนที่ response จากกระบวนการที่ 7a จะมาถึงรีโซลเวอร์
8	รีโซลเวอร์ทำการส่ง response ที่มีรายละเอียดหมายเลขไอพีปลอมของชื่อโดเมน www.gunnerthailand.com ไปยังไคลเอนต์

การโจมตีชนิดนี้ผู้โจมตีจำเป็นต้องทราบ หมายเลขไอพีของรีโซลเวอร์ ค่า ID ในส่วน header และพอร์ตที่รีโซลเวอร์ใช้ในการส่ง query ซึ่งหมายเลขไอพีและพอร์ตอาจได้จากการดักฟังแพ็กเก็ต หรือทำการส่ง query สอบถามชื่อโดเมนต่างๆ ไปยังเครือข่ายที่ผู้โจมตีเอง บ่อยครั้งที่พอร์ตอาจจะเป็นค่าเดิม ส่วน ID ในส่วน header อาจจะมีการเพิ่มจากของเดิมไปทีละหนึ่ง เช่น ID ของ query ที่ส่งมีค่า 20000 ดังนั้น ID ของ query ที่ส่งถัดไปมีค่า 20001

2. ช่องโหว่ที่ค้นพบโดย Dan Kaminsky

ช่องโหว่ของดีเอ็นเอสแบบ Dan Kaminsky ซึ่งคือช่องโหว่แบบ Cache Poisoning เหมือนกัน แต่ช่องโหว่ที่ถูกค้นพบโดย Dan Kaminsky นั้น ผู้โจมตีจะทำการโจมตีโดยให้ส่วน Authority และ Additional ซึ่งมีข้อมูลที่ผิดพลาดถูกบันทึกลงในแคชของเครื่องบริการที่ถูกโจมตี แตกต่างจาก Cache Poisoning แบบเดิมที่ ผู้โจมตีจะทำการโจมตีโดยให้ส่วน Answer ซึ่งมีข้อมูลที่ผิดพลาดถูกบันทึกลงในแคชของเครื่องบริการที่ถูกโจมตี ดังแสดงในภาพที่ 15



ภาพที่ 15 ช่องโหว่ที่ค้นพบโดย Dan Kaminsky

ตารางที่ 11 รายละเอียดการทำงานของช่องโหว่ที่ค้นพบโดย Dan Kaminsky

กระบวนการที่	รายละเอียด
1	ผู้โจมตีทำการส่ง query สอบถามหมายเลขไอพีของชื่อโดเมน www123.gunnerthailand.com ไปยังรีโซลเวอร์ที่ต้องการโจมตี
2	รีโซลเวอร์ทำการส่ง query สอบถามหมายเลขไอพีของชื่อโดเมน www123.gunnerthailand.com ไปยังเครื่องบริการ a.root-servers.net ซึ่งคือเครื่องบริการเจ้าของชื่อโดเมน root
3	เครื่องบริการ a.root-servers.net ทำการส่ง response กลับมาว่าไม่มีข้อมูลชื่อโดเมน www123.gunnerthailand.com ให้ไปสอบที่เครื่องบริการ m.gtld-servers.net แทน
4	รีโซลเวอร์ทำการส่ง query สอบถามหมายเลขไอพีของชื่อโดเมน www123.gunnerthailand.com ไปยังเครื่องบริการ m.gtld-servers.net ซึ่งคือเครื่องบริการเจ้าของชื่อโดเมน com

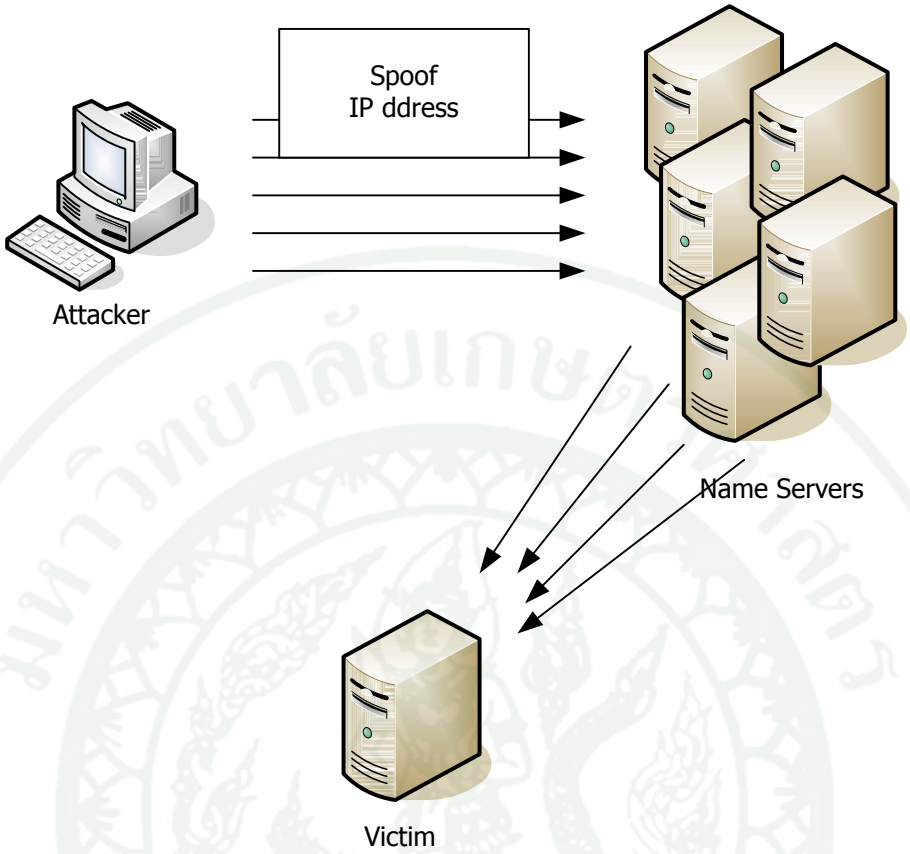
ตารางที่ 11 (ต่อ)

กระบวนการที่	รายละเอียด
5a	เครื่องบริการ m.gtld-servers.net ทำการส่ง response กลับมาว่าไม่มีข้อมูลชื่อโดเมน www123.gunnerthailand.com ให้ไปสอบที่เครื่องบริการ m.gtld-servers.net แทนโดยมีข้อมูลส่วน Authority และ Additional ดังภาพที่ 15
5b	ผู้โจมตีทำการทำการส่ง response ปลอมดังรูป จำนวนมากไปยังรีโซลเวอร์ก่อนที่ response จริงจาก m.gtld-servers.net ทำให้เนมเซิร์ฟเวอร์ดำเนินกระบวนการหาคำตอบต่อ แต่จะทำการสอบถามไปยังหมายเลขไอพีปลอม (20.20.20.20) ตามที่ได้รับข้อมูลผิดพลาดมา

จากภาพที่ 15 หากไคล์เอนต้องการทราบชื่อโดเมน หรือข้อมูลที่อยู่ในโซน gunnerthailand.com และส่ง query มายังรีโซลเวอร์ที่ถูกโจมตีนี้ รีโซลเวอร์จะทำการส่ง query สอบถามชื่อโดเมนหรือข้อมูลที่ต้องการทราบไปยังเครื่องบริการที่มีหมายเลขไอพี 20.20.20.20 แทนที่จะเป็น 173.245.59.104 หรือ bob.ns.cloudflare.com ซึ่งเป็นเครื่องบริการเจ้าของชื่อโดเมน gunnerthailand.com

3. การโจมตีแบบแอมพลิฟิเคชัน (DNS Amplification Attacks)

การโจมตีจากแบบหนึ่งซึ่งผู้โจมตีปลอมตัวเป็นผู้ถูกโจมตี โดยการปลอมเป็นหมายเลขไอพีเป็นหมายเลขไอพีของผู้ถูกโจมตี แล้วทำการส่ง query ที่คาดว่าจะได้รับตอบที่มีข้อมูลขนาดใหญ่ไปที่ เนมเซิร์ฟเวอร์หลายเครื่อง หลังจากเนมเซิร์ฟเวอร์หลายเครื่องนั้นได้รับ query ก็จะทำการส่ง response กลับไป ยังผู้ถูกโจมตีแทน ซึ่งจะทำให้การเชื่อต่ออินเทอร์เน็ตของผู้ถูกโจมตีรับภาระการใช้งานแบนด์วิดท์สูงจาก response ที่มีขนาดใหญ่ จากเนมเซิร์ฟเวอร์หลายๆ เครื่อง



ภาพที่ 16 การโจมตีแบบแอมพลิฟิเคชัน (DNS Amplification Attacks)

ดีเอ็นเอสเซค (DNSSEC) หรือ The Domain Name System Security Extensions

ดีเอ็นเอสเซคเป็นส่วนที่เพิ่มขยายของดีเอ็นเอสเกี่ยวกับความปลอดภัย สามารถทำงานร่วมกับดีเอ็นเอสได้ โดยอาศัยหลักวิทยาการเข้ารหัสลับด้วยกุญแจไม่สมมาตร (Asymmetric Key) และลายเซ็นดิจิตอล (Digital Signature) เพื่อให้บริการในการรับรองความถูกของข้อมูลที่ได้รับจากแหล่งกำเนิดของแต่ละชื่อโดเมน (Data Origin Authentication) ข้อมูลไม่ถูกเปลี่ยนแปลงระหว่างการรับส่ง (Data Integrity) และรับรองคำตอบที่ว่าไม่มีชื่อโดเมนหรือชนิดของระเบียนทรัพยากร (Resource Record) ที่ร้องขอนั้นจริงๆ (Authenticating Name and Type Non-Existence) แต่อย่างไรก็ดี ดีเอ็นเอสเซคไม่สามารถป้องกันการโจมตีเพื่อให้ระบบไม่สามารถให้บริการได้ (Denial-of-Service) และไม่รองรับการเข้ารหัส-ถอดรหัสข้อความที่รับและส่ง

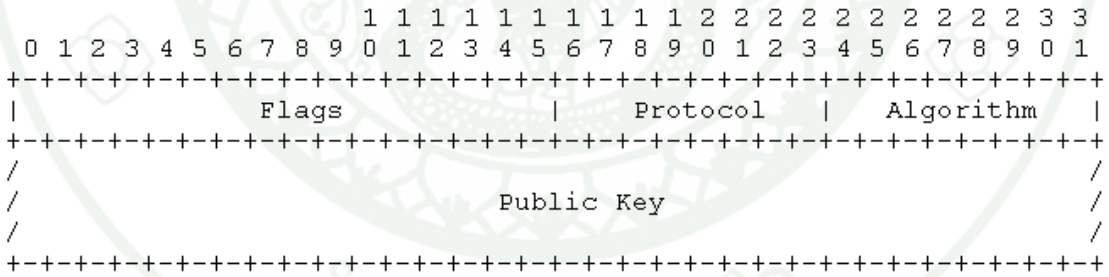
การปรับเปลี่ยนโพรโตคอล

1. ระเบียนทรัพยากรชนิดใหม่

เนื่องจากดีเอ็นเอสเซคให้บริการด้านความปลอดภัย ทำให้ต้องมีการปรับโพรโทคอลต่างจากเดิม ซึ่งมีการกำหนดระเบียนทรัพยากรชนิดใหม่ 4 ชนิดคือ DNS public key (DNSKEY), Delegation Signer (DS), Resource Record Signature (RRSIG) และ Next Secure (NSEC)

โดย DNSKEY ใช้เก็บข้อมูลเกี่ยวกับกุญแจสาธารณะ (public key) ของแต่ละโซนหรือแต่ละชื่อโดเมน DS โดยข้อมูลบางส่วนใน DS จะทำขึ้นมาจากการนำชื่อโดเมนของ DNSKEY และข้อมูล RData ใน DNSKEY นำมาต่อกันแล้วมาผ่านอัลกอริทึมเข้ารหัส RRSIG ใช้เก็บลายเซ็นดิจิตอลของระเบียนทรัพยากรชนิดต่างๆ และข้อมูลที่ใช้ระบุถึงกุญแจสาธารณะตัวไหนที่ใช้ในการทำลายเซ็นดิจิตอลรวมทั้งวันหมดอายุ NSEC ใช้เก็บชื่อโดเมนในลำดับถัดไปและชนิดของระเบียนทรัพยากรของชื่อโดเมนนั้นๆ

1.1. DNS Public Key (DNSKEY)



ภาพที่ 17 โครงสร้าง RData ของระเบียนทรัพยากร DNSKEY

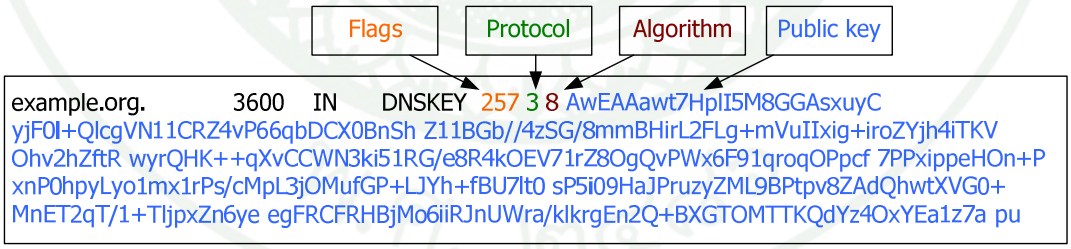
ที่มา: RFC4034 (2005)

ดีเอ็นเอสเซคใช้หลักการวิทยาการเข้ารหัสลับด้วยกุญแจไม่สมมาตรและลายเซ็นดิจิตอลในการรับรองความถูกต้องของข้อมูล โดยกุญแจส่วนบุคคลถูกใช้ทำการลายเซ็นดิจิตอล และกุญแจสาธารณะถูกเก็บไว้ในระเบียนทรัพยากร DNSKEY ซึ่งมีโครงสร้างส่วนของ RData ดังภาพที่ 17 และสามารถดูรายละเอียดต่างๆ ใน RData ได้จากตารางที่ 12

ตารางที่ 12 รายละเอียดของโครงสร้าง RData ของระเบียนทรัพยากร DNSKEY

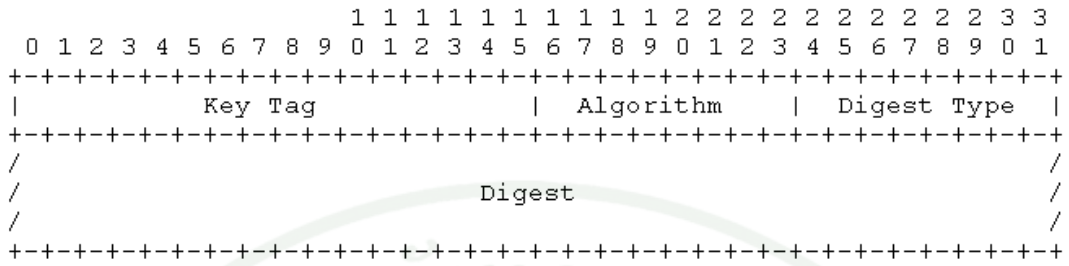
ส่วน	รายละเอียด
Flags	ขนาด 16 บิต บิตที่ 0 ถึง 6 และ 8 ถึง 14 เป็น 0 ทั้งหมดสำรองไว้ใช้ในอนาคต บิตที่ 7 มีค่าเป็น 0 แสดงว่ากุญแจสาธารณะชนิดอื่นๆ ถูกเก็บในระเบียนทรัพยากร DNSKEY ห้ามนำไปตรวจสอบลายเซ็นดิจิตอล บิตที่ 7 มีค่าเป็น 1 แสดงว่ากุญแจสาธารณะของโซนนี้ บิตที่ 15 เป็น 1 แสดงว่าระเบียนทรัพยากร DNSKEY บรรจุกุญแจสาธารณะนี้ถูกไปใช้ทำระเบียนทรัพยากร DS หรือถูกนำไปตั้งค่า Trust Anchor
Protocol	ขนาด 8 bit ต้องมีค่าเป็น 3 เท่านั้น
Algorithm	ตัวเลขที่ระบุขั้นตอนวิธี (algorithm) ที่ใช้ในการเข้ารหัสและรูปแบบของกุญแจสาธารณะ
Public Key	ใช้เก็บข้อมูลของกุญแจสาธารณะซึ่งรูปแบบขึ้นอยู่กับขั้นตอนวิธีที่ระบุในส่วน Algorithm

ตัวอย่างของระเบียนทรัพยากร DNSKEY ของโซน example.org ดังแสดงในภาพที่ 18



ภาพที่ 18 ตัวอย่างของระเบียนทรัพยากร DNSKEY ของโซน example.org

1.2. Delegation Signer (DS)



ภาพที่ 19 โครงสร้าง RData ของระเบียนทรัพยากร DS

ที่มา: RFC4034 (2005)

ข้อมูลบางส่วนใน DS จะทำขึ้นมาจากการนำชื่อโดเมนของ DNSKEY และข้อมูล RData ใน DNSKEY นำมาต่อกันแล้วมาผ่านอัลกอริทึมเข้ารหัสดังแสดงในภาพที่ 19 ดังนั้นสามารถกล่าวได้ว่าระเบียนทรัพยากร DS ใช้ยืนยันระเบียนทรัพยากร DNSKEY ประกอบด้วยส่วนต่างๆ สามารถดูรายละเอียดของส่วนประกอบจากตารางที่ 13

digest = digest_algorithm(DNSKEY owner name | DNSKEY RDATA);
"|" แสดงการต่อกัน
DNSKEY RDATA = Flags | Protocol | Algorithm | Public Key

ภาพที่ 20 สูตรการสร้าง digest

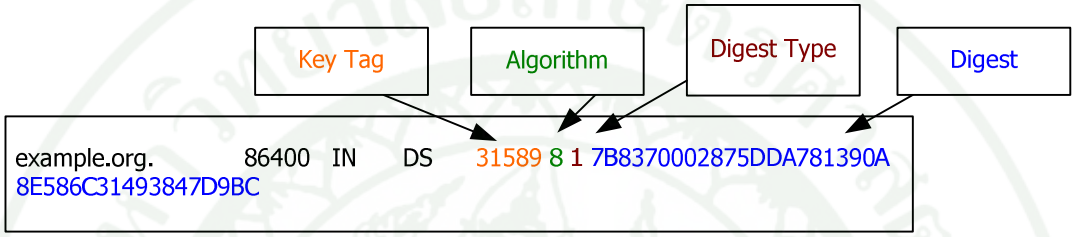
ตารางที่ 13 รายละเอียดของโครงสร้าง RData ของระเบียนทรัพยากร DS

ส่วน	รายละเอียด
Key Tag	ขนาด 16 บิต เป็นตัวเลขที่ใช้ระบุระเบียนทรัพยากร DNSKEY
Algorithm	ขนาด 8 บิต เป็นตัวเลขที่ใช้ระบุอัลกอริทึมที่ใช้ในระเบียนทรัพยกร DNSKEY
Digest Type	ขนาด 8 บิต เป็นตัวเลขที่ใช้ระบุอัลกอริทึมที่ใช้ทำ digest ในส่วน Digest

ตารางที่ 13 (ต่อ)

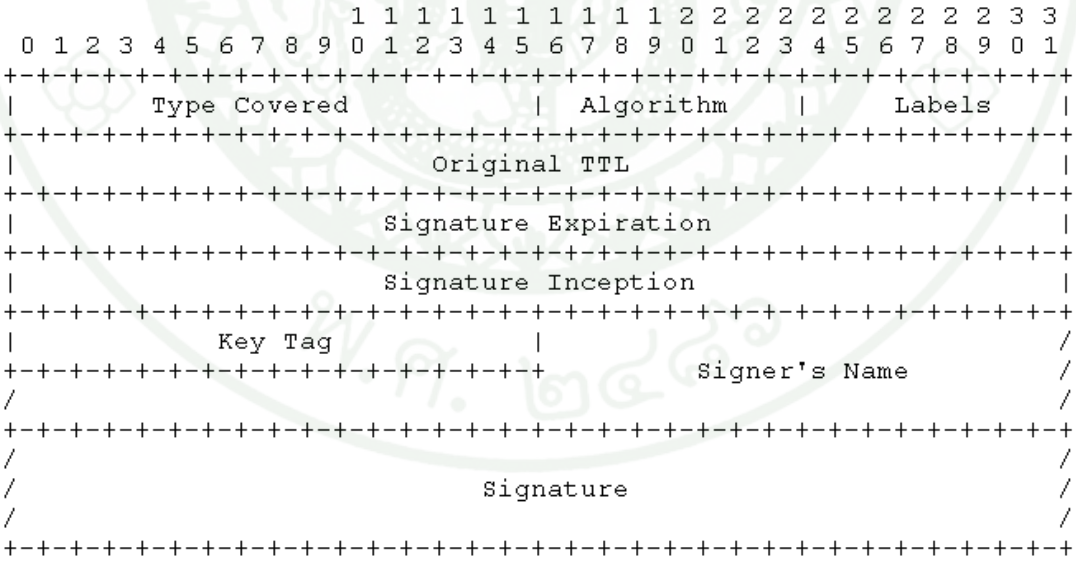
ส่วน	รายละเอียด
Digest	เก็บ digest ที่ได้จากคำนวนอัลกอริทึมที่ใช้ทำ digest ตาม Digest Type

ตัวอย่างของระเบียนทรัพยากร DS ของชื่อโดเมน example.org ดังแสดงในภาพที่ 21



ภาพที่ 21 ตัวอย่างของระเบียนทรัพยากร DS ของชื่อโดเมน example.org

1.3. Resource Record Signature (RRSIG)



ภาพที่ 22 โครงสร้าง RDATA ของระเบียนทรัพยากร RRSIG

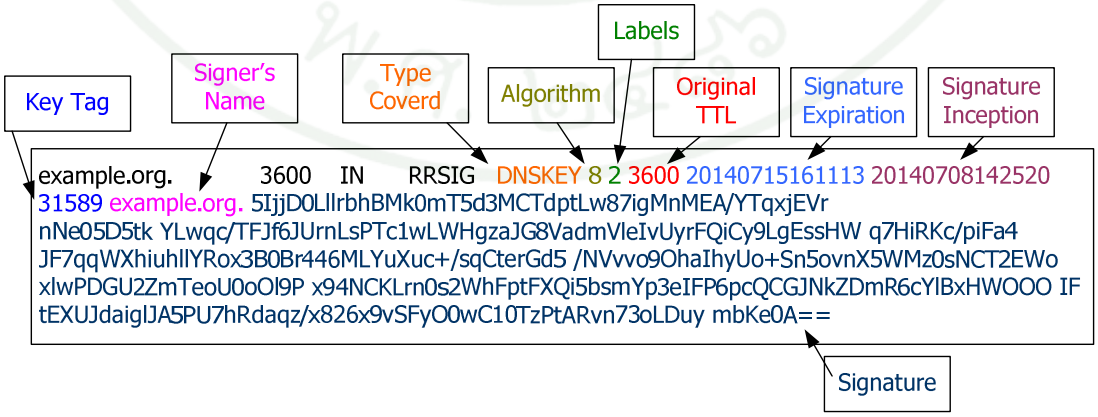
ที่มา: RFC4034 (2005)

ระเบียนทรัพยากรที่ให้เก็บลายเซ็นดิจิตอลของทะเบียนทรัพยากรแต่ละชนิด เพื่อใช้ในการตรวจสอบว่าข้อมูลถูกเปลี่ยนแปลงระหว่างการรับส่งหรือไม่

ตารางที่ 14 รายละเอียดโครงสร้าง RData ของระเบียนทรัพยากร RRSIG

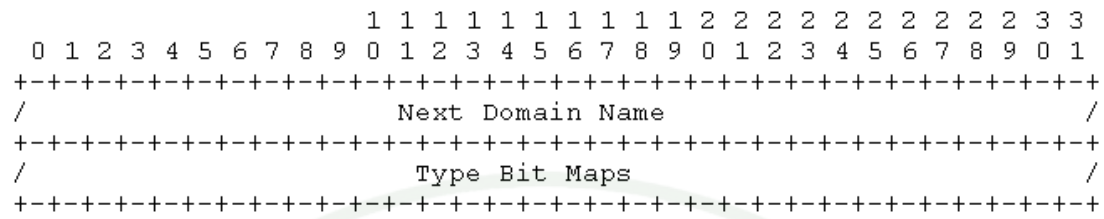
ส่วน	รายละเอียด
Type Covered	ระบุว่าเก็บลายเซ็นของระเบียนทรัพยากรชนิดอะไร
Algorithm Number	ระบุว่าอัลกอริทึมที่ใช้ในการสร้างลายเซ็น
Labels	ระบุจำนวนของป้ายในชื่อโดเมน
Original TTL	ระบุเวลา TTL ของระเบียนทรัพยากร
Signature Expiration	ใช้รวมกับ Signature Inception เพื่อระบุช่วงเวลาที่ลายเซ็นจะไม่หมดอายุ
Signature Inception	ใช้รวมกับ Signature Expiration เพื่อระบุช่วงเวลาที่ลายเซ็นจะไม่หมดอายุ
Key Tag	เก็บค่าของ Key Tag ของระเบียนทรัพยากร DNSKEY ที่ใช้ตรวจสอบลายเซ็น
Signer's Name	ระบุชื่อโดเมนของระเบียนทรัพยากร DNSKEY ที่ใช้สร้างลายเซ็น
Signature	เก็บลายเซ็นดิจิตอล

ตัวอย่างของระเบียนทรัพยากร RRSIG ของโซน example.org ดังแสดงในภาพที่ 23



ภาพที่ 23 ตัวอย่างของระเบียนทรัพยากร RRSIG ของโซน example.org

1.4. Next Secure (NSEC)



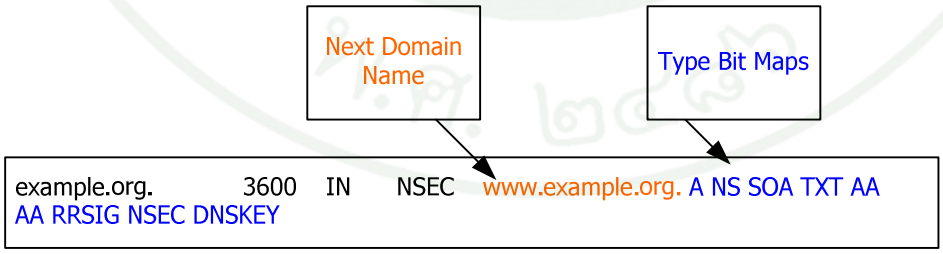
ภาพที่ 24 โครงสร้าง RData ของระเบียนทรัพยากร NSEC

ที่มา: RFC4034 (2005)

ระเบียนทรัพยากรชนิดนี้ถูกใช้รับรองคำตอบที่ว่าไม่มีข้อมูลที่ร้องข้อนั้นจริงๆ โดยใช้แสดงชื่อโดเมนในลำดับถัดไปและชนิดของระเบียนทรัพยากรของชื่อโดเมนนั้นๆ

ตารางที่ 15 รายละเอียดโครงสร้าง RData ของระเบียนทรัพยากร NSEC

ส่วน	รายละเอียด
Next Domain Name	บรรจุชื่อโดเมนถัดไป จากชื่อโดเมนของระเบียนทรัพยากร NSEC
Type Bit Maps	แสดงถึงชนิดของระเบียนทรัพยากรของชื่อโดเมนในส่วน Next Domain Name



ภาพที่ 25 ตัวอย่างของระเบียนทรัพยากร NSEC

ตัวอย่างของระเบียนทรัพยากร NSEC ของโซน example.org ซึ่งมีความหมายว่าชื่อโดเมนถัดจาก example.org คือ www.example.org และมีระเบียนทรัพยากรชนิด A, NS, SOA, TXT, AAAA, RRSIG, NSEC และ DNSKEY ของระเบียนทรัพยากรชื่อโดเมน example.org

2. ชนิดของกุญแจในดีเอ็นเอสเซค

ชนิดของกุญแจไม่สมมาตรที่ใช้ในดีเอ็นเอสเซคมีสองแบบ คือ Zone Signing Key (ZSK) โดยกุญแจส่วนบุคคล (private key) ใช้สร้างลายเซ็นดิจิตอลของระเบียนทรัพยากรชนิดต่างๆ ที่อยู่แฟ้มข้อมูลโซน และ Key Signing Key (KSK) โดยกุญแจส่วนบุคคลใช้ในการสร้างลายเซ็นดิจิตอลของ DNSKEY ซึ่งกุญแจสาธารณะชนิด ZSK ถูกเก็บใน DNSKEY หรือกุญแจสาธารณะชนิด KSK จะใช้ยืนยันกุญแจสาธารณะชนิด ZSK ของแต่ละโซนหรือแต่ละชื่อโดเมน ผ่านการตรวจสอบลายเซ็นดิจิตอลของชื่อโดเมนนั้น ส่วนการยืนยันกุญแจสาธารณะชนิด KSK ที่เก็บใน DNSKEY จะใช้ DS เนื่องจากข้อมูลบางส่วนใน DS ทำขึ้นมาจากการนำ ชื่อโดเมนของ DNSKEY และข้อมูลบางส่วนใน DNSKEY นำมาต่อกันแล้วมาผ่านอัลกอริทึมเข้ารหัส

3. เครื่องบริการเจ้าของชื่อโดเมน (Authoritative Name Server) ในดีเอ็นเอสเซค

สำหรับเครื่องบริการเจ้าของชื่อโดเมนที่ให้บริการดีเอ็นเอสเซคของแต่ละชื่อโดเมน ผู้ดูแลต้องทำการสร้างกุญแจไม่สมมาตรอย่างน้อย 1 คู่ สำหรับแต่ละโซน จากนั้นดำเนินการ Zone Signing ซึ่งคือกระบวนการเพิ่มระเบียนทรัพยากรชนิดใหม่ 4 ชนิด โดยอาจมี DS เป็นส่วนเสริมได้ เนื่องจาก DS ของชื่อโดเมนนั้นๆ จะถูกบรรจุในแฟ้มข้อมูลโซน (Zone File) ของเครื่องบริการเจ้าของชื่อโดเมนของชื่อโดเมนที่อยู่ระดับบนในโครงสร้างของดีเอ็นเอส เช่น DS ของ example.org จะต้องถูกเก็บไว้ที่เครื่องบริการเจ้าของชื่อโดเมนของ org เป็นต้น

4. รีโซลเวอร์ (Resolver) ในดีเอ็นเอสเซค

ที่รีโซลเวอร์ต้องทำการเปิดฟังก์ชันสนับสนุนการทำงานดีเอ็นเอสเซคและฟังก์ชันตรวจสอบข้อมูล (Validation) ในการตรวจสอบจะต้องตั้งค่า Trust Anchor ซึ่งคือเอนทิตี (entity) ที่สามารถเชื่อถือได้ เช่น กุญแจสาธารณะชนิด KSK ของชื่อโดเมน root สำหรับเป็นจุดเริ่มต้นในการตรวจสอบกุญแจสาธารณะของชื่อโดเมนต่างๆ เนื่องจากเนมเซิร์ฟเวอร์ root ดูแลโดยองค์กรที่ตั้งขึ้นโดยไม่แสวงหากำไร

5. ข้อความในดีเอ็นเอสเซค

สำหรับข้อความในดีเอ็นเอสมีสองแบบคือ query และ response โดยไคลเอนต์ รีโซลเวอร์ และเนมเซิร์ฟเวอร์ต่างๆ ใช้สื่อสารระหว่างกัน การส่งข้อความในดีเอ็นเอสเซคจะต้องสนับสนุนการทำงานที่เรียกว่า EDNS0 ซึ่งคือกระบวนการในการเพิ่มระเบียนทรัพยากรที่เรียกว่า OPT ไปกับ query หรือ response เพื่อให้คู่สนทนาทราบว่ามีบัฟเฟอร์ขนาดเท่าใดในการรับส่งข้อมูล และมีการตั้งค่าบิต DNSSEC OK (DO) ให้มีค่าเป็น 1 ใน query ของไคลเอนต์ที่ส่งไปยังรีโซลเวอร์ หรือรีโซลเวอร์ส่งไปยังเนมเซิร์ฟเวอร์ต่างๆ ทำให้รีโซลเวอร์หรือเนมเซิร์ฟเวอร์นั้นๆ ทราบว่าเป็นการร้องขอแบบดีเอ็นเอสเซคเมื่อรีโซลเวอร์หรือเนมเซิร์ฟเวอร์นั้นๆ จะต้องตอบด้วย response แบบดีเอ็นเอสเซคด้วย

6. ตัวบ่งชี้ในส่วนหัวของข้อความ

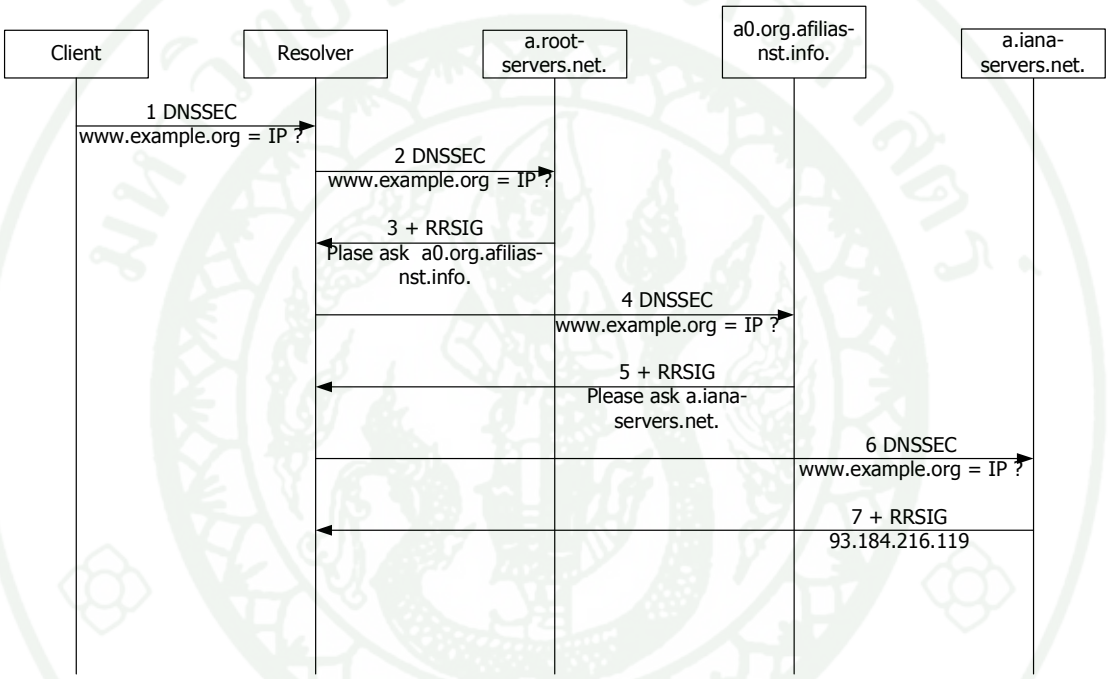
ในส่วนหัวของข้อความในดีเอ็นเอสเซคมีการกำหนดบทบาทใหม่ให้บิต Authenticated Data (AD) และบิต Checking Disable (CD) ดังแสดงในภาพที่ 8 โดยบิต AD จะกำหนดให้มีค่าเป็น 1 ใน response เมื่อรีโซลเวอร์ทำกระบวนการตรวจสอบข้อมูล แล้วพบว่าข้อมูลไม่ถูกเปลี่ยนแปลงระหว่างการส่งและมาจากแหล่งกำเนิดจริง หรือกล่าวได้ว่าข้อมูลนั้นปลอดภัย ในส่วนของบิต CD ถูกกำหนดให้มีค่าเป็น 1 ใน query ที่รีโซลเวอร์ส่งไปยังเนมเซิร์ฟเวอร์ต่างๆ เมื่อเนมเซิร์ฟเวอร์ได้รับและทำการส่ง response โดยไม่ต้องทำกระบวนการตรวจสอบข้อมูล

7. กระบวนการหาคำตอบในดีเอ็นเอสเซค

กระบวนการตรวจสอบข้อมูลที่ไคลเอนต์สอบถามมาปลอดภัยหรือไม่ จะถูกดำเนินการโดยรีโซลเวอร์ ซึ่งรีโซลเวอร์จะดำเนินกระบวนการหาคำตอบโดยหาข้อมูลที่ต้องใช้สำหรับการตรวจสอบข้อมูล เช่น กุญแจสาธารณะของชื่อโดเมนระดับต่างๆ ที่เก็บใน DNSKEY ไว้สำหรับตรวจสอบลายเซ็นดิจิตอลใน RRSIG และคำตอบที่ไคลเอนต์ต้องการทราบ ในที่นี้จะขออธิบายจากตัวอย่างว่า ไคลเอนต์ทำการส่ง query แบบดีเอ็นเอสเซคสอบถามระเบียนทรัพยากรชนิด A หรือหมายเลขไอพีของ www.example.org ไปที่รีโซลเวอร์ที่มีการกุญแจสาธารณะชนิด KSK ของชื่อโดเมน root มาทำการตั้งค่าเป็น Trust Anchor ไว้ การดำเนินการสามารถถูกพิจารณาเป็น 2 ส่วน ดังนี้

7.1. กระบวนการหาคำตอบสำหรับส่วนที่ถูกสอบถามแบบดีเอ็นเอสเซค

รีโซลเวอร์จะทำกระบวนการหาคำตอบ เหมือนในดีเอ็นเอสโดยทั่วไปเพื่อให้ได้คำตอบว่าระเบียนทรัพยากรชนิด A ของ www.example.org คืออะไร แต่การส่ง query จะเป็นแบบดีเอ็นเอสเซค ซึ่งจะทำให้ได้รับ response กลับมาเป็นแบบดีเอ็นเอสเซคด้วย หรือก็คือจะได้รับ RRSIG ของระเบียนทรัพยากรชนิด A ของ www.example.org กลับมาพร้อมกับระเบียนทรัพยากรชนิด A ของ www.example.org ด้วย ดังแสดงในภาพที่ 26

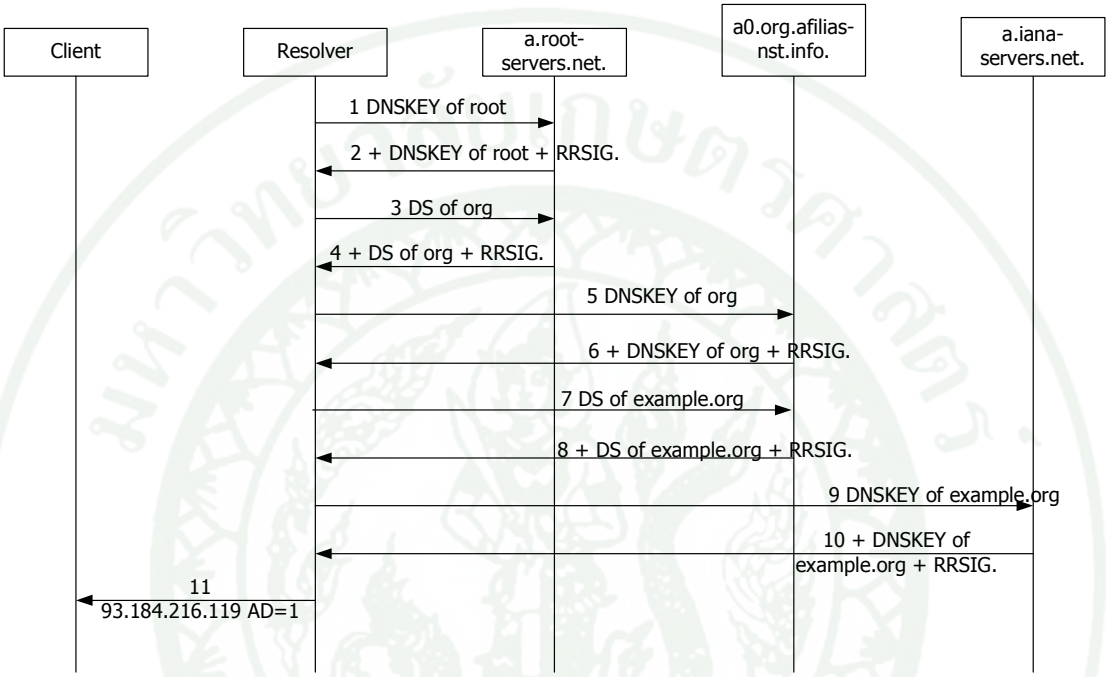


ภาพที่ 26 กระบวนการหาคำตอบสำหรับส่วนที่ถูกสอบถามแบบดีเอ็นเอสเซค

7.2. กระบวนการหาคำตอบสำหรับการตรวจสอบกุญแจสาธารณะ

ข้อสังเกตถ้ารีโซลเวอร์ทราบกุญแจสาธารณะ ชนิด ZSK ของ example.org และสามารถยืนยันได้ว่าถูกต้องเชื่อถือได้ ก็จะสามารถนำมาตรวจสอบลายเซ็นดิจิตอล ของคำตอบใน response สำหรับสอบถามระเบียนทรัพยากรชนิด A ของ www.example.org ได้ หากถูกต้อง รีโซลเวอร์จะทำการส่ง response แบบดีเอ็นเอสเซคไปยังไคลเอนต์ พร้อมกับกำหนดบิต AD ให้มีค่าเป็น 1 เพื่อแจ้งไคลเอนต์ว่าคำตอบปลอดภัยเชื่อถือได้ และไม่ถูกเปลี่ยนแปลงระหว่างการรับส่งข้อมูล ดังนั้นรีโซลเวอร์จำเป็นต้องทราบระเบียนทรัพยากร DNSKEY และ DS ของชื่อโดเมนต่างๆที่เกี่ยวข้อง รีโซล

เวอร์จึงดำเนินกระบวนการหาคำตอบเพื่อให้ได้ข้อมูลเกี่ยวกับ DNSKEY และ DS จากนั้นรีโซลเวอร์จะตรวจสอบความถูกต้องของกุญแจสาธารณะต่างๆ จึงจะสามารถตรวจสอบความถูกต้องของข้อมูลได้ กระบวนการหาคำตอบในส่วนนี้ดังแสดงในภาพที่ 27 และตารางที่ 16 กล่าวถึงรายละเอียดในการดำเนินการ



ภาพที่ 27 กระบวนการหาคำตอบสำหรับการตรวจสอบกุญแจสาธารณะ

ตารางที่ 16 กระบวนการหาคำตอบสำหรับส่วนการตรวจสอบกุญแจสาธารณะ

กระบวนการที่	รายละเอียด
1	รีโซลเวอร์ทำการสอบถาม DNSKEY ของชื่อโดเมน root จาก a.root-servers.net ซึ่งคือเครื่องบริการเจ้าของชื่อโดเมน root
2	เครื่องบริการ a.root-servers.net ทำการ response ที่บรรจุ DNSKEY ของชื่อโดเมน root ทั้งหมดพร้อมกับ RRSIG กลับไปยังรีโซลเวอร์
3	รีโซลเวอร์ทำการสอบถาม DS ของชื่อโดเมน org จาก a.root-servers.net
4	เครื่องบริการ a.root-servers.net ทำการ response ที่บรรจุ DS ของชื่อโดเมน org ทั้งหมดพร้อมกับ RRSIG กลับไปยังรีโซลเวอร์

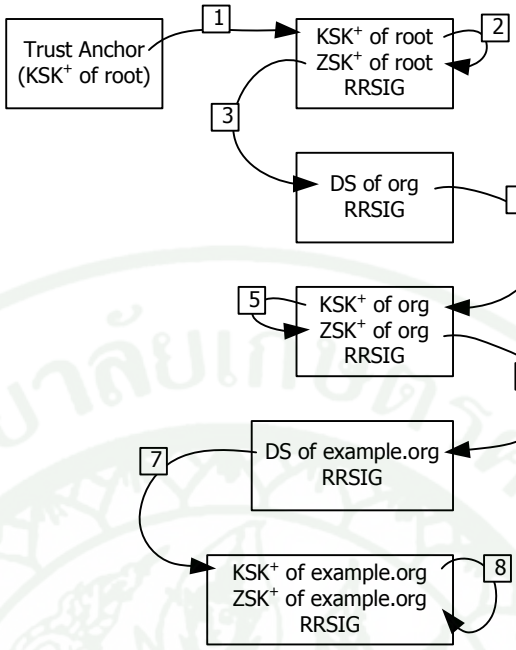
ตารางที่ 16 (ต่อ)

กระบวนการที่	รายละเอียด
5	รีโซลเวอร์ทำการสอบถาม DNSKEY ของชื่อโดเมน org จาก a0.org.afilias-nst.info ซึ่งคือเครื่องบริการเจ้าของชื่อโดเมน org
6	เครื่องบริการ a0.org.afilias-nst.info ทำการ response ที่บรรจุ DNSKEY ของชื่อโดเมน org ทั้งหมดพร้อมกับ RRSIG กลับไปยังรีโซลเวอร์
7	รีโซลเวอร์ทำการสอบถาม DS ของชื่อโดเมน example.org จาก a0.org.afilias-nst.info
8	เครื่องบริการ a0.org.afilias-nst.info ทำการ response ที่บรรจุ DS ของชื่อโดเมน example.org ทั้งหมดพร้อมกับ RRSIG กลับไปยังรีโซลเวอร์
9	รีโซลเวอร์ทำการสอบถาม DNSKEY ของชื่อโดเมน example.org จาก a.iana-servers.net ซึ่งคือเครื่องบริการเจ้าของชื่อโดเมน example.org
10	เครื่องบริการ a.iana-servers.net ทำการ response ที่บรรจุ DNSKEY ของชื่อโดเมน example.org ทั้งหมดพร้อมกับ RRSIG กลับไปยังรีโซลเวอร์

8. กระบวนการตรวจสอบกุญแจสาธารณะ

ข้อสังเกตถ้ารีโซลเวอร์ทราบกุญแจสาธารณะ ชนิด ZSK ของ example.org และสามารถยืนยันได้ว่าถูกต้องเชื่อถือได้ ก็จะสามารถนำมาตรวจสอบลายเซ็นดิจิตอล ของคำตอบใน response สำหรับสอบถามระเบียนทรัพยากรชนิด A ของ www.example.org ได้

การยืนยันกุญแจสาธารณะ ชนิด ZSK ของ example.org นั้น รีโซลเวอร์ต้องเริ่มต้น โดยตรวจสอบค่า Trust Anchor กับกุญแจสาธารณะชนิด KSK ของชื่อโดเมน root เป็นตัวเดียวกันหรือไม่ หากเป็นตัวเดียวกัน รีโซลเวอร์จะเชื่อถือกุญแจสาธารณะชนิด ZSK ของชื่อโดเมน root จากการตรวจสอบลายเซ็นดิจิตอล โดยใช้กุญแจสาธารณะ ชนิด KSK ได้ด้วย



ภาพที่ 28 ลำดับการตรวจสอบกุญแจสาธารณะ

ลำดับถัดมารีโซลเวอร์จะใช้กุญแจสาธารณะชนิด ZSK ของชื่อโดเมน root ที่เชื่อถือได้ในกระบวนการด้านข้างต้นแล้วยืนยันความถูกต้องของ DS ของ org หาก DS ของ org เชื่อถือได้ก็จะถูกรีโซลเวอร์นำไปใช้ยืนยันกุญแจสาธารณะชนิด KSK ของ org

รีโซลเวอร์จะดำเนินการตรวจสอบกุญแจสาธารณะแต่ละชนิดของแต่ละชื่อโดเมนไปจนกระทั่งสามารถยืนยันการยืนยันกุญแจสาธารณะ ชนิด ZSK ของ example.org ได้ ลำดับการตรวจสอบกุญแจสาธารณะเรียกว่า Chain of Trust ดังแสดงในภาพที่ 28 และสามารถดูรายละเอียดการตรวจสอบกุญแจสาธารณะได้จากตารางที่ 17

ตารางที่ 17 รายละเอียดการตรวจสอบกุญแจสาธารณะ

กระบวนการที่	รายละเอียด
1	รีโซลเวอร์ทำการตรวจสอบว่า Trust Anchor กับกุญแจสาธารณะชนิด KSK ของโซน root ในระเบียนทรัพยากร DNSKEY เป็นตัวเดียวกันหรือไม่

ตารางที่ 17 (ต่อ)

กระบวนการที่	รายละเอียด
2	รีโซลเวอร์สามารถนำกุญแจสาธารณะชนิด KSK ของโซน root ในระเบียนทรัพยากร DNSKEY ตรวจสอบลายเซ็นดิจิทัล เพื่อยืนยันกุญแจสาธารณะชนิด ZSK ของโซน root ในระเบียนทรัพยากร DNSKEY
3	รีโซลเวอร์สามารถนำกุญแจสาธารณะชนิด ZSK ของโซน root ในระเบียนทรัพยากร DNSKEY ตรวจสอบลายเซ็นดิจิทัล เพื่อยืนยันระเบียนทรัพยากร DS ของโซน org
4	รีโซลเวอร์สามารถใช้ระเบียนทรัพยากร DS ของโซน org ยืนยันความถูกต้องของกุญแจสาธารณะชนิด KSK ของโซน org ในระเบียนทรัพยากร DNSKEY
5	รีโซลเวอร์สามารถนำกุญแจสาธารณะชนิด KSK ของโซน org ในระเบียนทรัพยากร DNSKEY ตรวจสอบลายเซ็นดิจิทัล เพื่อยืนยันกุญแจสาธารณะชนิด ZSK ของโซน org ในระเบียนทรัพยากร DNSKEY
6	รีโซลเวอร์สามารถนำกุญแจสาธารณะชนิด ZSK ของโซน org ในระเบียนทรัพยากร DNSKEY ตรวจสอบลายเซ็นดิจิทัล เพื่อยืนยันระเบียนทรัพยากร DS ของโซน example.org
7	รีโซลเวอร์สามารถใช้ระเบียนทรัพยากร DS ของโซน example.org ยืนยันความถูกต้องของกุญแจสาธารณะชนิด KSK ของโซน example.org ในระเบียนทรัพยากร DNSKEY
8	รีโซลเวอร์สามารถนำกุญแจสาธารณะชนิด KSK ของโซน example.org ในระเบียนทรัพยากร DNSKEY ตรวจสอบลายเซ็นดิจิทัล เพื่อยืนยันกุญแจสาธารณะชนิด ZSK ของโซน example.org ในระเบียนทรัพยากร DNSKEY

ในดีเอ็นเอสเซคมีการกำหนดให้เรียก เนมเซิร์ฟเวอร์ที่สนับสนุนดีเอ็นเอสเซคว่า Security-Aware Name Server ส่วน Validating Security-Aware Resolver สำหรับรีโซลเวอร์ที่สนับสนุนดีเอ็นเอสเซครวมทั้งเปิดฟังก์ชันตรวจสอบข้อมูลด้วย และ Non-Validating Security-Aware Resolver สำหรับรีโซลเวอร์ที่สนับสนุนดีเอ็นเอสเซคแต่ไม่ได้เปิดฟังก์ชันตรวจสอบข้อมูล

อุปกรณ์และวิธีการ

การทดสอบถึงความพร้อมในการให้บริการดีเอ็นเอสเซคของไอเอสพีในประเทศไทย มีวัตถุประสงค์เพื่อเสนอแนวทางในการทดสอบเครือข่ายสำหรับการใช้งานดีเอ็นเอสเซค เสนอรูปแบบการใช้งานดีเอ็นเอสเซคผ่านแต่ละไอเอสพี และเป็นแรงผลักดันให้ไอเอสพีหรือองค์กรธุรกิจต่างๆ เล็งเห็นความสำคัญของการใช้งานดีเอ็นเอสเซค

อุปกรณ์

1. เครื่องคอมพิวเตอร์หน่วยประมวลผล Intel Mobile Core 2 Duo T7400 2.16GHz หน่วยความจำ 3 GB และฮาร์ดดิสก์บรรจุข้อมูล 300 GB

2. โปรแกรม dig

3. โปรแกรม bind เวอร์ชั่น 9.8.4

3. ระบบปฏิบัติการ Microsoft Windows XP

วิธีการ

ผู้วิจัยใช้โปรแกรม dig เพื่อส่ง query ไปยังรีโซลเวอร์ (Resolver) หรือเนมเซิร์ฟเวอร์ (name server) ต่างๆ จากนั้นนำ response ที่ได้รับมาสรุปผล และติดตั้งโปรแกรม bind เวอร์ชั่น 9.8.4 ซึ่งสนับสนุนดีเอ็นเอสเซค สำหรับการทำรีโซลเวอร์ขึ้นเองเพื่อใช้ในการทดสอบ โดยเมื่อติดตั้ง bind จะมีคำสั่ง dig มาพร้อมกันด้วย

การทดสอบความพร้อมของไอเอสพีกับบริการดีเอ็นเอสเซคผู้วิจัยเสนอรูปแบบการทดสอบทั้งหมด 3 แบบ คือแบบที่ 1 คือจำลองการทำงานของ Local Validating Security-Aware Resolver แบบที่ 2 คือทดสอบการตรวจสอบข้อมูลเนมเซิร์ฟเวอร์ของไอเอสพี และแบบที่ 3 คือใช้งาน Local Validation Security-Aware Resolver กับ Non-Validating Security-Aware Name Server ของไอเอสพี

สำหรับการทดสอบแต่ละแบบผู้วิจัยทำการทดสอบกับเครือข่ายของไอเอสพีจำนวน 6 ราย สามารถดูรายละเอียดได้จากตารางที่ 18 โดยบริการอินเทอร์เน็ตของ 3BB JINET TOT และ TRUE เป็นแบบ ADSL บริการของ PROEN เป็นแบบ VPN และสุดท้ายผู้วิจัยได้รับความอนุเคราะห์เข้า

ทดสอบที่ CAT ซึ่งเป็นห้องสำหรับให้ลูกค้าใช้งานอินเทอร์เน็ต โดยผู้วิจัยทำการทดลองแต่ละแบบเป็นเวลาแบบละ 5 วัน และนำผลการที่ได้มาวิเคราะห์ดังที่อธิบายในส่วนต่อไป

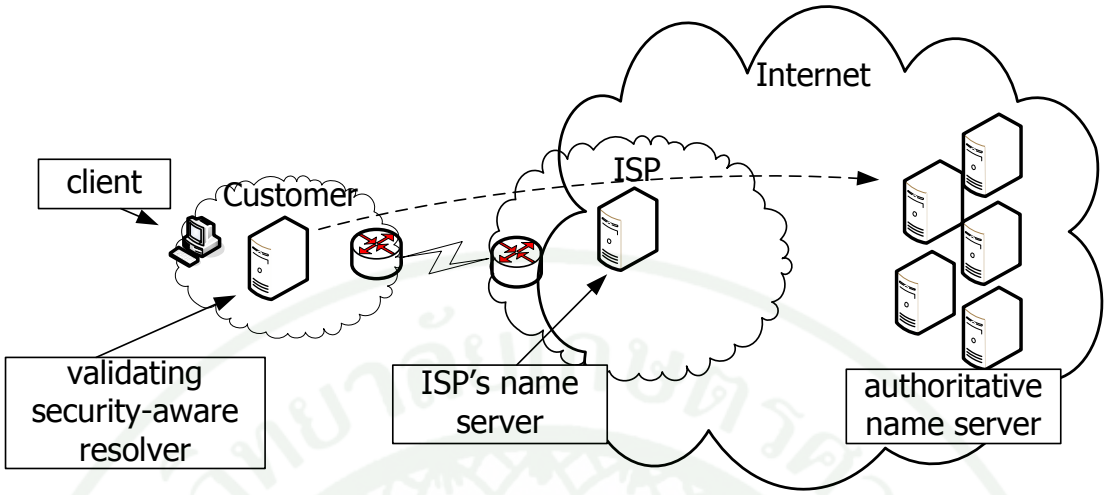
ในการส่ง query ผู้วิจัยทำการสร้างแฟ้มกลุ่มคำสั่ง (batch file) พร้อมทั้งระบุคำสั่ง dig ที่ใช้ในการทดสอบลงในแฟ้มกลุ่มคำสั่ง จากนั้นทำการเชื่อมต่ออินเทอร์เน็ตของไอเอสพีที่จะทำการทดสอบ แล้วจึงทำการเปิดแฟ้มกลุ่มคำสั่งให้ทำงาน

ตารางที่ 18 บริการอินเทอร์เน็ตและหมายเลขไอพีเนมเซิร์ฟเวอร์ของไอเอสพี

ISP	บริการ	หมายเลขไอพี
3BB	ADSL	110.164.252.222
CAT	Customer Room	61.19.245.245
JINET	ADSL	203.147.0.3
PROEN	VPN (PPTP)	202.170.119.9
TOT	ADSL	203.113.127.199
TRUE	ADSL	203.144.207.29

1. จำลองการทำงานของ Local Validating Security-Aware Resolver

การเข้าถึงบริการดีเอ็นเอสเซคของลูกค้าของไอเอสพี หากเนมเซิร์ฟเวอร์ของไอเอสพีไม่สนับสนุนการทำงานในดีเอ็นเอสเซค ผู้ใช้งานสามารถเข้าถึงบริการดีเอ็นเอสเซคได้ด้วยการติดตั้ง Validating Security-Aware Resolver ภายในเครือข่ายของตนเอง ดังที่แสดงในภาพที่ 29



ภาพที่ 29 การใช้งานผ่าน Local Validating Security-Aware Resolver

สมมติฐานผู้วิจัยไม่ทราบว่าเครือข่ายของไอเอสพีรองรับการให้บริการดีเอ็นเอสเซคหรือไม่ จึงทำการทดลองโดยการส่ง query แตกต่างกัน 5 แบบ ซึ่งถูกจำลองให้ตัวบ่งชี้ (flag) ต่างๆ ในส่วนหัว (header) ของ query เหมือนกับการที่รีโซลเวอร์ส่ง query ในการหาคำตอบ ไปยังเนมเซิร์ฟเวอร์จำนวน 456 เครื่อง ซึ่งเป็นเครื่องบริการเจ้าของชื่อโดเมน (Authoritative Name Server) ของโดเมนระดับ Top-Level (TLD) จำนวน 66 โดเมนในอินเทอร์เน็ตที่ผ่านการ Zone Signing แล้วเฉพาะชื่อโดเมนที่เป็นอักขระละตินอ้างอิงจาก ICANN Research (2014) พร้อมนำ response มาวิเคราะห์และสรุปผล สามารถดูตัวอย่างคำสั่งได้จาก ตารางที่ 19

ตารางที่ 19 ตัวอย่างคำสั่ง dig ที่ใช้ในการส่ง query สำหรับการทดสอบที่ 1

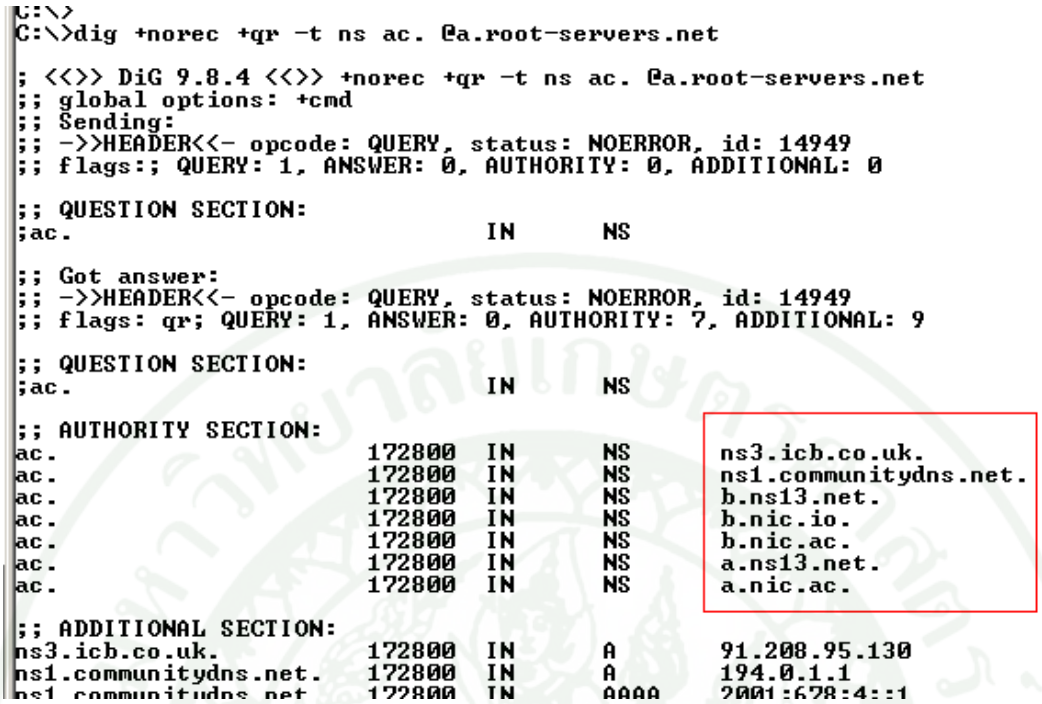
คำสั่ง	ตัวอย่างคำสั่ง	หมายเหตุ
1	dig +nodnssec +norec +retry=0 +ignore +qr +bufsize=4096 any ac. @b.nic.io.	UDP+noDNSEC (UN)
2	dig +nodnssec +norec +tcp +retry=0 +ignore +qr any ac. @b.nic.io.	TCP+noDNSSEC (TN)
3	dig +dnssec +cdflag +norec +retry=0 +ignore +qr +bufsize=4096 any ac. @b.nic.io.	UDP+DNSSEC (U)
4	dig +dnssec +cdflag +norec +retry=0 +ignore +qr +bufsize=4096 -t a ac. @b.nic.io.	UDP+DNSSEC +Type A (UA)

ตารางที่ 19 (ต่อ)

คำสั่ง	ตัวอย่าง	หมาย
5	dig +dnssec +cdflag +norec +tcp +retry=0 +ignore +qr any ac. @b.nic.io.	TCP+DNSSEC (T)

ตัวอย่างคำสั่งด้านบนเป็นการสร้าง query ส่งไปยัง 1 ใน 456 เครื่องบริการ ที่มีชื่อโดเมน b.nic.io ซึ่งเป็นเครื่องบริการเจ้าของชื่อโดเมนของชื่อโดเมน acโดยสอบถาม RR ของชื่อโดเมน ac โดย query ที่ใช้ TCP ในการรับส่งข้อมูลได้แก่คำสั่งที่ 2 และ 5 ซึ่งต้องระบุ +tcp ในคำสั่ง ส่วน query เป็นแบบดีเอ็นเอสเซคได้แก่คำสั่งที่ 3 ถึง 5 ซึ่งต้องระบุ +dnssec ในคำสั่ง ถัดมา query สอบถามระเบียนทรัพยากรทั้งหมดของชื่อโดเมนนั้นได้แก่คำสั่งที่ 1,2,3 และ 5 ซึ่งต้องระบุ any ในคำสั่งทำให้ response ที่กลับมามีขนาดใหญ่ และ query สอบถามหมายเลขไอพี ของชื่อโดเมนนั้นๆ ได้แก่คำสั่งที่ 4 ซึ่งต้องระบุ –t a ในคำสั่ง

จากตัวอย่างคำสั่งในตารางที่ 19 ในการส่ง query แต่ละแบบนั้น จำเป็นต้องระบุชื่อโดเมนของเนมเซิร์ฟเวอร์หลังเครื่องหมาย @ ที่จะส่ง query ไป ผู้วิจัยได้ทำการหาชื่อโดเมนของเครื่องบริการเจ้าของชื่อโดเมนระดับ Top-Level ต่างๆ โดยการส่ง query สอบถามชื่อโดเมนของเครื่องบริการเจ้าของชื่อโดเมนระดับ Top-Level นั้นๆ ไปที่เนมเซิร์ฟเวอร์ root ซึ่งจะได้รับ response กลับจากเนมเซิร์ฟเวอร์ root ที่มีรายละเอียดของชื่อโดเมนของเครื่องบริการเจ้าของชื่อโดเมนระดับ Top-Level นั้นๆ สามารถดูตัวอย่างการหาชื่อโดเมนของเครื่องบริการเจ้าของชื่อโดเมนระดับ Top-Level ได้จากภาพที่ 30 โดยชื่อโดเมนของเครื่องบริการเจ้าของชื่อโดเมนระดับ Top-Level อยู่ภายในกรอบสี่เหลี่ยม



```
C:\>
C:\>dig +norec +qr -t ns ac. @a.root-servers.net

; <<>> DiG 9.8.4 <<>> +norec +qr -t ns ac. @a.root-servers.net
;; global options: +cmd
;; Sending:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 14949
;; flags:; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;ac.                            IN      NS

;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 14949
;; flags: qr; QUERY: 1, ANSWER: 0, AUTHORITY: 7, ADDITIONAL: 9

;; QUESTION SECTION:
;ac.                            IN      NS

;; AUTHORITY SECTION:
ac.                     172800  IN      NS      ns3.icb.co.uk.
ac.                     172800  IN      NS      ns1.communitydns.net.
ac.                     172800  IN      NS      b.ns13.net.
ac.                     172800  IN      NS      b.nic.io.
ac.                     172800  IN      NS      b.nic.ac.
ac.                     172800  IN      NS      a.ns13.net.
ac.                     172800  IN      NS      a.nic.ac.

;; ADDITIONAL SECTION:
ns3.icb.co.uk.          172800  IN      A       91.208.95.130
ns1.communitydns.net.   172800  IN      A       194.0.1.1
ns1.communitydns.net    172800  IN      AAAA    2001:628:4::1
```

ภาพที่ 30 ตัวอย่างการหาชื่อโดเมนของเครื่องบริการเจ้าของชื่อโดเมน

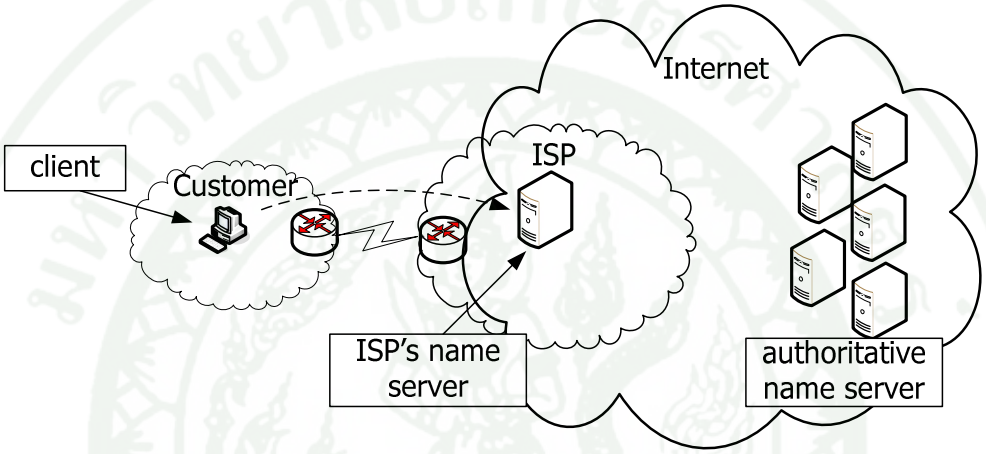
ผู้วิจัยทำการหาชื่อโดเมนของเครื่องบริการเจ้าของชื่อโดเมนตามวิธีการที่กล่าวข้างต้น พบว่า มีทั้งหมด 456 ชื่อโดเมนหรือมีเครื่องบริการเจ้าของชื่อโดเมนจำนวน 456 เครื่อง ที่ต้องทำการส่ง query ไปสอบถาม สามารถดูข้อมูลของชื่อโดเมนระดับ Top-Level ทั้ง 66 ชื่อโดเมน รวมทั้งชื่อโดเมนของเครื่องบริการเจ้าของชื่อโดเมนระดับ Top-Level ทั้ง 456 เครื่องได้จากตารางที่ 25 และสามารถดูช่วงวันในการทดสอบแสดงในจากตารางที่ 20

ตารางที่ 20 วันที่ทำการทดลองที่ 1 และ 2

ISP	ช่วงเวลาที่ทำการทดสอบ
3BB	21-03-2013 ถึง 29-03-2013
CAT	19-08-2013 ถึง 23-08-2013
JINET	21-03-2013 ถึง 30-03-2013
PROEN	21-03-2013 ถึง 28-03-2013
TOT	18-04-2013 ถึง 23-04-2013
TRUE	05-04-2013 ถึง 22-04-2013

2. ทดสอบการตรวจสอบข้อมูลเนมเซิร์ฟเวอร์ของไอเอสพี

ในแบบที่ 2 ผู้วิจัยต้องการทดสอบว่าเนมเซิร์ฟเวอร์ของไอเอสพีรองรับบริการดีเอ็นเอสเซค และสามารถตรวจสอบข้อมูลได้หรือไม่ การที่เนมเซิร์ฟเวอร์ของทางไอเอสพีเป็น Validating Security-Aware Name Server จะทำให้ผู้ใช้บริการสามารถเข้าถึงดีเอ็นเอสเซคได้เลย โดยผู้ใช้บริการคือไม่ต้องดำเนินการอะไร ดังที่แสดงในภาพที่ 31



ภาพที่ 31 การใช้งานเครื่องแม่ข่ายของทางไอเอสพี

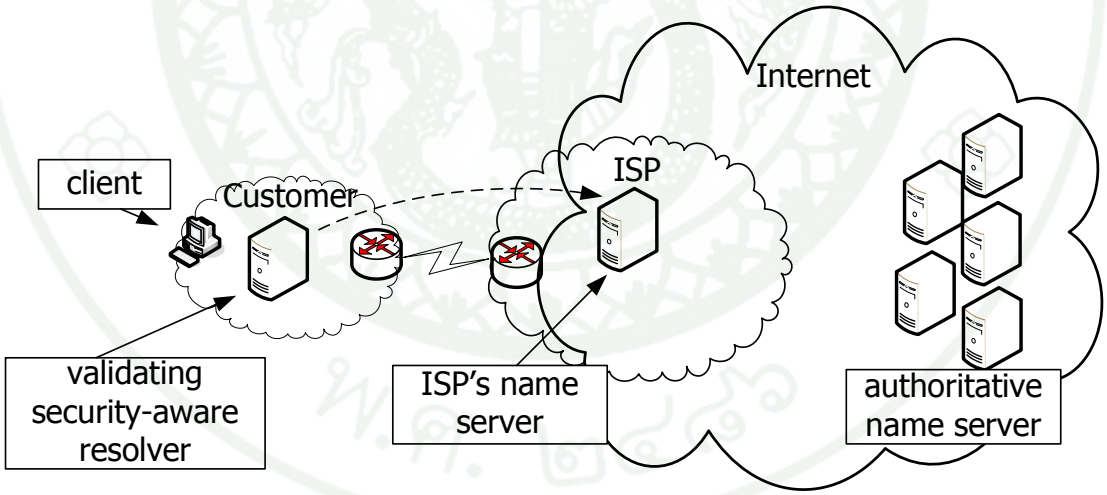
ดังนั้นผู้วิจัยทำการทดสอบโดยส่ง query สอบถามหมายเลขไอพีของชื่อโดเมนที่ทำการสุ่มจากอินเทอร์เน็ตจำนวน 435 ชื่อโดเมน ภายใต้ TLD จำนวน 66 โดเมนที่ผ่านการ Zone Signing แล้ว ไปยังเนมเซิร์ฟเวอร์ของทางไอเอสพี ในการทดลองผู้วิจัยใช้คำสั่งดังตัวอย่างคำสั่งที่ 1 ในตารางที่ 21 เป็นการส่ง query สอบถามหมายเลขไอพีของชื่อโดเมนตัวอย่างเช่น www.name.ac ไปยัง 110.164.252.222 ซึ่งเป็นเนมเซิร์ฟเวอร์ของทาง 3BB ค่าหมายเลขไอพีของเนมเซิร์ฟเวอร์จะเปลี่ยนไปตามไอเอสพีที่ทำการทดสอบโดยมีรายละเอียดดังตารางที่ 18 และทำการส่ง query ถามหมายเลขไอพีของชื่อโดเมนจำนวน 435 ชื่อโดเมนเดียวกันนี้ ไปยัง Validating Security-Aware Name Server ที่ผู้วิจัยติดตั้งเองเพื่อใช้ผลในการเปรียบเทียบ สามารถดูรายละเอียดชื่อโดเมนจำนวน 435 ชื่อโดเมนที่ทำการสุ่มจากอินเทอร์เน็ตได้จากตารางที่ 26 และช่วงวันในการทดสอบแบบที่ 2 ได้จากตารางที่ 20

ตารางที่ 21 ตัวอย่างคำสั่ง dig ที่ใช้ในการส่ง query ของการทดสอบที่ 2

คำสั่ง	ตัวอย่างคำสั่ง
1	dig @110.164.252.222 +dnssec +qr +retry=0 -t a www.name.ac.

3. ใช้งาน Local Validation Security-Aware Resolver กับ Non-Validating Security-Aware Name Server ของไอเอสพี

สมมติฐานถ้าเนมเซิร์ฟเวอร์ของผู้ให้บริการไอเอสพีสนับสนุนและเปิดการทำงานดีเอ็นเอสเซคแต่ไม่สามารถรับรองความถูกต้องของชื่อโดเมนที่สอบถามได้ โดยสังเกตได้จากการมี RRSIG กลับมากับ respose ด้วย ดังนั้นหากผู้ใช้บริการต้องการฟังก์ชันตรวจสอบข้อมูล ผู้ใช้งานควรจะติดตั้ง Local Validation Security-Aware Resolver และทำการตั้งค่าส่งต่อ (forward) query ไปยังเนมเซิร์ฟเวอร์ของทางไอเอสพีเพื่อที่จะสามารถตรวจสอบข้อมูลและลดภาระการทำงานของรีโซลเวอร์ที่ติดตั้งขึ้นดังที่แสดงในภาพที่ 32



ภาพที่ 32 การใช้งาน Local Validation Security-Aware Resolver กับ Non-Validating Security-Aware Name Server ของไอเอสพี

ดังนั้นผู้วิจัยจึงทำการทดลองในแบบที่ 3 คือส่ง query สอบถามหมายเลขไอพีของชื่อโดเมนที่ทำการสุ่มจากอินเทอร์เน็ตจำนวน 435 ชื่อโดเมน ไปยัง Validating Security-Aware Resolver ที่ทำการติดตั้งเอง แต่มีการตั้งค่าให้ส่งต่อ query ไปยังเนมเซิร์ฟเวอร์ของไอเอสพีที่มี

รายละเอียดหมายเลขไอพีตามตารางที่ 18 โดยใช้คำสั่งที่ 1 จากตารางที่ 21 แต่มีการเปลี่ยนหมายเลขไอพีเป็น 127.0.0.1 เพื่อส่ง query ไปยังรีโซลเวอร์ที่ติดตั้งเอง และทำการทดลองเดียวกันนี้แต่มีการตั้งค่าให้ส่งต่อ query ไปยังเนมเซิร์ฟเวอร์ของทาง Google ที่หมายเลขไอพีหมายเลข 8.8.8.8 อ้างอิงจาก Google (2014) ซึ่งสามารถให้บริการดีเอ็นเอสเซคและตรวจสอบข้อมูลได้ เพื่อใช้ในการเปรียบเทียบความถูกต้องของผลลัพธ์ที่ได้ ในแต่ละวันที่ทำการทดสอบเนมเซิร์ฟเวอร์ของไอเอสพีต่างๆ โดยผู้วิจัยจะทำการทดสอบกับเนมเซิร์ฟเวอร์ของ Google ไปในวันเวลาเดียวกันด้วย

ตารางที่ 22 วันที่ทำการทดลองที่ 3

ISP	ช่วงเวลาที่ทำการทดสอบ
3BB	05-11-2013 ถึง 09-11-2013
CAT	28-10-2013 ถึง 01-11-2013
JINET	21-10-2013 ถึง 26-10-2013
PROEN	21-10-2013 ถึง 26-10-2013
TOT	21-10-2013 ถึง 26-10-2013
TRUE	28-10-2013 ถึง 15-11-2013

การทดสอบในแบบที่ 1 สามารถนำไปสู่ผลสรุปได้ว่าเครือข่ายของไอเอสพี รองรับการใช้งานดีเอ็นเอสเซคหรือไม่ และการทดสอบแบบที่ 2 จะสามารถระบุได้ว่าเนมเซิร์ฟเวอร์ของทางไอเอสพีรองรับการทำงานดีเอ็นเอสเซค และเปิดฟังก์ชันการตรวจสอบข้อมูลหรือไม่ หากเนมเซิร์ฟเวอร์ของทางไอเอสพีรองรับและเปิดการทำงานดีเอ็นเอสเซค แต่ไม่ทำการเปิดฟังก์ชันการตรวจสอบข้อมูล ผู้ใช้บริการสามารถเข้าถึงบริการดีเอ็นเอสเซคในลักษณะของการทดสอบในแบบที่ 3 ได้นอกเหนือจากลักษณะการเข้าถึงบริการดีเอ็นเอสเซคในแบบที่ 1

ผลและวิจารณ์

การทดสอบความพร้อมของไอเอสพีกับบริการดีเอ็นเอสเซค ผู้วิจัยเสนอรูปแบบการทดสอบทั้งหมด 3 แบบ คือแบบที่ 1 คือจำลองการทำงานของ Local Validating Security-Aware Resolver แบบที่ 2 คือทดสอบการตรวจสอบข้อมูลเนมเซิร์ฟเวอร์ของไอเอสพี และแบบที่ 3 คือใช้งาน Local Validation Security-Aware Resolver กับ Non-Validating Security-Aware Name Server ของไอเอสพี เพื่อตอบสมมติฐานว่าเครื่อข่ายของไอเอสพีรองการการทำงานดีเอ็นเอสเซค รวมทั้งเสนอรูปแบบการเข้าถึงบริการดีเอ็นเอสเซคผ่านแต่ละไอเอสพี และสามารถระบุเนมเซิร์ฟเวอร์ของทางไอเอสพีนั้นรองรับและเปิดการทำการดีเอ็นเอสเซค รวมทั้งทำการเปิดฟังก์ชันการตรวจสอบข้อมูลหรือไม่

ผล

ผลลัพธ์จากการทดลองแยกสรุปตามวิธีการทดลอง 3 แบบ ซึ่งบางการทดลองสามารถใช้ผลการทดลองก่อนหน้าอธิบายแทนได้ ดังแสดงรายละเอียดต่อไปนี้

1. ผลการทดลองที่ 1 จำลองการทำงานของ Local Validating Security-Aware Resolver

ผลของการส่ง query จำลองแบบ Validating Security-Aware Resolver ในการหาคำตอบผ่านอินเทอร์เน็ตของผู้ให้บริการต่างๆ ได้ผลดังตารางที่ 23 ซึ่งแสดงค่าเฉลี่ยของจำนวนคำร้องที่ไม่ได้รับ response ของแต่ละคำสั่งหน่วยเป็นร้อยละ จากผลทดลองเป็นเวลา 5 วัน โดยไม่รวมความผิดพลาดที่เกิดจากไม่สามารถหาหมายเลขไอพีของเนมเซิร์ฟเวอร์ตามชื่อโดเมนที่ระบุ ความผิดพลาดที่เกิดจากเนมเซิร์ฟเวอร์ปลายทางปฏิเสธจะดำเนินการตาม query (REFUSED), ความผิดพลาดที่เกิดจากเนมเซิร์ฟเวอร์มีปัญหาไม่สามารถดำเนินการตาม query ได้ (SERVFAIL) และความผิดพลาดที่ response ถูกแบ่งเนื่องจากขนาดใหญ่เกินกว่าจะส่งในครั้งเดียว (TC มีค่าเท่ากับ 1) ยกเว้นผลจากคำสั่งที่ 1 และ 3 ของ TOT ที่คิดจากผลการทดลอง 4 วัน เนื่องจากในการทดลองวันที่ 5 พบว่าการเชื่อมต่ออินเทอร์เน็ตมีปัญหา

ตารางที่ 23 ค่าเฉลี่ยหน่วยเป็นร้อยละของจำนวนที่ไม่ได้รับ response

ISP	1 (UN)	2 (TN)	3 (U)	4 (UA)	5 (T)
3BB	7.37	3.11	7.76	3.2	3.33
CAT	3.42	0.88	3.64	0.96	1.05
JINET	12.41	0.96	12.94	1.8	0.92
PROEN	16.14	2.11	17.81	3.55	2.19
TOT	10.75	1.6	10.75	2.28	1.27
TRUE	7.41	2.5	7.85	2.72	2.37

ผู้วิจัยนำผลการทดสอบที่ได้จากคำสั่งที่ใช้โพรโทคอล UDP ในการส่ง query แบบดีเอ็นเอสและดีเอ็นเอสเซคมาเปรียบเทียบกัน จะเห็นได้ว่าค่าเฉลี่ยร้อยละของจำนวนที่ไม่ได้รับ response ของการส่ง query มีค่าใกล้เคียงกันของแต่ละไอเอสพี และผลที่ได้จากคำสั่งที่ใช้โพรโทคอล TCP ในการส่ง query แบบดีเอ็นเอสและดีเอ็นเอสเซคมาเปรียบเทียบกัน จะเห็นได้ว่าค่าเฉลี่ยที่เป็นร้อยละของจำนวนที่ไม่ได้รับ response ของการส่ง query มีค่าใกล้เคียงกันของแต่ละไอเอสพี รวมทั้งผลการทดสอบของคำสั่งที่ 4 ของทุกไอเอสพี ซึ่ง response จากคำสั่งนี้ 4 จะมีขนาดไม่เกิน 1000 ไบต์ และค่าเฉลี่ยของจำนวนที่ไม่ได้รับ response ใกล้เคียงกับการใช้ TCP ในการทดสอบ แสดงว่าอุปกรณ์เครือข่ายไม่ได้ทำการทิ้ง (discard) แพ็กเก็ตที่เป็นดีเอ็นเอสเซค

2. ผลการทดลองโจทย์ที่ 2 ทดสอบการตรวจสอบข้อมูลเนมเซิร์ฟเวอร์ของไอเอสพี

ผลการทดลองที่ 2 พบว่าเนมเซิร์ฟเวอร์ของไอเอสพีทั้ง 6 ผู้ให้บริการ ไม่สามารถรับรองความถูกต้องของชื่อโดเมนที่สอบถามได้เลย แต่เนมเซิร์ฟเวอร์ของ TRUE รองรับการใช้งานดีเอ็นเอสเซคเนื่องจากพบ RRSIG ใน response ที่ได้รับจากคำตอบของเนมเซิร์ฟเวอร์ของ TRUE ทำให้สามารถสรุปได้ว่า เนมเซิร์ฟเวอร์ของ TRUE สามารถให้บริการดีเอ็นเอสเซคแต่ไม่เปิดฟังก์ชันการตรวจสอบข้อมูล ส่วนเนมเซิร์ฟเวอร์ของไอเอสพีที่เหลืออาจจะไม่สนับสนุนการให้บริการดีเอ็นเอสเซคหรือสนับสนุนแต่ไม่เปิดการให้บริการดีเอ็นเอสเซคทำให้ไม่ปรากฏ RRSIG ใน response ซึ่งเนมเซิร์ฟเวอร์ของทาง 3BB ส่ง response กลับมาแจ้งข้อผิดพลาดถึงรูปแบบของ query ที่ส่งไปสอบถาม (FORMERR) ส่วนเนมเซิร์ฟเวอร์ของไอเอสพีที่เหลือส่ง response กลับเป็น response ที่เกิดจาก query แบบดีเอ็นเอสธรรมดา

3. ผลการทดลองโจทย์ที่ 3 ใช้งาน Local Validation Security-Aware Resolver กับ Non-Validating Security-Aware Name Server ของไอเอสพี

ผลการทดลองแบบที่ 3 ดังตารางที่ 24 ซึ่งแสดงจำนวนชื่อโดเมนที่ปลอดภัยจากการทดสอบกับเนมเซิร์ฟเวอร์ของไอเอสพี และได้ผลใกล้เคียงกับการทดสอบกับเนมเซิร์ฟเวอร์ของ Google ด้วย จากตารางที่ 24 แสดงว่าผู้ใช้บริการสามารถเข้าถึงบริการดีเอ็นเอสเซคในแบบที่ 3 ผ่าน 3BB JINET PROEN และ TRUE ได้ ดังจะเห็นว่าไคลเอนต์ได้รับ response ของชื่อโดเมนที่ปลอดภัยประมาณ 60 ชื่อโดเมน ในขณะที่จำนวน response ของชื่อโดเมนที่ปลอดภัยจากรีโซลเวอร์ที่ติดตั้งเองผ่านการทดสอบกับ CAT และ TOT มีค่าเป็น 0 ซึ่งสาเหตุอาจมากจากเนมเซิร์ฟเวอร์ของไอเอสพีไม่สนับสนุนบริการดีเอ็นเอสเซคหรือโปรแกรมสนับสนุนแต่ไม่ได้เปิดการทำงานในส่วนของดีเอ็นเอสเซคจึงไม่มี RRSIG กลับมาพร้อม response ที่รีโซลเวอร์ที่ติดตั้งเองสอบถามไป ทำให้รีโซลเวอร์ไม่สามารถตรวจสอบความถูกต้องของข้อมูลได้

ตารางที่ 24 จำนวนชื่อโดเมนที่ปลอดภัย

ISP	DAY-1	DAY-2	DAY-3	DAY-4	DAY-5
3BB	48	50	46	46	51
CAT	0	0	0	0	0
JINET	56	66	63	61	62
PROEN	67	67	65	66	67
TOT	0	0	0	0	0
TRUE	65	67	59	66	66

สังเกตได้ว่าผลการทดลองตามตารางที่ 24 แสดงว่าเนมเซิร์ฟเวอร์ของ 3BB JINET และ PROEN สามารถให้บริการดีเอ็นเอสเซคได้ ซึ่งไม่ตรงกับการสรุปการใช้งานในการทดลองที่ 2 ที่สรุปว่าเนมเซิร์ฟเวอร์ของ TRUE รองรับการใช้งานดีเอ็นเอสเซคเท่านั้น แสดงว่าบางไอเอสพีน่าจะมีปรับปรุงเนมเซิร์ฟเวอร์ของตนเอง

ถึงแม้พบว่า 3BB, JINET และ PROEN ทำการปรับปรุงเนมเซิร์ฟเวอร์ของตนเองสนับสนุนและเปิดการทำงานของดีเอ็นเอสเซคแต่ไม่สามารถระบุได้ว่าเปิดการทำงานฟังก์ชันตรวจสอบข้อมูลด้วยหรือไม่ ทั้งนี้การทดลองเมื่อเดือนพฤศจิกายน ปี 2556

จากการทดสอบทั้ง 3 แบบ ไม่สามารถสรุปได้ว่าเนมเซิร์ฟเวอร์ของทางไอเอสพีทั้ง 6 ไอเอสพีเปิดฟังก์ชันการตรวจสอบข้อมูลหรือไม่ แต่สามารถสรุปได้ว่าเครือข่ายของทั้ง 6 ไอเอสพีรองรับการทำงานของดีเอ็นเอสเซคได้ ดังนั้นผู้ใช้บริการสามารถเข้าถึงบริการดีเอ็นเอสเซคผ่านไอเอสพีทั้ง 6 ไอเอสพีได้ โดยการติดตั้งรีโซลเวอร์ที่รองรับและเปิดการทำงานดีเอ็นเอสเซค รวมทั้งเปิดฟังก์ชันการตรวจสอบข้อมูลด้วย และเนมเซิร์ฟเวอร์ของ 3BB, JINET, PROEN และ TRUE รองรับการทำงานดีเอ็นเอสเซคแต่ไม่สามารถสรุปได้ว่าเปิดฟังก์ชันการตรวจสอบข้อมูลหรือไม่ ดังนั้นผู้ใช้บริการสามารถเข้าถึงบริการดีเอ็นเอสเซคผ่าน 3BB, JINET, PROEN และ TRUE ได้โดยทำการติดตั้งรีโซลเวอร์ที่รองรับและเปิดการทำงานดีเอ็นเอสเซค และทำการตั้งค่าให้ส่งต่อ query ไปยังเนมเซิร์ฟเวอร์ของทางไอเอสพีได้

วิจารณ์

จากผลการทดสอบไม่สามารถระบุได้ชัดเจนว่าเนมเซิร์ฟเวอร์ของทางไอเอสพีเปิดฟังก์ชันการตรวจสอบข้อมูล ถ้าหากว่าเนมเซิร์ฟเวอร์ของทางไอเอสพีนั้นรองรับและเปิดการทำงานดีเอ็นเอสเซค เนื่องมาจากวันในการทำการทดสอบทั้ง 3 แบบไม่ได้ดำเนินในวันเดียวกันทั้งหมด เนื่องมาจากผู้วิจัยพบว่า พฤติกรรมในการหาคำตอบของรีโซลเวอร์ที่ใช้โปรแกรม bind เวอร์ชัน 9.8 ซึ่งรองรับการทำงานของดีเอ็นเอสเซคในการดำเนินการ ระหว่างเครื่องที่เปิดฟังก์ชั้นการทำงานดีเอ็นเอสเซคกับไม่เปิดการทำงานดีเอ็นเอสเซคค่าตัวบ่งชี้ต่างๆ ใน query ที่ส่งเพื่อหาคำตอบนั้นเหมือนกัน แม้ว่ารีโซลเวอร์จะได้รับ query แบบดีเอ็นเอส หรือดีเอ็นเอสเซคจากไคลเอนต์ และค่าบิต CD ใน query ที่เนมเซิร์ฟเวอร์ของทางไอเอสพีได้รับ ในการทดสอบแบบที่ 2 และแบบที่ 3 ต่างกันโดยการทดลองแบบที่ 2 ค่าบิต CD มีค่าเป็น 0 แต่ในการทดสอบแบบที่ 3 ค่าบิต CD มีค่าเป็น 1 จึงทำการทดสอบแบบที่ 3 เพิ่ม รวมทั้งการปรับปรุงเนมเซิร์ฟเวอร์ของทางไอเอสพีเองเพื่อให้รองรับการใช้งานดีเอ็นเอสเซค ทำให้ผลจากการทดสอบแบบที่ 2 และแบบที่ 3 มีผลสรุปไม่ตรงกัน

การเลือกไอเอสพีสำหรับการทดสอบ ผู้วิจัยได้ทำการเลือกทดสอบกับไอเอสพีที่สามารถหาทดสอบได้ เป็นที่รู้จักและมีเครือข่ายขนาดใหญ่ หากสังเกตรายชื่อไอเอสพีต่อไปนี้ CAT, ADC, BB connect, CSL, Jastel, SBN, Symphony, TCCT, TIG และ TOT เป็นไอเอสพีที่ให้บริการ International Internet Gateway และ Thailand Internet Exchange หรือเป็นไอเอสพี tier 2 ตามโครงสร้างของอินเทอร์เน็ต โดยไอเอสพีที่ผู้วิจัยทำการทดสอบ 5 ใน 6 ผู้ให้บริการมีความเกี่ยวข้องกับไอเอสพี tier 2 ตามที่กล่าวข้างต้น จากการขอความอนุเคราะห์ไปยังไอเอสพี 4 ไอเอสพีซึ่งได้รับความอนุเคราะห์เพียงรายเดียว ซึ่งไอเอสพี 3 ใน 4 ผู้ให้บริการนี้ความเกี่ยวข้องกับไอเอสพี tier 2 ตามที่กล่าวข้างต้นเช่นกัน

การทดสอบกับเนมเซิร์ฟเวอร์ของทางไอเอสพี ถือได้ว่าเป็นการโจมตีเนมเซิร์ฟเวอร์ของไอเอสพีนั้นๆ ทำให้อาจมีผลกระทบต่อผู้ใช้บริการหรือไอเอสพีเอง จึงดำเนินการทดสอบกับเนมเซิร์ฟเวอร์ของไอเอสพีเพียงเครื่องเดียว

สรุปและข้อเสนอแนะ

สรุป

ผลการทดลองของการสำรวจถึงความพร้อมการให้บริการดีเอ็นเอสเซคของไอเอสพีในประเทศไทย ตั้งแต่เดือนมีนาคน ปี 2556 จนถึงเดือนพฤศจิกายน ปี 2556 ผู้วิจัยพบว่าเครือข่ายของไอเอสพีทั้ง 6 รายรองรับการทำงานของดีเอ็นเอสเซค และไอเอสพีจำนวน 4 ใน 6 รายที่เนมเซิร์ฟเวอร์สนับสนุนการทำงานของดีเอ็นเอสเซค ส่วนอีก 2 รายนั้น เนมเซิร์ฟเวอร์อาจไม่สนับสนุนการทำงานของดีเอ็นเอสเซคหรืออาจสนับสนุนการทำงานของดีเอ็นเอสเซคแต่ไม่เปิดการทำงานดีเอ็นเอสเซค

ในการทดลองที่ 1 ผู้วิจัยนำผลการทดสอบที่ได้จากคำสั่งที่ใช้โพรโทคอล UDP ในการส่ง query แบบดีเอ็นเอสและดีเอ็นเอสเซคมาเปรียบเทียบกัน และผลที่ได้จากคำสั่งที่ใช้โพรโทคอล TCP ในการส่ง query แบบดีเอ็นเอสและดีเอ็นเอสเซคมาเปรียบเทียบกัน จะเห็นได้ว่าค่าเฉลี่ยที่เป็นร้อยละของจำนวนที่ไม่ได้รับ response ของการส่ง query ทั้ง UDP และ TCP มีค่าใกล้เคียงกันของแต่ละไอเอสพี รวมทั้งผลการทดสอบที่ response แบบดีเอ็นเอสเซคจะมีขนาดไม่เกิน 1000 ไบต์ และค่าเฉลี่ยของจำนวนที่ไม่ได้รับ response ใกล้เคียงกับการใช้ TCP ในการทดสอบ แสดงว่าอุปกรณ์เครือข่ายไม่ได้ทำการทิ้ง (discard) แพ็กเก็ตที่เป็นดีเอ็นเอสเซค ดังนั้นสามารถสรุปได้ว่าเครือข่ายของไอเอสพีทั้ง 6 รายรองรับการใช้งานดีเอ็นเอสเซค และผู้ใช้บริการของไอเอสพีดังกล่าวสามารถเข้าถึงบริการดีเอ็นเอสเซคได้ โดยการติดตั้งรีโซลเวอร์ที่รองรับการทำงานของดีเอ็นเอสเซค พร้อมทั้งทำการเปิดการทำงานดีเอ็นเอสเซคและฟังก์ชันตรวจสอบข้อมูล

จากผลการทดลองที่ 2 และ 3 จะได้ว่าเนมเซิร์ฟเวอร์ของไอเอสพีจำนวน 4 ใน 6 สนับสนุนการทำงานของดีเอ็นเอสเซค แต่ไม่สามารถระบุได้ว่าเนมเซิร์ฟเวอร์ของทางไอเอสพีนั้นทำการเปิดฟังก์ชันตรวจสอบข้อมูลได้ ดังนั้นผู้ใช้บริการของไอเอสพี 4 รายได้แก่ 3BB, JINET, PROEN และ TRUE สามารถเข้าถึงบริการดีเอ็นเอสเซคได้ โดยการติดตั้งรีโซลเวอร์ที่รองรับการทำงานของดีเอ็นเอสเซค พร้อมทั้งทำการเปิดการทำงานดีเอ็นเอสเซคและฟังก์ชันตรวจสอบข้อมูล

ดังนั้นหากผู้ใช้บริการต้องการเข้าถึงบริการดีเอ็นเอสเซคก็สามารถติดตั้ง Validation Security-Aware Resolver ขึ้นในภายในเครือข่ายของตนเองได้ หรือสามารถใช้งานเนมเซิร์ฟเวอร์ขององค์กรที่รองรับการทำงานของดีเอ็นเอสเซคเช่น Google ในการเข้าถึงบริการดีเอ็นเอสเซคได้

ข้อเสนอแนะ

ผู้วิจัยเห็นว่าควรมีการสนับสนุนให้ทางไอเอสพีทำการปรับปรุงเนมเซิร์ฟเวอร์ที่ให้บริการหาคำตอบแก่ลูกค้าให้สนับสนุนการทำงานของดีเอ็นเอสเซคและเปิดฟังก์ชันตรวจสอบข้อมูลด้วย

โดยปกติแล้วในส่วนเครือข่ายของทางไอเอสพีจะไม่มีการโยนทิ้งแพ็กเก็ตของผู้ใช้บริการ ดังนั้นผู้ดูแลเครือข่ายควรตรวจสอบเครือข่ายของตนเองว่ารองรับการทำงานของดีเอ็นเอสเซคหรือไม่ ซึ่งสามารถตรวจสอบได้โดยการทำทดลองแบบที่ 1 และนำ response มาสรุปผล หรืออย่างน้อยควรจะทำการทดลองโดยการส่ง query แบบ DNSSEC ซึ่งใช้ UDP และ TCP ดังตัวอย่างคำสั่งการใช้งานคำสั่งที่ 3 และ 5 จากตารางที่ 19 และนำ response มาสรุปผล

รวมทั้งการปรับขนาดบัฟเฟอร์ใน EDNS0 ให้เหมาะสมกับเครือข่ายที่ใช้งาน จะช่วยให้การใช้งานดีเอ็นเอสเซคได้ดีขึ้น โดยสังเกตจากจำนวนเฉลี่ยร้อยละที่ไม่ได้รับ response ที่มีขนาดเล็กจะมีค่าน้อย และใกล้เคียงค่าของ response ที่ใช้ TCP ในการรับส่งข้อมูล ซึ่งในผลการทดสอบแบบที่ 1 จำนวนเฉลี่ยร้อยละที่ไม่ได้รับ response ของคำสั่งที่ 3 และ 4 จากตารางที่ 19 โดยเนมเซิร์ฟเวอร์ใช้ UDP ในการส่ง query และ response ซึ่งคำสั่งที่ 4 จากตารางที่ 19 ซึ่ง response ที่ได้จะมีขนาดไม่เกิน 1000 ไบต์ จะมีค่าเฉลี่ยร้อยละที่ไม่ได้รับ response น้อยกว่าและใกล้เคียงค่าของ response ที่ใช้ TCP ในการรับส่งข้อมูล ซึ่งผู้วิจัยคิดว่าผลที่แตกต่างกันนั้น อาจมีผลมาจากการทำ Fragmentation ไอพีแพ็กเกตของอุปกรณ์ต่างๆ ที่ของไอพีแพ็กเกตผ่าน ดังนั้นหากปรับขนาดบัฟเฟอร์ใน EDNS0 ให้เหมาะสมกับเครือข่ายที่ใช้งาน เช่นปรับขนาดบัฟเฟอร์ใน EDNS0 น้อยกว่า 1500 ไบต์ในเครือข่ายอีเทอร์เน็ต (Ethernet) เพื่อลดความผิดพลาดในการทำ Fragmentation ไอพีแพ็กเกต จะทำให้ค่าเฉลี่ยร้อยละที่ไม่ได้รับ response ของคำสั่งที่ 3 ลดลง และถ้าหากเนมเซิร์ฟเวอร์ได้รับ response ที่มีขนาดเกินบัฟเฟอร์ที่ประกาศไว้ เนมเซิร์ฟเวอร์จะทำการรับส่งข้อมูลใหม่ด้วยการใช้ TCP แทน

เอกสารและสิ่งอ้างอิง

Mockapetris, P. 1987. RFC 1034. **Domain Names - Concepts and Facilities**. Available Source: http://www.ietf.org/rfc/rfc1034.txt, July 24, 2014.

Mockapetris, P. 1987. RFC 1035. **Domain Names - Implementation and Specification**. Available Source: http://www.ietf.org/rfc/rfc1035.txt, July 24, 2014.

Arends, R., R. Austein, M. Larson, D. Massey, and S. Rose, 2005. RFC 4033. **DNS Security Introduction and Requirements**. Available Source: http://www.ietf.org/rfc/rfc4033.txt, July 24, 2014.

Arends, R., R. Austein, M. Larson, D. Massey, and S. Rose, 2005. RFC 4034. **Resource Records for the DNS Security Extensions**. Available Source: http://www.ietf.org/rfc/rfc4034.txt, July 24, 2014.

Arends, R., R. Austein, M. Larson, D. Massey, and S. Rose, 2005. RFC 4035. **Protocol Modifications for the DNS Security Extensions**. Available Source: http://www.ietf.org/rfc/rfc4035.txt, July 24, 2014.

Damas, J., M. Graff and P. Vixie, 2013. RFC 6891. **Extension Mechanisms for DNS (EDNS(0))**. Available Source: http://tools.ietf.org/html/rfc6891, July 24, 2014.

Paul Albitz and Cricket Liu. 2001. **DNS and BIND**. O'Reilly & Associates, Inc., California (CA).

Matthew Olney, Patrick Mullen and Kevin Miklavcic, 2008. SOURCEFIRE, INC., **Dan Kaminsky's 2008 DNS Vulnerability**. Available Source: http://tools.ietf.org/html/rfc6891, July 24, 2014.

Karen Evans, 2008. **MEMORANDUM FOR CHIEF INFORMATION OFFICERS**, M-08-23. Available Source: http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2008/m08-23.pdf, July 24, 2014.

Ron Aitchison, 2011. **Pro DNS and BIND 10**, Apress. Available Source: ftp://61.135.158.199/pub/books/Apress.Pro.DNS.and.BIND.10.Feb.2011.pdf, July 24, 2014.

Sainstitute. 2003. Security Associates Institute, **Attacking the DNS Protocol – Security Paper v2**. Available Source: http://www.net-security.org/dl/articles/Attacking_the_DNS_Protocol.pdf, July 24, 2014.

ICANN Research. 2014. **TLD DNSSEC Report**. Available Source: http://stats.research.icann.org/dns/tld_report, July 24, 2014.

Google. 2014. **Introduction to Google Public DNS**. Available Source: https://developers.google.com/speed/public-dns/docs/intro, July 24, 2014.

ภาคผนวก

ภาคผนวก ก

ชื่อโดเมน และ ชื่อโดเมนของเนมเซิร์ฟเวอร์ที่นำมาทดสอบ

ตารางผนวกที่ ก1 ชื่อโดเมนระดับ Top-Level และเนมเซิร์ฟเวอร์ที่ทำการทดสอบ

ลำดับ	TLD ที่	TLD	ชื่อโดเมนของเนมเซิร์ฟเวอร์
1	1	ac.	b.nic.io.
2		ac.	b.ns13.net.
3		ac.	ns3.icb.co.uk.
4		ac.	ns1.communitydns.net.
5		ac.	a.ns13.net.
6		ac.	a.nic.ac.
7		ac.	b.nic.ac.
8	2	ag.	a0.cctld.afilias-nst.info.
9		ag.	c0.cctld.afilias-nst.info.
10		ag.	b0.cctld.afilias-nst.info.
11		ag.	b2.cctld.afilias-nst.info.
12		ag.	a2.cctld.afilias-nst.info.
13		ag.	d0.cctld.afilias-nst.info.
14	3	arpa	A.ROOT-SERVERS.NET
15		arpa	B.ROOT-SERVERS.NET
16		arpa	C.ROOT-SERVERS.NET
17		arpa	D.ROOT-SERVERS.NET
18		arpa	E.ROOT-SERVERS.NET
19		arpa	F.ROOT-SERVERS.NET
20		arpa	G.ROOT-SERVERS.NET
21		arpa	H.ROOT-SERVERS.NET
22		arpa	I.ROOT-SERVERS.NET
23		arpa	J.ROOT-SERVERS.NET
24		arpa	K.ROOT-SERVERS.NET
25		arpa	L.ROOT-SERVERS.NET
26		arpa	M.ROOT-SERVERS.NET

ตารางผนวกที่ ก1 (ต่อ)

ลำดับ	TLD ที่	TLD	ชื่อโดเมนของเนมเซิร์ฟเวอร์
27	4	asia	c0.asia.afilias-nst.info.
28		asia	d0.asia.afilias-nst.asia.
29		asia	a2.asia.afilias-nst.info.
30		asia	a0.asia.afilias-nst.info.
31		asia	b2.asia.afilias-nst.org.
32		asia	b0.asia.afilias-nst.asia.
33	5	at.	ns2.univie.ac.at.
34		at.	ns-uk.nic.at.
35		at.	r.nic.at.
36		at.	j.nic.at.
37		at.	ns1.univie.ac.at.
38		at.	ns9.univie.ac.at.
39		at.	n.nic.at.
40		at.	d.nic.at.
41	6	be.	amsterdam.ns.dns.be.
42		be.	prague.ns.dns.be.
43		be.	x.dns.be.
44		be.	m.ns.dns.be.
45		be.	london.ns.dns.be.
46		be.	brussels.ns.dns.be.
47	7	bg.	bg.cctld.authdns.ripe.net.
48		bg.	ns.register.bg.
49		bg.	ns2.register.bg.
50		bg.	ns3.register.bg.
51		bg.	sunic.sunet.se.
52		bg.	ns-ext.isc.org.

ตารางผนวกที่ ก1 (ต่อ)

ลำดับ	TLD ที่	TLD	ชื่อโดเมนของเนมเซิร์ฟเวอร์
53	8	biz.	f.gtld.biz.
54		biz.	b.gtld.biz.
55		biz.	a.gtld.biz.
56		biz.	e.gtld.biz.
57		biz.	k.gtld.biz.
58		biz.	c.gtld.biz.
59	9	br.	e.dns.br.
60		br.	b.dns.br.
61		br.	a.dns.br.
62		br.	d.dns.br.
63		br.	f.dns.br.
64		br.	c.dns.br.
65	10	bz.	a0.cctld.afilias-nst.info.
66		bz.	a2.cctld.afilias-nst.info.
67		bz.	b0.cctld.afilias-nst.org.
68		bz.	b2.cctld.afilias-nst.org.
69		bz.	c0.cctld.afilias-nst.info.
70		bz.	d0.cctld.afilias-nst.org.
71	11	cat.	b.nic.ch.
72		cat.	ns.nic.cat.
73		cat.	cat.pch.net.
74		cat.	ns1.nic.es.
75		cat.	nsc.nic.de.
76		cat.	dns4.ad.
77		cat.	anyc1.irondns.net.
78		cat.	sns-pb.isc.org.

ตารางผนวกที่ ก1 (ต่อ)

ลำดับ	TLD ที่	TLD	ชื่อโดเมนของเนมเซิร์ฟเวอร์
79	12	ch.	c.nic.ch.
80		ch.	a.nic.ch.
81		ch.	d.nic.ch.
82		ch.	h.nic.ch.
83		ch.	e.nic.ch.
84		ch.	b.nic.ch.
85		ch.	f.nic.ch.
86	13	cl.	a.nic.cl.
87		cl.	c.nic.cl.
88		cl.	sns-pb.isc.org.
89		cl.	b.nic.cl.
90		cl.	cl-ns.anycast.pch.net.
91		cl.	cl1.dnsnode.net.
92	14	co.	ns4.cctld.co.
93		co.	ns2.cctld.co.
94		co.	ns1.cctld.co.
95		co.	ns6.cctld.co.
96		co.	ns5.cctld.co.
97		co.	ns3.cctld.co.
98	15	com.	h.gtld-servers.net.
99		com.	m.gtld-servers.net.
100		com.	b.gtld-servers.net.
101		com.	f.gtld-servers.net.
102		com.	e.gtld-servers.net.
103		com.	c.gtld-servers.net.
104		com.	g.gtld-servers.net.

ตารางผนวกที่ ก1 (ต่อ)

ลำดับ	TLD ที่	TLD	ชื่อโดเมนของเนมเซิร์ฟเวอร์
105		com.	l.gtld-servers.net.
106		com.	d.gtld-servers.net.
107		com.	j.gtld-servers.net.
108		com.	i.gtld-servers.net.
109		com.	a.gtld-servers.net.
110		com.	k.gtld-servers.net.
111	16	cz.	d.ns.nic.cz.
112		cz.	b.ns.nic.cz.
113		cz.	f.ns.nic.cz.
114		cz.	c.ns.nic.cz.
115		cz.	a.ns.nic.cz.
116	17	de.	f.nic.de.
117		de.	s.de.net.
118		de.	z.nic.de.
119		de.	l.de.net.
120		de.	a.nic.de.
121	18	dk.	p.nic.dk.
122		dk.	s.nic.dk.
123		dk.	a.nic.dk.
124		dk.	l.nic.dk.
125		dk.	b.nic.dk.
126		dk.	c.nic.dk.
127	19	edu.	l.edu-servers.net.
128		edu.	a.edu-servers.net.
129		edu.	f.edu-servers.net.
130		edu.	d.edu-servers.net.

ตารางผนวกที่ ก1 (ต่อ)

ลำดับ	TLD ที่	TLD	ชื่อโดเมนของเนมเซิร์ฟเวอร์
131		edu.	c.edu-servers.net.
132		edu.	g.edu-servers.net.
133	20	eu.	a.nic.eu.
134		eu.	l.eu.dns.be.
135		eu.	l.nic.eu.
136		eu.	m.nic.eu.
137		eu.	p.nic.eu.
138		eu.	x.nic.eu.
139		eu.	y.nic.eu.
140	21	fi.	a.fi.
141		fi.	b.fi.
142		fi.	c.fi.
143		fi.	d.fi.
144		fi.	e.fi.
145		fi.	f.fi.
146		fi.	g.fi.
147		fi.	h.fi.
148		fi.	i.fi.
149	22	fr.	c.nic.fr.
150		fr.	d.nic.fr.
151		fr.	d.ext.nic.fr.
152		fr.	g.ext.nic.fr.
153		fr.	e.ext.nic.fr.
154		fr.	f.ext.nic.fr.
155	23	gi.	a0.cctld.afilias-nst.info.
156		gi.	a2.cctld.afilias-nst.info.

ตารางผนวกที่ ก1 (ต่อ)

ลำดับ	TLD ที่	TLD	ชื่อโดเมนของเนมเซิร์ฟเวอร์
157		gi.	b0.cctld.afilias-nst.org.
158		gi.	b2.cctld.afilias-nst.org.
159		gi.	c0.cctld.afilias-nst.info.
160		gi.	d0.cctld.afilias-nst.org.
161	24	gl.	a.nuuk.nic.gl.
162		gl.	b.nic.gl.
163		gl.	d.nic.gl.
164		gl.	gl1.dyntld.net.
165		gl.	gl2.dyntld.net.
166		gl.	gl3.dyntld.net.
167		gl.	gl4.dyntld.net.
168	25	gov.	a.gov-servers.net.
169		gov.	b.gov-servers.net.
170	26	gr.	grdns-br.ics.forth.gr.
171		gr.	gr-us.ics.forth.gr.
172		gr.	grdns-at.ics.forth.gr.
173		gr.	gr-aix.ics.forth.gr.
174		gr.	grdns.ics.forth.gr.
175		gr.	estia.ics.forth.gr.
176		gr.	gr-m.ics.forth.gr.
177		gr.	grdns-de.denic.de.
178	27	hn.	a0.cctld.afilias-nst.info.
179		hn.	tld1.rds.org.hn.
180		hn.	tld2.rds.org.hn.
181		hn.	b0.cctld.afilias-nst.org.
182		hn.	b2.cctld.afilias-nst.org.

ตารางผนวกที่ ก1 (ต่อ)

ลำดับ	TLD ที่	TLD	ชื่อโดเมนของเนมเซิร์ฟเวอร์
183		hn.	a2.cctld.afilias-nst.info.
184		hn.	d0.cctld.afilias-nst.org.
185		hn.	c0.cctld.afilias-nst.info.
186	28	in.	d0.in.afilias-nst.org.
187		in.	a2.in.afilias-nst.info.
188		in.	ns7.cdns.net.
189		in.	b0.in.afilias-nst.org.
190		in.	c0.in.afilias-nst.info.
191		in.	b2.in.afilias-nst.org.
192		in.	a1.in.afilias-nst.in.
193		in.	b1.in.afilias-nst.in.
194		in.	a0.in.afilias-nst.info.
195	29	info	. d0.info.afilias-nst.org.
196		info	. a0.info.afilias-nst.info.
197		info	. b0.info.afilias-nst.org.
198		info	. c0.info.afilias-nst.info.
199		info	. b2.info.afilias-nst.org.
200		info	. a2.info.afilias-nst.info.
201	30	io.	b.ns13.net.
202		io.	a.ns13.net.
203		io.	b.nic.io.
204		io.	ns1.communitydns.net.
205		io.	ns3.icb.co.uk.
206		io.	b.nic.ac.
207		io.	a.nic.io.
208	31	jp.	a.dns.jp.

ตารางผนวกที่ ก1 (ต่อ)

ลำดับ	TLD ที่	TLD	ชื่อโดเมนของเนมเซิร์ฟเวอร์
209		jp.	b.dns.jp.
210		jp.	c.dns.jp.
211		jp.	d.dns.jp.
212		jp.	e.dns.jp.
213		jp.	f.dns.jp.
214		jp.	g.dns.jp.
215	32	kr.	b.dns.kr.
216		kr.	c.dns.kr.
217		kr.	d.dns.kr.
218		kr.	e.dns.kr.
219		kr.	f.dns.kr.
220		kr.	g.dns.kr.
221	33	la.	ns1.centralnic.net.
222		la.	ns2.centralnic.net.
223		la.	ns3.centralnic.net.
224		la.	ns4.centralnic.net.
225		la.	ns5.centralnic.net.
226		la.	ns6.centralnic.net.
227		la.	ns7.centralnic.net.
228		la.	ns8.centralnic.net.
229	34	lc.	d0.cctld.afilias-nst.org.
230		lc.	b2.cctld.afilias-nst.org.
231		lc.	b0.cctld.afilias-nst.org.
232		lc.	a2.cctld.afilias-nst.info.
233		lc.	c0.cctld.afilias-nst.info.
234		lc.	a0.cctld.afilias-nst.info.

ตารางผนวกที่ ก1 (ต่อ)

ลำดับ	TLD ที่	TLD	ชื่อโดเมนของเนมเซิร์ฟเวอร์
235	35	li.	a.nic.li.
236		li.	b.nic.li.
237		li.	c.nic.li.
238		li.	d.nic.li.
239		li.	e.nic.li.
240		li.	f.nic.li.
241		li.	h.nic.li.
242	36	lk.	c.nic.lk.
243		lk.	d.nic.lk.
244		lk.	l.nic.lk.
245		lk.	m.nic.lk.
246		lk.	p.nic.lk.
247		lk.	t.nic.lk.
248		lk.	ns1.ac.lk.
249		lk.	ripe.nic.lk.
250	37	lu.	g.dns.lu.
251		lu.	i.dns.lu.
252		lu.	j.dns.lu.
253		lu.	k.dns.lu.
254		lu.	p.dns.lu.
255		lu.	ns1.dns.lu.
256		lu.	ns5.dns.lu.
257	38	me.	d0.cctld.afilias-nst.org.
258		me.	c0.cctld.afilias-nst.info.
259		me.	a2.me.afilias-nst.info.
260		me.	ns.nic.me.

ตารางผนวกที่ ก1 (ต่อ)

ลำดับ	TLD ที่	TLD	ชื่อโดเมนของเนมเซิร์ฟเวอร์
261		me.	a0.cctld.afilias-nst.info.
262		me.	b2.me.afilias-nst.org.
263		me.	b0.cctld.afilias-nst.org.
264		me.	ns2.nic.me.
265	39	mm.	ns2.nic.net.mm.
266		mm.	ns0.nic.net.mm.
267		mm.	ns1.nic.net.mm.
268		mm.	mm.cctld.authdns.ripe.net.
269	40	mn.	c0.cctld.afilias-nst.info.
270		mn.	b2.cctld.afilias-nst.org.
271		mn.	d0.cctld.afilias-nst.org.
272		mn.	ns3.magic.mn.
273		mn.	ns2.magic.mn.
274		mn.	a2.cctld.afilias-nst.info.
275		mn.	b0.cctld.afilias-nst.org.
276		mn.	a0.cctld.afilias-nst.info.
277		mn.	ns1.magic.mn.
278		mn.	ns4.magic.mn.
279	41	muse	um. anyc1.irondns.net.
280		muse	um. nic.museum.
281		muse	um. ns.icann.org.
282		muse	um. sns-pb.isc.org.
283		muse	um. ns5.knipp.de.
284	42	my.	ns-my.nic.fr.
285		my.	ns5.jaring.my.
286		my.	ns20.iij.ad.jp.

ตารางผนวกที่ ก1 (ต่อ)

ลำดับ	TLD ที่	TLD	ชื่อโดเมนของเนมเซิร์ฟเวอร์
287		my.	dns2.mynic.net.my.
288		my.	ns6.jaring.my.
289		my.	dns.mynic.net.my.
290		my.	ns2.cuhk.edu.hk.
291	43	na.	sns-pb.isc.org.
292		na.	na1.dyntld.net.
293		na.	na2.dyntld.net.
294		na.	merlin.net.na.
295		na.	na-ns.anycast.pch.net.
296		na.	anyc2.irondns.net.
297		na.	ns5.nominum.com.
298		na.	ns6.nominum.eu.
299	44	nc.	ns2.nc.
300		nc.	censvrns0001.ird.fr.
301		nc.	nc.cctld.authdns.ripe.net.
302		nc.	any-ns1.nc.
303		nc.	ns1.nc.
304	45	net.	a.gtld-servers.net.
305		net.	b.gtld-servers.net.
306		net.	c.gtld-servers.net.
307		net.	d.gtld-servers.net.
308		net.	e.gtld-servers.net.
309		net.	f.gtld-servers.net.
310		net.	g.gtld-servers.net.
311		net.	h.gtld-servers.net.
312		net.	i.gtld-servers.net.

ตารางผนวกที่ ก1 (ต่อ)

ลำดับ	TLD ที่	TLD	ชื่อโดเมนของเนมเซิร์ฟเวอร์
313		net.	j.gtld-servers.net.
314		net.	k.gtld-servers.net.
315		net.	l.gtld-servers.net.
316		net.	m.gtld-servers.net.
317	46	nl.	nl1.dnsnode.net.
318		nl.	ns1.nic.nl.
319		nl.	ns2.nic.nl.
320		nl.	ns3.nic.nl.
321		nl.	ns4.nic.nl.
322		nl.	ns-nl.nic.fr.
323		nl.	sns-pb.isc.org.
324	47	nu.	ns.eu.nic.nu.
325		nu.	ns.de.nic.nu.
326		nu.	ns.nl.nic.nu.
327		nu.	ns.nic.nu.
328		nu.	ns.se.nic.nu.
329	48	org.	c0.org.afilias-nst.info.
330		org.	b0.org.afilias-nst.org.
331		org.	a0.org.afilias-nst.info.
332		org.	b2.org.afilias-nst.org.
333		org.	d0.org.afilias-nst.org.
334		org.	a2.org.afilias-nst.info.
335	49	pl.	a-dns.pl.
336		pl.	c-dns.pl.
337		pl.	d-dns.pl.
338		pl.	e-dns.pl.

ตารางผนวกที่ ก1 (ต่อ)

ลำดับ	TLD ที่	TLD	ชื่อโดเมนของเนมเซิร์ฟเวอร์
339		pl.	f-dns.pl.
340		pl.	g-dns.pl.
341		pl.	h-dns.pl.
342		pl.	i-dns.pl.
343	50	pm.	c.nic.fr.
344		pm.	d.ext.nic.fr.
345		pm.	d.nic.fr.
346		pm.	e.ext.nic.fr.
347		pm.	f.ext.nic.fr.
348		pm.	g.ext.nic.fr.
349	51	pr.	descartes.nic.pr.
350		pr.	pr-dns.denic.de.
351		pr.	golomb.nic.pr.
352		pr.	pr-ns.anycast.pch.net.
353		pr.	pascal.nic.pr.
354	52	re.	e.ext.nic.fr.
355		re.	d.nic.fr.
356		re.	c.nic.fr.
357		re.	g.ext.nic.fr.
358		re.	f.ext.nic.fr.
359		re.	d.ext.nic.fr.
360	53	se.	a.ns.se.
361		se.	b.ns.se.
362		se.	c.ns.se.
363		se.	d.ns.se.
364		se.	e.ns.se.

ตารางผนวกที่ ก1 (ต่อ)

ลำดับ	TLD ที่	TLD	ชื่อโดเมนของเนมเซิร์ฟเวอร์
365		se.	f.ns.se.
366		se.	g.ns.se.
367		se.	h.ns.se.
368		se.	i.ns.se.
369		se.	j.ns.se.
370	54	sh.	a.nic.sh.
371		sh.	a.ns13.net.
372		sh.	ns3.icb.co.uk.
373		sh.	b.nic.ac.
374		sh.	b.nic.io.
375		sh.	ns1.communitydns.net.
376		sh.	b.ns13.net.
377	55	si.	c.dns.si.
378		si.	sss.dns.si.
379		si.	g.dns.si.
380		si.	h.dns.si.
381		si.	e.dns.si.
382		si.	b.dns.si.
383		si.	d.dns.si.
384		si.	f.dns.si.
385	56	su.	f.dns.ripn.net.
386		su.	ns5.msk-ix.net.
387		su.	e.dns.ripn.net.
388		su.	ns9.ripn.net.
389		su.	d.dns.ripn.net.
390		su.	ns.ripn.net.

ตารางผนวกที่ ก1 (ต่อ)

ลำดับ	TLD ที่	TLD	ชื่อโดเมนของเนมเซิร์ฟเวอร์
391	57	sx.	b.ns.sx.
392		sx.	c.ns.sx.
393		sx.	a.ns.sx.
394	58	tf.	g.ext.nic.fr.
395		tf.	c.nic.fr.
396		tf.	f.ext.nic.fr.
397		tf.	d.ext.nic.fr.
398		tf.	e.ext.nic.fr.
399		tf.	d.nic.fr.
400	59	th.	ns.thnic.net.
401		th.	th.cctld.authdns.ripe.net.
402		th.	ams.sns-pb.isc.org.
403		th.	dns1.thnic.co.th.
404		th.	ns-a.thnic.co.th.
405		th.	ns-e.thnic.co.th.
406		th.	sfba.sns-pb.isc.org.
407	60	tm.	a.nic.tm.
408		tm.	ns1.communitydns.net.
409		tm.	b.nic.io.
410		tm.	ns3.icb.co.uk.
411		tm.	a.ns13.net.
412		tm.	b.nic.ac.
413		tm.	b.ns13.net.
414	61	tw.	a.dns.tw.
415		tw.	b.dns.tw.
416		tw.	c.dns.tw.

ตารางผนวกที่ ก1 (ต่อ)

ลำดับ	TLD ที่	TLD	ชื่อโดเมนของเนมเซิร์ฟเวอร์
417		tw.	d.dns.tw.
418		tw.	e.dns.tw.
419		tw.	f.dns.tw.
420		tw.	g.dns.tw.
421		tw.	h.dns.tw.
422		tw.	ns.twnic.net.
423	62	ug.	ns.icann.org.
424		ug.	ug.cctld.authdns.ripe.net.
425		ug.	root.eahd.or.ug.
426		ug.	ns-ext.isc.org.
427		ug.	anycast.eahd.or.ug.
428	63	uk.	ns1.nic.uk.
429		uk.	ns2.nic.uk.
430		uk.	ns3.nic.uk.
431		uk.	ns4.nic.uk.
432		uk.	ns5.nic.uk.
433		uk.	ns6.nic.uk.
434		uk.	ns7.nic.uk.
435		uk.	nsa.nic.uk.
436		uk.	nsb.nic.uk.
437		uk.	nsc.nic.uk.
438		uk.	nsd.nic.uk.
439	64	us.	e.cctld.us.
440		us.	c.cctld.us.
441		us.	a.cctld.us.
442		us.	b.cctld.us.

ตารางผนวกที่ ก1 (ต่อ)

ลำดับ	TLD ที่	TLD	ชื่อโดเมนของเนมเซิร์ฟเวอร์
443		us.	f.cctld.us.
444		us.	k.cctld.us.
445	65	wf.	d.nic.fr.
446		wf.	g.ext.nic.fr.
447		wf.	c.nic.fr.
448		wf.	f.ext.nic.fr.
449		wf.	e.ext.nic.fr.
450		wf.	d.ext.nic.fr.
451	66	yt.	g.ext.nic.fr.
452		yt.	c.nic.fr.
453		yt.	d.ext.nic.fr.
454		yt.	d.nic.fr.
455		yt.	f.ext.nic.fr.
456		yt.	e.ext.nic.fr.

ตารางผนวกที่ ก2 ชื่อโดเมนเนมที่ทำการสุ่มได้จากอินเทอร์เน็ต

อันดับ	ชื่อโดเมน
1	www.name.ac
2	www.japan-nic.ac
3	www.pro.ac
4	www.sqn.ac
5	directory.ac
6	www.nic.ag
7	www.dr.ag
8	www.mywebsite.ag
9	www.jag.ag
10	www.worldofit.ag
11	www.melbourne.ag
12	www.ch.ag
13	www.webm.ag
14	asia.asia
15	smilehost.asia
16	whois.asia
17	www.idn.asia
18	www.webworks.asia
19	www.asia-nic.asia
20	pioneer.domains.asia
21	www.domainname.at
22	www.nic.at
23	geeks.thedailywh.at
24	www.hjp.at
25	en.edis.at
26	domains.letseat.at
27	www.realtime.at

ตารางผนวกที่ ก2 (ต่อ)

อันดับ	ชื่อโดเมน
28	www.yourname.at
29	www.domainnames.be
30	www.dns.be
31	www.easyhost.be
32	www.register.be
33	www.tuonome.be
34	www.domaining.be
35	telenet.be
36	support.mobistar.be
37	www.register.bg
38	www.web.need.bg
39	host.bg
40	freehosting.bg
41	www.cloud.bg
42	www.inet.bg
43	trademark.bg
44	www.webfactory.bg
45	www.whois.biz
46	www.it-biz.biz
47	cheap-biz-domain-names.biz
48	www.godaddy.biz
49	biz-domain.biz
50	www.resell.biz
51	www.thaiton.biz
52	www.cgi.br
53	registro.br
54	www.cg.org.br

ตารางผนวกที่ ก2 (ต่อ)

อันดับ	ชื่อโดเมน
55	www.marcaria.com.br
56	www.daniel.adv.br
57	egov.ufsc.br
58	www.nic.br
59	nic.bz
60	www.belizenic.bz
61	www.edata.bz
62	www.eu-domain.bz
63	www.domain.za.bz
64	idn.bz
65	ww.108.bz
66	www.crv.bz
67	www.domini.cat
68	www.fundacio.cat
69	www.gencat.cat
70	www.barcelonaturisme.cat
71	www.konig.cat
72	www.tomas.cat
73	www.nic.ch
74	www.switch.ch
75	www.inic.ch
76	www.englishforum.ch
77	polylex.epfl.ch
78	www.marcaria.ch
79	www.swisscom.ch
80	www.nic.cl
81	www.name.cl

ตารางผนวกที่ ก2 (ต่อ)

อันดับ	ชื่อโดเมน
82	www.marcaria.cl
83	www.alessandri.cl
84	www.spanish.cl
85	www.prolesur.cl
86	www.cointernet.co
87	www.networksolutions.co
88	www.domainnamesales.co
89	empirebuilders.co
90	www.coauctions.co
91	www.nima.co
92	www.domainname.com
93	www.thaidomainnames.com
94	www.chaiyohosting.com
95	www.godaddy.com
96	www.name.com
97	checkip.narak.com
98	www.thai-domain.com
99	www.example.com
100	www.domains.cz
101	www.dns-info.cz
102	www.nic.cz
103	en.soud.cz
104	www.smartweb.cz
105	help.regzone.cz
106	www.o2.cz
107	www.denic.de
108	www.netlaw.de

ตารางผนวกที่ ก2 (ต่อ)

อันดับ	ชื่อโดเมน
109	com.de
110	www.marcaria.de
111	www.tucows.de
112	www.sedo.de
113	www.inf.tu-dresden.de
114	www.dk-hostmaster.dk
115	www.web-solutions.dk
116	netarkivet.dk
117	www.domainbox.dk
118	www.mwblaw.dk
119	www.difo.dk
120	www.simplylaw.dk
121	net.educause.edu
122	kb.iu.edu
123	itservices.stanford.edu
124	ist.mit.edu
125	www.utexas.edu
126	www.cs.indiana.edu
127	webcomm.tufts.edu
128	www.eurid.eu
129	www.whois.eu
130	ec.europa.eu
131	www.register.eu
132	www.domainextension.eu
133	www.en.eu
134	www.web-solutions.eu
135	www.ficora.fi

ตารางผนวกที่ ก2 (ต่อ)

อันดับ	ชื่อโดเมน
136	www.domain.fi
137	www.finlex.fi
138	www.viestintavirasto.fi
139	www.suomi.fi
140	www.hostingservice.fi
141	www.nic.funet.fi
142	www.afnic.fr
143	www.e-zone.fr
144	www.domainesinfo.fr
145	www.club-nd.fr
146	www.bnamed.fr
147	www.marcaria.fr
148	www.regimbeau.fr
149	www.nic.gi
150	www.isolas.gi
151	www.gra.gi
152	gibnet.gi
153	www.computers.gi
154	www.sapphire.gi
155	www.justconsulting.gi
156	www.nic.gl
157	www.qr.gl
158	www.businesscatalog.gl
159	www.nl.gl
160	www.biz.gl
161	www.illuut.gl
162	www.pro.gl

ตารางผนวกที่ ก2 (ต่อ)

อันดับ	ชื่อโดเมน
163	www.ba.gl
164	www.dotgov.gov
165	www.usability.gov
166	www.azgita.gov
167	www.howto.gov
168	www.maine.gov
169	www.mass.gov
170	energy.gov
171	www.hostmaster.gr
172	dnhost.gr
173	www.papaki.gr
174	www.papaki.gr
175	www.iaas.gr
176	www.domains24.gr
177	www.eett.gr
178	oteshop.ote.gr
179	www.nic.hn
180	dot.hn
181	buy.hn
182	www.cool.hn
183	www.netsys.hn
184	www.de.hn
185	www.co.hn
186	dhbk.hn
187	www.registry.in
188	www.net4.in
189	www.inregistry.in

ตารางผนวกที่ ก2 (ต่อ)

อันดับ	ชื่อโดเมน
190	www.inforum.in
191	domains.oneindia.in
192	www.bigrock.in
193	info.info
194	www.thaiadsense.info
195	www.cheap-info-domains.info
196	www.dotinfodomainames.info
197	www.afilias.info
198	www.1and1.info
199	www.cheapestdomain.info
200	www.nic.io
201	gun.io
202	docs.orchestra.io
203	put.io
204	www.claim.io
205	udrp.io
206	gondor.io
207	jprs.co.jp
208	set.jp
209	www.domain-name-registration.jp
210	tm.softbank.jp
211	www.ocn.ne.jp
212	asahi-net.jp
213	www.aftermarket.jp
214	domain.nida.or.kr
215	whois.kisa.or.kr
216	www.domain.kr

ตารางผนวกที่ ก2 (ต่อ)

อันดับ	ชื่อโดเมน
217	www.marcaria.co.kr
218	www.internetbrothers.co.kr
219	dpnm.postech.ac.kr
220	en.bab.la
221	www.maintenance.la
222	www.uk.la
223	mrs.la
224	javier.la
225	webnames.la
226	easy.la
227	www.nic.lc
228	www.isisworld.lc
229	english.lc
230	www.now.lc
231	www.clan.lc
232	www.ctsl.lc
233	www.domain.lc
234	www.game.lc
235	tech.li
236	support.paper.li
237	www.longisland.li
238	zip.li
239	kutu.li
240	jmp.li
241	zimmer.li
242	www.earth.li
243	www.nic.lk

ตารางผนวกที่ ก2 (ต่อ)

อันดับ	ชื่อโดเมน
244	www.webhost.lk
245	www.domainnames.lk
246	www.lankacom.lk
247	www.entersys.lk
248	www.icta.lk
249	www.schoolnet.lk
250	www.webvision.lk
251	www.dns.lu
252	www.site.lu
253	www.root.lu
254	www.paperjam.lu
255	www.netsite.lu
256	www.focus.lu
257	www.domain.me
258	help.flavors.me
259	domainoffers.me
260	www.bobparsons.me
261	zeeis.me
262	www.internetnews.me
263	www.nic.mm
264	www.redlink.net.mm
265	www.mmnic.net.mm
266	www.mptngw.net.mm
267	www.directory.com.mm
268	www.mpt.net.mm
269	www.nic.mn
270	www.domain.mn

ตารางผนวกที่ ก2 (ต่อ)

อันดับ	ชื่อโดเมน
271	www.mol.mn
272	manage.magicnet.mn
273	www.search.mn
274	nempls.mn
275	www.nic.museum
276	about.museum
277	musedoma.museum
278	www.whois.museum
279	archives.icom.museum
280	ens.museum
281	www.domainregistry.my
282	www.exabytes.com.my
283	www.bft.com.my
284	www.shinjiru.com.my
285	www.superregistration.my
286	www.sellonline.my
287	www.info.na
288	www.iway.na
289	www.intertech.com.na
290	www.internet.na
291	www.parliament.gov.na
292	swakop.omadhina.co.na
293	www.domaine.nc
294	www.holcim.nc
295	cci-info.nc
296	dl.xlpm.nc
297	sites.wamland.nc

ตารางผนวกที่ ก2 (ต่อ)

อันดับ	ชื่อโดเมน
298	traffic.indeo.nc
299	www.ird.nc
300	www.whois.net
301	www.internic.net
302	www.bcoms.net
303	www.idotz.net
304	www.thaisite.net
305	www.gkg.net
306	domainwhiz.net
307	www.ezynow.net
308	www.europeregistry.nl
309	domain.co.nl
310	www.sidn.nl
311	www.co.nl
312	www.domain-names.nl
313	www.marqu.nl
314	www.domain-registry.nl
315	www.nunames.nu
316	uk.nu
317	www.domain-name-registration.nu
318	www.kyrkomusik.nu
319	www.nic.nu
320	bink.nu
321	en.wikipedia.org
322	www.pir.org
323	www.domains.org
324	www.thairegister.org

ตารางผนวกที่ ก2 (ต่อ)

อันดับ	ชื่อโดเมน
325	www.chillingeffects.org
326	www.org-domain-names.org
327	www.dns.pl
328	www.namedrive.pl
329	hrd.pl
330	www.rejestracjadomen.pl
331	ipsix.pl
332	www.bartosiewicz.pl
333	netart.pl
334	www.nic.pm
335	www.class.pm
336	listen.pm
337	hollywood.pm
338	www.voip.pm
339	www.firenze.pm
340	www.doctors.pm
341	nic.pr
342	www.marcaria.pr
343	www.caribbeanbusiness.pr
344	www.twentyyearsof.pr
345	dotc.pr
346	canovanas.pr
347	www.domain.re
348	www.futu.re
349	www.noise.re
350	www.dot.re
351	www.motors.re

ตารางผนวกที่ ก2 (ต่อ)

อันดับ	ชื่อโดเมน
352	afnic.re
353	depienne.re
354	thepiratebay.se
355	www.iis.se
356	www.sedirekt.se
357	www.julian.se
358	www.bluerange.se
359	signius.se
360	www.marcaria.se
361	www.nic.sh
362	rake.sh
363	www.hohwacht-ostsee.sh
364	blog.layer8.sh
365	burghhouse.co.sh
366	moonbeams.co.sh
367	sudo.sh
368	engli.sh
369	www.registry.si
370	www.arnes.si
371	www.domains.si
372	www.dominio.si
373	www.item.si
374	www.presentia.si
375	www.de.si
376	www.register.su
377	rogue.su
378	who.su

ตารางผนวกที่ ก2 (ต่อ)

อันดับ	ชื่อโดเมน
379	www.fid.su
380	www.nic.su
381	www.chronicle.su
382	registry.sx
383	www.sxmregulator.sx
384	www.ingrid.roth.tf
385	www.chris.schmidt.tf
386	www.mexico.tf
387	bourjois.tf
388	bazos.tf
389	thompson.tf
390	www.goodmedia.co.th
391	www.domainname.in.th
392	domain-name.gict.co.th
393	www.pathosting.co.th
394	www.thnic.co.th
395	www.com.co.th
396	www.nic.tm
397	law.tm
398	www.play.tm
399	www.google.tm
400	www.axu.tm
401	lawyers.tm
402	www.twnic.net.tw
403	www.dotz.tw
404	www.webnic.tw
405	www.marcaria.com.tw

ตารางผนวกที่ ก2 (ต่อ)

อันดับ	ชื่อโดเมน
406	www.csie.ncu.edu.tw
407	officeshoes.tw
408	www.registry.co.ug.
409	web-hosting.co.ug
410	www.infopoint.co.ug
411	pixelmagic.co.ug
412	forum.mak.ac.ug
413	www.spacenet.co.ug
414	www.nominet.org.uk
415	www.123-reg.co.uk
416	www.fasthosts.co.uk
417	www.names.co.uk
418	easily.co.uk
419	ukdomain-names.co.uk
420	www.neustar.us
421	www.cms.kids.us
422	www.dot-us-domain-names.us
423	www.usdomainname.us
424	www.getfreedomain.us
425	www.coupon.wf
426	ads.wf
427	www.101domains.wf
428	russia.wf
429	www.italy.wf
430	career.wf
431	italia.yt
432	doctor.yt

ตารางผนวกที่ ก2 (ต่อ)

อันดับ	ชื่อโดเมน
433	med.yt
434	www.ski.yt
435	computer.yt

ภาคผนวก ข

ผลงานตีพิมพ์

2014 International Computer Science and Engineering Conference: ICSEC 2014 Thai Track

ความพร้อมในการให้บริการดีเอ็นเอสเซคของไอเอสพีในประเทศไทย

DNSSEC Readiness of Thai ISPs

สัญชัย นิจวิภากุล[1], สุชุมาล กิติสิน[1], และ ชวลิต ศรีสถาพรพัฒน์[1]
[1]ภาควิชาวิทยาการคอมพิวเตอร์ คณะวิทยาศาสตร์ มหาวิทยาลัยเกษตรศาสตร์, กรุงเทพฯ
E-mail: g521440171@ku.ac.th, fscisms@ku.ac.th, fscicls@ku.ac.th

บทคัดย่อ

รัฐบาลกลางของสหรัฐอเมริกาเล็งเห็นความสำคัญในการใช้งานดีเอ็นเอสเซค (DNSSEC) และทำการออกนโยบายปรับเปลี่ยนทุกชื่อโดเมนภายใต้ gov ให้ใช้งานผ่านดีเอ็นเอสเซคได้ภายในเดือนธันวาคม ปี 2552 เนื่องจากมีการโจมตีช่องโหว่ของดีเอ็นเอส (DNS) ซึ่งเป็นหัวใจของการใช้อินเทอร์เน็ต ดังนั้นผู้วิจัยจึงทำการสำรวจถึงความพร้อมการให้บริการดีเอ็นเอสเซคของไอเอสพี (ISP) หรือผู้ให้บริการอินเทอร์เน็ตในประเทศไทย เพื่อความปลอดภัยในการใช้งานอินเทอร์เน็ตในระดับสากล จากผลการทดลองตั้งแต่เดือนมีนาคม ปี 2556 จนถึงเดือนพฤศจิกายน ปี 2556 ผู้วิจัยพบว่าไอเอสพีจำนวน 4 ใน 6 รายที่เครื่องบริการชื่อโดเมน (name server) สนับสนุนการทำงานของดีเอ็นเอสเซค และเชื่อว่าไอเอสพีที่เหลือจะดำเนินการปรับปรุงการให้บริการดีเอ็นเอสเซคในไม่ช้า

คำสำคัญ: ดีเอ็นเอส, ดีเอ็นเอสเซค

Abstract

This Federal government of the US recognized the importance of DNSSEC; then, issued a policy that all domain names under gov domain needs to be modified to incorporate DNSSEC to their name servers by December of 2009. Because of the vulnerabilities of DNS which is primary service of the Internet is now increasingly major concerned. Therefore, the experiments in order to survey on the availability DNSSEC service in Thai ISPs to ensure international standard security of the Internet usage. The experiments was done during March 2013 until November 2013 and it was found that 4 out of 6 ISPs are equipped with name servers supporting DNSSEC and the trends shows that the rests will continue to improve their service to support DNSSEC soon.

Keywords: DNS, DNSSEC

1. บทนำ

ดีเอ็นเอส [1-2] เป็นหัวใจที่สำคัญใช้งานอินเทอร์เน็ต เนื่องจากดีเอ็นเอสทำหน้าที่ แปลงชื่อโดเมนเป็นเลขที่อยู่ไอพีจึงทำให้อุปกรณ์ต่างๆ ในอินเทอร์เน็ตสามารถสื่อสารและรับส่งข้อมูลถึงกันได้ โดยทั่วไปแล้วแต่ละองค์กรจะมี เครื่องบริการเจ้าของชื่อโดเมน (Authoritative Name Server) และเครื่องบริการหาชื่อโดเมน (resolver) ซึ่งให้บริการหาคำตอบ (resolution) ให้แก่โคลเอนต์และทำการบรรทึกข้อมูลที่ได้ลงแคช

Dan Kaminsky พบช่องโหว่ของดีเอ็นเอสในปี 2551 [3] ในกรณีเครื่องบริการหาชื่อโดเมนถูกโจมตีแล้ว จะทำให้โคลเอนต์ที่ใช้บริการได้รับคำตอบการแปลชื่อโดเมนเป็นเลขที่อยู่ไอพีที่ไม่ถูก ต้องทำให้เสียบัตรเครดิตหรือรหัสผ่านของโคลเอนต์รั่วไหลได้ ดังนี้จึงส่งผลให้องค์กรและธุรกิจปรับตัวตาม รวมทั้งรัฐบาลกลางของสหรัฐอเมริกาเล็งเห็นความสำคัญในการใช้งานดีเอ็นเอสเซค และทำการออกนโยบายปรับเปลี่ยนทุกชื่อโดเมนภายใต้ gov ให้ใช้งานผ่านดีเอ็นเอสเซคได้ภายในเดือนธันวาคม ปี 2552 [4]

ซึ่งการปรับเปลี่ยนจากดีเอ็นเอสเป็นดีเอ็นเอสเซคนั้นข้อความ (message) ที่รับส่งกันระหว่างเครื่องบริการชื่อโดเมน หรือโคลเอนต์กับเครื่องบริการชื่อโดเมน สามารถมีขนาดใหญ่กว่าข้อความที่ดีเอ็นเอสใช้ในการรับส่ง เนื่องจากมีกระบวนการต่างๆเพิ่มขึ้นเพื่อให้บริการด้านความปลอดภัย ในปี 2551 เดียวกันนี้มีการศึกษาว่า อุปกรณ์เครือข่ายบางรุ่นที่ใช้งานเชื่อต่ออินเทอร์เน็ตไม่สนับสนุนการทำงานกับดีเอ็นเอสเซค [5] ผู้วิจัยจึงทำการสำรวจความพร้อมการให้บริการดีเอ็นเอสเซคของไอเอสพีในประเทศไทยเพื่อความปลอดภัยในการใช้งานอินเทอร์เน็ตในระดับสากล

2. ดีเอ็นเอสเซค

ดีเอ็นเอสเซค [6-9] เป็นส่วนที่เพิ่มขยายของดีเอ็นเอสเกี่ยวกับความปลอดภัย สามารถทำงานร่วมกับดีเอ็นเอสได้ โดยอาศัยหลักวิทยาการเข้ารหัสลับด้วยกุญแจไม่สมมาตร (Asymmetric Key) และลายเซ็นดิจิตอล (Digital Signature) เพื่อให้บริการในการรับรองความถูกของข้อมูลที่ได้รับจากแหล่งกำเนิดของแต่ละชื่อโดเมน (data origin authentication) ข้อมูลไม่ถูกเปลี่ยนแปลงระหว่างการรับส่ง (data integrity) และรับรองคำตอบที่ว่าไม่มีชื่อโดเมนหรือชนิดของระเบียนทรัพยากร (Resource Record) ที่ร้องขอนั้นจริงๆ (authenticating name and type non-existence) แต่อย่างไรก็ดี ดีเอ็นเอสเซคไม่สามารถป้องกันการโจมตีเพื่อให้ระบบไม่สามารถให้บริการได้ (Denial-of-Service) และไม่รองรับการเข้ารหัส-ถอดรหัสข้อความที่รับและส่ง

Name	Type	Class	TTL	RDLength	RDATA

รูปที่ 1 รูปแบบของระเบียนทรัพยากร

ข้อมูลของดีเอ็นเอสหรือระเบียนทรัพยากร ประกอบไปด้วย Name, Type, Class, TTL, RDLength และ RDATA ดังรูปที่ 1 ค่าของส่วน Name คือชื่อโดเมนของระเบียนทรัพยากรนั้นๆ ส่วน Type จะเป็นค่าที่แสดงถึงชนิดของระเบียนทรัพยากร ส่วน Class จะเป็นตัวเลขที่แสดงว่าทำงานในระบบใด เช่นถ้าใช้งานในอินเทอร์เน็ตจะมีค่าเท่ากับ 1 ส่วน TTL จะเป็นระยะเวลาวินาทีที่ระเบียนทรัพยากร นั้นจะถูกเก็บไว้ในแคชของเครื่องบริการหาชื่อโดเมน ส่วน RDLength แสดงว่าความยาวของ RDATA และส่วนสุดท้าย RDATA จะเก็บข้อมูลเกี่ยวกับระเบียนทรัพยากรตามชนิด

เนื่องจากดีเอ็นเอสเซคให้บริการด้านความปลอดภัย จึงมีการเพิ่มและปรับโพรโทคอล โดยมีการกำหนดระเบียนทรัพยากรชนิดใหม่ 4 ชนิดคือ 1.DNS public key (DNSKEY), 2.Delegation Signer (DS), 3.Resource Record Signature (RRSIG) และ 4.Next Secure (NSEC)

โดย 1.DNSKEY ใช้เก็บข้อมูลเกี่ยวกับกุญแจสาธารณะ (public key) ของแต่ละชื่อโดเมน 2.ข้อมูลบางส่วนใน DS จะทำขึ้นมาจากการนำชื่อโดเมนของ DNSKEY และข้อมูล RDATA ใน DNSKEY นำมาต่อกันแล้วมาผ่านอัลกอริทึมเข้ารหัส 3.RRSIG ใช้เก็บลายเซ็นดิจิตอลของระเบียนทรัพยากรชนิดต่างๆ และข้อมูลที่ใช้ระบุถึงกุญแจสาธารณะตัวไหนที่ใช้ในการทำลายเซ็นดิจิตอลรวมทั้งวันหมดอายุ และ 4.NSEC ใช้เก็บชื่อโดเมนในลำดับถัดไปและชนิดของระเบียนทรัพยากรของชื่อโดเมนนั้นๆ

สำหรับเครื่องบริการเจ้าของชื่อโดเมน ที่ให้บริการดีเอ็นเอสเซคของแต่ละชื่อโดเมน ผู้ดูแลต้องทำการสร้างกุญแจไม่สมมาตรอย่างน้อย 1 คู่ สำหรับแต่ละชื่อโดเมน จากนั้นดำเนินการ zone signing ซึ่งคือกระบวนการเพิ่มระเบียนทรัพยากรชนิดใหม่ 4 ชนิด โดยอาจมี DS เป็นส่วนเสริมได้ เนื่องจาก DS ของชื่อโดเมนนั้นๆ จะถูกบรรจุในแฟ้มข้อมูลโซน (zone file) ของเครื่องบริการเจ้าของชื่อโดเมน ของชื่อโดเมนที่อยู่ระดับบนในโครงสร้างของดีเอ็นเอสเช่น DS ของ example.org จะต้องถูกเก็บไว้ที่เครื่องบริการเจ้าของชื่อโดเมนของ org. เป็นต้น

ชนิดของกุญแจไม่สมมาตรที่ใช้ในดีเอ็นเอสเซคมีสองแบบ คือ Zone Signing Key (ZSK) โดยกุญแจส่วนบุคคล (private key) ชนิด ZSK ใช้สร้างลายเซ็นดิจิตอลของระเบียนทรัพยากรชนิดต่างๆ ที่อยู่แฟ้มข้อมูลโซน และ Key Signing Key (KSK) โดยกุญแจส่วนบุคคลชนิด (KSK) ใช้ในการสร้างลายเซ็นดิจิตอลของ DNSKEY ซึ่งกุญแจสาธารณะชนิด ZSK ถูกเก็บใน DNSKEY หรือกุญแจสาธารณะชนิด KSK จะใช้ยืนยันกุญแจสาธารณะชนิด ZSK ของแต่ละชื่อโดเมน ผ่านการตรวจสอบลายเซ็นดิจิตอลของชื่อโดเมนนั้น ส่วนการยืนยันกุญแจสาธารณะชนิด KSK ที่เก็บใน DNSKEY จะใช้ DS เนื่องจากข้อมูลบางส่วนใน DS ทำขึ้นมาจากการนำชื่อโดเมนของ DNSKEY และข้อมูลบางส่วนใน DNSKEY นำมาต่อกันแล้วมาผ่านอัลกอริทึมเข้ารหัส

ในการใช้งานดีเอ็นเอสเซคที่เครื่องบริการหาชื่อโดเมน (resolver) ต้องทำการเปิดฟังก์ชันสนับสนุนการทำงานดีเอ็นเอสเซค และฟังก์ชันตรวจสอบข้อมูล (validation) โดยการตรวจสอบจะต้องตั้งค่า Trust Anchor ซึ่งคือเอนทิตี (entity) ที่สามารถเชื่อถือได้ เช่น กุญแจสาธารณะชนิด KSK ของชื่อโดเมน root สำหรับเป็นจุดเริ่มต้นในการตรวจสอบกุญแจสาธารณะของชื่อโดเมนต่างๆ เนื่องจากเครื่องบริการชื่อโดเมน root ดูแลโดยองค์กรที่ตั้งขึ้นโดยไม่แสวงหากำไรและเชื่อถือได้

สำหรับข้อความในดีเอ็นเอสมีสองแบบคือ ข้อคำถาม (query) และข้อตอบ (response) ถูกไคลเอนต์ เครื่องบริการหาชื่อโดเมน และเครื่องบริการชื่อโดเมนต่างๆ ใช้สื่อสารระหว่างกัน การส่งข้อความในดีเอ็นเอสเซคจะต้องสนับสนุนการทำงานที่เรียกว่า EDNS0 [10] ซึ่งคือกระบวนการในการเพิ่มระเบียนทรัพยากรที่เรียกว่า pseudo-RR ชนิด OPT (option) ไปกับข้อคำถามหรือข้อคำตอบ เพื่อให้คู่สนทนาทราบว่ามีบัฟเฟอร์ขนาดเท่าใดในการรับส่งข้อมูล และมีการตั้งค่าบิต DNSSEC OK (DO) ให้มีค่าเป็น 1 ในข้อคำถามของไคลเอนต์ที่ส่งไปยังเครื่องบริการหาชื่อโดเมน หรือเครื่องบริการหาชื่อโดเมนส่งไปยังเครื่องบริการชื่อโดเมนต่างๆ ทำให้เครื่องบริการหาชื่อโดเมนหรือเครื่องบริการชื่อโดเมนนั้นๆ ทราบว่าเป็นการร้องขอแบบดีเอ็นเอสเซค เมื่อเครื่องบริการหาชื่อโดเมน

หรือเครื่องบริการชื่อโดเมนนั้นๆ ก็จะต้องตอบด้วยข้อคำตอบแบบดีเอ็นเอสิเซคด้วย

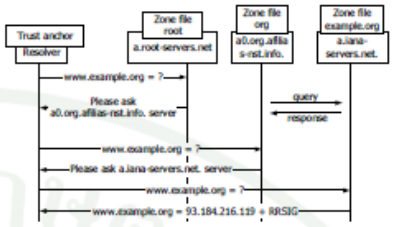
โดยปกติแล้วการส่งข้อคำถามและข้อคำตอบใช้โพรโทคอล UDP แต่จะสามารถใช้ TCP เมื่อโคลเอนต์หรือเครื่องบริการชื่อโดเมนได้รับข้อคำตอบที่ค่า Truncated (TC) เท่ากับ 1 ในส่วนหัว (header) หมายความว่าข้อคำตอบ ที่ได้รับโดยใช้ UDP ในการรับส่งข้อมูลไม่ครบถ้วน ทำให้โคลเอนต์หรือเครื่องบริการชื่อโดเมนนั้นจำเป็นต้องเปลี่ยนมาใช้ TCP ในการรับส่งข้อมูลแทน

รูปที่ 2 รูปแบบตัวบ่งชี้ (flag) ต่างๆในส่วนหัวของข้อความ

ในส่วนหัวของข้อความในดีเอ็นเอสิเซคมีการกำหนดบทบาทใหม่ให้บิต authenticated data (AD) และบิต checking disable (CD) ดังแสดงในรูปที่ 2 โดยหากบิต CD ถูกกำหนดให้มีค่าเป็น 1 ในข้อคำถามที่เครื่องบริการหาชื่อโดเมนส่งไปยังเครื่องบริการชื่อโดเมนต่างๆ เมื่อเครื่องบริการชื่อโดเมนได้รับและทำการส่งข้อคำตอบ โดยไม่ต้องทำกระบวนการตรวจสอบข้อมูล ส่วนบิต AD จะกำหนดให้มีค่าเป็น 1 ในข้อคำตอบเมื่อเครื่องบริการหาชื่อโดเมนทำกระบวนการตรวจสอบข้อมูล แล้วพบว่าข้อมูลไม่ถูกเปลี่ยนแปลงระหว่างการส่งและมาจากแหล่งกำเนิดจริง หรือกล่าวได้ว่าข้อมูลนั้นปลอดภัย

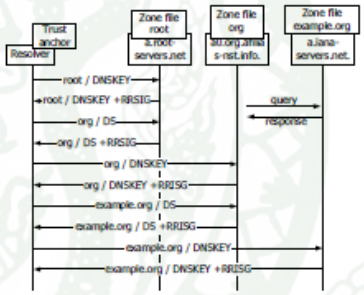
ในกระบวนการตรวจสอบข้อมูลที่โคลเอนต์ทำการสอบถามว่าปลอดภัยหรือไม่ ดำเนินการโดยเครื่องบริการหาชื่อโดเมนทำการหาคำตอบโดยหาข้อมูลที่ต้องใช้สำหรับการตรวจสอบข้อมูล เช่น กุญแจสาธารณะของชื่อโดเมนระดับต่างๆที่เก็บใน DNSKEY ไว้สำหรับตรวจสอบลายเซ็นดิจิตอลใน RRSIG และคำตอบที่โคลเอนต์ต้องการทราบ ในที่นี้จะขออธิบายจากตัวอย่างเช่น โคลเอนต์ทำการส่งข้อคำถามแบบดีเอ็นเอสิเซคสอบถามระเบียนทรัพยากรชนิด A หรือเลขที่อยู่ไอพีของ www.example.org ไปที่เครื่องบริการหาชื่อโดเมนที่มีการกุญแจสาธารณะชนิด KSK ของชื่อโดเมน root มาทำการตั้งค่าเป็น Trust Anchor ไว้

การดำเนินการสามารถพิจารณาเป็น 2 ส่วน โดยส่วนแรกเครื่องบริการหาชื่อโดเมนจะทำกระบวนการหาคำตอบ เหมือนในดีเอ็นเอสิโดยทั่วไปเพื่อให้ได้คำตอบว่าระเบียนทรัพยากรชนิด A ของ www.example.org คืออะไร แต่การส่งข้อคำถามจะเป็นแบบดีเอ็นเอสิเซค ซึ่งจะทำให้ได้รับข้อคำตอบกลับมาเป็นแบบดีเอ็นเอสิเซคด้วย หรือก็คือจะได้รับ RRSIG ของระเบียนทรัพยากรชนิด A ของ www.example.org กลับมาพร้อมกับระเบียนทรัพยากรชนิด A ของ www.example.org ดังแสดงในรูปที่ 3



รูปที่ 3 กระบวนการหาแอดที่อยู่ไอพีของ www.example.org

มีข้อสังเกตดังนี้ถ้าเครื่องบริการหาชื่อโดเมนทราบกุญแจสาธารณะชนิด ZSK ของ example.org และสามารถยืนยันได้ว่าถูกต้องเชื่อถือได้ ก็จะสามารถนำมาตรวจสอบลายเซ็นดิจิตอลในข้อคำตอบสำหรับสอบถามระเบียนทรัพยากรชนิด A ของ www.example.org ได้ หากถูกต้อง เครื่องบริการหาชื่อโดเมนจะทำการส่งข้อคำตอบแบบดีเอ็นเอสิเซคไปยังโคลเอนต์ พร้อมกับกำหนดบิต AD ให้มีค่าเป็น 1 เพื่อแจ้งโคลเอนต์ว่าคำตอบปลอดภัยเชื่อถือได้ และไม่ถูกเปลี่ยนแปลงระหว่างการรับส่งข้อมูล



รูปที่ 4 กระบวนการหาคำตอบเพื่อตรวจสอบกุญแจสาธารณะ

สำหรับส่วนที่สองจะเห็นได้ว่าเครื่องบริการหาชื่อโดเมน (resolver) ต้องยืนยันว่ากุญแจสาธารณะชนิด ZSK ของ example.org นั้นเชื่อถือได้และถูกต้อง โดยลำดับการตรวจสอบกุญแจสาธารณะเรียกว่าโซ่ของความเชื่อถือ (chain of trust) ซึ่งเริ่มต้นโดยเครื่องบริการหาชื่อโดเมนดำเนินกระบวนการหาคำตอบ ดังรูปที่ 4 โดยสอบถาม DNSKEY ของชื่อโดเมน root ได้จากเครื่องบริการชื่อโดเมน root ซึ่งจะได้ข้อคำตอบที่มี DNSKEY ทั้งหมดที่อยู่ในแฟ้มข้อมูลโซนของชื่อโดเมน root รวมทั้ง RRSIG ที่เกี่ยวข้องด้วย ดังนั้นจะเห็นได้ว่าเครื่องบริการหาชื่อโดเมนมีข้อมูลกุญแจสาธารณะชนิด KSK และ ZSK ของชื่อโดเมน root และถ้าหากว่า Trust Anchor กับกุญแจสาธารณะชนิด KSK ของชื่อโดเมน root เป็นกุญแจเดียวกัน เครื่องบริการหาชื่อโดเมนจะเชื่อถือกุญแจสาธารณะชนิด

ZSK ของชื่อโดเมน root จากการตรวจสอบลายเซ็นดิจิตอล โดยใช้กุญแจสาธารณะชนิด KSK ได้ด้วย

ลำดับถัดมาเครื่องบริการหาชื่อโดเมนทำการหาคำตอบโดยสอบถาม DS ของชื่อโดเมน org จากเครื่องบริการชื่อโดเมน root ซึ่งเครื่องบริการหาชื่อโดเมนจะได้ข้อคำตอบเป็น DS และ RRSIG ที่เกี่ยวข้อง โดยเครื่องบริการหาชื่อโดเมนจะใช้กุญแจสาธารณะชนิด ZSK ของชื่อโดเมน root ที่เชื่อถือได้ในกระบวนการค้นข้างต้นมาทดสอบเพื่อยืนยันความถูกต้องของ DS ของ org ซึ่ง DS ของ org จะถูกนำไปใช้ยืนยันกุญแจสาธารณะชนิด KSK ของ org

จากนั้นเครื่องบริการหาชื่อโดเมนจะทำการหาคำตอบ โดยสอบถาม DNSKEY ของ org และ DS ของ example.org ได้จากเครื่องบริการเจ้าของชื่อโดเมนของ org เมื่อได้ข้อคำตอบกลับมาแล้ว เครื่องบริการหาชื่อโดเมนทำการตรวจสอบกุญแจสาธารณะชนิด KSK ของ org ว่าเป็นกุญแจเดียวกันกับที่เก็บใน DS ของ org ถ้าเป็นกุญแจเดียวกัน เครื่องบริการหาชื่อโดเมนจะสามารถยืนยันกุญแจสาธารณะชนิด ZSK ของ org ได้และสามารถยืนยันกุญแจสาธารณะชนิด KSK ที่เก็บในรูปแบบ DS ของ example.org ได้

จนในที่สุดเครื่องบริการหาชื่อโดเมนจะทำการหาคำตอบโดยสอบถาม DNSKEY ของ example.org ได้จากเครื่องบริการเจ้าของชื่อโดเมนของ example.org และทำการตรวจสอบกุญแจสาธารณะชนิด KSK และ ZSK ของ example.org และนำกุญแจสาธารณะชนิด ZSK ไปตรวจสอบลายเซ็นดิจิตอลที่มากับข้อคำตอบสำหรับสอบถามระเบียนทรัพยากรชนิด A ของ www.example.org ได้ยืนยันว่าข้อมูลปลอดภัยหรือไม่

ในดีเอ็นเอสเซคมีการกำหนดให้เรียก เครื่องบริการชื่อโดเมนที่สนับสนุนดีเอ็นเอสเซคว่า security-aware name server ส่วน validating security-aware resolver เป็นการเรียกสำหรับเครื่องบริการหาชื่อโดเมนที่สนับสนุนดีเอ็นเอสเซครวมทั้งเปิดฟังก์ชันตรวจสอบข้อมูลด้วย และ non- validating security-aware resolver เป็นการเรียกสำหรับเครื่องบริการหาชื่อโดเมนที่สนับสนุนดีเอ็นเอสเซคแต่ไม่ได้เปิดฟังก์ชันตรวจสอบข้อมูลดังจะกล่าวอ้างถึงในส่วนต่อไป

3. การทดลองและผลการทดลอง

ในการทดสอบความพร้อมของไอเอสพีกับบริการดีเอ็นเอสเซค ผู้วิจัยเสนอรูปแบบการทดสอบทั้งหมด 3 แบบ คือแบบที่ 1 คือจำลองการทำงานของ local validating security-aware resolver แบบที่ 2 คือ ทดสอบการตรวจสอบข้อมูลเครื่องบริการชื่อโดเมนของไอเอสพี และแบบที่ 3 คือใช้งาน local validation security-aware resolver กับ non-validating security-aware name server ของไอเอสพี

ตารางที่ 1 บริการอินเทอร์เน็ตและแอทที่อยู่ไอพีของเครื่องบริการชื่อโดเมนของไอเอสพี

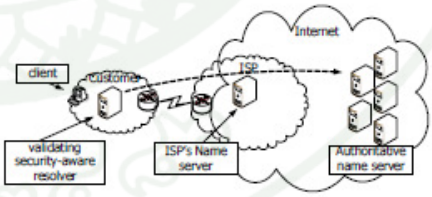
ISP	Service Type	IPv4
3BB	ADSL	110.164.252.222
CAT	Customer Room	61.19.245.245
JINET	ADSL	203.147.0.3
PROEN	VPN-PPTP	202.170.119.9
TOT	ADSL	203.113.127.199
TRUE	ADSL	203.144.207.29

ผู้วิจัยใช้โปรแกรม dig เพื่อส่งข้อคำถามไปยังเครื่องบริการหาชื่อโดเมน หรือเครื่องบริการชื่อโดเมนต่างๆ จากนั้นนำข้อคำตอบที่ได้รับมาสรุปผล และติดตั้งโปรแกรม bind เวอร์ชั่น 9.8.4 ซึ่งสนับสนุนการทำงานดีเอ็นเอสเซค สำหรับการทำเครื่องบริการหาชื่อโดเมนขึ้นเองเพื่อใช้ในการทดสอบ โดยเมื่อติดตั้ง bind จะมีคำสั่ง dig รวมมาพร้อมกันด้วย

ในการทดสอบแต่ละแบบผู้วิจัยทำการทดสอบกับเครือข่ายของไอเอสพีจำนวน 6 รายที่สามารถเข้าถึงและทำการทดสอบได้ โดยบริการอินเทอร์เน็ตของ 3BB JINET TOT และ TRUE เป็นแบบ ADSL บริการของ PROEN เป็นแบบ VPN และสุดท้ายผู้วิจัยได้รับความอนุเคราะห์เข้าทดสอบที่ CAT ซึ่งเป็นห้องสำหรับให้ลูกค้าใช้งานอินเทอร์เน็ต ซึ่งเครื่องบริการชื่อโดเมนของทางไอเอสพีอาจมีมากกว่า 1 ตัว แต่ที่ทำการทดสอบเป็นไปตามตารางที่ 1 โดยผู้เขียนทำการทดลองแต่ละแบบเป็นเวลาแบบละ 5 วัน และนำผลการที่ได้มาวิเคราะห์ดังที่อธิบายในส่วนต่อไป

3.1 จำลองการทำงานของ local validating security-aware resolver

การเข้าถึงบริการดีเอ็นเอสเซคของลูกค้าของไอเอสพี หากเครื่องบริการชื่อโดเมนของไอเอสพี ไม่สนับสนุนการทำงานในดีเอ็นเอสเซค ผู้ใช้งานสามารถเข้าถึงบริการดีเอ็นเอสเซคได้ด้วยการติดตั้ง validating security-aware resolver ภายในเครือข่ายของตนเอง ดังที่แสดงในรูปที่ 5



รูปที่ 5 ติดตั้ง local validating security-aware resolver

สมมติฐานผู้วิจัยไม่ทราบว่าเครือข่ายของไอเอสพี รองรับการให้บริการดีเอ็นเอสเซคหรือไม่ จึงทดลองโดยการส่งข้อคำถามแตกต่างกัน 5 แบบ ซึ่งถูกจำลองให้ค่าตัวบ่งชี้ในส่วนหัวของข้อความ เหมือนกับการที่เครื่องบริการหาชื่อโดเมนส่งข้อคำถามในการหาคำตอบ ไปยังเครื่องบริการชื่อโดเมนจำนวน 456 เครื่อง ซึ่งเป็นเครื่องบริการเข้าของชื่อโดเมนจำนวน 66 ชื่อโดเมน โดยชื่อโดเมนทั้ง 66 ชื่อโดเมน เป็นชื่อโดเมนของโดเมนระดับบน (Top-Level Domains) ในอินเทอร์เน็ตที่ผ่านการ zone signing แล้วเฉพาะโดเมนที่เป็นอักขระลาติน [11] พร้อมนำข้อคำตอบมาวิเคราะห์และสรุปผล สามารถดูตัวอย่างคำสั่งได้จาก ตารางที่ 2 โดยคำสั่ง 1 ถึง 5 ใช้สำหรับทดสอบในแบบที่ 1

ตารางที่ 2 แสดงค่าเฉลี่ยของจำนวนที่ไม่ได้รับข้อคำตอบ

	คำสั่ง dig	หมายเหตุ
1	dig +nodnssec +norec +retry=0 +ignore +qr +bufsize=4096 any ac. @b.nic.io.	UDP+noDNSEC (UN)
2	dig +nodnssec +norec +tcp +retry=0 +ignore +qr any ac. @b.nic.io.	TCP+noDNSSEC (TN)
3	dig +dnssec +cdflag +norec +retry=0 +ignore +qr +bufsize=4096 any ac. @b.nic.io.	UDP+DNSSEC (U)
4	dig +dnssec +cdflag +norec +retry=0 +ignore +qr +bufsize=4096 -t a ac. @b.nic.io.	UDP+DNSSEC +Tyep A (UA)
5	dig +dnssec +cdflag +norec +tcp +retry=0 +ignore +qr any ac. @b.nic.io.	TCP+DNSSEC (T)
6	dig @110.164.252.222 +dnssec +qr +retry=0 -t a www.name.ac.	
7	dig @127.0.0.1 +dnssec +qr +retry=0 -t a www.name.ac	เพิ่มการตั้งค่าส่งต่อ query

ผลของการส่งข้อคำถามจำลองแบบ validating security-aware resolver ในการหาคำตอบผ่านอินเทอร์เน็ตของผู้ให้บริการต่างๆ ได้ผลดังตารางที่ 3 ซึ่งแสดงค่าเฉลี่ยของจำนวนคำร้องที่ไม่ได้รับข้อคำตอบของแต่ละคำสั่งหน่วยเป็นร้อยละ จากผลทดลองเป็นเวลา 5 วัน โดยไม่รวมความผิดพลาดที่เกิดจากไม่สามารถหาแอทที่อยู่ไอพีของเครื่องบริการชื่อโดเมนตามชื่อโดเมนที่ระบุ ความผิดพลาดที่เกิดจากเครื่องบริการชื่อโดเมนปลายทางปฏิเสธจะดำเนินการตามข้อคำถาม (REFUSED) ความผิดพลาดที่เกิดจากเครื่องบริการชื่อโดเมนมีปัญหา ไม่สามารถดำเนินการตามข้อคำถามได้ (SERVFAIL) และความผิดพลาดที่ข้อคำตอบถูกแบ่งเนื่องจากขนาดใหญ่เกินกว่าจะส่งในครั้งเดียว (TC มีค่าเท่ากับ 1)

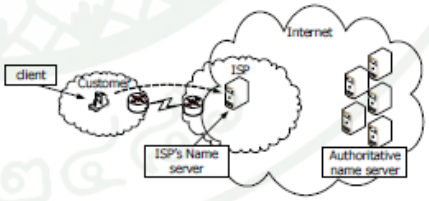
ตารางที่ 3 แสดงค่าเฉลี่ยของจำนวนที่ไม่ได้รับข้อคำตอบ

ISP	1 (UN)	2 (TN)	3 (U)	4 (UA)	5 (T)
3BB	7.37	3.11	7.76	3.2	3.33
CAT	3.42	0.88	3.64	0.96	1.05
JINET	12.41	0.96	12.94	1.8	0.92
PROEN	16.14	2.11	17.81	3.55	2.19
TOT	10.75	1.6	10.75	2.28	1.27
TRUE	7.41	2.5	7.85	2.72	2.37

ผู้วิจัยนำผลการทดสอบที่ได้จากคำสั่งที่ใช้โพรโทคอล UDP ในการส่งข้อคำถามแบบดีเอ็นเอส และดีเอ็นเอสเซคมาเปรียบเทียบกัน จะเห็นได้ว่าค่าเฉลี่ยของจำนวนที่ไม่ได้รับข้อคำตอบของการส่งข้อคำถาม มีค่าใกล้เคียงกันของแต่ละไอเอสพี และผลที่ได้จากคำสั่งที่ใช้โพรโทคอล TCP ในการส่งข้อคำถามแบบดีเอ็นเอส และดีเอ็นเอสเซคมาเปรียบเทียบกัน จะเห็นได้ว่าค่าเฉลี่ยของจำนวนที่ไม่ได้รับข้อคำตอบของการส่งข้อคำถาม มีค่าใกล้เคียงกันของแต่ละไอเอสพี รวมทั้งผลการทดสอบของคำสั่งที่ 4 ของทุกไอเอสพี ซึ่งข้อคำตอบจากคำสั่ง 4 นี้จะมีขนาดไม่เกิน 1000 ไบต์ และค่าเฉลี่ยของจำนวนที่ไม่ได้รับข้อคำตอบใกล้เคียงกับการใช้ TCP ในการทดสอบ แสดงว่าอุปกรณ์เครือข่ายไม่ได้ทำการทิ้ง (discard) แพ็กเกจที่เป็นดีเอ็นเอสเซค

3.2 ทดสอบการตรวจสอบข้อมูลเครื่องบริการชื่อโดเมนของไอเอสพี

ในแบบที่ 2 ผู้วิจัยต้องการทดสอบว่าเครื่องบริการชื่อโดเมนของไอเอสพี รองรับบริการดีเอ็นเอสเซค และสามารถตรวจสอบข้อมูลได้หรือไม่ การที่เครื่องบริการชื่อโดเมนของทางไอเอสพีเป็น validating security-aware name server จะทำให้ผู้ใช้บริการสามารถเข้าถึงดีเอ็นเอสเซคได้เลย โดยผู้ใช้บริการคือไม่ต้องดำเนินการอะไร ดังที่แสดงในรูปที่ 6

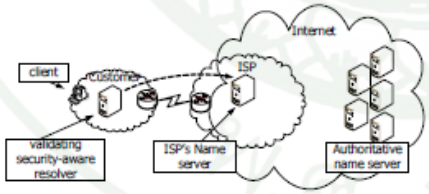


รูปที่ 6 ทดสอบการตรวจสอบข้อมูล name server ของไอเอสพี

ดังนั้นผู้วิจัยทำการทดสอบโดยส่งข้อคำถามสอบถามแอดเดรสไอพีของชื่อโดเมนที่ทำการสุ่มจากอินเทอร์เน็ตจำนวน 435 ชื่อโดเมน ภายใต้ชื่อโดเมนของโดเมนระดับบนจำนวน 66 ชื่อโดเมนที่ผ่านการ zone signing แล้ว ไปยังเครื่องบริการชื่อโดเมนของทางไอเอสพี ในการทดลองผู้วิจัยใช้คำสั่งดังตัวอย่างคำสั่งที่ 6 ในตารางที่ 2 เป็นการส่งข้อคำถาม โดยสอบถามแอดเดรสไอพีของชื่อโดเมน www.name.ac ไปยัง 110.164.252.222 ซึ่งเป็นเครื่องบริการชื่อโดเมนของทาง 3BB ค่าแอดเดรสไอพีของเครื่องบริการชื่อโดเมนจะเปลี่ยนไป ตามไอเอสพีที่ทำการทดสอบ โดยมีรายละเอียดดังตารางที่ 1 และทำการส่งข้อคำถามสอบถามแอดเดรสไอพีของชื่อโดเมนจำนวน 435 ชื่อโดเมนเดียวกันนี้ ไปยัง validating security-aware name server ที่ผู้วิจัยติดตั้งเองเพื่อใช้ผลในการเปรียบเทียบ

แม้ว่าเครื่องบริการชื่อโดเมนของไอเอสพีทั้ง 6 ผู้ให้บริการ ไม่สามารถรับรองความถูกต้องของชื่อโดเมนที่สอบถามได้เลย แต่เครื่องบริการชื่อโดเมนของ TRUE รองรับและเปิดการใช้งานดีเอ็นเอสเซค เนื่องจากพบ RRSIG ในข้อคำตอบที่ได้รับจากคำตอบของเครื่องบริการชื่อโดเมนของ TRUE ทำให้สามารถสรุปได้ว่าเครื่องบริการชื่อโดเมนของ TRUE สามารถให้บริการดีเอ็นเอสเซค แต่ไม่เปิดฟังก์ชันการตรวจสอบข้อมูล ส่วนเครื่องบริการชื่อโดเมนของไอเอสพีที่เหลืออาจจะไม่สนับสนุนการให้บริการดีเอ็นเอสเซค หรือสนับสนุนแต่ไม่เปิดการให้บริการดีเอ็นเอสเซค ทำให้ไม่ปรากฏ RRSIG ในข้อคำตอบ ซึ่งเครื่องบริการชื่อโดเมนของทาง 3BB ส่งข้อคำตอบกลับมาแจ้งข้อผิดพลาดถึงรูปแบบของข้อคำถามที่ส่งไปสอบถาม (FORMERR) ส่วนเครื่องบริการชื่อโดเมนของไอเอสพีที่เหลือส่งข้อคำตอบเหมือนกับเป็นข้อคำตอบที่เกิดจากข้อคำถามแบบดีเอ็นเอสธรรมดา

3.3 ใช้งาน local validation security-aware resolver กับ non-validating security-aware name server ของไอเอสพี



รูปที่ 7 ใช้งานกับ non-validating security-aware name server ของไอเอสพี

จากการทดลองแบบที่ 2 แสดงว่าเครื่องบริการชื่อโดเมนของผู้ให้บริการไอเอสพีทั้ง 6 ราย ไม่สามารถรับรองความถูกต้องของชื่อโดเมนที่สอบถามได้เลย ดังนั้นหากผู้ใช้บริการต้องการฟังก์ชันตรวจสอบข้อมูล ผู้ใช้งานควรจะติดตั้ง local validation security-aware resolver และทำการตั้งค่าส่งต่อ (Forward) ข้อคำถามไปยังเครื่องบริการชื่อโดเมนของทางไอเอสพี เพื่อที่จะสามารถตรวจสอบข้อมูลและลดภาระการทำงานของเครื่องบริการหาชื่อโดเมนที่ติดตั้งขึ้นดังที่แสดงในรูปที่ 7

ดังนั้นผู้วิจัยจึงทำการทดลองในแบบที่ 3 คือส่งข้อคำถามสอบถามไอพีแอดเดรสของชื่อโดเมนที่ทำการสุ่มจากอินเทอร์เน็ตจำนวน 435 ชื่อโดเมน ไปยัง validating security-aware resolver ที่ทำการติดตั้งเอง แต่มีการตั้งค่าให้ส่งต่อข้อคำถามไปยังเครื่องบริการชื่อโดเมนของไอเอสพี ที่มีรายละเอียดไอพีแอดเดรสตามตารางที่ 1 โดยใช้คำสั่งที่ 7 จากตารางที่ 2 และทำการทดลองเดียวกันนี้ แต่มีการตั้งค่าให้ส่งต่อข้อคำถามไปยังเครื่องบริการชื่อโดเมนของทาง google แทนที่แอดเดรสไอพีหมายเลข 8.8.8.8 ซึ่งสามารถให้บริการดีเอ็นเอสเซค และตรวจสอบข้อมูลได้ [12] เพื่อใช้ในการเปรียบเทียบความถูกต้องของผลลัพธ์ที่ได้ ในแต่ละวันที่ทำการทดสอบเครื่องบริการชื่อโดเมนของไอเอสพีต่างๆ โดยผู้วิจัยจะทำการทดสอบกับเครื่องบริการชื่อโดเมนของ google ไปในวันเดียวกันด้วย

ตารางที่ 6 จำนวนชื่อโดเมนที่ปลอดภัย

ISP	DAY-1	DAY-2	DAY-3	DAY-4	DAY-5
3BB	48	50	46	46	51
CAT	0	0	0	0	0
JINET	56	66	63	61	62
PROEN	67	67	65	66	67
TOT	0	0	0	0	0
TRUE	65	67	59	66	66

ผลการทดลองดังตารางที่ 6 ซึ่งแสดงจำนวนชื่อโดเมนที่ปลอดภัยจากการทดสอบกับเครื่องบริการชื่อโดเมนของไอเอสพี และได้ผลใกล้เคียงกับการทดสอบกับเครื่องบริการชื่อโดเมนของ google ด้วย จากตารางที่ 6 แสดงว่าผู้ใช้บริการสามารถเข้าถึงบริการดีเอ็นเอสเซคในแบบที่ 3 ผ่าน 3BB JINET PROEN และ TRUE ได้ ดังจะเห็นว่าโคลเอนต์ได้รับข้อคำตอบของชื่อโดเมนที่ปลอดภัยประมาณ 60 ชื่อโดเมน ในขณะที่จำนวนข้อคำตอบของชื่อโดเมนที่ปลอดภัยจากเครื่องบริการหาชื่อโดเมนที่ติดตั้งเอง ผ่านการทดสอบกับ CAT และ TOT มีค่าเป็น 0 ซึ่งสาเหตุอาจมาจากเครื่องบริการชื่อโดเมนของไอเอสพี ไม่สนับสนุนบริการดีเอ็นเอสเซคหรือโปรแกรมสนับสนุนแต่ไม่ได้เปิดการทำงานในส่วนของดีเอ็นเอสเซค จึงไม่มี RRSIG กลับมาพร้อมข้อคำตอบของเครื่องบริการหาชื่อโดเมนที่ติดตั้งเองสอบถามไป ทำให้เครื่องบริการหาชื่อโดเมนไม่สามารถตรวจสอบความถูกต้องของข้อมูลได้

สังเกตได้ว่าผลการทดลองตามตารางที่ 6 แสดงว่าเครื่องบริการชื่อโดเมนของ 3BB JINET และ PROEN สามารถให้บริการดีเอ็นเอสเซคได้ ซึ่งไม่ตรงกับการสรุปการใช้งานในการทดลองที่ 2 ที่สรุปว่าเครื่องบริการชื่อโดเมนของ TRUE รองรับการใช้งานดีเอ็นเอสเซคเท่านั้น แสดงว่าบางไอเอสพีน่าจะมีปรับปรุงเครื่องบริการชื่อโดเมนของตนเอง

ถึงแม้พบว่า 3BB, JINET และ PROEN ทำการปรับปรุงเครื่องบริการชื่อโดเมนของตนเองสนับสนุนและเปิดการทำงานของดีเอ็นเอสเซค แต่ไม่สามารถระบุได้ว่าเปิดการทำงานฟังก์ชันตรวจสอบข้อมูลด้วยหรือไม่ ทั้งนี้การทดลองเมื่อเดือนพฤศจิกายน ปี 2556

4.บทสรุปและข้อเสนอแนะ

ผู้วิจัยได้ทำการเลือกทดสอบกับไอเอสพีที่สามารถหาทดสอบได้เป็นที่รู้จักและมีเครือข่ายขนาดใหญ่ หากสังเกตรายชื่อไอเอสพีต่อไปนี้ CAT, ADC, BB connect, CSL, Jastel, SBN, Symphony, TCCT, TIG และ TOT เป็นไอเอสพีที่ให้บริการ International Internet Gateway และ Thailand Internet Exchange หรือเป็นไอเอสพี tier 2 ตามโครงสร้างของอินเทอร์เน็ต โดยไอเอสพีที่ผู้วิจัยทำการทดสอบ 5 ใน 6 ผู้ให้บริการมีความเกี่ยวข้องกับไอเอสพี tier 2 ตามที่กล่าวข้างต้น จากการขอความอนุเคราะห์ไปยังไอเอสพี 4 ไอเอสพีซึ่งได้รับความอนุเคราะห์เพียงรายเดียว ซึ่งไอเอสพี 3 ใน 4 ผู้ให้บริการนี้ความเกี่ยวข้องกับไอเอสพี tier 2 ตามที่กล่าวข้างต้นเช่นกัน

และการทดสอบกับเครื่องบริการชื่อโดเมนของทางไอเอสพีหากมีปริมาณมากเกิน อีกได้ว่าเป็นการโจมตีเครื่องบริการชื่อโดเมนของไอเอสพี ซึ่งทำให้อาจมีผลกระทบต่อผู้ใช้บริการหรือไอเอสพีเอง จึงดำเนินการทดสอบกับเครื่องบริการชื่อโดเมนของไอเอสพีเพียงเครื่องเดียว

ผลการทดลองของการสำรวจถึงความพร้อมการให้บริการดีเอ็นเอสเซคของไอเอสพีในประเทศไทย ตั้งแต่เดือนมีนาคม ปี 2556 จนถึงเดือนพฤศจิกายน ปี 2556 ผู้วิจัยพบว่าผู้ให้บริการไอเอสพีจำนวน 4 ใน 6 รายที่เครื่องบริการชื่อโดเมน สนับสนุนการทำงานของดีเอ็นเอสเซคส่วนอีก 2 รายนั้น เครื่องบริการชื่อโดเมนอาจไม่สนับสนุนการทำงานของดีเอ็นเอสเซค หรืออาจสนับสนุนการทำงานของดีเอ็นเอสเซคแต่ไม่เปิดการทำงาน ดีเอ็นเอสเซค ดังนั้นหากผู้ใช้บริการต้องการเข้าถึงบริการดีเอ็นเอสเซคก็สามารถติดตั้ง validation security-aware resolver ขึ้นในภายในเครือข่ายของตนเองได้ หรือสามารถใช้งานเครื่องบริการชื่อโดเมนขององค์กรที่รองรับการทำงานของดีเอ็นเอสเซคเช่น google ในการเข้าถึงบริการดีเอ็นเอสเซคได้

ผู้วิจัยเห็นว่าควรมีการสนับสนุนให้ทางไอเอสพีทำการปรับปรุงเครื่องบริการชื่อโดเมน ที่ให้บริการหาคำตอบแก่ลูกค้าให้สนับสนุนการทำงานของดีเอ็นเอสเซค และเปิดฟังก์ชันตรวจสอบข้อมูลด้วย

5. กิตติกรรมประกาศ

ขอขอบคุณบัณฑิตวิทยาลัยและภาควิชาวิทยาการคอมพิวเตอร์ที่ได้สนับสนุนด้านอุปกรณ์ ด้านเงินทุนนำเสนองาน และสถานที่ตลอดระยะเวลาในการทำวิทยานิพนธ์

ขอขอบคุณผู้จัดการฝ่ายสื่อสารข้อมูล นาย วสัน เสนาะกรรณ์ และวิศวกร นางสาว สุนีรัตน์ ไจหาร สำหรับความกรุณาให้เข้าทดสอบอินเทอร์เน็ตของ CAT และ ขอขอบคุณผู้ที่ให้ความอนุเคราะห์ในการใช้งานอินเทอร์เน็ตของ 3BB JINET TOT และ TRUE

เอกสารอ้างอิง

[1] Karen Evans, "M-08-23", MEMORANDUM FOR CHIEF INFORMATION OFFICERS, August 22, 2008.

[2] P. Mockapetris, "DOMAIN NAMES - CONCEPTS AND FACILITIES", RFC 1034, November 1987.

[3] P. Mockapetris, "DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION", RFC 1035, November 1987.

[4] Matthew Olney, Patrick Mullen and Kevin Miklavcic, "Dan Kaminsky's 2008 DNS Vulnerability", SOURCEFIRE, INC., July 25, 2008.

[5] Ray Bellis and Lisa Phifer, "DNSSEC Impact on Broadband Routers and Firewalls", nominet, September, 2008.

[6] R. Arends, R. Austein, M. Larson, D. Massey and S. Rose, "DNS Security Introduction and Requirement", RFC 4033, March 2005.

[7] R. Arends, R. Austein, M. Larson, D. Massey, and S. Rose, "Resource Records for the DNS Security Extensions", RFC 4034, March 2005.

[8] R. Arends, R. Austein, M. Larson, D. Massey, and S. Rose, "Protocol Modifications for the DNS Security Extensions", RFC 4035, March 2005.

[9] Ron Aitchison, "Pro DNS and BIND 10", Apress, February 23, 2011.

[10] J. Damas, M. Graff and P. Vixie, "Extension Mechanisms for DNS (EDNS(0))", RFC 6891, April 2013.

[11] "TLD DNSSEC Report", ICANN Research, avaliable: http://stats.research.icann.org/dns/tld_report.

[12] "Introduction to Google Public DNS", google, avaliable: https://developers.google.com/speed/public-dns/docs/intro.

ประวัติการศึกษาและการทำงาน

ชื่อ นายสัญชัย นิจวิภากุล

เกิดวันที่ 24 พฤษภาคม 2526

สถานที่เกิด อำเภอป้อมปราบฯ จังหวัดกรุงเทพฯ

ประวัติการศึกษา วศ.บ. (คอมพิวเตอร์) มหาวิทยาลัยเกษตรศาสตร์ วิทยาศรีราชา

ตำแหน่งปัจจุบัน -

สถานที่ทำงานปัจจุบัน -

ผลงานดีเด่นและ/หรือรางวัลทางวิชาการ -

ทุนการศึกษาที่ได้รับ -