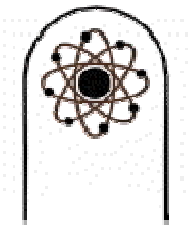


HelwanUniversity
Faculty of Engineering
Department of Electronics, Communications and Computer Engineering

Security in the Wireless Application Protocol

A Thesis Presented

By

Tamer Mohamed Barakat

B.sc., Communications and Electronics Engineering,

HelwanUniversity

Submitted to the Department of Electronics, Communications and Computer Engineering
HelwanUniversity

In partial fulfillment of the requirements for the degree of

MASTER OF SCIENCE
In
Communications Engineering

Under Supervision of

Dr. Ibrahim I. Ibrahim
Professor
Faculty of Engineering
HelwanUniversity

Dr. Ihab A. Ali
Associate Professor
Faculty of Engineering
HelwanUniversity

Dr. Nabil A. Abdelaziz
Assistant Professor
Faculty of Engineering
Helwan University

2004

ABSTRACT

This thesis addresses one of the important topics in mobile networks, which is Wireless Application Protocol (WAP).

The security of the WAP is based on public-key cryptosystem such as RSA cryptosystem to achieve the authentication between server and client. This cryptosystem suffers from several strong attacks as well as slow decryption process. So, a new public-key cryptosystem named PKQ cryptosystem presented which solve the slowness of the decryption process but still suffers from the same attacks that defeat the RSA cryptosystem such as low exponent attack and common modulus attack.

In this thesis, a modification of the PKQ cryptosystem is proposed which make the PKQ cryptosystem stand against those attacks. It also shows that the decryption time of the modified PKQ cryptosystem is faster than that before.

Then, design of the WAP based on the modified PKQ cryptosystem will be presented to get the optimum authentication between server and client.

Finally, it will be shown that the modified PKQ cryptosystem may fit to work in order to optimize the security of WAP.

KEYWORDS: Public-key; RSA cryptosystem; PKQ cryptosystem; Modified PKQ cryptosystem; Low exponent attack; Common modulus attack; WAP; WTLS protocol; Handshake protocol.

كلية الهندسة

قسم هندسة الالكترونيات و الاتصالات و الحاسبات

السرية في بروتوكول التطبيقات اللاسلكية

إعداد

م/ تامر محمد عبد الرحمن بركات

رسالة مقدمة إلى كلية الهندسة – جامعة حلوان

كجزء من متطلبات الحصول على درجة
الماجستير في هندسة الاتصالات

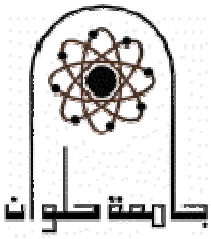
تحت إشراف

أ.د. إبراهيم إسماعيل إبراهيم **أ.م.د. إيهاب عبد الوهاب على**

أستاذ مساعد بالقسم **أستاذ بالقسم**

د. نبيل عبد ربه عبد العزيز

مدرس بالقسم



كلية الهندسة-جامعة حلوان

إسم الباحث: تامر محمد عبد الرحمن بركات

عنوان الرسالة: السرية فى بروتوكول التطبيقات اللاسلكية

مستخلص الرسالة

هذه الرسالة تتناول واحد من أهم الموضوعات فى مجال شبكات الموبايل ألا وهي السرية فى برتوكول التطبيقات اللاسلكية. هذه السرية تعتمد على نظام تشفير ذو المفتاح العام يسمى RSA لكي تتم عملية الثقة بين الخادم والمستخدم، هذا النظام له عيوب عديدة من أهمها أن سرعة عملية فك الشفرة تستغرق وقت طويل بالإضافة الى أنه يعاني من عمليات هجوم كثيرة من الدخلاء.

تقدم هذه الرسالة تحليل عميق لنظام تشفير آخر يسمى PKQ والذي يحل واحد من مشاكل الـ RSA وهي سرعة عملية فك الشفرة ولكن مازال يعاني من نفس عمليات الهجوم من الدخلاء ثم يتم تعديل النظام التشفير PKQ ومنها يتم تحسين السرية له بحيث يقاوم عمليات الهجوم التي كانت تطبق عليه. يتم عمل تصميم لبروتوكول التطبيقات اللاسلكية والذي يعتمد علي نظام التشفير PKQ المعدل ثم يتم تقييمه الأداء لبروتوكول التطبيقات اللاسلكية باستخدام نظام التشفير PKQ المعدل ومقارنته بنظام التشفير RSA.

الرسالة منظمة كالتالي:

الفصل الأول:

مقدمة الرسالة وتتضمن الدوافع والأهداف وكذا الخطوط العريضة للرسالة.

الفصل الثاني:

مقدمة عامة عن أنظمة التشفير ذات المفتاح العام وأهما نظام التشفير RSA وأيضاً PKQ وأهم مشاكلهم. دراسة البنية الاساسية لبرتوكول التطبيقات اللاسلكية وأهم المشاكل التي يتعرض لها.

الفصل الثالث:

يعرض تحليل لنظام التشفير PKQ ومدى تأثير عمليات الهجوم عليه، ويتم وضع المتطلبات اللازمة لتحسين هذا النظام قبل استخدامه في بروتوكول التطبيقات اللاسلكية.

الفصل الرابع:

يعرض تعديل فى نظام التشفير PKQ لتحسين السرية له. ثم يعرض دراسة تأثير عمليات الهجوم على النظام المعدل وعرض الأثبات على أن عمليات الهجوم أصبحت لا تطبق على نظام معين.

الفصل الخامس:

يقدم تصميم لبروتوكول التطبيقات اللاسلكية والتي تعتمد عملية الثقة بين الخادم والسمتخدم على نظام التشفير PKQ المعدل. يتم تقييم الآداء بنظام التشفير PKQ المعدل ومقارنته بنظام التشفير RSA واستنتاج النتائج التي تثبت أن نظام التشفير PKQ المعدل أصبح أسرع وأقوى من نظام التشفير RSA.

الفصل السادس:

يعرض الخلاصة والملاحظات المستنتجة من الرسالة وأيضا البحث المستقبلي.

ملخص الرسالة

بروتوكول التطبيقات اللاسلكية مطروح بواسطة الجمعية العامة للتطبيقات اللاسلكية لوضع مواصفات خاصة للتطبيقات التي تعمل من خلال شبكات الاتصالات اللاسلكية. السرية فى بروتوكول التطبيقات اللاسلكية يعتمد على نظام التشفير ذات المفتاح العام مثل RSA للحصول على أعلى ثقة بين الخادم والسمتخدم.

نظام التشفير RSA يعاني من مشاكل عديدة أهما أنه يعاني من العديد من عمليات الهجوم من الدخلاء ، من أهم هذه العمليات: هجوم بسبب اختيار قيمة صغيرة لمفتاح التشفير العام وآخر بسبب استخدام معامل مشترك بين المستخدمين والأخير بسبب اختيار قيمة صغيرة لمفتاح فك الشفرة.

المشلكة الثانية وهي أن عملية فك الشفرة تأخذ وقت طويل إذا تم اختيار قيمة كبيرة لمفتاح فك الشفرة لتفادي الهجوم الناتج عن ذلك. وبالتالي فإن التكلفة تزيد. تم التغلب على أحد المشاكل بواسطة نظام تشفير جديد ذات المفتاح العام يسمى PKQ وفيه عملية فك الشفرة أسرع بثلاث مرات من نظام التشفير RSA.

في هذه الرسالة تم التحليل التشفيري لنظام التشفير PKQ وتبين أنه مازال يعاني من عمليات الهجوم التي يعانيها نظام التشفير RSA ماعدا عملية الهجوم الناتجة عن اختيار قيمة صغيرة لمفتاح فك الشفرة.

من خلال هذا التحليل لوحظ أن بعض عمليات الهجوم ناتجة بسبب أن مفتاح التشفير دائما عدد إحادي وهذا يسهل على المهاجم إجراء بعض العمليات الرياضية وكسر هذا النظام.

لذلك نستنتج أن نظام التشفير PKQ يمكن استخدامه في بروتوكول التطبيقات اللاسلكية للحصول على أعلى ثقة بين الخادم والمستخدم بشرط إيجاد حل لجعله يقاوم الهجمات السابقة.

لذا تقدم هذه الرسالة تعديل لنظام التشفير PKQ حيث يجعل مفتاح التشفير عبارة عن عدد مركب.

قبل أي تحليل تشفيري للنظام المقترح لابد من اثبات أنه يمكن استرجاع الرسالة الأصلية بعد تشفيرها بالنظام المعدل، لذا يتم إثبات صحة النظام المعدل باسترجاع الرسالة الاصلية بعد تشفيرها بهذا النظام.

من خلال التحليل التشفيري لنظام التشفير PKQ المعدل تبين أنه قد قاوم عمليات الهجوم التي كان يعانى منها قبل عملية التعديل.

تم قياس الآداء للنظام المعدل ومقارنته بنظام التشفير PKQ قبل التعديل وقد تبين أن عملية فك الشفرة فى نظام التشفير PKQ المعدل أصبح أسرع بحوالي ٢.٣ مرة من النظام الغير معدل.

بعد التأكد من صلاحية نظام التشفير PKQ المعدل لابد من استخدامه فى تصميم برتوكول التطبيقات اللاسلكية للوصول الى سرية عالية. من خلال هذا التصميم تبين أن شهادة المستخدم التي تتضمن بعض المعلومات الهامة له تنتقل الى الخادم من غير أي تشفير، لذلك أي مهاجم يمكن معرفة هذه المعلومات لذا يتم تشفير شهادة المستخدم بواسطة نظام التشفير PKQ المعدل.

تم عمل التقييم الكامل لأداء نظام التشفير PKQ المعدل ومقارنته بنظام التشفير RSA المستخدم حالياً في بروتوكول التطبيقات اللاسلكية. عملية التقييم تعتمد على عاملين مهمين: الأول هو الوقت الذي يستغرقه الخادم فى إنهاء عمليته وكذا الوقت الذي يستغرقه المستخدم أثناء عملية المصافحة، العامل الثاني هو الوقت اللازم لاستجابة بروتوكول التطبيقات اللاسلكية والذي يعتمد اعتماد كلي على الوقت المستغرق من قبل الخادم والمستخدم.

لكل عامل من هذان العاملان، تم تقييم الآداء لنظام التشفير PKQ ومقارنته بنظام التشفير RSA ثم عرض هذه النتائج لقيم مختلفة للعامل (n). من خلال النتائج التي تم التوصل اليها وجد أن الآداء لنظام التشفير PKQ المعدل أحسن بكثير من نظام التشفير RSA لكل قيم المعامل. لذلك نوصي في هذه الرسالة باستخدام نظام التشفير PKQ المعدل فى تصميم برتوكول التطبيقات اللاسلكية للوصول لأعلى ثقة بين الخادم والمستخدم.

أخيراً، يتضح أن نظام التشفير PKQ المعدل والمقترح فى هذه الرسالة هو نظام تشفير قوي في مقاومة العديد من عمليات الهجوم ويمكن استخدامه بنطاق واسع في التطبيقات التي تحتاج أنظمة تشفير ذات مفتاح عام للوصول الى أعلى سرية.