A SECURITY MODEL OF VOICE EAVESDROPPING PROTECTION OVER DIGITAL NETWORKS

SATHAPORN KASSUVAN

**A THESIS SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR
THE DEGREE OF MASTER OF SCIENCE
(COMPUTER SCIENCE)
FACULTY OF GRADUATE STUDIES
MAHIDOL UNIVERSITY
2006**

ISBN 974-04-7458-6
COPYRIGHT OF MAHIDOL UNIVERSITY

โมเดลความปลอดภัยของการป้องกันการดักฟังบนเครือข่ายดิจิตอล (A SECURITY MODEL OF VOICE EAVESDROPPING PROTECTION OVER DIGITAL NETWORKS)

สถาพร กาศสุวรรณ 4437184 SCCS/M

วท.ม. (วิทยาการคอมพิวเตอร์)

คณะกรรมการควบคุมวิทยานิพนธ์ : ศุภชัย ตั้งวงศ์ศานต์, Ph.D., ชมทิพ พรพนมชัย, D.Tech.Sc., สุพัฒนา เอื้อทวีเกียรติ, Ph.D.

บทคัดย่อ

การศึกษาครั้งนี้เป็นการวิจัยเพื่อพัฒนา โมเดลความปลอดภัยของการป้องกันการดักฟังบนเครือข่ายดิจิตอล โดยการสร้างวิธีการเข้ารหัสและการแลกเปลี่ยนคีย์ (key) เป็นการส่วนตัวระหว่างคู่สนทนา หรือเรียกว่าระบบการแปลงรูปแบบข้อมูลเสียง (Voice Data Transformation System) ซึ่งจะทำให้เกิดความเป็นส่วนตัวในการสนทนาอย่างแท้จริง

การทำงานของระบบดังกล่าวประกอบด้วยสองขั้นตอนหลัก ดังนี้ ขั้นตอนแรกคือการแลกเปลี่ยนคีย์เป็นการส่วนตัว เพื่อที่จะได้นำคีย์นั้นไปใช้ในการเข้ารหัสในระหว่างการสนทนาและขั้นตอนที่สองคือการเข้ารหัสข้อมูลเสียงระหว่างการสนทนาที่ถูกบีบอัดข้อมูลด้วยมาตรฐาน G.729, G.723.1, G.726 หรือ AMR โดยผู้ใช้งานสามารถที่จะเลือกทางเลือก (option) ในการเข้ารหัสได้ด้วยตัวเองว่าจะใช้การเข้ารหัสข้อมูลทั้งหมดหรือการเข้ารหัสข้อมูลแต่เพียงบางส่วน สำหรับในกรณีการเข้ารหัสเพียงบางส่วนหรือการเข้ารหัสแบบ 1-to-M block นั้นเป็นการเข้ารหัสที่บล็อก (block) แรกของข้อมูลและเว้นไว้ไม่เข้ารหัสเป็นจำนวน M-1 บล็อกถัดไปสลับอย่างนี้ไปจนจบการสนทนา ทั้งนี้ M คือจำนวนบล็อกในแต่ละกลุ่ม (group) ของข้อมูล (packets) ที่นำมาเข้ารหัส ซึ่งมีค่าที่เป็นไปได้เท่ากับ 1, 2, 3, 4 หรือ 5 โดยวิธีการดังกล่าวจะยากสำหรับผู้ดักฟังที่พยายามจะเปิดเผยข้อมูลเสียงของผู้พูดหรือคีย์ลับ (cryptanalysis)

จากนั้นเราได้ทำการทดลองปฏิบัติและทดสอบต้นแบบของระบบ (system prototype) บนพื้นฐานของการออกแบบเชิงแนวคิด (conceptual design) ซึ่งผลของการทดลองปฏิบัตินั้นพบว่าระบบสามารถทำงานได้อย่างถูกต้องตามที่ได้ออกแบบไว้ และแม้ว่าในกรณีของการเข้ารหัสที่ 20 เปอร์เซ็นต์ของข้อมูลทั้งหมด ระบบยังคงมีความปลอดภัยของข้อมูลเสียงอยู่ นอกจากนี้แล้วการเข้ารหัสเพียงบางส่วนยังใช้เวลาในการเข้ารหัสน้อยกว่าการเข้ารหัสข้อมูลทั้งหมดซึ่งถือได้ว่าผลการทดลองที่ได้เป็นที่น่าพอใจ ทั้งนี้ระบบที่ได้นำเสนอนี้เหมาะสมที่จะนำไปใช้เพื่อป้องกันการดักฟังเสียงบนเครือข่ายดิจิตอลได้อย่างมีประสิทธิภาพโดยไม่ต้องมีการปรับเปลี่ยนระบบเครือข่ายเดิม และยังเป็นไปได้ที่จะนำระบบนี้ไปประยุกต์ใช้จริงกับเครือข่ายโทรศัพท์เคลื่อนที่หรือเครือข่ายอินเตอร์เน็ตเพื่อให้เกิดโอกาสทางธุรกิจอีกด้วย

65 หน้า. ISBN 974-04-7458-6

A SECURITY MODEL OF VOICE EAVESDROPPING PROTECTION OVER DIGITAL NETWORKS.

SATHAPORN KASSUVAN 4437184 SCCS/M

M.Sc.(COMPUTER SCIENCE)

THESIS ADVISOR : SUPACHAI TANGWONGSAN, Ph.D., CHOMTIP PORNPANOMCHAI, D.Tech.Sc., SUPATANA AUETHAVEKIAT, Ph.D.

ABSTRACT

The purpose of this research is to develop a security model for voice eavesdropping protection over digital networks. The proposed model provides an encryption scheme and a personal secret key exchange between communicating parties, a so-called voice data transformation system, resulting in a real-privacy conversation.

Operation of this system comprises two main processes. The first one is the personal secret key exchange to allow use of a key in the encryption process during the conversation. The other one is the encryption of G.729, G.723.1, G.726 or AMR encoded voice data in the conversation. In doing so, users can choose the option of encryption by themselves, that is, either all frame or partial frame encryption. In partial frame encryption or 1-to-M block encryption, the first block of each packet is encrypted while the remaining M-1 blocks are left unchanged, alternating like this until the end of the conversation. In this process, M is the number of blocks in each group of packets to be encrypted, possibly 1, 2, 3, 4, or 5, giving those who wish to tap the encrypted voice or apply a method of cryptanalysis to the conversation, a difficult task.

The system prototype was implemented and tested based on its conceptual design. The results of the implementation indicate that the system can perform its function accurately as designed. Even in the case of 20% of the whole data being encrypted, the system could still provide speech security. Moreover, partial frame encryption would take less time than all frame encryption, which the experimental result yields quite satisfactorily. In this regard, the proposed system is suitable for effective use in voice eavesdropping protection over digital networks, without the requirement to change presently existing network systems. Also, it would be possible to extend this system to mobile phone networks or Internet networks for the sake of business purposes.

KEY WORDS: SECURITY MODEL / VOICE EAVESDROPPING PROTECTION / DIGITAL NETWORKS

65 P. ISBN 974-04-7458-6