

فن الاخفاء

مقدمة :

الرسائل غير المرئية أو المخفية أو المغطاة كلها تصب في نفس المعنى في عالم التكنولوجيا "ستيجنوجرافي". حيث لا يعلم عن وجود الرسالة إلا المرسل والمستقبل، والرسالة نفسها تبدو بصورة أخرى. وبالرجوع إلى اللغة اليونانية القديمة، نستطيع أن نترجم هذه الكلمة إلى "فن إخفاء الكتابة".

هذا المفهوم تم استخدامه وتطبيقه منذ مئات السنين، حيث كان الملوك والأمراء القدامى يستخدمون العبيد لكتابة الرسائل على ظهورهم. أو كانوا يخلقوا رؤوسهم ثم يكتبوا عليها. كما كانت تستخدم الحيوانات لهذا الغرض أيضا. وبعد ذلك، ظهر الحبر الخفي في الصورة وأصبح وسيلة إخفاء الكتابة الجديد. وعند ظهور نهضة الحاسبات والتكنولوجيا، دخل فإ الإخفاء إلى عصر جديد ممكن أن يطلق عليه بالعصر الرقمي.

وبأخذ نظرة دقيقة لهذه العملية نستطيع أن نفصل عناصرها. حيث هناك الغطاء أو الحامل، وهو ما يتم إخفاء الرسالة فيه، ويكون غالبا صورة أو مقطع صوتي أو فيديو. وهناك الرسالة نفسها، وممكن أن تكون من أي نوع. وهناك أيضا مفتاح الإخفاء، وهو المستخدم في الإخفاء نفسه، ولا يعلمه إلا المرسل والمستقبل.

فن إخفاء الكتابة والتشفير :

يخطئ كثير من الناس عندما يعتبرون أن التشفير (Cryptography) وإخفاء الكتابة هما نفس الشيء. فبأخذ نظرة دقيقة وتقنية نرى أن التشفير هو دراسة لطرق إرسال الرسالة بصورة أخرى لا يستطيع فك رموزها إلا المرسل والمستقبل. وهذا يختلف عن فن الإخفاء حيث أن التشفير يغير من هيئة محتوى الرسالة

لكنه لا يخفي وجودها. أما إخفاء الكتابة فيخفي وجود الرسالة من الأساس. يمكن تقسيم أساليب فن التشفير إلى:

- **أساليب تحويل الكتابة:** وتبنى إما على مبدأ الإبدال، أي يتم تحويل كل عنصر من الرسالة إلى عنصر آخر. ومبدأ النقل، وفيه يتم إعادة ترتيب حروف الرسالة.

- **أساليب معالجة الكتابة:** حيث يتم تقسيم الرسالة إلى قطع، وإدخالها على عملية تعالج هذه القطع باستخدام خوارزميات رياضية.

أساليب الإخفاء :

تتمحور فكرة الإخفاء في إدخال الرسالة ر داخل الغطاء غ لتكوين الهدف المخفي. ويمكن تمثيله بهذه المعادلة:
الهدف المخفي = الرسالة المراد إخفاءها + الغطاء + مفتاح الإخفاء

وبشكل عام، يكن تقسيم أساليب الإخفاء إلى أربعة أساليب أساسية:

١- الإخفاء النصي:

ويكون ذلك بكتابة نص يمكن استخلاص الرسالة المخفية منه. إما بطريقة نصية بان يكون أول حرف من كل كلمة يمثل حرف من الرسالة المخفأة. أو بطريقة نحوية أو لفظية.

٢- الإخفاء الصوتي:

إخفاء رسالة داخل إشارة صوتية ممكن أن يكون في مجال الزمن أو مجال الطيف. ويتم بإحدى الطرق التالية:
- **ترميز البت المنخفض:** هذه الطريقة لها سعة إدخال عالية (٤١,٠٠٠ bps). لكنها عرضة للاكتشاف. وفيها يتم إبدال

أكثر بت غير مهم (Least Significant Bit) من كل إشارة صوتية

- **الطيف الممتد:** يتم فيها إدخال الرسالة داخل الترددات الأعلى من اللازم. وتعتبر أكثر طريقة من ناحية الإخفاء لكن سعة الإدخال فيها منخفضة (٤ bps)

- **تغطية الإدراك:** هي أكثر طريقة من ناحية سعة الإدخال (٤٥٠,٠٠٠ bps) لكنها أكثرها عرضة للاكتشاف. ويتم فيها إدخال نص الرسالة داخل مناطق لا يمكن للإنسان إدراكها من الإشارة الضوئية.

٣- **الإخفاء الفيديوي:** مشتق من الإخفاء بالصور حيث أن مقاطع الفيديو ليست إلا مجموعة من الصور المتتالية. لذلك فإننا نستطيع تطبيق أساليب الإخفاء الصوري.

٤- **الإخفاء الصوري:** هو أكثر طريقة تمت دراستها من قبل الباحثين. توجد عدة طرق لإدخال رسائل في صور .

كان هذا مقدمه عن الاخفاء او فن الاخفاء

تم استخدام اخفاء البيانات او النصوص في

العمليات السرية

كما انه يستخدم في الجامعات للتواصل بين
الطلاب دون معرفة المشرف او المراقب * _ ٨
في وقت الاختبار او وقت المحاضرات في
المعامل الالكترونية او الاختبارات الالكترونية او
في نظام البلاك بورد الذي تم تطبيقه مؤخرا في
جامعاتنا السعودية (الملك خالد ,الملك سعود)
قمت بتصميم خوارزمية بسيطة وقام
صديقي أدهم ببرمجة اداة او برنامج لها

هذا فيديو يتكلم عن طريقة استخدام الاداة وكيف
يكون اخفاء الملفات داخل صورة ٨_ ٨

http://www.youtube.com/watch?v=kLSIOC_2c-Q

المراجع :

- Stinson* "Cryptography: theory and practice"
- *Huaiqing Wang, Shuozhong Wang* Communications of the ACM " Cyber warfare: steganography vs. steganalysis " <http://www.acmqueue.com>
 - *Neil F. Johnson, Zoran Duric, Sushil Jajodia*, Center for Secure Information Systems George Mason University "Information Hiding: Steganography and Watermarking – Attacks and Countermeasures"
 - *Gary C. Kessler* Associate Professor Computer and Digital Forensics Program Champlain College Burlington " An Overview of Steganography for the Computer Forensics Examiner"
 - Curran, K. and Bailey, K. "An Evaluation of Image Based Steganography Methods." *Int. J. of Digital Evidence*, Fall 2003.
 - <http://en.wikipedia.org>

كتب بواسطة

Xss mAn

Email :4bdull4h@w.cn

Group : T-T34M

هذا الكتاب اهداء الى كل من :

THE INJECTOR , <http://sec4ever.com>, العقل المفكر