การเข้ารหัสผ่านระบบเครือข่ายเพื่อเพิ่มความมั่นคงปลอดภัยของการส่งข้อมูลยืนยันตัวตน
Using Data Encryption Over Network for Secure Identity Authentication

อมฤทธิ์ จันทนลาช
คณะบริหารศาสตร์ มหาวิทยาลัยเฉลิมกาญจนา
99 หมู่ 6 ต.โพธิ์ อ.เมือง จ.ศรีสะเกษ 33000
E-mail: ritt555@yahoo.com

บทคัดย่อ

ในปัจจุบันการใช้งานอินเทอร์เน็ตมีบทบาทที่สำคัญในการเข้าสู่ประชาคมอาเซียน (AEC) ซึ่งช่วยอำนวยความสะดวกให้แก่ผู้ใช้ไม่ว่าจะเป็นการทำงานด้านการส่งข้อมูลข่าวสารระหว่างที่หนึ่งไปยังอีกที่หนึ่ง ในรูปแบบสื่อ ทั้งภาพเสียง ตัวอักษรและมัลติมีเดีย ได้อย่างรวดเร็วฉับไวทันเวลาที่ต้องการ หากแต่ในปัจจุบันมีการใช้คอมพิวเตอร์ที่ไม่เหมาะสม เช่น นำไปใช้แพร่ภาพ ลามกอนาจาร นำภาพไปตัดต่อเข้าสู่ระบบคอมพิวเตอร์ทำให้ผู้อื่นเสียหาย ปลอมแปลงข้อมูลคอมพิวเตอร์ของผู้อื่นโดยไม่ได้รับอนุญาต ทำให้เกิดความเสียหายแก่ผู้อื่น หรือเกิดความเสียหายแก่ประเทศชาติ จึงได้มีการนำเสนอวิธีการแก้ปัญหานี้มาก่อน โดยการยืนยันตัวตนภายใน อย่างไรก็ตามการแก้ปัญหาการยืนยันตัวตนภายในยังไม่สามารถเพิ่มความมั่นคงปลอดภัยได้เท่าที่ควร เพราะ Log File จัดเก็บที่เครื่อง Authentication เองภายในองค์กร บทความนี้ผู้วิจัยนำเสนอเทคนิคการเพิ่มความมั่นคงปลอดภัย โดยการส่งข้อมูลดิบไปไว้อีกเครื่องด้วยการเข้ารหัสแลกเปลี่ยนคีย์ระหว่างสองเครื่อง เพื่อช่วยให้ Log File มีความมั่นคงปลอดภัยเพิ่มขึ้น
คำสำคัญ: การเข้ารหัส, การยืนยันตัวตน, ความปลอดภัย

ABSTRACT

Nowadays, the Internet has an important role in the ASEAN community (AEC) and provides convenient for users. Whether it's working on the transmission quickly of information between one to another form of media, including text, photographs, audio and multimedia. But today the improper use of the Internet such as the widespread use of pornography editing the pictures into the Internet. Cause any harm forged by others without permission. Make harm to the others or the country. We have proposed a solution by Log File. However, the authors find this cannot secure as they should be. Because the Log File storage device authentication within the organization. In this article the researcher prefer a technique to enhance the security by sending raw data to another machine and then encryption key exchange between two computers for Log File with in extend security.
Keywords: Data Encryption, Identify Authentication, Security

1. บทนำ

Free Radius เป็นโปรแกรมโอเพ่นซอร์สสำหรับระบบลีนุกซ์ ซอฟต์แวร์นี้สามารถทำงานร่วมกับ EAP-MD5 และ EAP-TLS ซึ่งเป็นระบบสำหรับตรวจสอบผู้ใช้โดยเฉพาะที่ใช้กันอยู่ทั่วไป ที่ใช้ในการจัดการ Account และใช้ในการตรวจสอบสิทธิ์ตามมาตรฐาน IEEE 802.1X ตามแนวคิด AAA (Accounting, Authentication, Authorize) RADIUS Server คือ Server ที่ทำหน้าที่ในการตรวจสอบสิทธิ์ของการขอเข้าใช้งานของ User ที่ส่งมาจาก NAS กับฐานข้อมูลที่อยู่ที่ตัว RADIUS Server เอง หรือจะเป็นฐานข้อมูลจากภายนอกอื่นๆ เช่น MS-SQL Server, Oracle, Database, MySQL, LDAP Database เป็นต้น

หลังจากได้ข้อมูลต่างๆจนครบแล้ว และทำการตรวจสอบสิทธิ์เรียบร้อยแล้ว RADIUS Server ก็จะส่งผลกลับมายัง NAS เป็น (Access-Accept) ถ้าข้อมูลนั้นถูกต้องและได้รับอนุญาต หรือ (Access-Reject) ถ้าข้อมูลนั้นไม่ได้รับอนุญาต ต่อไป NAS ก็จะทำการเชื่อมต่อหรือยกเลิกการเชื่อมต่อตามที่ RADIUS Server ได้ส่งมา โดยทั่วไปแล้ว NAS จะมีการส่งข้อมูลต่างๆ เช่น วันที่ เวลาที่ Username นั้นใช้งาน เพื่อที่จะให้ RADIUS Server ทำการจัดเก็บในฐานข้อมูลด้วย

ในปัจจุบันซอฟต์แวร์ดักจับข้อมูล มีการพัฒนาเพิ่มขึ้นเป็นจำนวนมากเช่น Wire Shark เป็นต้น ซึ่งการยืนยันตัวตนด้วย Radius กับ ChilliSpot เพียงอย่างเดียวก็อาจมีความเสี่ยงได้

ดังนั้นงานวิจัยฉบับนี้จึงได้นำเสนอวิธีการใหม่โดยการเขียนภาษา Shell Script ส่ง Log File ไปยังเครื่อง Centralized Log เครื่องฝั่ง Authentication Gateway และ Centralized Log ต้องมีการแลกเปลี่ยนคีย์ เพื่อเพิ่มความมั่นคงปลอดภัยเพิ่มขึ้น

โครงสร้างของงานวิจัยฉบับนี้มีดังนี้ หัวข้อที่ 2 กล่าวถึง ภาพรวมของ Log File และซอฟต์แวร์ที่ใช้จัดการ Log File แบบรวมศูนย์ หัวข้อที่ 3 กล่าวถึงเนื้อหาและวิธีการของงานวิจัยที่ผู้วิจัยต้องการที่จะนำเสนอ หัวข้อที่ 4 กล่าวถึงการวิเคราะห์ทางด้านความมั่นคงปลอดภัยและการวิเคราะห์ประสิทธิภาพของงานวิจัยที่ผู้วิจัยต้องการที่จะนำเสนอ และหัวข้อที่ 5 กล่าวถึงข้อสรุปของงานวิจัยฉบับนี้

2. ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

เนื่องจากการใช้งานเครือข่ายอินเทอร์เน็ตมีเพิ่มมากขึ้นเรื่อย ๆ ในชีวิตประจำวัน ดังนั้นการยืนยันตัวตนจึงเป็นสิ่งสำคัญเพื่อให้การใช้งานอินเทอร์เน็ตสามารถตรวจสอบ บุคคลในองค์กรว่าใคร เข้ามาทำอะไร เวลาไหนบ้าง เพื่อเป็นการป้องกันการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ปี 2550 [1]

2.1 Free Radius

Free Radius ซอฟต์แวร์นี้สามารถทำงานร่วมกับ EAP-MD5 และ EAP-TLS ซึ่งเป็นระบบสำหรับตรวจสอบผู้ใช้ ChilliSpot เป็น ซอฟต์แวร์โอเพ่นซอร์ส ที่นำมาใช้ในการควบคุมการใช้งานเครือข่าย ไร้สาย เรียกว่า Wireless Controller นิยมนำมาใช้เป็น Gateway ติดตั้งไว้บน Linux Box เพื่อคอยดักแพ็กเก็จ TCP Port 80 และส่งหน้าจอ ล็อกอิน ไปยังผู้ใช้งาน โดย ChilliSpot จะทำงานร่วมกับโปรแกรม Radius ซึ่งทำหน้าที่บริหารจัดการฐานข้อมูลของ User ทั้งนี้โปรแกรม ChilliSpot กับ Free Radius อาจจะติดตั้งอยู่บนเครื่องเดียวกันหรือต่างเครื่องกันก็ได้ [2]

2.2 Log File

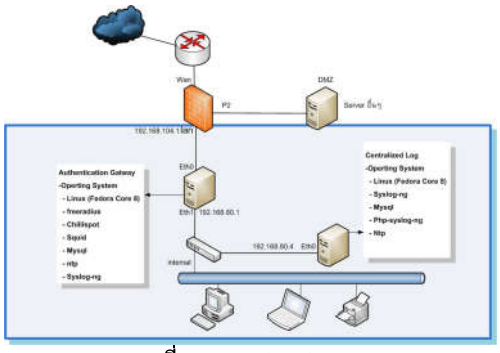
Log File เป็นไฟล์ที่ใช้สำหรับบันทึกการกระทำต่างๆ บนระบบคอมพิวเตอร์ ซึ่งมีการเก็บข้อมูลจำนวนมาก Log File ส่วนใหญ่จะเก็บข้อมูลในรูปแบบของข้อความ (Text File) เป็นการบันทึกข้อมูลทีละบรรทัด โดยโปรแกรมระบบหรือโปรแกรมประยุกต์ต่างๆ ในระบบคอมพิวเตอร์ เช่น แต่ละครั้งที่ผู้ใช้ทำการล็อกอินเข้าใช้งานอินเทอร์เน็ต ก็จะมี Log File ที่ชื่อว่า Squid Log โดยจะบันทึกข้อมูลทั้งหมดไม่ว่าการกระทำนั้นสำเร็จหรือไม่สำเร็จ Log File ที่เกิดขึ้นจากระบบปฏิบัติการ รวมทั้งโปรแกรมประยุกต์ จะแสดงข้อความต่างๆ ที่บ่งบอกถึงการทำงานและปัญหาต่างๆ ที่เกิดขึ้นในระหว่างการทำงานเพื่ออำนวยความสะดวกในการตรวจสอบ [3]

3. รายละเอียดการพัฒนา

3.1 ภาพรวมของระบบ

การทำงานของระบบที่นำเสนอ ได้แบ่งการทำงานออกเป็น 3 ส่วน ส่วนแรกเป็นเครื่องลูกข่ายทำหน้าที่เป็นเครื่อง ผู้ใช้ระบบภายในสำหรับออกอินเทอร์เน็ต ส่วนที่สองเป็นเครื่อง Authentication Gateway เป็นเครื่องสำหรับใช้ในการจัดเก็บข้อมูล

การจราจรบนเครือข่ายว่ามีใคร เข้ามาทำอะไร เวลาไหน เมื่อไหร่ ไอพีอะไร และหยุดการใช้งานเวลาไหน ส่วนที่สามเป็นเครื่อง Centralized Log ซึ่งทำหน้าที่คอยรับข้อมูลดาต้าดิบ จากเครื่อง Authentication Gateway ซึ่งเป็นข้อมูลที่ไม่มีการประมวลผล หรือข้อมูล Log File แล้วจัดเก็บลงในฐานข้อมูลเพื่อส่งไปยังเครื่อง Centralized Log ดังภาพที่ 1

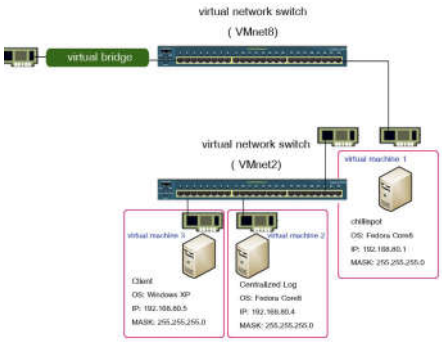


ภาพที่ 1 Centralized Log

3.2 การออกแบบและพัฒนาระบบ

ในส่วนของการออกแบบและพัฒนาระบบผู้วิจัยได้พัฒนาระบบขึ้นโดยใช้ภาษา PHP, โปรแกรม Radius และ Chillispot [4] เพื่อใช้ในการพิสูจน์ตัวตนในการเข้าสู่ระบบอินเทอร์เน็ต และได้ใช้ Syslog-ng โดยวิธีการติดตั้งของ Peter Harrison [5] ซึ่งทั้งหมดติดตั้งไว้ที่ตำแหน่ง Internal ซึ่งทำหน้าที่เป็น Authentication Gateway เพื่อใช้ในการจัดเก็บข้อมูลการจราจรบนเครือข่าย หลักการการออกแบบระบบมีขั้นตอนและสิ่งที่จำเป็นในการทำระบบมีดังนี้

3.2.1 ทำการจำลองระบบ Network โดยใช้โปรแกรม VMware Server ดังภาพที่ 2



ภาพที่ 2 Virtual Network Diagram

เป็นการวางเครื่อง Authentication Gateway ติดตั้งขวางก่อนจะออกสู่อินเทอร์เน็ต ซึ่งการติดตั้งแบบนี้จะเป็นการบังคับ ให้ผู้ใช้งานในระบบที่ต้องการใช้งานอินเทอร์เน็ตทุกคน ต้องทำการยืนยันตัวตนก่อนใช้อินเทอร์เน็ต โดยการติดตั้ง Authentication Gateway จะใช้ ChilliSpot เป็น ซอฟต์แวร์โอเพ่นซอร์ส ที่นำมาใช้ในการควบคุมการใช้งานเครือข่าย ซึ่งใช้เป็น Gateway ติดตั้งไว้บน Linux เพื่อคอยดักแพ็กเก็จ TCP Port 80 และส่งหน้าจอ ล็อกอิน ไปยังผู้ใช้งาน โดย ChilliSpot จะทำงาน ร่วมกับโปรแกรม Free Radius ซึ่งทำหน้าที่บริหารจัดการฐานข้อมูลของ User ทั้งนี้โปรแกรม ChilliSpot กับ Free Radius จะติดตั้งอยู่เครื่องเดียวกัน

เมื่อผู้ใช้บริการต้องการที่จะให้งานเครือข่ายอินเทอร์เน็ต จะบังคับให้ป้อนชื่อผู้ใช้และรหัสผ่านเพื่อเป็นการยืนยันตัวตน โดยระบบบัญชีรายชื่อทั้งหมดจะถูกเก็บไว้ที่ Radius และขณะเดียวกันตัว Radius จะตรวจสอบสิทธิ์และบันทึกข้อมูลการเข้าใช้งานระบบทั้งหมดไว้ เช่น ล็อกออนเวลาเท่าไรและได้หมายเลขไอพีอะไร รวมถึงเวลาที่เข้ามาใช้งาน โดยจะมี Software ที่ติดตั้งบน Authentication Gateway กับ Centralized Log ได้ใช้ซอฟต์แวร์ตาม Network Diagram [6]

3.2.2 ทำการออกแบบจำลองระบบโดยใช้เครื่องมือ Authentication Gateway ในโปรแกรม VMware Server ซึ่งโปรแกรม VMware Server เป็นโปรแกรมที่ใช้สร้างคอมพิวเตอร์เสมือน (Virtual Machine) ขึ้นบนระบบปฏิบัติการเดิมที่มีอยู่ โดยคอมพิวเตอร์เสมือนที่สร้างขึ้นมานั้นจะมีสภาพแวดล้อมเหมือนกับคอมพิวเตอร์จริง เครื่องหนึ่ง ซึ่งประกอบด้วยพื้นที่ดิสก์ที่ใช้ร่วมกับพื้นที่ดิสก์ของเครื่องนั้นๆ การ์ดแสดงผล การ์ดเน็ตเวิร์ก พื้นที่ของหน่วยความจำ ซึ่งจะแบ่งการทำงานมาจากหน่วยความจำหลักของเครื่องนั้นๆ ซึ่งผู้วิจัยจะทำการทดลองด้วยโปรแกรมนี้

4. การทดสอบการใช้งาน

ผู้วิจัยได้ทำการทดสอบโดยใช้โปรแกรม VMware Server ซึ่งจาก Diagram จะมีอยู่ด้วยกันทั้งหมด 3 เครื่อง

4.1 สภาพแวดล้อมที่ใช้ในการทดสอบ

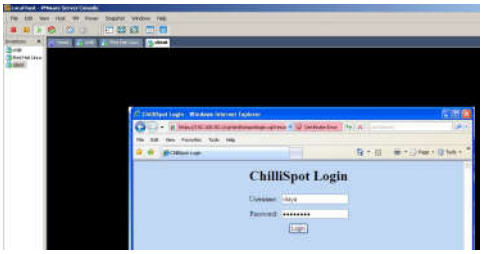
การทดสอบระบบในครั้งนี้จะใช้เครือข่ายที่จำลองขึ้น ดังภาพที่ 2 แสดงระบบเครือข่ายการเชื่อมต่อ

โดย VMnet 8 เป็น Virtual Bridged เพื่อออกสู่อินเทอร์เน็ตติดต่อกับเครื่องที่ลง VMware ส่วนเครื่อง Virtual Machine 1 เป็นเครื่อง Authentication Gateway ส่วนเครื่อง Virtual Machine 2 เป็นเครื่อง Centralized Log และเครื่อง Virtual Machine 3 เป็นเครื่อง Client โดยเครื่อง Virtual Machine 1, 2, 3 ต่อเข้ากับ VMnet 2

4.2 ผลการทดลองและการวิเคราะห์ผล

4.2.1 ผลการทดลองการใช้งาน

เมื่อ User ล็อกอิน เปิด Web Browser เพื่อเข้าเว็บเป็นการเริ่มต้น Http Request ไปยัง อินเทอร์เน็ต ChilliSpot จะตรวจพบ Http Request แล้ว Redirect ไปยังหน้า Web Portal เพื่อให้ป้อน Username และ Password ก่อน เมื่อผู้ใช้ป้อน Username และ Password แล้ว ChilliSpot จะนำ Username และ Password นั้นไปตรวจสอบที่ Radius Server ถ้าถูกต้องก็จะ Redirect หน้าเว็บไปยังเว็บในอินเทอร์เน็ตที่ผู้ใช้เข้าในตอนแรก ประวัติการใช้อินเทอร์เน็ตของผู้ใช้จะถูกบันทึกโดย Firewall Log ดังภาพที่ 3



ภาพที่ 3 การป้อน Username / Password

เมื่อทำการ Login เสร็จก็จะสามารถใช้อินเทอร์เน็ตได้ แสดง Log File ที่ถูกจัดเก็บไว้ที่เครื่อง Authentication Gateway ที่ตำแหน่ง /var/log/radius/radacct/192.168.80.1/

4.2.2 ผลการทดลอง Log File เมื่อ User เข้าใช้งานอินเทอร์เน็ต

ChilliSpot Log

Mar 17 00:53:47 Chilli Thu Mar 17 00:53:47 2016 : Auth : Login OK: [amarit] (from client Chilli port 0 cli 00-0C-29-37-63-C7)

4.2.3 ผลการทดลอง Log File ของ User ซึ่งจะแสดง วัน เดือน ปี เวลาที่เริ่มใช้อินเทอร์เน็ต และเวลาที่สิ้นสุดไอพีที่เข้าใช้หมายเลข Mac Address Protocol Wirless-802.11

Radius Log

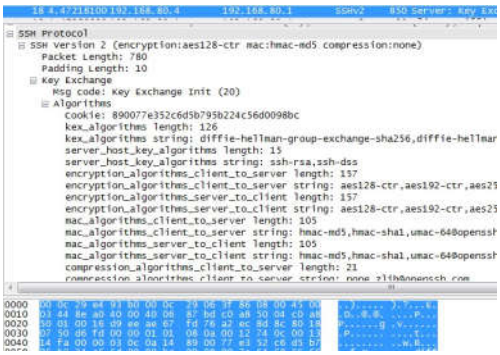
Thu Mar 17 00:53:47 2016
Acct-Status-Type = Start
User-Name = “amarit”
Calling-Station-Id=“00-0C-29-37-63-C7”
Called-Station-Id = “00-0C-29-E6-58-41”
NAS-Port-Type = Wirless-802.11
NAS-Port-Id = “00000000”
NAS-IP-Address = 192.168.182.6
NAS-Identifier = “nas01”
Framed-IP-Address = 192.168.182.6
Acct-Session-Id = “4d80f8da00000000”
Client-IP-Address = 192.168.80.1
Acct-Unique-Session-Id= “3a995b610fc712a4”
Timestamp = 1300298027

4.2.4 ผลการทดลอง Log File ของ User วันเวลาไอพีที่ล็อกอินเข้ามาใช้เว็บอะไรบ้าง

Squid Log

17032016:00:53:14: 5 192.168.182.6 TCP- IMS_HIT/304 325 GET http://192.168.80.1/welcome.html - NONE/- text/html
17032016:00:53:14: 5 192.168.182.6 TCP- IMS_HIT/304 325 GET http://192.168.80.1/chillispot.phg - NONE/- text/html

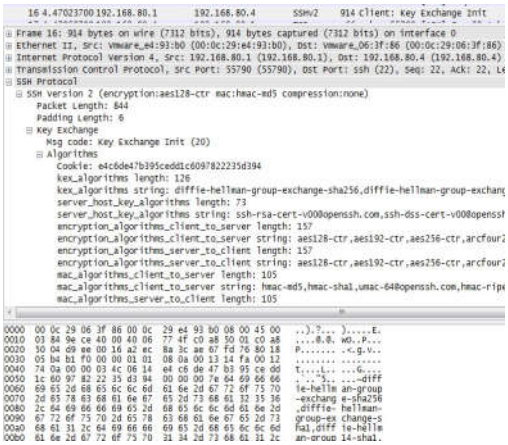
4.2.5 ผลการทดลองการส่งข้อมูลการยืนยันตัวตนโดยการเข้ารหัสผ่านระบบเครือข่าย โดยการเขียน Shell Script ส่งไปที่เครื่อง Centralized Log โดยการแลกเปลี่ยนคีย์ระหว่างเครื่อง Authentication Gateway กับเครื่อง Centralized Log ดังภาพที่ 4



ภาพที่ 4 การเข้ารหัสคีย์แลกเปลี่ยนคีย์ฝั่งเครื่อง Authentication Gateway

การทำงานของ Shell Script เมื่อ Crontab ที่ตั้งไว้ใน Linux ทำงาน ก็จะส่ง Log File จากเครื่อง Authentication Gateway ไปที่เครื่อง Centralized Log ซึ่งได้เข้ารหัส Ssh, Dsa เพื่อเพิ่มความมั่นคงปลอดภัยขึ้น

4.2.6 ผลการทดลองการส่งข้อมูลการยืนยันตัวตนโดยการเข้ารหัสผ่านระบบเครือข่าย โดยการเขียน Shell Script ส่งไปที่เครื่อง Centralized Log โดยการแลกเปลี่ยนคีย์ระหว่างเครื่อง Centralized Log กับเครื่อง Authentication Gateway ดังภาพที่ 5



ภาพที่ 5 การเข้ารหัสแลกเปลี่ยนคีย์ฝั่งเครื่อง Centralized Log

4.2.7 ผลการทดลองแสดงการล็อกอินของผู้ดูแลระบบเองว่าล็อกอินเข้ามาวันไหนเวลาไหนโปรโตคอลที่ใช้

<u>Ssh Log</u>

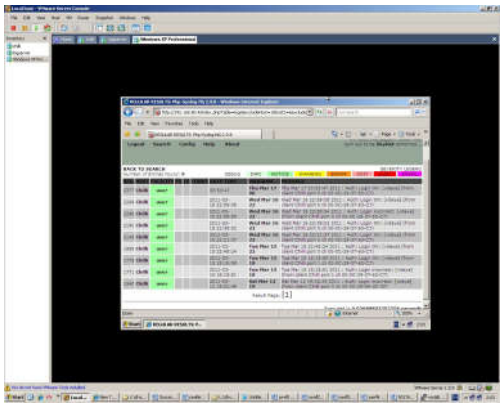
Mar 16 21:44:49 Logserver login: pam_unix (Login:session) session opened for user root by LOGIN (uid=0)

Mar 16 21:44:49 Logserver login: ROOT LOGIN ON tty1

Mar 16 21:45:28 Logserver sshd[2423] : Accepted Password for root from 192.168.252.1 port 1437 ssh2

Mar 16 21:45:28 logserver sshd[2423] subsystem request for sftp

4.2.8 ผลการทดลองการใช้เครื่องมือเพื่อสะดวกในการแสดง Log ที่เครื่อง Centralized Log ผ่านหน้าเว็บ ดังภาพที่ 6



ภาพที่ 6 โปรแกรม php-syslog-ng เพื่อตรวจสอบข้อมูลการเข้าใช้บริการอินเทอร์เน็ต

ใช้โปรแกรม php-syslog-ng แสดงข้อมูลของผู้ใช้งานการจราจรทางคอมพิวเตอร์ โดยโปรแกรมสามารถตรวจสอบข้อมูลการเข้าใช้บริการอินเทอร์เน็ตได้ค่อนข้างสมบูรณ์

5. บทสรุป

การเข้าสู่ประชาคมอาเซียน (AEC) ในปี 2558 อินเทอร์เน็ตมีความจำเป็นในการแลกเปลี่ยนข้อมูลทาง

การค้าของตลาดอาเซียน ทำให้ปริมาณการใช้งานอินเทอร์เน็ตมีสูงมากขึ้น ดังนั้นการเพิ่มความมั่นคงปลอดภัยของการส่งข้อมูลยืนยันตัวตนจึงเป็นสิ่งสำคัญ ซึ่งในงานวิจัยนี้มีการเข้ารหัสของข้อมูลโดยการแลกเปลี่ยนคีย์เพื่อเพิ่มความมั่นคงปลอดภัยระหว่างเครื่องลูกข่ายและเครื่องแม่ข่าย โดยสามารถรับข้อมูลจากเครื่องลูกข่ายและส่งข้อมูลไปยังเครื่องแม่ข่ายได้อย่างถูกต้อง อีกทั้งยังสามารถอำนวยความสะดวกกับผู้ดูแลระบบสามารถทำงานได้มีประสิทธิภาพมากขึ้น

งานวิจัยนี้สามารถนำไปพัฒนาต่อโดยการดัก Traffic Firewall ขาเข้า-ขาออกและเก็บ Log File ก่อนจะออกสู่อินเทอร์เน็ตและจำกัด Bandwidth ของเครื่อง User

6. กิตติกรรมประกาศ

งานวิจัยเรื่อง “การเข้ารหัสผ่านระบบเครือข่ายเพื่อเพิ่มความมั่นคงปลอดภัยของการส่งข้อมูลยืนยันตัวตน” โดยได้ความช่วยและเหลือสนับสนุนจากบุคคลหลายฝ่าย โดยเฉพาะอย่างยิ่ง ดร.สุชีราภรณ์ ธุวานนท์ ที่กรุณาให้คำปรึกษา ให้คำแนะนำ ตรวจสอบ และแก้ไขข้อบกพร่องต่าง ๆ ด้วยความเอาใจใส่อย่างดียิ่ง ทำให้การวิจัยสำเร็จสมบูรณ์ได้ ผู้วิจัยขอขอบพระคุณทุกท่านเป็นอย่างสูงไว้ ณ ที่นี้

7. เอกสารอ้างอิง

[1] กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร. (2551). **คู่มือการปฏิบัติและแนวทางการป้องกันเพื่อหลีกเลี่ยงการกระทำความผิดเกี่ยวกับคอมพิวเตอร์**. กรุงเทพฯ : สำนักกำกับการใช้เทคโนโลยีสารสนเทศ.

[2] อาณัติ รัตนถิรกุล. (2552). **ติดตั้งและบริหาร Linux Web Hosting ใช้งานในองค์กร**. กรุงเทพฯ : บริษัท ซีเอ็ดยูเคชั่น จำกัด (มหาชน).

[3] ภูวดล ด่านระหาญ. (2550). **Syslog-ng (Syslog new generation).** สืบค้นจาก http://www.msit.mut.ac.th/newweb/phpfile/show.php?Qid=776.

[4] วิบูลย์ วราสิทธิชัย. (2550). **การติดตั้ง chillispot server สำหรับ WIFI แบบ web login**. สืบค้นจาก http://netserv.cc.psu.ac.th/documents/doc_download/158-chillispotp-6.

[5] Peter Harrison. (2013). **How to config syslog-ng.** Retrieve from http://www.linuxhomenetworking.com/wiki/index.php/Quick_HOWTO_:_Ch05_:_Troubleshooting_Linux_with_syslog.

[6] ศุภโชค สุขเกษม. (2548). **การวิเคราะห์ข้อมูลกิจกรรมของระบบเพื่อตรวจจับการบุกรุก**. วิทยานิพนธ์ วิทยาศาสตรมหาบัณฑิต สาขาวิทยาการคอมพิวเตอร์มหาวิทยาลัย สงขลานครินทร์.