مدير كلمات مرور Password Manager

الوصف

- الهدف هو إنشاء نظام يسمح بتسجيل كلمات المرور بشكل آمن
- يبنى النظام على Server-Client Model: مخدم لتخزين كلمات المرور (server) وبرنامج عميل للتحكم بكلمات المرور (client)
- الاعتماد على الـ Sockets وفق اتصال TCP/IP
- الاعتماد في المخدم على Multi-Threading أو Event-Driven (أي من الممكن أن يخدّم أكثر من client في الوقت نفسه)

وبحيث تكون النتائج النهائية للمشروع تدعم أمن المعلومات وخاصة من النواحي التالية:

- سرية المعلومات Confidentiality
- سلامة المعلومات Integrity
- عدم النكران Non-Repudiation
- Authentication, Authorization
- End-to-End Encryption
- التأكد من أن الشخص أو السيرفر الذي يتم التواصل معه هو فعلاً الشخص المراد التواصل معه
- تجنب استخدام خوارزميات وطرق تشفير ضعيفة

مراحل الوظيفة

المرحلة الأولى

قم بإنشاء نظام يسمح للعميل client بإجراء الطلبات التالية مع المخدم server:

- طلب إنشاء مستخدم جديد في النظام وفق اسم معين وكلمة دخول مستخدم معينة
- تسجيل دخول مستخدم قديم
- طلب إضافة عنصر كلمة مرور جديد إلى الحساب تتضمن
  - عنوان لعنصر كلمة المرور
  - اسم مستخدم أو إيميل
  - كلمة المرور
  - وصف
  - ملفات مرفقة
- طلب استعراض عنصر كلمة مرور موجود مسبقاً
- طلب تعديل عنصر كلمة مرور موجود مسبقاً
- طلب حذف عنصر كلمة مرور موجود مسبقاً

ملاحظات:

- يقوم المخدم بعد تنفيذ كل طلب request بإرسال رد مناسب response إلى العميل يبلغه بنجاح العملية أو فشلها أو بالمعلومات المطلوبة
- لا يطلب تنفيذ أي أمان مرتبط بالـ cryptography في هذه المرحلة

المرحلة الثانية

الهدف في هذه المرحلة هو المحافظة على سرية المعلومات وسلامتها في الشبكة Confidentiality, Data Integrity وذلك عن طريق استخدام التشفير المتناظر والـ MAC.

ملاحظات:

- يستثنى طلب إنشاء مستخدم جديد وطلب تسجيل مستخدم قديم من سرية المعلومات وسلامتها، أي أن هذين الطلبين لن يكونا آمنين في هذه المرحلة
- يتم تسجيل كلمة دخول المستخدم في قاعدة معطيات المخدم كما هي
- يتم استخدام كلمة دخول المستخدم كمفتاح للتشفير المتناظر عند التواصل مع ذلك المستخدم
- يتم تشفير الـ requests والـ responses في الشبكة
- لا يقبل المخدم أو المستخدم أي request أو response من دون MAC مناسب
- لا يستطيع المستخدم التعديل إلا على كلمات مروره هو (Authorization)

المرحلة الثالثة

الهدف في هذه المرحلة هو المحافظة على سرية المعلومات باستخدام التشفير الهجين PGP

- عند تهيئة المخدم يتم توليد public-private keys خاصة به ويتم تخزين تلك المفاتيح بشكل مناسب في المخدم.
- تنفيذ handshaking بين المخدم والعميل عند كل جلسة اتصال:
  - يطلب العميل الـ public key الخاص بالمخدم.
  - يقوم العميل بتوليد session key وإرساله مشفراً للمخدم، وعلى المخدم أن يرجع للعميل رداً مناسباً يدل على وصول مفتاح الجلسة إليه وموافقته عليه.
  - يتم استخدام الـ session key في تشفير المعلومات والتأكد من سلامتها كما في المرحلة الثانية
- طلبات أخرى في هذه المرحلة:
  - يجب تأمين جميع الطلبات بما فيها إنشاء مستخدم جديد وتسجيل دخول مستخدم قديم
  - يجب حفظ كلمة دخول المستخدم في قاعدة معطيات المخدم بشكل آمن

المرحلة الرابعة

الهدف في هذه المرحلة هو حفظ كلمات مرور المستخدم في السيرفر بشكل آمن واستخدام التوقيع الرقمي Digital Signature:

- عند إنشاء مستخدم جديد يقوم برنامج العميل بتوليد public-private keys خاصة بالعميل ويقوم بحفظ مفاتيحه عنده.
- عند إنشاء مستخدم جديد يقوم برنامج العميل بإرسال الـ public key الخاص بالعميل إلى المخدم ليحفظه في قاعدة معطيات المخدم.
- يتم تشفير كلمات المرور قبل نقلها إلى المخدم بواسطة private key الخاص بالعميل، بحيث يقوم المخدم بحفظ كلمات المرور عنده مشفرة، ولا يستطيع المخدم نفسه معرفة قيم كلمات المرور المخزنة. وبالتالي حتى لو تم اختراق المخدم فلا يستطيع المخترق معرفة كلمات مرور أي مستخدم.

يتم استخدام التوقيع الرقمي لكل طلب يتم إرساله للمخدم وذلك لـ:

- ضمان الـ Authentication والـ Authorization لذلك الطلب
- ضمان سلامة البيانات Data Integrity
- ضمان عدم النكران Non-Repudiation وذلك ليستطيع المخدم أن يثبت في المستقبل أن المستخدم فعلاً قام بذلك الطلب.

المرحلة الخامسة

الهدف في هذه المرحلة هو إمكانية مشاركة كلمات المرور بين العملاء

- يمكن لعميل ما أن يشارك عنصر كلمة مرور محدد مع عميل آخر يقوم بتحديده وفق الاسم أو الرقم التعريفي الخاص به.
- نسمي العميل الذي يريد مشاركة عنصر كلمة مروره عميل ١، والعميل المراد مشاركة كلمة المرور معه عميل ٢.
- يتم إرسال طلب مشاركة كلمة المرور إلى السيرفر من قبل العميل ١ مشفراً بحيث لا يستطيع فك التشفير إلا العميل ٢ وكذلك يقوم العميل ١ بالتوقيع على الطلب.
- يقوم السيرفر بحفظ طلبات المشاركة عنده ويرسلها للعميل ٢ عندما يقوم بفتح برنامجه.
- يستطيع العميل ٢ تصفح طلبات المشاركة والتأكد من صحتها وسلامتها ومن جهة إرسالها، ويستطيع معرفة قيمتها والموافقة على إضافتها إلى كلمات مروره.

المرحلة السادسة

الهدف من المرحلة السادسة هو استخدام الشهادات الرقمية Digital Certificates والاستعانة بـ Certificate Authority

وفق ما يلي:

- التأكد من أن المخدم الذي يتم التواصل معه هو فعلاً المخدم المراد التواصل معه وذلك باستخدام Signed Certificate خاصة بالمخدم من قبل CA موثوق مسبقاً.
  - يقوم المخدم بتوليد CSR وإرسالة إلى الـ CA
  - يقوم الـ CA بالتحقق من هوية المخدّم وارتباطه بالـ Public Key الموجود في الـ CSR.
  - في حال نجاح عملية التحقق يقوم الـ CA بإرسال الشهادة الرقمية للمخدم، يتحتم على المخدم بعدها استخدامها عند كل عملية اتصال لإثبات صحة الـ Public Key الخاص به.

طلب إضافي: التأكد من أن العميل الذي يتم التواصل معه هو فعلاً العميل المراد التواصل معه عن طريق Client Certificates يتم إنشاؤها بخطوات شبيهة لما سبق.

مواعيد التسليم والمناقشة

المرحلة	موعد التسليم والمناقشة	العلامة
الأولى والثانية والثالثة	يوم الأحد 12 كانون الأول	12
الرابعة والخامسة والسادسة	يوم الأحد 26 كانون الأول	12

ملاحظات إضافية

- عدد الطلاب في المجموعة الواحدة على الأكثر 5
- التقييم مبني على إنجاز المشروع وعلى الفهم الفردي، أي أنه على كل طالب في المجموعة فهم المشروع المنجز كاملاً.

مدرّسو العملي

مع تمنياتنا بالتوفيق