الخلاصة

إن عدد المستخدمين لشبكة الأنترنيت يزداد يوما بعد آخر، وهناك الكثير من الأعمال والمؤسسات الصناعية والوكالات التجارية والدوائر العسكرية ...الخ صارت تعتمد على الأنترنيت بصورة رئيسية كأداة للإتصالات، مصدر للمعلومات ، أو كأداة لنقل وتبادل البرامجيات والنتاجات الأخرى، لذا فالعالم اليوم بدأ فعلا يصبح قرية الكترونية . . .

لكن، ولسوء الحظ، إن المعلومات المرسلة عبر الأنترنيت هي عرضة للكثير من أنواع الأعتداء عليها خلال مرورها بالإنترنيت من مصدرها الى جهتها المقصودة. إن الدور الرئيسي لهذه الدراسة قد أعطي لإيجاد حلول لمشاكل الإنترنيت والشبكات الآتية

- مشكلة هجمات إعادة البث.
- مشكلة تكاملية البيانات.
- مشكلة تحليل المسار.
- مشكلة الهجمات المحايدة.

وذلك قد دفعنا الى تقديم بعض خوارزميات التشفير ودوال الإختزال بشيء من التفصيل.

إن الحلول المقترحة في هذه الدراسة تعتمد بالأساس على أمنية بروتوكول الشبكة الذي تم تعريفه بأنماط الأستخدام، خوارزميات التشفير، دوال الهضم، وتبادل المفاتيح. أن الأمنية المقترحة في هذه الدراسة تعتمد على خطة أمنية ديناميكية لحماية نقل البيانات وذلك بأستخدام إثنا عشرة إجراءا تعمل في بيئة منمذجة وبأسلوب تعاضدي وليست بيئة شبكات حقيقية . وهذه الإجراءات هي :

- إجراء أمنية بروتوكول الشبكة.
- إجراء تغليف الحزمة التشفيري المخَول.
- إجراء تغليف الحزمة اللاتشفيري المخَول.
- إجراء تغليف الحزمة النفقي التشفيري المخَول.
- إجراء تغليف الحزمة النفقي اللاتشفيري المخَول.
- إجراء رفع تغليف الحزمة التشفيري المخَول.
- إجراء رفع تغليف الحزمة اللاتشفيري المخَول.
- إجراء رفع تغليف الحزمة النفقي التشفيري المخَول.
- إجراء رفع تغليف الحزمة النفقي اللاتشفيري المخَول.
- إجراء ايجاد مهضوم الحزمة.
- إجراء تشفير الحزمة.

إن النظام المقترح يعمل بطريقة بيئة الشبكات المنمذجة وليست بيئة شبكات حقيقية . إن النظام أعلاه تمت نمذجته بأستخدام لغة البرمجة الصورية هدفية التوجه دلفي ٦

PDF created with pdfFactory trial version www.pdffactory.com

Abstract

The Number of paticipants of the Internet is increasing day by day and more businesses, industrail companies, financial agencies, military circuits, ..., etc., have been using the Internet as a backbone for their works, they are using it as a communication tool to exchange the software and other products, So the world is really begin to become an " ***Electronic Village***".

Unfortunately, the Information transmitted over the Internet is subject to many kinds of attacks during its travelling along this Super HighWay from its source to its destination. The key role of this study is given to find solutions for the following Internet and networks` secuirty problems:

- Replay attacks problem.
- Data Integrity problem.
- Traffic-flow analysis problem.
- Passive attacks problem.

This has led us to select the cryptographic algorithms and hash functions to be presented. This is based on the Internet Protocol Security (*IPSec*), Which is defined by modes of implemetation, encryption algorithms, hash functions, and key management. The security suggested in this study depends on a dynamic "*SECURITY POLICY* " for the protection of the traffic depending on twelve modules workink in a simulated co-operational environment and not in real networking environment. These modules are as follows:

- ***IP Security Module.***
- ***RC5 (Rivest Cipher Five) Module for encryption and decryption.***
- ***MD5 (Message Digest Five) Module to calculate the packet digest used in integrity assurance.***
- ***Transport-ESP (Encapsulating Security Payload) Module to thwart the passive attacks problem.***
- ***Tunnel-ESP Module to thwart the traffic-analysis problem.***
- ***Transport-AH (Authentication Header) Module to solve data integrity problem.***
- ***Tunnel-AH Module to solve data integrity problem througth tunnels.***
- ***Anti-Replay Module to thwart the replay attacks.***
- ***De-Transport-ESP Module.***
- ***De-Tunnel-ESP Module.***
- ***De-Transport-AH Module.***
- ***De-Tunnel-AH Module.***

PDF created with pdfFactory trial version www.pdffactory.com