التحليل الأمني الرياضي لبروتوكول الإشارة

اسم الطالبة: نوال زايد عمر المزيني

المشرف : د. افتخار أحمد خان

المستخلص

يعد بروتوكول الإشارة أحد بروتوكولات التشفير الأكثر شيوعًا والتي تم تصميمها بواسطة Open Whisper System. .يقوم هذا البروتوكول بتشفير محادثات المراسلات الفورية (IM)و يعتبر بروتوكول الأمان الأساسي للعديد من التطبيقات مثل WhatsApp و Google Allo و Facebook Messenger. لذلك اصبح بروتوكول الاشارة هدفا للكثير من المخترقين حيث ان وجود أي ثغرة في تركيب هذا البروتوكول تشكل خطرا على تطبيقات المراسلات الفورية التي تستخدم هذا البروتوكول. لذلك ، التحليل الأمني الرياضي لبروتوكول الإشارة ضروريًا لضمان قدرته في مجال الأمان. في هذه الرسالة ، تم إجراء تحليل أمني رياضي لبروتوكول الأمن باستخدام Scyther ، والتي تعد اداة لتحليل البروتوكولات التشفيرية والتأكد من تحقق المتطلبات الأمنية لكل بروتوكول. وقد تم استخدامه في تحليل البروتوكولات المختلفة. تم تحليل بروتوكول الإشارة في هذا البحث إلى ثلاث مراحل ؛ مرحلة التسجيل ، مرحلة إرسال واستقبال الرسالة ، و مرحلة الرد على الرسالة. تمت معالجة النتائج التي تم الحصول عليها ومقارنتها مع أساليب التحقق من المتطلبات الامنية للبروتوكولات التشفيرية.

FORMAL SECURITY ANALYSIS OF THE SIGNAL PROTOCOL

Nawal Zaied Al-Muzaini

Supervised By
Dr. Iftikhar Ahmad Khan

ABSTRACT

Signal Protocol is one of the most popular cryptographic protocols which is designed by Open Whisper System. It delivers end-to-end encryption for instant messaging (IM) conversations. Further, it is considered the core security protocol for numerous applications such as WhatsApp, Google Allo and Facebook Messenger. The increase use of the Signal Protocol in different IM application has made it imperative which is a big attraction for the intruders. Therefore, a formal analysis of the Signal Protocol is deemed necessary to ensure its capability in security domain. In this thesis, a formal analysis of the security protocol is conducted using Scyther, which is a model checking tool and it has been used in the analysis of different protocols. The Signal Protocol in this work is analyzed into three phases; registration phase, sending and receiving message phase, and sending a reply phase. The obtained results are addressed and compared to the mathematical and other model checking approaches