كلية الهندسة المعلوماتية ـ جامعة دمشق

السنة الخامسة -أمن نظم المعلومات -عملي

إنشاء مخدم تابع لجامعة دمشق

الوصف

- الهدف هو إنشاء نظام يعمل على الربط بين كيان جامعة دمشق وبين الطالب والدكتور الجامعي
- يبنى النظام على Server-Client Model: مخدم للجامعة (server) ومتصفح للمستخدمين (الطالب والدكتور) (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
- التأكد من أن الشخص أو السيرفر الذي يتم التواصل معه هو فعلاً الشخص المراد التواصل معه
- تجنب استخدام خوارزميات وطرق التشفير الضعيفة

مراحل الوظيفة

المرحلة الأولى

قم بإنشاء نظام يسمح للعميل client بطلب request من المخدم server وفق الخانات التالية:

- عنوان الآي بي الخاص بالسيرفر
- الـ port الذي يعمل عليه السيرفر
- إنشاء حساب للعميل على السيرفر بحيث يحتوي اسم العميل وكلمة السر
- تسجيل دخول العميل الى السيرفر باستخدام اسم العميل وكلمة السر

وبعد أن يستقبل السيرفر ذلك الطلب المكون من الخانات السابقة يقوم بما يتناسب مع كيان العميل المطلوب والتحقق من السماحية المطلوبة للعميل، يتم السماح للعميل بالولوج إلى النظام الجامعي ويرسل السيرفر رسالة نجاح أو فشل الطلب الى العميل.

المرحلة الثانية

الهدف في هذه المرحلة هو المحافظة على سرية المعلومات في الشبكة Confidentiality وذلك عن طريق التشفير المتناظر بحيث نفترض أن المخدم والعميل متفقان مسبقاً على مفتاح التشفير المتناظر (من الممكن أن يكون الرقم الوطني للعميل) حيث يكون محتوى البيانات المرسلة هو استكمال المعلومات الإدارية الخاصة بالعميل (رقم الهاتف – رقم الموبايل - مكان السكن- الخ)

ملاحظة: يطلب تشفير المعلومات في كل من الـ request والـ response

المرحلة الثالثة

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

- يتم توليد public-private keys خاصة بالعميل والسيرفر فقط عند أول محاولة اتصال لأي منهما ويتم تخزين تلك المفاتيح لكل طرف عنده.
- تنفيذ handshaking بين السيرفر والعميل عند كل اتصال، يتم فيها تبادل مفاتيح الـ public key المطلوبة
- يقوم العميل بتوليد الـ session key وإرساله للمخدم باستخدام PGP، وعلى المخدم أن يرجع للعميل رداً يدل على وصول مفتاح الجلسة إليه وموافقته عليه.
- بعد الاتفاق على session key, يتم تشفير الـ request والـ response ضمن الجلسة الحالية باستخدام مفتاح الجلسة.
- يقوم السيرفر بحفظ الـ public keys الخاصة بالعملاء الذين يسمح لهم بالولوج الى النظام الجامعي.

ملاحظة: مفتاح الجلسة هو مفتاح التشفير المتناظر ويتم تغييره في كل جلسة (اتصال)

ملاحظة: يمكن للطالب إرسال قائمة توصيف عن المشاريع العملية المنجزة من قبل العميل ويرسل المخدم رسالة تأكيد وصول المعلومات.

المرحلة الرابعة

الهدف في هذه المرحلة هو استخدام الدكتور الجامعي فقط للتوقيع الرقمي Digital Signature لغرض:

- سلامة البيانات Data Integrity ولضمان أن البيانات لم يتم تعديلها خلال الشبكة
- عدم النكران Non-Repudiation وذلك لإثبات أن المستخدم قام فعلاً بإرسال قائمة علامات مادة معينة في وقت معين، وإثبات أن السيرفر قام فعلاً بتأكيد وصول القائمة و توليد وإرسال ID معرف لتخزين تلك القائمة لديه في وقت معين.

المرحلة الخامسة

الهدف من المرحلة الخامسة هو ما يلي:

- التأكد من أن الدكتور الجامعي الذي يتم التواصل معه هو فعلاً الكيان المراد التواصل معه وذلك باستخدام Signed Certificate خاصة بالدكتور الجامعي من قبل CA موثوق مسبقاً (رئاسة جامعة دمشق).
  - يقوم الدكتور الجامعي بتوليد CSR وإرساله إلى الـ CA
  - يقوم الـ CA بالتحقق من هوية الدكتور وارتباطه بالـ Public Key الموجود في الـ CSR حيث يطلب منه حل معادلة رياضية معينة للتأكد من هويته.
  - في حال نجاح عملية التحقق يقوم الـ CA بإرسال الشهادة الرقمية لمقدم الطلب، يتحتم على الدكتور بعدها استخدامها عند كل عملية اتصال لإثبات صحة الـ Public Key الخاص به.
- التأكد من أن العميل الذي يتم التواصل معه هو فعلاً العميل المراد التواصل معه وإمكانية تطبيق Authentication والـ Authorization عن طريق شهادات رقمية خاصة بالعملاء Client Certificate يتم إنشاؤها بخطوات شبيهة لما سبق حيث من الممكن أن تحدد الـ Client Certificate صلاحيات العميل على السيرفر من حيث قراءة قائمة علامات معينة.

- **وظيفة الويب [علامتان]**

يجب تنفيذ هجوم الوارد في المحاضرة Xss بهدف XSS Attacks to Change Other People's Profiles وذلك على منصة Elgg التي تم الشرح عنها مسبقاً ضمن المحاضرات.

مواعيد التسليم والمناقشة

الاختصاص	موعد التسليم والمناقشة	العلامة
الذكاء الصنعي	يوم الخميس 28 كانون الأول	28
الشبكات والنظم الحاسوبية	يوم الثلاثاء 26 كانون الأول	28
البرمجيات	يتم التحديد من قبل الأستاذ عبيدة	28

ملاحظات إضافية

- عدد الطلاب في المجموعة الواحدة 4 على الأكثر .
- يجب اشتراك نفس الطلاب لتنفيذ المشروع و وظيفة الويب علماً أن مقابلة الوظيفة والمشروع يتم بنفس المواعيد المحددة في الجدول السابق.
- يجب تسليم تقرير ملخص يشمل شرح المراحل العملية التي تم تنفيذها لإنجاز مراحل المشروع وشرح التوابع الواردة فيها
- يمكن للطالب استخدام لغة البرمجة التي يرغب بها على أن يتمكن من خلالها من إنجاز جميع مراحل المشروع المطلوبة.

بالتوفيق للجميع..

مدرّسو العملي

م. آلاء خدام الجامع م. عبيدة حسن م. أحمد جمعة