جامعة دمشق
كلية الهندسة المعلوماتية

وظيفة امن المعلومات

إعداد الطلاب:

عمار طلال حسين

عمر ماردیني

يقدم التطبيق نظام مراسلة بين نظيرين (Peer-to-Peer - P2P) يضمن أمان الاتصال. من خلال الجمع بين تقنيات التشفير المتماثل (Symmetric) والتشفير غير المتماثل (Asymmetric)، يُظهر النظام كيف يمكن حماية المحادثات الخاصة من الوصول غير المصرح به.

نظرة عامة على النظام(System Overview)

تم تصميم هذا النظام لتمكين نظيرين من تبادل الرسائل بشكل آمن. يعمل النظام كما يلي:

1- Initialization

يقوم المستضيف (Host) بإنشاء خادم(Server) ، بينما يتصل العميل (Client) باستخدام عنوان IP الخاص بالمستضيف.

2- Key Exchange

يتم تبادل المفاتيح العامة باستخدام خوارزمية RSA لإنشاء الثقة ومشاركة مفتاح متماثل بأمان.

3- Communication

تُشفّر الرسائل باستخدام المفتاح المتماثل لزيادة الكفاءة. يتم استخدام التشفير غير المتماثل للتبادل الأولي للرسائل الحساسة أو الخاصة.

4- Modes of Messaging

Normal(عادي): الاتصالات النصية بدون تشفير (للرسائل غير الحساسة).

Symmetric(متماثل): يتم تشفير الرسائل بمفتاح مشترك لتحقيق سرعة المعالجة.

Asymmetric(غير متماثل): يتم تشفير الرسائل باستخدام المفتاح العام للنظير لزيادة الأمان.

تقنيات التشفير(Cryptographic Techniques)

Symmetric Encryption (Fernet)

التشفير المتماثل يستخدم مفتاحًا واحدًا مشتركًا لكل من التشفير وفك التشفير. في هذا المشروع، استخدمنا وحدة Fernet من مكتبة cryptography في بايثون، التي توفر تطبيقًا قويًا للتشفير المتماثل.

تضمن Fernet سلامة البيانات وسريتها مع كونها كفؤة حسابيًا، مما يجعلها مثالية للاتصال في الوقت الحقيقي.

Asymmetric Encryption (RSA)

التشفير غير المتماثل يستخدم زوجًا من المفاتيح - المفتاح العام والمفتاح الخاص. يقوم المرسل بتشفير الرسائل باستخدام المفتاح العام للمستقبل، ويفك المستقبل التشفير باستخدام مفتاحه الخاص.

تم تنفيذ هذه التقنية باستخدام خوارزميةRSA ، التي تُعتبر وسيلة آمنة لمشاركة المفاتيح وتشفير الرسائل.

تبادل المفاتيح:

يتم إنشاء زوج من المفاتيح (مفتاح عام وخاص) باستخدام خوارزمية .RSA تُتبادل هذه المفاتيح بأمان بين النظيرين لإنشاء الثقة. بعد ذلك، يُشارك مفتاح متماثل عبر هذه القناة الآمنة، مما يجمع بين قوة الطريقتين التشفيريتين.

المكتبات والأدوات المستخدمة(Libraries and Tools)

1- Socket

تُستخدم مكتبة socket لتسهيل اتصالات TCP بين النظيرين، مما يُمكّن تبادل البيانات في شكل نظير-إلى-نظير.

2- Threading

تُستخدم وحدة threading لضمان أن عمليات إرسال الرسائل واستلامها تتم بالتزامن دون عرقلة النظام.

3- Cryptography

تُنفّذ مكتبة cryptography تقنيات التشفير الآمنة:

Fernet: لتوفير التشفير المتماثل.

RSA: لإنشاء أزواج المفاتيح العامة والخاصة للتشفير غير المتماثل.

Serialization: لترميز المفاتيح وفك ترميزها لنقلها.

الخوارزميات وسير العمل(Algorithms and Workflow)

1- Initialization

يبدأ المستضيف خادمًا وينتظر الاتصال.

يتصل العميل باستخدام عنوان IP الخاص بالمستضيف.

يتم إنشاء قناة اتصال ثنائية الاتجاه.

2- Public Key Exchange

يقوم كل نظير بإنشاء زوج من مفاتيح RSA

يتم إرسال المفتاح العام إلى النظير الآخر بعد ترميزه.

يتيح هذا التبادل مشاركة المفتاح المتماثل بأمان.

3- Symmetric Key Sharing

يتم إنشاء مفتاح متماثل باستخدام Fernet

يُشفّر هذا المفتاح باستخدام المفتاح العام للنظير ويُرسل بأمان.

بمجرد أن يمتلك النظيران المفتاح المتماثل، تبدأ عملية الاتصال المشفر بكفاءة.

4- Message Encryption and Sending

يختار المستخدم نمط الاتصال (عادي، متماثل، أو غير متماثل).

بناءً على النمط، تُرسل الرسائل كـ:

نص عادي.

مشفر باستخدام المفتاح المتماثل.

مشفر باستخدام المفتاح العام للنظير.

يقوم المستلم بفك تشفير الرسائل بناءً على النمط المستخدم.

يظهر التطبيق التكامل الفعّال بين تقنيات التشفير المختلفة لتطوير نظام اتصال آمن بين نظيرين. من خلال الجمع بين كفاءة التشفير المتماثل وأمان التشفير غير المتماثل، يضمن النظام حماية الرسائل بشكل قوي.