تطبيق دردشة

التوصيف

- التطبيق يقوم بإرسال رسائل دردشة بين طرفين عن طريق خادم وسيط يتم توجيه الرسائل له بداية ليعيد توجيهها.
- يبنى النظام على Server-Client Model: مخدم لإدارة الدردشة وتحقيق الوظائف الأمنية (server) وبرنامج عميل يقوم بإرسال الرسائل (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- إنشاء بنية النظام

قم بإنشاء نظام يسمح بما يلي:

- تسجيل عميل جديد في النظام بالاعتماد على رقم هاتفه وكلمة مرور
- تحقيق ارسال رسالة بين عميلين بالاعتماد على رقم الهاتف بحيث يوجد لدى العميل مجموعة من الأرقام المخزنة سابقا كما يمكنه الإرسال لأرقام جديدة
- يرسل المخدم تنبيه بإتمام عملية الارسال أو فشلها
- استعراض الرسائل السابقة لدى العميل
- تخزين الرسائل في المخدم.

لا يتم في هذه المرحلة تطبيق سياسات أمنية

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.

- لكل عميل مفتاح تشفير خاص به يخزن عند السيرفر
- يقوم السيرفر بفك تشفير الرسائل الواردة من العميل ما ليعيد تشفيرها بمفتاح التشفير الخاص بالعميل الوجهة

- ❖ يتم تشفير ردود المرسلة من المخدم أيضا.
- ❖ عمليات المراسلة بين العملاء والردود الخاصة بالسيرفر يجب أن يستخدم فيها MAC مناسب

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 الخادم 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

المرحلة الرابعة

الهدف في هذه المرحلة هو استخدام التوقيع الرقمي Digital Signature لغرض:

- ❖ سلامة البيانات Data Integrity و لضمان أن البيانات لم يتم تعديلها خلال الشبكة.
- ❖ عدم النكران Non-Repudiation وذلك لإثبات أن العميل قام فعلاً بإرسال رسالة دردشة في وقت معين، أو إثبات أن السيرفر قام فعلاً بإرجاع رد على الرسالة في وقت معين.
- ❖ يقوم كل عميل بتوليد مفاتيح public-private خاصة به.

المرحلة الخامسة

الهدف من المرحلة الخامسة هو ما يلي:

- ❖ التأكد من أن السيرفر الذي يتم التواصل معه هو فعلاً السيرفر المراد التواصل معه وذلك باستخدام Signed Certificate خاصة بالسيرفر 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 حيث يطلب منه وضع نص معين وفق رابط معين، وربما يتصل بمقدم الطلب هاتفياً.
- ❖ في حال نجاح عملية التحقق يقوم الـ CA بإرسال الشهادة الرقمية لمقدم الطلب، يتحتم على السيرفر 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 عن طريق شهادات رقمية خاصة بالعملاء Client Certificate يتم إنشاؤها بخطوات شبيهة لما سبق حيث من الممكن أن تحدد الـ Client Certificate
- ❖ يتم التشفير في هذه المرحلة بين العميلين باستخدام المفاتيح العامة لكل منهما فلا يمكن للسيرفر فك التشفير.

وظيفة الويب:

تنفيذ هجمة XSS كما يلي:

تقوم Alice بزيارة بروفايل المهاجم وعندها يتغير الوصف الخاص بصفحتها ليصبح "Attacker is my Hero"

ملاحظات:

1- يسمح باشتراك 5 طلاب حد أقصى في الوظيفة.

2- تجرى المقابلات النهائية بتاريخ 29/12/2022 وفق ما يحدده أستاذ كل اختصاص.

3- توضع علامة صفر للمشاريع المتشابهة أو المسروقة.

مدرّسو العملي

م. براء الطبّاع م. آلاء خدام الجامع م.أحمد الجمعة م.يارا يوسف م.صفاء كيوان