الفهرس

1- مقدمة

من المعلوم أن التحقق من هوية المستخدم يعتبر أحد أهداف امن المعلومات وذلك عند الدخول إلى أنظمة الكمبيوتر وقواعد البيانات ومواقع المعلوماتية وعموما فإنه يمكن عمل ذلك من خلال العديد من الوسائل ، هذه الوسائل هي مجموعة من الآليات والإجراءات والأدوات والمنتجات التي تستخدم للوقاية من أو تقليل المخاطر والتهديدات التي تتعرض لها الكمبيوترات والشبكات وبالعموم نظم المعلومات وقواعدها كما أنها متعددة من حيث الطبيعة والغرض . ومن ذلك مجموعة وسائل الأمن المتعلقة بالتعريف بشخص المستخدم وموثوقية الاستخدام ومشروعيته Identification and authentication ، وهي الوسائل التي تهدف إلى ضمان استخدام النظام أو الشبكة من قبل الشخص المخول بهذا الاستخدام ، وتضم هذه الطائفة كلمات السر بأنواعها ، والبطاقات الذكية المستخدمة للتعريف ، ووسائل التعريف البيولوجية التي تعتمد على سمات معينة في شخص المستخدم متصلة ببنائه البيولوجي ، ومختلف أنواع المنتجات التي تزود كلمات سر آنية أو وقتية متغيرة الكترونيا ، والمفاتيح المشفرة ، بل تضم هذه الطائفة ما يعرف بالأقفال الإلكترونية التي تحدد مناطق النفاذ
ووسائل التعريف تختلف تبعا للتقنية المستخدمة ، وهي نفسها وسائل أمن الوصول إلى المعلومات أو الخدمات في قطاعات استخدام النظم أو الشبكات أو قطاعات الأعمال الإلكترونية ، وبشكل عام ، فان هذه الوسائل تتوزع إلى ثلاثة أنواع :-

1 - شئ ما يملكه الشخص مثل البطاقة البلاستيكية أو غير ذلك .
2 – شئ ما يعرفه الشخص مثل كلمات السر أو الرمز أو الرقم الشخصي غير ذلك
3– شيء ما يرتبط بذات الشخص أو موجود فيه مثل بصمة الإصبع أو بصمة العين والصوت وغيرها .

وتعد وسائل التعريف والتوثق الأقوى ، تلك الوسائل التي تجمع بين هذه الوسائل جميعا على نحو لا يؤثر على سهولة التعريف وفعاليته في ذات الوقت . وأيا كانت وسيلة التعريف التي سيستتبعها توثق من قبل النظام ، فإنها بذاتها وبما ستصل باستخدامها تخضع لنظام أمن وإرشادات أمنية يتعين مراعاتها ، فكلمات السر على سبيل المثال ، وهي الأكثر شيوعا من غيرها من النظم ، تتطلب أن تخضع لسياسة مدروسة من حيث طولها ومكوناتها والابتعاد عن تلك الكلمات التي يسهل تخمينها أو تحريها وكذلك خضوع الاستخدام لقواعد عدم الإطلاع وعدم الإفشاء والحفاظ عليها .

2- أجهزة التحقق (Two-Factor Authentication Devices)

يوجد عدد من الأدوات والتقنيات من مختلف المزودين توفر التحقق من هوية المستخدم بعاملين ، هذه الحلول تختلف فيما بينها من حيث الأمنية
والتكلفة وسهولة الاستخدام .
إضافة إلى الأجهزة المستخدم فإن المنظمة بحاجة إلى برمجيات على الخادم (Server) لفك الرموز والتعرف على الجهاز .
كما يطرح بعض المزودين نظامي (SDK) أو(API) والخاصة بالربط مع موقع المنظمة على الانترنت ، ويطرح آخرون (Authentication Servers) المستخدم للتحقق وإدارة الأدوات ، بعض هذه الخوادم تدعم أجهزة خاصة بمزودين معينين بينما هذه الأجهزة تدعم رموز من عدد من المزودين ، هذه البرامج تتيح للمنظمة حرية ومرونة اختيار الأجهزة أو المقارنة بينها .
ومتى ما استخدمت وسائل تعريف ملائمة لإتاحة الوصول للنظام ، ومتى ما تحققت عملية التوثق والمطابقة والتأكد من صحة التعريف (الهوية) فان المرحلة التي تلي ذلك هي تحديد نطاق الاستخدام (Authorization) وهو ما يعرف بالتخويل أو التصريح باستخدام قطاع ما من المعلومات في النظام ، وهذه المسالة تتصل بالتحكم بالدخول أو التحكم بالوصول إلى المعلومات أو أجزاء النظام (Access Control) system .
وفي التطبيقات الأكثر حساسية, مثل البنوك قد يكون مطلوب أكثر من كلمة سر أو شفرة لتوثيق ونقل الأموال من بنك إلي آخر أو من حساب إلى آخر. ويعيب هذه الطريقة أن على المستخدم أن يتذكر أو يكتب في مكان ما كل كلمات السر المتعددة, وكذلك عليه أن يحفظ ترتيب الدخول باستخدامها .
وهناك طريقة أخرى تخول للمستخدم الوصول إلى مستويات مختلفة من النظام مثل :
-1قراءة الملفات فقط .
-2الكتابة على الملفات .
-3تنفيذ الأوامر على الملف .
-4إلغاء الملفات .
ويعيب هذه الطريقة أيضا احتياجها لنظام مطابقة مركزي مما يتطلب سعة تخزينية كبيرة قد تزيد من احتمالات الاختراق. ومع الإمكانيات الأخرى للاختراق عبر البرمجيات كبيرة الحجم وعبر منافذ الشبكة الدولية فقد ظهرت طبقة التشفير

يوجد نوعين من أجهزة (Tow Factors Devices) :
1- Connected devices هي الأجهزة المرتبطة مباشرة مع نظام التحقق بواسطة وصلة مثل (USB, Bluetooth) وهذا النوع لا يحتاج كثيراً لتدخل المستخدم .
2

3- أنواع أجهزة التحقق (Type Of Two-Factor Authentication Devices)

وفيما يلي سنناقش عدد من هذه الأجهزة مع المقارنة فيما بينها بناء على عدد من العوامل .

4- أمثلة لأجهزة التحقق

1- Hardware One Time Password Generators

هذا الجهاز يعتبر مولد لكلمات المرور ويعرف بـ (OTP) ويعتبر من أكثر الأجهزة انتشارا على نحو واسع كما أنه رخيص وسهل الاستخدام .

يعتمد هذا الجهاز على خوارزميات لتوليد كلمات السر ويوجد منه نوعان :

1- A time-synchronous OTP والذي ينشئ رقم متغير بناءً على ساعة داخلية (مؤقت) متزامنة مع الخادم (Server).

2- A counter based OTP عداد داخلي يزيد كلما تم توليد رمز جديد وكذلك يكون متزامن مع الخادم (Server) .

2- Software Based One Time Password Generators

3- Terminal Profiling

4- TAN Lists

5- SMS Tokens

هذا النوع يستعمل كوسيط لتوليد عدد متغير يمكن استخدامه كعامل آخر للتحقق ويوجد منه نوعان :

– instant SMS tokens :

بحيث ترسل رسالة مباشرة عند التحقق بنجاح من هوية المستخدم ، ثم ينتظر المستخدم حتى يستلم الرقم المتغير لإتمام عملية التحقق .

- With batch SMS on the other hand :

بحيث يتسلم المستخدم قائمة من الأرقام المتغيرة المرتبط بحروف بحيث يقوم بإدخال الرقم المتغير إضافة إلى الحروف .

6- Smartcards and Chip Readers

تعتبر من أكثر الأنواع أمنية ويوجد منه نوعان :

– connected : يمكن أن يكون واجهة مباشرة مع المستخدم لكي يتم تبادل ما هو مشفر بينهما ، كما انه يحتاج برامج على الجهاز الخادم.

- unconnected : هذا النوع لا يحتاج واجهة يعمل المستخدم كوسيط بين الجهاز والخادم .

7- Chip Enabled USB

8- Virtual Keypads

5- مقارنة بين الأجهزة

6- المراجع

[1] http://www.computerweekly.com
[2] http://www.bbbonline.org
[3] http://www.computerworld.com
[4] http://www.phishspot.com
[5] http://news.com.com
[6] http://www.finextra.com

هذا البحث من إعداد الطالب / محمد بن عبد الله الشمراني
الرقم الجامعي/ 418001119 الماهـــــــــــــــــر