نظام بنكي للحوالات المالية

الوصف

الهدف هو إنشاء نظام بنكي يمكن للعملاء من خلاله إرسال حوالات إلى بعضهم البعض بالاعتماد على Server-Client Model وشبكة TCP/IP وبحيث يعمل سيرفر البنك بتقنية الـ Multi-Threading (يسمح بتخديم أكثر من زبون في الوقت ذاته) ويتم تخزين قيم خاصة بكل عميل في السيرفر: رقم العميل واسم العميل وقيمة للإيداعات الموجودة لديه.

مراحل الوظيفة

المرحلة الأولى

قم بإنشاء نظام يسمح للعميل بإرسال حوالة مالية إلى عميل آخر لدى البنك، بإرسال طلب من الـ client إلى الـ server، يتم تشفير المعلومات المرسلة من خلال كلمة سر متفق عليها مسبقاً بين العميل وبين البنك (السيرفر) عند إرسال أي حوالة، يجب تحديد قيمة الإيداع ورقم العميل المرسل إليه وجملة تعبر عن سبب الحوالة، وينبغي إعادة تأكيد في حال نجاح العملية أو فشلها (مثلا في حال عدم كفاية قيمة إيداعات المرسل).

المرحلة الثانية

لتحسين النظام يتم استخدام التشفير الهجين PGP ومفاتيح تشفير مولدة في كل جلسة (أي من أجل كل عملية إرسال)، بدلاً من استخدام كلمة السر المتفق عليها مسبقاً.

- يتم توليد public-private keys خاصة بالعميل فقط عند أول محاولة اتصال له أو عند تنصيبه للبرنامج ويتم تخزين تلك المفاتيح في قاعدة بياناته. وذلك بهدف تبادل الـ public keys بين السيرفر والعميل، بهدف إمكانية تبادل مفاتيح الجلسات.
- يتم توليد مفتاح الجلسة session key عند برنامج العميل client عند كل اتصال. بحيث يتم تشفير كل اتصال بمفتاح مختلف.
- يتم استخدام التشفير المتناظر لنقل بيانات الحوالات المالية للاستفادة من سرعته.

المرحلة الثالثة

يتم استخدام التوقيع الرقمي في كل عملية تحويل، وذلك لأهداف يطلب تحقيقها:

- سلامة البيانات Data Integrity ولضمان أن بيانات الحوالة المالية لم يتم تعديلها خلال النقل على الشبكة
- عدم النكران Non-Repudiation وذلك لضمان البنك عدم نكران المرسل إرساله للحوالة المالية

ولجعل النظام منيعاً ضد الـ replay-attack يقوم السيرفر باستخدام session key مختلف في كل مرة، أي لا يقبل استخدام الـ session key نفسه مرتين. وكذلك يتم وضع Unique ID لكل عملية تحويل Transaction من قبل برنامج العميل، بحيث يمنع السيرفر (االبنك) تكرار حوالتين لهما نفس الـ Unique ID.

المرحلة الرابعة

قرر البنك لضمان الوثوقية في التعاملات أن يمنع أي تطبيق client من العمل حتى يقوم العميل بإثبات هويته عن طريق Signed Certificate من قبل CA موثوق مسبقاً وذلك حسب الخطوات التالية:

- يقوم الكترونيا بتوليد CSR وإرساله إلى الـ CA
- يقوم العميل بإجراء اتصال هاتفي مع الـ CA وإثبات ارتباطه بالـ Public Key الخاص به عن طريق تأكيد الـ CSR FingerPrint
- في حال نجاح عملية التحقق يتم إرسال شهادة رقمية له Client Certificate الكترونيا، يتحتم على التطبيق لديه استخدامها عند كل عملية تحويل يقوم بها للتأكد من هويته.
- كذلك يكون للسيرفر Signed Certificate من قبل نفس الـ CA.

ملاحظات

- ممكن أن يكون الـ Client هو عبارة عن برنامج Desktop أو تطبيق هاتف، ولا يقبل تمثيل برنامج العميل كتطبيق وب بسبب بعض الإشكاليات في تحقيق مفاهيم الوظيفة عندما يكون برنامج العميل هو المتصفح.
- باستثناء المرحلة الأولى يرجى الانتباه إلى توليد المفاتيح بشكل ديناميكي بعد تنزيل التطبيق.
- يمكن لأربعة طلاب على الأكثر الاشتراك في الوظيفة باشتراط المشاركة بينهم في الحل والفهم الكامل.
- يمكن استخدام أي لغة برمجة ويفضل الجافا.
- يطلب وضع تقرير مختصر عن مراحل الوظيفة وشرح الكود البرمجي بتعليقات comments واضحة.

مواعيد التسليم والمناقشة

المرحلة	موعد التسليم والمناقشة	العلامة
الأولى والثانية	03/12/2019	11
الثالثة والرابعة	17/12/2019	11

مشرف العملي **مدرّسو العملي**

م. الأمجد توفيق اصطيف م. براء الطباع م. صفاء كيوان

مع تمنياتنا بالتوفيق