أمن المعلومات
دراسة خاصة حول أخفاء المعلومات في الحاسبات الألكترونية

بيداء جاسم محسن
قسم علوم الحاسبات، كلية التربية- ابن الهيثم ، جامعة بغداد

الخلاصة

تستخدم تقنيات التشفير بشكل واسع هذه الأيام كوسيلة لضمان السرية والموثوقية في الاتصالات الإلكترونية. تضمن العمل في هذا البحث توضيح وشرح أهم الطرائق المستخدمة في إخفاء المعلومات مثال على ذلك إخفاء الرسائل السرية في رسائل أخرى وإخفاء المعلومات في ملفات صورية وملفات صوتية.

المقدمة

لقد ادرك الناس أهمية الابقاء على سرية رسائل معينة ، وذلك منذ الاف السنين ولم يتأخروا بالطبع في أدراك المزايا التي يمكن الحصول عليها في اعتراض المعلومات السرية مما أدى الى وجود معركة مستمرة ومثيرة بين واضعي الرموزومحلليها.وكان وسط الاتصالات ميدان هذه المباريات.والذي تبدل بشكل ملحوظ مع مرور الزمن.ولم يسرى فن الاتصالات عن بعد النورالا بعد ابتكار التلغراف . ولكن المجتمع يعتمد ، في الوقت الحاضر وبدرجة كبيرة على الوسائل الحديثة والسريعة والدقيقة لارسال الرسائل ، فضلا عن الى الاشكال التي أتخذها لمدة طويلة كخدمات البريد والسعاة .وقد توفرت لنا الان وسائل اكثر تقنية وتعقيداًكاللاسلكي والتلفزيون والهاتف والتلكس والوصلات العالية السرعة للبيانات.ان الهدف الرئيس عادة هوفقط ارسال رسائل باقصى ما يمكن من السرعة.وهناك عدد من الحالات تكون فيها المعلومات سرية حيث يستطيع معترض او مسترق للسمع الاستفادة بدرجة كبيرة من المعرفة التي يحصل عليها من

خلال مراقبة دائرة المعلومات ، وفي حالات كهذه يجب ان يتخذ المتراسلون خطو
لاخفاء وحماية محتويات رسائلهم ويختلف بالطبع مقدار الحماية اللازمة فقد يفي في بعض
الحالات منع متنصت عرضي من فهم الرسالة ولكن هناك حالات أخرى تفرض بعض
حاسمة عدم تمكين حتى المعترض الاشد تصميماً من فهمها .

توجد عدة طرائق للحفاظ على سرية البيانات منها استخدام وسائط لارسال البيانات التي
تكون غير قابلة للأعتراض NON _ Interceptible , بالتأكيد مع هذه الوسائط ستكون
تكون كل الرسائل ذات سرية تامة. لكن أغلب طرق الأتصال لاتحقق هذا الهدف ، حتى
ان وجدت طريقة أتصال تقربنا من هذا الهدف سوف تكون بطيئة ومكلفة. فضلا عن
العملية لارسال عدد كبير من الرسائل مستحيلة ، لذا لابد من أستخدام انظمة خاص
لتشفير وأخفاء المعلومات المرسلة (3).

الغاية من الدراسة

تقود المعلومات إلى كل من عناصر الحضارة والتقدم ونتيجة لزيادة كمية المعلومات
المرسلة عبر خطوط الاتصالات المعتادة ولأهمية المعلومات أصبحت مشكلة حمايتها
والحفاظ عليها موضع اهتمام العاملين والباحثين في هذا الميدان .

تم التركيز في هذه الدراسة على توضيح وشرح أهم الطرائق المستعملة في إخفاء
المعلومات والأساليب المستخدمة في ذلك .

مفهوم أمن البيانات

يمكن تعريف أمن البيانات بأنه أسلوب تأمين وصول البيانات المطلوبة دون زيادة أو
نقصان وفي الصيغة السليمة الصحيحة إلى المستفيد في الوقت الملائم وبدون تأخير (6).

إستراتيجيات حماية المعلومات

هناك بعض الإجراءات المتخذة لحماية البيانات والمعلومات منها:

-**تشفير وأخفاء البيانات** (4):- يمكن تعريف مصطلح التشفير بانه يشير الى الأساليب
والوسائل الفنية التي يمكن بواسطتها اخفاء المعنى الحقيقي للرسائل المرسلة او إخفاء
الرسائل المرسلة ضمن ملفات معينة. بحيث لا يمكن لاحد المسترقين التلاعب بمحتويات
الرسالة او الكشف عن معناها او تعديلها او إضافة أجزاء لها. ويعد هذا الأساس من اكثر
الأساليب أمانا لضمان عدم التسرب للبيانات المنقولة عبر الشبكات.

حماية البرامجيات (5) :- من الإجراءات المتخذة في حماية البرامجيات سواء كانت برامج مساعدة او برامج النظم التطبيقية او برامج الأخبار هي :

. التأكد من كون البرنامج الذي دخل التنفيذ هو النسخة المعتمدة ومحاولة اكتشاف أي تغيير غير مأذون على البرنامج .

. تحديد عدد مرات التنفيذ لكل برنامج خلال مدة زمنية معتمدة ومنع أي محاولة للتنفيذ خارج المعايير المقبولة .

. تسجيل حالات الانتهاء غير العادي للتشغيل .

. تطبيق تدابير السلامة القصوى في حالة اعادة تشغيل البرنامج بعد توقفه بصورة غير اعتيادية .

.ضرورة الاحتفاظ بنسخ احتياطية للبرامج المهمة والحساسة في حالة حدوث كارثة .

. الاحتفاظ بسجل لكل عمليات التعديل في البرامج ولاسيما البرامج المأخوذة من الخارج.

. يجب عدم تحميل أي برنامج إلابعد فحصه والتأكد من خلوه من الفيروسات.

. تركيب برامج مضادة للفيروسات ويجب ان تكون دائماً في الذاكرة .

- **حماية قواعد وملفات البيانات** : يقصد بقاعدة المعلومات هو تجميع البيانات الموجودة في مركز الحاسبة في قاعدة بيانات واحدة او اكثر بحيث يتشارك المستفيدون في مركز الحاسبة في نفس البيانات التي تهم اكثر من مستفيد بدلاً من استقلال كل مستفيد بملفاته ومعلوماته وهذا ما يدعونا الى التحوط ومعالجة جانب من الامنية والسرية لهذه البيانات وادامتها بما يضمن الحفاظ عليها من التخريب والتداول غير المشروع .

أهمية إخفاء المعلومات

برزت الحاجة إلى إخفاء المعلومات عبر التاريخ ولاسيما في أثناء الحروب بوسائل عدة منها التنقيب والأحبار السرية ، فعلى سبيل المثال كان للأحبار السرية استعمالات كثيرة ولزمن طويل ، حيث كان الجاسوس يراسل الجهة المنتسب اليها بوساطة استخدام الحبر السري دون معرفة من الدول التي يقوم بها وكذلك الامر عندما يراد أن يستلم رسالة من الطرف الثاني ، وكانت هناك عدة أنواع عديدة من الحبر السري كلما أنكشف نوع منها أكتشف المختصون نوعاً جديداً (1) .

ومع ظهور الاتصال الإلكتروني وتبادل الرسائل والملفات بين الشبكات حول العالم وال
تعد عصب الحياة الاساسية للعديد من المؤسسات والدول ،أصبح بالامكان نقل بيانات
الحاسبات من موقع الى أخر خلال لحظات دون الحاجة الى السفر أو ارسال رسائل خط
فأصبحت فرصة الامساك بالعميل تكاد ان تكون معدومة لانه مايأتي :-

أولاً : لم يكتب شيئاً بخط يده

ثانياً : صعوبة أكتشاف وجود البيانات الخفية

ثالثاً : يمكن ارسال البريد من أي موقع متاح ومن ثم فلن تتعرف الدول المعنية على
موقعه.

وكذلك يمكن أخفاء البيانات مهما كانت أهميتها وحجمها وأسترجاعها من قبل الطرف
الأخر فقط.

أسباب الاخفاء

يمكن تلخيص اسباب الاخفاء كما يأتي (2):

- وسيلة ضمان لعدم الكشف عن المعلومات المراد اخفائها .
- الحفاظ على الخصوصية باستخدام الاخفاء (privacy) والسرية (security) .

طرائق اخفاء النصوص والبيانات

عادة ما يتم اخفاء البيانات ضمن الملفات الصور والاصوات وذلك لكبر حجم هذه
الملفات وامكانية اخفاء البيانات فيها، لان الصور تستغل مساحة خزنية كبيرة فلا تتأثر
بوجود بيانات ضمنية ولا تؤثر فيها كثيراً (1).

شروط الاخفاء

هنالك عدة شروط للاخفاء منها:

- ان تتضمن عدم امكانية معرفة المقابل اين تم الاخفاء .
- ان لا تشوه الصورة او الصوت مما يؤدي الى كشف عملية الاخفاء

وممكن ان يتم الاخفاء للبيانات في الملفات الاتية :

- ملفات الصور بكل انواعها .
- الاغاني والافلام لكبر حجمها (صوت او صوت وصورة)
- استخدامات ضعيفة تتم لاخفاء النصوص ضمن نصوص اخرى .

- تقنيات برمجة النوافذ مثال water mark ولصق صورة خلف صورة .

طرائق اخفاء البيانات

عادة الاخفاء في الصوت والصور يتم باستخدام الثنائية الاخيرة في البايت (LSB) وذلك لان تأثيرها على الصوت والصورة يكون قليل فمثلاً اذا كان البايت يحمل الرقم 150 واصبح 151 فانه لن يتاثر بهذه الزيادة اليسيرة – عند الاخذ بالاعتبار ان البايت المستخدم يكون من صفر الى 255 قيمة كذلك فان الجزء الواحد من الصوت على مستوى البايت سوف لن يكون له تأثير على بقية بايتات الصوت .

- اخفاء نص (text) في ملف بيانات

تتم عملية اخفاء نص (text) في ملف البيانات من خلال استخدام الاسكي (code) غير المشفرة الموجودة ضمن الحاسبة حيث يتم اختيار الاسكي التي لا تكون تابعة الى أي (رمز – حرف – رقم) وذلك لان استخدام هذا النوع من الاسكي سوف لايؤثر على شكل الملفات التي تتم فيها الاخفاء .

- اخفاء بيانات في ملفات الصور

الاخفاء في الصور التي تتم باستخدام الثنائية الاخيرة في البايت (LSB) وذلك لان تأثيرها على الصورة قليل . فمثلاً اذا كان اللون الاصلي رقمه 150 واصبح 151 فانه لن يتاثر بهذه الزيادة اليسيرة عند الاخذ بالاعتبار ان الالوان المستخدمة هي 256 لونا كذلك فان الجزء الواحد من الصورة والمسمى بال Pixelمكون من اربعة بايتات واحدة منها لتحديد الموقع والثلاثة الاخريات هن للالوان(الاحمر ، الازرق ، الاخضر)

حيث ان الاخفاء يتم في احد الالوان الثلاثة .

ويسمى هذا النوع من ال(Pixels) بـ (RGB Pixel) .

- النقاط المهمة في عملية اخفاء البيانات

عند استخدام طريقة اخفاء البيانات في ملفات معينة هناك عدة نقاط يجب ملاحظتها لكي تتم عملية الاخفاء بصورة جيدة فمثلاًعند أخفاء البيانات في ملفات الصور يجب ملاحظة النقاط الاتية :

- يتم اختيار نوع من الملفات بحيث يكون أي تغيير فيها واضح قدر الامكان .

- النص المدخل غيرمحدد أي انه مفتوح على ان ينتهي بعلامة مميزة .
- المفتاح المستخدم هو مجموعة من الحروف غير محددة العدد على ان تكون منتهية بعلامة مميزة . ويستفاد منها بعدم خزن ثنائيات النص المطلوب إخفائها في ملف الصور بالتسلسل، وذلك لضمان عدم قدرة الشخص المقابل بالعثور عليها بشكل مباشر .
يتم استخدام اسلوب قراءة Pixel (أي 4 بايت في آن واحد) فاذا كان رقم المفتاح 1 تتم عملية الاخفاء فيها واذا كان صفر لا تقوم بالاخفاء فيها وانما تقوم بتحقيق طفرة عشوائية تحدد من 1 الى 4 نقاط صورية مثلاً .
العمليات المستخدمة في اخفاء واظهار النص وكما يأتي :

- **الاخفاء:** تبدأ العملية بالسؤال عن اسم الملف للصورة التي يراد ان تخفي فيها البيانات والملف الناتج عن عملية الاخفاء ثم يسأل عن مفتاح العملية وتحديد فيما اذا كان المطلوب الاخفاء ام الاظهار ومن ثم يتم ادخال النص المراد اخفائه في الصورة .
- **الاظهار** : تبدأ العملية بالسؤال عن الملف او الصورة التي يوجد فيها الاخفاء وعن الملف الذي نريد ان نضع النتيجة فيه ثم يسأل عن مفتاح العملية وتحديد فيما اذا كانت العملية اخفاء او اظهار وثم يطبع النص المدخل سابقاً واظهاره على شاشة الحاسبة .

التعامل مع المفاتيح : يتم تحويل النص المدخل او الحروف المدخلة كمفتاح الى ثنائية وتنزل في مصفوفة ذات بعد واحد وهناك مؤشر يتحرك عليها بالتتابع فاذا كانت تحتوي واحد فيعني ان تتم عملية الاخفاء لثنائية واحدة من النص والعكس اذا كانت عملية اظهار فهذا يعني ان البايت تمت معالجته والصورة تحوي ثنائية مخفية .

الاستنتاجات والتوصيات

تعد المعلومات اداة مهمة في تنظيم المعارف البشرية ، ويعد علم المعلومات احد الادوات المهمة لحل المشاكل المعقدة . وقد وفرت الكتابة بالشيفرة سرية المعلومات المرسلة عبر قنوات الاتصالات ، حيث كان بالامكان استراق السمع واعتراض الرسائل ممكناً .

وقد وفرت عملية اخفاء المعلومات ضمن ملفات معينة فرصة اكبر لحماية المعلومات والحفاظ على سريتها ومن اجل المحافظة على سرية ودقة المعلومات بصورة افضل من الممكن تطوير عمليات الاخفاء المعروضة في هذه الدراسة للوصول الى المستوى المطلوب .

ان التقدم الحاصل في علم الحاسبات الالكترونية اليوم يقابله ايضاً زيادة في خبرة المتسللين على شبكات المعلومات وانتهاك أمنها . لذلك ظهرت العديد من الطرائق المهمة للمحافظة على سرية وامن المعلومات المنقولة عبر الشبكات ومن هذه الطرائق عمليات تشفير واخفاء المعلومات ضمن ملفات مختلفة منها ملفات صوتية او صورية او ملفات معلومات وقد تم اعطاء شرح موجز لهذه الطرائق ضمن هذه الدراسة .

المصادر

1. Sechneier , B.(1996) Applied cryptography , protocols , algorithms and source code in C ,John Wily and Sons , Inc .U.S.A.

2. اندرية غلام (1999) " التشفير" ، كتاب " التدقيق والامان والرقابة في ظل استخدام الحاسبات الالكترونية " صدار اتحاد المصارف العربية ، الطبعة الثالثة /ص243-261.

3. د. راسم سميح عبد الرحيم(1997) " الاستثمار في التكنولوجيا " كتاب " الصناعة لمصرفية العربية في عالم المعلوماتية والاتصالات الحديثة " ، اصدار اتحاد المصارف العربي .

4. داود سلمان يعقوب (2001) امن المعلومات المخزونة والمنقولة عبر الحاسبات الالكترونية بحث دبلوم عالي / المعهد العالي للتطوير الامني و الاداري بغداد ، ص16.س

5. د. سلوى انور طه (1990) ، امنية البيانات / المركز القومي للحاسبات ، بغداد ص25-27 .

6. سعد علي حماد (1999) امن الحاسبة الالكترونية – بحث دبلوم عالي / المعهد العالي للتطور الامني الاداري–ص14 .

IBN AL- HAITHAM J. FOR PURE & APPL. SCI. VOL.18 (4) 2005

Information Security Study for Information Hiding in Electronic Computers

H. J. Muhasin
Department of Computer Science, College of Education, Ibn Al-Haitham, University of Baghdad

Abstract

Cryptographic technologies are nowadays widely recognized as the essential tool for security and trust in electronic communication. The research produces some important methods to hide information like this hide secret messages in other messages, graphic images and sound files.