المقالات العلمية

All about certificates

الكاتب : حسن علي التريكي
المراجع: خالد الرويلي

ماجد الربيعان

النسخة: الأولى

تنبيه:
تعتبر هذه المقالة مشاركة من كاتبها في زيادة التوعية والمحتوى الخاص بأمن المعلومات، وقد راجعها مراجع واحد على الأقل، ولا يتحمل مركز التميز لأمن المعلومات أي تبعات لهذه المقالة، ولا أي معلومات تطرح في هذه المقالة ولايضمن دقة المعلومة وصحتها.

الشهادات الرقمية (certificate) :

تعريف الشهادة الرقمية : هي وثيقة رقمية تحتوي على مجموعة من المعلومات التي تقود إلى التحقق من هوية الشخص أو المنظمة أو الموقع الإلكتروني و تشفر المعلومات التي يحويها جهاز الخادم (server) عبر ما يسمى بتقنية (SSL Layer securS sockecS).

يمكننا تشبيه الشهادة الرقمية بجواز سفر أو وثائق اعتماد رقمية تتم أثناء الاتصال بين الخادم(server) و العميل (client) فحينما يريد العميل ارسال معلومات تتصف بالسرية أو الحساسية يقوم متصفح الانترنت و بشكل آلي بالدخول إلى جهاز خادم (server) خاص للتأكد من هوية الجهة التي يرغب في إرسال المعلومات إليها و التالي يضمن الحصول على قناة اتصال آمنة .

ماهي محتويات الشهادة الرقمية ؟

تحتوي الشهادة الرقمية على العديد من المعلومات و لكن من أهم تلك المعلومات ما يلي :

- اسم مالك الشهادةالرقمية (سواء أكان شخص أم شركة) (certificate 'name sholder)
- الرقم التسلسلي للشهادة الرقمية بالإضافة إلى تاريخ انتهاء صلاحيتها(serial expiration and number)
- نسخة من المفتاح العام لمالك الشهادة الرقمية (public key)
- التوقيع الإلكتروني للجهة التي أصدرت الشهادة الرقمية (digital CA of signature)

كيفية الحصول على شهادة رقمية :

لابد من عمل طلب توقيع الكتروني للشهادة الرقمية من إحدى الجهات الموثوقة و المتخصصة في إصدار الشهادات الرقمية و هو ما يسمى باللغة الانجليزية (CSR Request Signing Certificate).

المفتاح العام (key public) و المفتاح الخاص (ey privatek) :

عند طلب توقيع للشهادة الالكترونية (CSR) يقوم جهاز الخادم بإصدار مفتاحين و حيدين على مستوى العالم أحدهما عام و الآخر خاص .

وأما المفتاح العام فيدرج ضمن الشهادة الرقمية و يكون متاحا للجميع و يستخدم لتشفير الرسائل(messages) المرسلة إلى مالك الشهادة الرقمية.

أما المفتاح الخاص فيخزن في جهاز الكمبيوتر (local computer) و يستخدم لفك التشفير عن الرسائل المستقبلة و لعمل اتصال آمن بواسطة قناة اتصال مشفرة يقوم برنامج المتصفح (web browser) بارسال طلب إلى الجهاز الخادم (server web) للتأكد و الربط بين المفتاح الخاص و الشهادة الرقمية للمرسل.و من المهم أن نذكر أيضا بأن الجهاز الخادم هو الوحيد الذي يملك صلاحية الدخول للمفتاح الخاص و هو الوحيد القادر على فك تشفير المعلومات المرسلة عبر قناة الاتصال المشفرة .

عمل اتصال الكتروني آمن(كيفية عمل (SSL)) :

يتم الحصول على قناة اتصال آمنة و مشفرة عبر ما يسمى بعملية المصافحة (handshake) و هذه العملية تتم بالطريقة التالية :

١. عند محاولة الوصول إلى موقع إلكتروني يستخدم قناة الكترونية مشفرة باستخدام تقنية (SSL) فإن برنامج المتصفح للجهاز الزائر يطلب من جهاز الخادم "جلسة" (secure session) آمنة.
٢. يستجيب الجهاز الخادم للطلب و يرسل شهادته الرقمية للجهاز الزائر.
٣. يقوم برنامج المتصفح للجهاز الزائر بالتأكد من الشهادة الرقمية عبر الاتصال بجهة متخصصة في اصدار و توثيق الشهادات الرقمية بشرط أن يثق بهذه الجهة.
٤. إذا تأكد برنامج المتصفح من هوية الجهاز الخادم و أن الشهادة الرقمية ترتبط به فعلا و أن الشهادة الرقمية لاتزال سارية المفعول يقوم برنامج المتصفح بإنتاج مفتاح لهذه "الجلسة" و يقوم بتشفيره بالمفتاح العام للجهاز الخادم و يرسله إليه.
٥. يقوم الجهاز الخادم بفك التشفير عن " مفتاح الجلسة " باستخدام مفتاحه الخاص.
٦. بهذا تكون عملية المصافحة قد انتهت و حصل اتصال آمن بين المرسل و المستقبل

٧. يظهر رمز على شكل قفل في برنامج المتصفح (status bar) يبين أن هناك اتصال آمن و مشفر بين الطرفين.

عمليات الاصطياد (phishing) و كيف يمكن الوقاية منها باستخدام الشهادة الرقمية :

يلجأ مجرمو الانترنت عادة إلى سرقة أو نشر معلومات شخصية أو تتصف بالسرية من خلال ايهام الناس بأن الموقع الالكتروني الذي يستخدمونه هو موقع رسمي و موثوق كمواقع البنوك و غيرها و هذا ما يعرف بعملية الاصطياد حيث يظن المستخدم العادي بأن هذه المواقع هي مواقع مضمونة فيستجيب لطلب إدخال رقم بطاقته الائتمانية أو الرقم السري له .

و لكن يمكن الحماية من مثل تلك عمليات من خلال استخدام الشهادة الرقمية و يمكن للمستخدم العادي التنبه لعمليات الاحتيال هذه بالطرق التالية :

- لايوجد رمز القفل في برنامج المتصفح مما يدل على أن الاتصال غير آمن و أن عملية المصافحة لم تتم
- عدم تطابق الأسماء : إذا حاول المهاجم استخدام شهادة رقمية تعود إلى جهة أخرى فإن المتصفح سينذر المستخدم بعدم تطابق الشهادة الرقمية مع الموقع الالكتروني أو الجهة التي يحاول زيارتها.
- عدم موثوقية الجهة التي أصدرت الشهادة الرقمية : عند محاولة المهاجم استخدام شهادة رقمية تم اصدارها من جهة مجهولة فإن برنامج المتصفح سينذر المستخدم بأن الشركة أو الجهة التي أصدرت الشهادة الرقمية غير موثوقة.

مثال على عمليات الاصطياد :

الشكل التالي يبين رسالة من المهاجم يوهم المستخدمين بأنه يمثل قسم أمن المعلومات في موقع بيع الكتب العالمي "(www.amazon.com)" .تقول الرسالة بأن حساب المستخدم قد تم ايقافه مؤقتا لحين عمل تحديث للبيانات الشخصية

و في حالة عدم تحديث البيانات فإنه سوف يتم إلغاء الحساب نهائيا.

Date: Tue, 29 Nov 2005 17:17:04 -0500
To: ggr@qualcomm.com
Subject: Reactivate Your Account!
From: "service@amazon.com" <service@amazon.com>

Amazon.com

Dear Amazon member,

We regret to inform you that your Amazon account was been suspended for a period of 3-4 days,after that it will be terminated.

Your credit card on file with Amazon
Card number: XXXX-XXXX-XXXX-XXXX (Not shown for security purposes) Expiration date: XX/XX

Please sign in to your Amazon account and update your billing information:

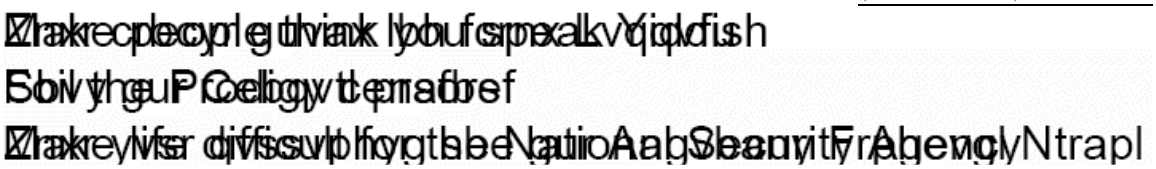
http://www.amazon.com/gp/css/homepage.html

If your account information is not update, your account on Amazon will be terminated.

Thank you for your time!
Amazon Security Departament

مقارنة بسيطة بين حماية المعلومات بالتشفير و بين حماية المعلومات بالشهادة الرقمية :

- أولا :التشفير (encryption)



عيوبه :

انتشار المعلومة السرية.

كثرة المفاتيح الواجب حمايتها.

صعوبة تبادل المفاتيح.

لاتصلح لعملية التوقيع الإلكتروني.

ميزة :

غالبا يستخدم خوارزمية سريعة.

- ثانيا : الشهادة الرقمية :

مميزاته :

صنع مفاتيح خاصة بكل شخص.

لكل شخص مفتاحين.

أحد المفاتيح متاح للجميع.

تصلح لعملية التوقيع الإلكتروني

عيب :

خوارزمية بطيئة

References:.

- www.scteachers.org
- www.ibiblio.org
- www.cfp٢٠٠٠.org
- www.usenix.org
- www.rotary.org