بروتوكول فعال وآمن لتبادل مفتاح التشفير بالارتكاز على المنحنى الإهليجي والنماذج الأمنية المرتبطة

إعداد

علي بسام علي الظاهر

المشرف

د. أحمد سلامة أبو سخن

المشرف المشارك

د. زياد هاشم الدسوقي

الملخص

في الوقت الحاضر، إن نجاح العديد من التطبيقات عبر الإنترنت يعتمد على حفظ البيانات المرسلة عبر الشبكات العالمية آمنة وبعيدة عن المتسللين. لتنفيذ هذه المهمة، يجب على الطرفين المتصلين تبادل المفاتيح أثناء الجلسة. بعض هذه التبادلات تسمى بروتوكولات إتفاقات المفاتيح يعد ECDH (Elliplic Curve–Diffie Hellman) أحد أكثر الخوارزميات كفاءة لتأمين البيانات. و ECDH أكثر كفاءة من التقنيات التقليدية الأخرى مثل RSA (Rivest–Shamir–Adleman) من حيث حجم المفتاح والحساب وعرض النطاق الترددي للشبكة. يتم استخدام بروتوكول إتفاق المفتاح المصدر (AKA) لإنشاء مفتاح جلسة مشتركة بين الطرفين المتواصلين. يتم استخدام مفتاح الجلسة لأهداف التشفير اللاحقة، معظم بروتوكولات إتفاقات المفاتيح مثل عائلة MQV (Menezes–Qu–

Vanstone) تولد مفتاح واحد لكل جلسة وبالتالي زيادة الفرص لتخمين مفتاح الجلسة، بروتوكول YAK (كإتفاق رئيسي قوي يعتمد على جمهور المفاتيح المصدقة) هي نوع مختلف من بروتوكول HMQV ثنائي المسار، ولكن يستخدم براهين Zero Knowledge لإثبات المعرفة بالقيم المؤقتة. يفتقر بروتوكول YAK إلى مفتاح تحكم مشترك وخصائص سرية إلى أمامية مثالية، وهو عرضة لبعض الهجمات بما في ذلك هجمات غير معروفة لمشاركة المفاتيح وتكرار المفاتيح. هذا يبطل الأمن الدلالي للبروتوكول في عدة نماذج أمنية. هناك أيضاً اعتبارات أخرى تتعلق بانتحال الهوية وهجمات مجموعات فرعية صغيرة.

في هذه الرسالة، ركزنا على تطوير مفتاح جلسات متعددة محسنة يقوم على ECDH. اقترحنا بروتوكول AKA فعال وآمن استناداً إلى أفكار تجزئة MQV (HMQV)، بروتوكول YAK مفاتيح الجلسات المتعددة.

يختلف البروتوكول المقترح عن البروتوكولات الأخرى (YAK و MQV و HMQV) في أنه ينتج مفاتيح جلسات متعددة في جلسة واحدة وبالتالي يجعل من الصعب على المتسللين لتخمين مفاتيح الجلسة. بالإضافة إلى ذلك، أظهرت نتائج محاكاة Scyther أن هذا البروتوكول المقترح وفر السرية الأمامية التامة (PFS)، في حين أن البروتوكولات الأخرى (MQV، HMQV و YAK) لم توفر ذلك أيضاً، أظهرت النتيجة من المحاكاة Scyther أن البروتوكول المقترح أثبت أنه آمن ضد مفتاح غير معروف (UKS)، انتحال المفتاح (KCI–R) وانتشار هجمات Krawczyk Canetti الممتد (Eck)، في حين أن البروتوكولات الأخرى (MQV و HMQV و YAK) ليست عرضة لهم. أخيراً وفر البروتوكول المقترح ميزة لتوقيع الرقمي التي تتحقق من صحة وسلامة الرسالة الرقمية على أساس خوارزمية هوية الصورة وتقنية التجزئة، بينما تسرب البروتوكولات الأخرى هذه الميزة. بجانب أنه أظهرت النتيجة أن البروتوكول المقترح ليس عرضة للخطر ضد هجوم الأمان الأساسي المعروف (KKS–R)، ولكن عرضة MQV. ومع ذلك، أظهرت نتيجة هذه الأطروحة أن عدد ضربات النقاط (PM) من البروتوكول المقترح أعلى من PM في الأعمال ذات الصلة. منذ ذلك الحين، في الأعمال ذات الصلة، يوجد مفتاح جلسة واحدة فقط يتم إنتاجه أثناء وجوده، في البروتوكول المقترح هناك تسعة مفاتيح في الجلسة المنتجة.