ELLIPTIC CURVE CRYPTOGRAPHY FOR EAVESDROPPING PROTECTION

THIDARAT HATTHABUNJONG

A RESEARCH PROJECT SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF MASTER OF SCIENCE (COMPUTER SCIENCE) FACULTY OF GRADUATE STUDIES MAHIDOL UNIVERSITY 2011

ELLIPTIC CURVE CRYPTOGRAPHY FOR EAVESDROPPING PROTECTION

THIDARAT HATTHABUNJONG 4937282 ITCS/M

M.Sc. (COMPUTER SCIENCE)

RESERCH PROJECT ADVISORY COMMITTEE: SUPACHAI TANGWONGSAN, Ph.D., VASAKA VISOOTTIVISETH, Ph.D., SONGSRI TANGSRIPAIROJ, Ph.D.

ABSTRACT

The purpose of this study was to develop a security model to prevent eavesdropping on VoIP networks that is efficient and effective. Our approach was to correct the weak points of previous research work which exchanged private keys between conversation partners and encrypted data with partial encryption patterns.

The scheme of correction was divided into two parts as follows:

First, the key exchange between conversation partners with the symmetric-key model using the Elliptic Curve Diffie-Hellman key exchange replaced the simple Diffie-Hellman key exchange.

Second, the process of data encryption which makes use of Elliptic Curve Cryptography (ECC) with partial encryption m:n model also enhanced the efficiency of eavesdropping protection.

A system prototype was built according to these specifications and a series of experiments were performed. The results showed that the new model performed better in terms of eavesdropping protection and the efficiency of implementation.

KEY WORDS: SECURITY MODEL/ VOICE EAVESDROPPING PROTECTION/ VOIP NETWORK

80 pages

การเข้ารหัสด้วย ELLIPTIC CURVE CRYPTOGRAPHY เพื่อป้องกันการดักฟัง
ELLIPTIC CURVE CRYPTOGRAPHY FOR EAVESDROPPING PROTECTION

ธิดารัตน์ หัตถบรรจง 4937282 ITCS/M

วท.ม. (วิทยาการคอมพิวเตอร์)

คณะกรรมการที่ปรึกษาสารนิพนธ์: ศุภชัย ตั้งวงศ์ศานต์, Ph.D., วัสกา วิสุทธิวิเศษ, Ph.D.,
ทรงศรี ตั้งศรีไพโรจน์, Ph.D.,

บทคัดย่อ

งานการศึกษานี้เป็นโครงงานเพื่อพัฒนาโมเดลความปลอดภัยของการป้องกันการดักฟังบนเครือข่าย VoIP ให้มีประสิทธิภาพมากยิ่งขึ้น โดยทำการแก้ไขข้อบกพร่องของงานวิจัยที่ได้เคยทำมาแล้ว ซึ่งมีการแลกเปลี่ยน key ที่ใช้ในการเข้ารหัสเป็นส่วนตัวระหว่างคู่สนทนา แล้วทำการเข้ารหัสข้อมูลแบบ partial encryption

ในการแก้ไขข้อบกพร่องแบ่งออกเป็นสองส่วนใหญ่ๆ คือ ส่วนแรก เป็นเรื่องเกี่ยวกับการแลกเปลี่ยน key ระหว่างคู่สนทนา เพื่อนำ key ที่แลกเปลี่ยนนั้นไปใช้ในการเข้ารหัสแบบ symmetric-key ซึ่งจะใช้ Elliptic curve Diffie-Hellman key exchange มาใช้แทนการแลกเปลี่ยน key ด้วย Diffie-Hellman key exchange ส่วนที่สองเป็นกระบวนการในการเข้ารหัสของข้อมูล ซึ่งเป็นการเข้ารหัส ด้วย Elliptic Curve Cryptography(ECC) ในรูปแบบ Partial encryption m:n เพื่อเพิ่มประสิทธิภาพของการป้องกันการดักฟังให้ดียิ่งขึ้น

จากนั้นได้ทำการสร้างระบบต้นแบบ ทำการทดลอง และทดสอบระบบต้นแบบ ผลที่ได้จากการทดลองแสดงให้เห็นว่าระบบต้นแบบที่ได้ดำเนินการมานั้นมีประสิทธิภาพในการป้องกันการดักฟังได้ดีขึ้น

80 หน้า