بسم الله الرحمن الرحيم

جامعة الملك سعود
كلية علوم الحاسب و المعلومات
قسم نظم المعلومات

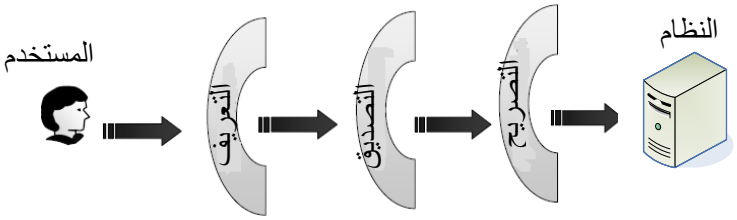
التعريف ، التصديق ، التصريح
Identification, Authentication, Authorization (IAA)

إعداد : م. سليمان بن هيشة

إشراف: د. خالد الغثبر

مقدمة

إن أنظمة تقنية المعلومات و البيانات التي تخزنها و تعالجها تعتبر من الموارد المهمة التي يجب حمايتها. المقدرة على تعريف هوية المستخدم (Identification) هي واحدة من الخطوات الأولى لحماية أنظمة تقنية المعلومات ، فلا تكون الأنظمة مفتوحة لكل من أراد الاتصال بها، والتعرف على المستخدم يكون بتزويد المستخدم عن معرفه عند طلب النظام كاسم المستخدم على سبيل المثال ، يأتي بعد ذلك التصديق من هوية المستخدم (Authentication) بأنه مسجل في النظام، و أخيرا تصريح المستخدم (Authorization) للاتصال بالنظام.



نقطتان مهمتان يجدر الأشارة لهما، الأولى وهي غالبا مايقال التصديق عند قصد التعريف أو التصريح ، و الثانية هي أنه بالإمكان عمل التصديق بدون التعريف بحيث تتم عملية التعريف آليا بدون علم المستخدم.

التصديق

وهي عملية اثبات الشخصية المزودة من قبل المستخدم، مثال: هل أنت سليمان؟، و بالإمكان تصنيفها إلى ثلاث مجموعات رئيسة:

- ماذا تعرف، مثل كلمة المرور.
- ماذا تملك، مثل مفتاح أو بطاقة.
- من أنت، مثل البصمة.

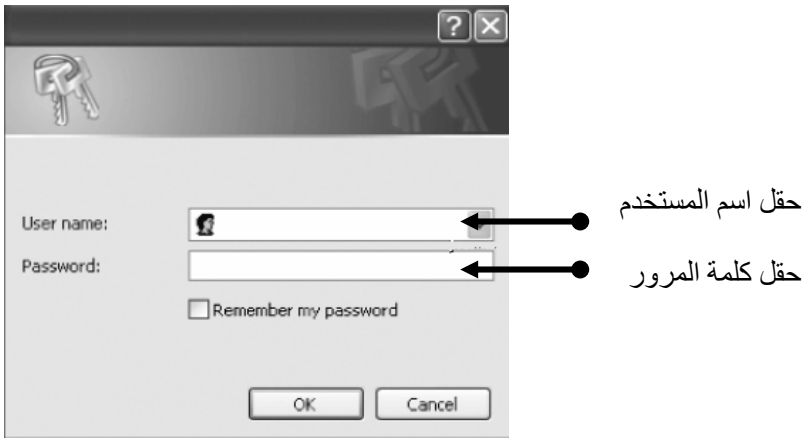
التصديق القوي

وهو استخدام طريقتين من الطرق الثلاث للتصديق.

أنواع التصديق

- **اسم المستخدم و كلمة المرور** (ماذا تعرف)

يعتبر هذا النوع من أضعف أنواع التصديق. ويجدر الإشارة هنا إلي مصطلح الدخول الواحد (Single-Sign-On) و هو الدخول لعدة أنظمة بحساب واحد معرف من جهة مركزية ، وتأتي هذه الطريقة لحل مشكلة أن يكون للمستخدم حساب مختلف لكل نظام، و من الأمثلة لهذه الطريقة هو حساب .NET و المقدم من مايكروسوفت.



- **جهاز التصديق** *(ماذا تملك)*

هو جهاز أمني يتم تصديق المستخدم عن طريق أذونات مناسبة مدمجة في الجهاز، و منها البطاقات الذكية.


في الصورة الأولى نوع من الأجهزة تظهر عليها أرقام ، هذه الأرقام تتغير آليا، يقوم المستخدم بتزويد هذه الأرقام للنظام عند طلب الاتصال كمعرف للمستخدم ، والنوع الثاني من الأجهزة في الصورة الأولى أيضا هي أجهزة يتم الحاقها بجهاز الحاسب و بها تتم عملية تصديق اتصال المستخدم آليا. في الصورة الثانية نوع آخر و هي بطاقات للتصديق تصدر ترددات راديو منخفضة قصيرة المدى.

في الصورة الثالثة تظهر البطاقة الذكية وهي نوع آخر من أجهزة التصديق المحمولة تحوي بداخلها على معالج ومنافذ إدخال وإخراج و ذاكرة ثابتة تتصل بالمعالج فقط ، هذا النوع من البطاقات قادر على توليد مفاتيح تصديق قوية ومتغيرة.

- **الصفات البشرية** *(من أنت)*

وهي استخدام الخصائص الفردية البشرية لتصديق المستخدم.

الخصائص البشرية الممكن استخدامها للتصديق تشمل:

- البصمة
- الوجه
- التوقيع
- طريقة الضغط على المفاتيح
- الصوت
- هندسية اليد
- القزحية، العين
- الشبكية، العين
- المسح لليد

عيوب هذا النوع يشمل:

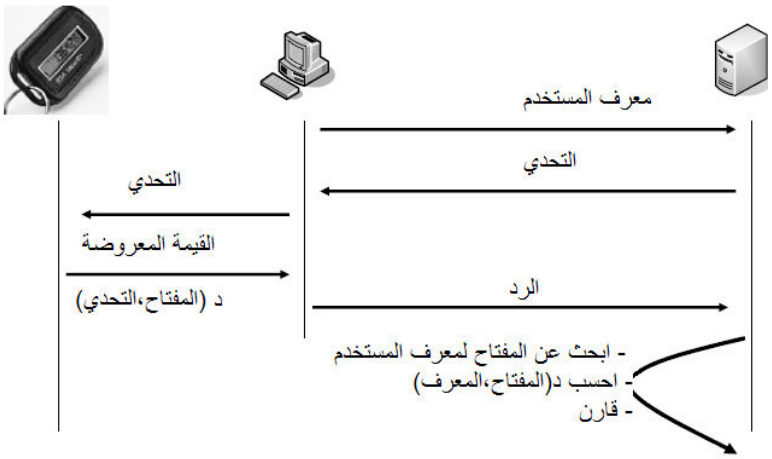
- ارتفاع ثمن تطبيقها
- صعوبة تطبيقها
- بعض الأحيان غير دقيقة
- احتمالية تكرار الصفات البشرية


في الصورة الأولى تظهر فأرة مدمج بها جهاز البصمة، وفي الصورة الثانية جهاز للبصمة.

- **الشهادات**

الشهادة تمكن النظام من التحقق عن طريق ربط المستخدم بمفتاح معلوم للنظام. هذه الشهادة الرقمية تصدرمن جهه شهادات مصرحة.

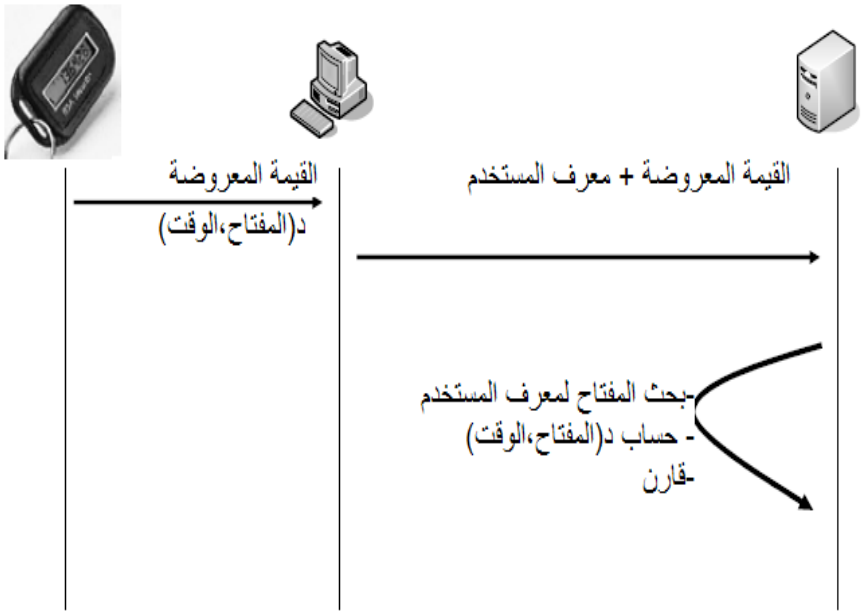
- **رد التحدي**
  - ***الطريقة الأولى:***



في هذه الصورة سلسلة من الخطوات لتصديق المستخدم طالب الاتصال، وهي:

1. يرسل المستخدم المعرف لطلب الاتصال بالخادم
2. يرد الخادم بقيمة متغيرة (التحدي)
3. يقوم المستخدم بادخال قيمة التحدي في جهاز التصديق عن طريق لوحة مفاتيح مزودة من جهاز التصديق
4. يقوم جهاز التصديق بعملية حسابية على قيمة التحدي المدخلة و المفتاح للمستخدم
5. تعرض نتيجة العملية الحسابية على شاشة جهاز التصديق
6. يقوم المستخدم بإرسال القيمة إلى الخادم (الرد)
7. يقوم الخادم بعد استقبال الرد بعدةخطوات:
   2.1 البحث عن المفتاح لمعرف المستخدم (نفسه الموجود في جهاز التصديق)
   2.2 يقوم بالعملية الحسابية على المفتاح و قيمة التحدي
   2.3 مقارنة الناتج بالقيمة المرسلة من قبل المستخدم ، إذاكانت متساوية ستتم عملية التصديق ، غير ذلك رفض طلب الاتصال.

  - ***الطريقة الثانية:***



في هذه الطريقة يكون الوقت متزامن بين جهاز التحقق و الخادم، يقوم جهاز التحقق بعملية حسابية على الوقت و المفتاح للمستخدم و يعرض النتيجة. سلسلة من الخطوات لتصديق المستخدم طالب الاتصال، وهي:

1. يرسل المستخدم المعرف لطلب الاتصال بالخادم مع القيمة المعروضة على جهاز التحقق
2. يقوم الخادم بعد استقبال الرد بعدةخطوات:
   2.4 البحث عن المفتاح لمعرف المستخدم (نفسه الموجود في جهاز التصديق)
   2.5 يقوم بالعملية الحسابية على المفتاح والوقت
   2.6 مقارنة الناتج بالقيمة المرسلة من قبل المستخدم ، إذاكانت متساوية ستتم عملية التصديق ، غير ذلك رفض طلب الاتصال.

عيب واحد لهذا النوع وهو أن قواعد بيانات المفاتيح في الخوادم ستكون حساسة جدا.

- **التصديق ثنائي الاتجاه**

وهو أن يقوم كل من العميل والخادم بتصديق بعضهم البعض و هو أقوى من التصديق أحادي الاتجاه عندما يقوم الخادم فقط بعملية التصديق للعميل.

ويمكن استخدام هذا النوع لمنع انتحال شخصية الخادم من قبل طرف ثالث عند التخاطب مع العميل.

- **التصديق متعدد الطرق**

وهو شبيه بالتصديق القوي. وهذا النوع موصى به بشدة في عملية التحقيق لمستخدمي الهواتف المحمولة عند شرائهم للخدمات والسلع عن طريقها.

التصريح (تحكم الاتصال بالأنظمة)

تخزن قيود اتصال المستخدمين بالانظمة في قائمة تحكم الاتصال (ACL)، وهي عبارة عن جدول موجود في نظام التشغيل. حقوق الاتصال في هذا الجدول مسجلة على تركيب معين وهو لكل فاعل (subject) -كالمستخدم أو جهاز- مسموح له الاتصال بشيء (object) في النظام –كملف أو مجلد-.

تتكون قائمة تحكم الاتصال في نظام التشغيل مايكروسوفت ويندوز من عناصر ممكن أن تكون لمستخدمين أو مجموعات.

الحقوق الموروثة

وهو أن يرث المستخدم قائمة تحكم الاتصال من المجموعة التي ينتمي إليها.

في هذه الصورة تظهر خصائص الاتصال بالمجلد "wireless web" ، في الجزء الأعلى اسماء المجموعات و المستخدمين و في الجزء الأسفل أذونات الاتصال لكل مستخدم أو مجموعة.

خاتمة

كما رأينا في هذه المقالة فإنه لابد من تنظيم عند طلب الاتصال بتعريف المستخدم و التحقق من هويته و تقييد الاتصال بالأشياء المصرحة له فقط من خلال قائمة تحكم الاتصال و بهذا نحقق الحماية للجهاز وللموارد داخل الجهاز.

المراجع

- M. Ciampa, "Security+ Guide to Networking Security Fundamentals", Second Edition, Thomson Course Technology, 2004.
- Nixu Ltd., "Identification, Authentication, Authorizing", http://www.tml.hut.fi/Opinnot/T-110.402/2003/Luennot/titu20031017.pdf.
- NIST Computer Security Handbook, " Identification and Authentication ", http://security.isu.edu/pdf/nistiadraft.pdf.
- PSCIOC/PSSDC Cross-Jurisdictional, "Identification, Authentication and Authorization Working Group", http://www.iccs-isac.org/eng/pubs/IAA_guidelines.pdf.
- J. Vollbrecht et al, "AAA Authorization Framework", http://www.faqs.org/rfcs/rfc2904.html.
- Digital IDs: The New Advantage, http://www.verisign.com/repository/clientauth/clientauth.html.
- Token-Based Authentication, http://developer.novell.com/research/appnotes/1999/november/01/03.htm.