الخلاصة

لأن الشبكةَ الدولية للانترنت بيئةُ مفتوحةُ، الكثير مِنْ العنايةِ يجب أنْ تُؤْخَذَ بنظر الأعتبار عندما يتم نقلِ المعلوماتَ الحسّاسةِ خصوصاً عندما تتَعلّق بالبياناتِ الماليةِ وهذا يَعتمدُ علـــى الأفـــراد الّذين من الصعب ان يَكُونوا جديرين بالثقةَ و بما ان الخطوةِ الأولى في أمنِ الشبكة هو التحقُّقُ من هوية المستخدم فأن هذه الإطروحةِ تُقدّمُ نموذج مقترح لتطبيقاتِ المصرفِ النقّالـــةِ الآمنـــةِ التي تَستعملُ كربيروس (نظام تحقُّقِ الشبكةَ).

إنّ هدفَ هذه الإطروحةِ أنْ تنشئ إتصالاً آمناً بين الزبائنِ والمصرف الالكتروني بطريقة يُمْكِنُ أنْ يَستعملوا هاتفهم الجوّالَ للدُخُول الى حساباتهم المصرفية بشكل آمن والقيام بتحويل الأرصدة أو استلام الدُفْعاتَ المالية أوتدقيق الأرصدة.

إنّ اضافة البطاقةِ الذكيةِ إلى كربيروس الكلاسيكي يُحسّنُ الأمنَ للتحقُّقِ مـــن الزبـــونِ بخَـــزْن المفاتيحِ المشفّرةِ (كلا من مفتاح الزبون و مفتاح المصرف الإلكتروني) وهذا ما يسمى بالتحقُّقَ ثنائي العاملِ، وكذلك يمنَع هجومِ القوةِ العنيفِ و غَشّ الشبكة ومشكلة الخزن للمفاتيح. وكـــذلك فأن التحسين الآخر للكربيرس هو ال PKINIT الذي يتم فيه إستعمال المفتاحِ الخاصّ لتشفير الرسالةَ والمفتاحَ العام لفك التشفير الرئيسي بدلا من استخدام المفاتيح المشتركة بـــين الزبـــون والمصرف الإلكتروني.

للحُصُول على منفعةَ تقنيةِ بطاقةِ مكوّناتِ جافا سوف يتم انشاء ثلاثة مكونات: أولاً برنامج بطاقةِ جافا المحدود (applet) المسمى (JCKrbKey) والذي يعمل كمنظم للمفاتيح ويخزن كلا من مفتاح المستخدم و المصرف الالكتروني اثناء التصيب لغرض الاستخدام في وقت اخر للتشفير وفك التشفير لبطاقات كربيرس. المكون الاخر هو تطبيق الهـــاتف النقـــال (J2ME MIDlet) المسمى (J2MEClientMIDlet) الذي يمثل واجهة للمستخدم حتى يدخل اسمه و كلمـــة

PDF created with pdfFactory trial version www.pdffactory.com

السر لطلب الخدمة من المصرف الالكتروني. والثالث هو السرفر الذي يستضيف تطبيق المصرف الالكتروني و المسمى (TomCat server).

وقد تم اختبار النموذج المقترح باستخدام اداة تسمى (kerksniff\kerbcrack) والتي تتضمن جزئين وهذا الاختبار ضد مايسمى بهجوم القوة العنيفة. وقد بينت نتائج الاختبار ان النموذج المقترح نجح في تحقيق هدف الاطروحة في بناء نظام تحقق للزبون متين.

PDF created with pdfFactory trial version www.pdffactory.com

ABSTRACT

Because the network is an open environment, a lot of care must be taken when transferring sensitive information especially when related with financial data. This depends on the principals to be trusted which is a problematic and since the first step in security is the authentication, this thesis presents a proposed modal for secure mobile bank (m-bank) applications using Kerberos (the network authentication protocol).

The aim of this thesis is to establish a secure communication between the clients and an m-bank application server in which they can use their mobile phone to securely access their bank accounts, make and receive payments, and check their balances.

The integration of smart card into classic Kerberos enhances the security for client authentication by storing the cryptographic keys (both the user and the bank keys) what is called dual factor authentication, and also secures the client authentication by preventing brute force attack, spoofing and key storage. Other enhancement to Kerberos is the PKINIT in which the message encrypted using the principal's private key and decrypted using the public key rather than the shared keys.

To get the benefit of the Java Card Technology, three components will be developed: First is Java Card applet called `JCKrbKey` applet works as a key manager that holds both the user's key and bank's key during the installation and for later use for encryption and decryption of Kerberos messages. The second component will be a J2ME MIDlet called `J2MEClientMIDlet` MIDlet provides a graphical user interface to the clients to access their account in the m-bank application. The third part is the bank's server side component that develops end to end Java application between the J2ME MIDlet and Java Servlet called `eBankServlet`.

The model has been tested using Kerksniff\Kerbcrack tool which is two part test against the brute force attack. The result of test proves that the model satisfies the aim of the thesis to build a robust client authentication.

PDF created with pdfFactory trial version www.pdffactory.com