# IMPLEMENTATION AND EVALUATION OF TLS ENABLED WEB SERVER WITHOUT TRUSTING THE OPERATING SYSTEM

**CHIRAPHAT CHAIPHET**

**A THESIS SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF MASTER OF SCIENCE (COMPUTER SCIENCE) FACULTY OF GRADUATE STUDIES MAHIDOL UNIVERSITY 2017**

IMPLEMENTATION AND EVALUATION OF TLS ENABLED WEB SERVER WITHOUT TRUSTING THE OPERATING SYSTEM

CHIRAPHAT CHAIPHET 5737762 ITCS/M

M.Sc.(COMPUTER SCIENCE)

THESIS ADVISORY COMMITTEE: SUDSANGUAN NGAMSURIYAROJ, Ph.D., VASAKA VISOOTTIVISETH, Ph.D., THITINAN TANTIDHAM, Ph.D.

ABSTRACT

Web servers use SSL/TLS protocol to establish secure communication between clients and servers. The mechanism of SSL/TLS relies on a key pair to validate the server and to protect the confidentiality of the data. However, many websites are running on third-party servers or on cloud environments where website owners have no control over the physical servers or the software including the operating systems but still need to trust and store the private key on the servers. While it is common to store the encrypted key on the disk, the web server still needs a decrypted key inside the memory during the operation. Thus, an adversary could obtain the private key residing on the web server's memory.

We proposed a secure enclave for a web server running the high privilege code that handles the secret keys inside an encrypted memory area by utilizing Intel Software Guard Extension (SGX). This secure enclave protects the key from an adversary by preventing external access to the secret keys memory area. The evaluation results showed 19% to 38% reduced throughput depending on which cipher suite is used and how a session key is handled.

KEY WORDS : SGX / ENCLAVE / TLS / KEY PROTECTION / WEB SERVER

41 pages

การพัฒนาและประเมินเครื่องแม่ข่ายเว็บที่ใช้ TLS โดยไม่เชื่อถือระบบปฏิบัติการ
IMPLEMENTATION AND EVALUATION OF TLS ENABLED WEB SERVER WITHOUT TRUSTING THE OPERATING SYSTEM

จีรภัทร ใจเพ็ชร 5737762 ITCS/M

วท.ม. (วิทยาการคอมพิวเตอร์)

คณะกรรมการที่ปรึกษาวิทยานิพนธ์: สุดสงวน งามสุริยโรจน์, Ph.D., วัสกา วิสุทธิวิเศษ, Ph.D., ฐิตินันท์ ตันติธรรม, Ph.D.

บทคัดย่อ

เครื่องแม่ข่ายของเว็บไซต์ในปัจจุบันใช้ SSL/TLS เป็นมาตรฐานในการเชื่อมต่ออย่างปลอดภัยระหว่างเครื่องแม่ข่ายและเครื่องลูกข่าย ซึ่งกระบวนการของ SSL/TLS นั้นอาศัยคู่ของกุญแจ (Public Key / Private Key) เพื่อพิสูจน์ตัวตนของเครื่องแม่ข่ายและเพื่อปกป้องความลับของข้อมูล อย่างไรก็ตามเว็บไซต์ในปัจจุบันมักใช้บริการเครื่องแม่ข่ายจากผู้ให้บริการอื่น เจ้าของเว็บไซต์ไม่มีสิทธิ์ในการควบคุมหรือเข้าถึงตัวเครื่องได้ แต่เจ้าของเว็บไซต์ก็ยังจำต้องไว้วางใจและฝากกุญแจส่วนตัว (Private Key) ไว้กับเครื่องแม่ข่ายของผู้ให้บริการ ถึงแม้ว่าจะสามารถเก็บกุญแจที่ถูกเข้ารหัสไว้บนดิสก์ได้ แต่เครื่องแม่ข่ายของเว็บไซต์ยังคงต้องการกุญแจที่ถอดรหัสแล้วในหน่วยความจำระหว่างให้บริการ ดังนั้นผู้ประสงค์ร้ายจะมีโอกาสเข้าถึงกุญแจส่วนตัวที่อยู่ในหน่วยความจำของเครื่องแม่ข่ายของเว็บไซต์ได้หากระบบมีช่วงโหว่ด้านความปลอดภัย

วิทยานิพนธ์เล่มนี้นำเสนอการใช้เทคโนโลยี Intel Software Guard Extension (SGX) เพื่อแบ่งพื้นที่หน่วยความจำบางส่วนเป็นพื้นที่เข้ารหัส ซึ่งจะมีเพียงเฉพาะชุดโปรแกรมที่ได้รับอนุญาตที่สามารถเข้าถึงข้อมูลได้โดยไม่ต้องการใช้เครื่องมือพิเศษนอกจากหน่วยประมวลผลของเครื่องแม่ข่ายเอง กระบวนการเข้ารหัสหน่วยความจำนี้สามารถป้องกันไม่ให้ผู้ประสงค์ร้ายนำเอากุญแจออกจากเครื่องแม่ข่ายได้ จากผลการประเมินประสิทธิภาพ พบว่าวิธีการนี้ทำให้ประสิทธิภาพของเครื่องแม่ข่ายลดลงร้อยละ 19 ถึงร้อยละ 38 ขึ้นอยู่กับว่าใช้กรรมวิธีเข้ารหัสและลักษณะการจัดการกุญแจอย่างไร เพื่อแลกกับความปลอดภัยของกุญแจเข้ารหัสที่สูงขึ้น



41 หน้า