ISSN 2170-0796

تطور تقنيات المصادقة وتأثير علم المقاييس الحيوية عليه

سليمان يعقوب الفرا (Sliman Jakub El-Fara)
Technology University of Lodz

المصادقة – تعريف و نظرة عامة

المصادقة (باللغة الإنجليزية: Authentication) في علم الحاسوب هو إجراء يقر النظام بمقتضاه ولوج المستخدم الى النظام. مهمته الأساسية التحقق من هوية المستخدم الراغب بالدخول إلى النظام والإقرار بناءاً عليه بالسماح أو منع المستخدم من الدخول. في علم الحاسوب نجد عدة مصطلحات مترادفة تستخدم للتعبير عن هذه العملية منها الاستيقان، التوثيق، المصادقة، التصديق، الإقرار، الإبرام و الموافقة، والتي ترد في مراجع علوم الحاسوب بشكل متفاوت حاملةً نفس المعنى الذي يقابله باللغة الانجليزية المصطلح authentication. في هذا المقال سأقوم باستخدام مصطلح المصادقة.

طرق المصادقة

عملية **المصادقة** تتم عن طريق تحديد هوية المستخدم الراغب بالدخول إلى النظام، فيتم بناءاً على ذلك اتخاذ القرار بالسماح لدخول المستخدم إلى النظام، أو رفضه. وقد قام العلماء بإجراء العديد من الأبحاث لتطوير طرق إنجاز مصادقة المستخدم وتحديد هويته والتي يمكن جمعها في ثلاث مجموعات رئيسية، وهي:-إنجاز مصادقة المستخدم باستخدام شيء يعرفه المستخدم – عامل معرفة (مثل كلمة السر أورقم التعريف الشخصي)- إنجاز مصادقة المستخدم باستخدام شيء يمتلكه المستخدم – عامل ملكية (مثل بطاقة الدخول أو الهاتف الخلوي)-إنجاز مصادقة المستخدم باستخدام شئ يوجد في المستخدم – عامل حيوي (مثل بصمة الاصبع أو بصمة العين)

قد يحدث أن يتم استخدام عدة تقنيات معاً لزيادة أمن المصادقة.

آلية إجراء المصادقة : في معظم التطبيقات عملية المصادقة تتم ضمن ثلاث خطوات أساسية:

عرض الهوية (identification):في هذه الخطوة يقوم المستخدم بالإعلان عن هويته للجهة التي ستقوم بإجراء المصادقة.

أمثلة:

– عند اتصال مستخدم شركة الاتصالات بمركز خدمة العملاء يقوم المستخدم بتقديم اسمه ورقم الهاتف لموظف الشركة.

– عند قيام المستخدم بتسجيل الدخول إلى موقع التواصل الاجتماعي يقوم المستخدم بإدخال اسم الدخول (أو البريد الإلكتروني).

مصادقة المستخدم (authentication): هنا تقوم الجهة المقابلة للمستخدم (النظام) بالتأكد من هوية المستخدم المعلنة مسبقاً بإستخدام إحدى تقنيات الاستيقان المعروفة.

ISSN 2170-0796

أمثلة:

– عند اتصال مستخدم شركة الاتصالات بمركز خدمة العملاء بعد أن يقوم المستخدم بتقديم اسمه ورقم الهاتف يقوم موظف مركز خدمة العملاء بالتأكد من هوية المستخدم (إجراء المصادقة) عن طريق السؤال عن رقم الهوية، والذي يقابل هنا كلمة السر.

-عند قيام المستخدم بتسجيل الدخول إلى موقع التواصل الاجتماعي يقوم المستخدم بإدخال كلمة السر، التي تتيح للنظام امكانية مصادقة المستخدم من خلال التحقق من مطابقة كلمة السر للكلمة المحددة مسبقاً أثناء عملية التسجيل.

ترخيص / تفويض المستخدم (authorisation): بعد أن يتأكد النظام من هوية المستخدم يقوم في هذه الخطوة بإعطاءه صلاحيات محددة بناءاً على هويته حيث يتم تحديد الأمور التي يؤذن للمستخدم القيام بها. ضمن الصلاحيات يمكن تحديد نطاق المعلومات التي يمكن للمستخدم الوصول إليها، وكذلك الأمور التي يمكنه فعلها بهذه المعلومات.

أمثلة:

– في المثال المتعلق بمستخدم شركة الاتصالات تتاح للمستخدم امكانية السؤال عن فاتورة هاتفه حيث يقع ذلك ضمن صلاحياته، لكن ذات المستخدم لن يحصل على أي معلومات متعلقة بحسابات المشتركين الآخرين، حيث أنه لا يمتلك الترخيص / التفويض لذلك.

-في المثال المتعلق بمستخدم موقع التواصل الاجتماعي نجد المستخدم قادراً على متابعة مشاركات الأعضاء المضافين في قائمة أصدقائه، لكنه غير قادر على مشاهدة جميع بيانات المستخدمين غير المضافين في قائمة أصدقائه حيث أن هذا الأمر يخرج عن إطار صلاحياته.

المصادقة الثنائية (Two-factor authentication)

هي نوع من المصادقة تستخدم فيه أكثر من طريقة مصادقة واحدة في آن واحد بقصد زيادة الأمان. في هذا النوع من المصادقة يتم اختيار طرق المصادقة من بين مجموعتين مختلفتين من المجموعات الأساسية:

إنجاز مصادقة المستخدم باستخدام شيء يعرفه المستخدم (مثل كلمة السر أو رقم التعريف الشخصي)

إنجاز مصادقة المستخدم باستخدام شيء يمتلكه المستخدم (مثل بطاقة الدخول أو الهاتف الخلوي)

إنجاز مصادقة المستخدم باستخدام شئ يوجد في المستخدم (مثل بصمة الاصبع أو بصمة العين)

على سبيل المثال تقوم بعض شركات الأعمال التجارية بالدمج بين الطريقة الأولى والثانية، بحيث يقوم مستخدم الحساب بإجراء المصادقة باستخدام كلمة السر بالإضافة إلى استخدام هاتفه الخلوي بحيث يقوم بإعادة كتابة كلمة سرية تصله برسالة قصيرة على هاتفه الخلوي.في هذه الحالة نحصل على طريقة لإجراء المصادقة بشكل أكثر أماناً حيث يتطلب الدخول الحصول على شئ يعرفه المستخدم (كلمة السر) بالإضافة إلى شئ يستخدمه (هاتفه الخلوي).

من الأمثلة الأخرى على المصادقة الثنائية تلك المستخدمة في المختبرات الطبية الحديثة، حيث يقوم العامل بإدخال رقمه السري (مصادقة باستخدام شئ يعرفه المستخدم) ومن ثم يقوم بمسح بصمة العين (مصادقة باستخدام شئ يوجد في المستخدم). من أكبر المميزات لأنظمة المصادقة التنائية أنها تعطي أماناً أكبر، حيث أن عملية الإستيلاء على كلمة مرور المستخدم بالإضافة إلى هاتفه الخلوي أصعب من الإستيلاء على أحد الأمرين ما يجعلها تستخدم بكثرة في الأنظمة التي تطلب مقداراً كبيراً من الحماية والأمان. كلما كان مستوى الحماية والأمان المطلوبين للنظام أكبر، كلما وجدنا زيادة في طرق المصادقة المستخدمة. في بعض الأحيان قد تصل حماية النظام إلى درجة يطلب فيها من المستخدم إجراء عدة فحوص حيوية (كإجراء مسح بصمة الإصبع والعين) بالإضافة إلى إستخدام رقم التعريف الشخصي (PIN) وكلمة سر للاستخدام الواحد. ولكن مثل هذه الأنواع تبقى شكلاً من أشكال المصادقة الثنائية حيث أنها تستخدم طرق مصادقة من مجموعتين (العامل الحيوي والعامل المعرفي في هذه الحالة).

ISSN 2170-0796

أبرز أشكال المصادقة الحيوية في الوقت الحالي

اليوم أصبحت المصادقة منتشرة بشكل واسع في شتى مجالات الحياة التي دخلها علم الحاسوب بدءاً من المواقع الإلكترونية وحسابات الأجهزة الشخصية التي تستخدم كلمة السر للتحقق من هوية المستخدم والسماح له بتسجيل الدخول وانتهاءاً على أنظمة المصادقة في المختبرات العسكرية التي تستخدم بصمة العين للتحقق من هوية العاملين بها للسماح لهم بالدخول إلى المختبرات والوصول إلى المعلومات والأبحاث السرية، كلها أمثلة لتقنيات المصادقة التي أصبحت جزءاً من حياتنا. في هذا المقال سأتطرق إلى أشهر طرق المصادقة المستخدمة في الوقت الحالي، ومنها:

مصادقة كلمة السر (Password authentication):المصادقة باستخدام كلمة السر من الطرق الأكثر شيوعا واستخداماً، لكنها بالإضافة إلى ذلك الأقل أمناً ما يجعلها غير مناسبة للاستخدامات التي تطلب درجة عالية من الأمان.

عملية مصادقة كلمة السر تعتمد على أن المستخدم يقوم بتأكيد هويته من خلال إدخال مجموعة من الرموز، والتي قام بتزويد النظام بها مسبقاً عند أول عملية تسجيل، بحيث يقوم النظام بمقارنة الكلمة المدخلة مع تلك المخزونة لديه. تطابق الكلمتين في هذه الحالة يعني التحقق من هوية المستخدم والسماح له بالدخول.

هناك عدة عوامل تحدد درجة أمان كلمة السر منها: طول كلمة السر ونوع الحروف المستخدمة وفترة استخدام كلمة السر. مع أنه بإمكاننا زيادة أمان كلمة السر من خلال اختيار كلمات طويلة نسبياً ومتعددة في الحروف المستخدمة وتغييرها بشكل دوري إلا أن درجة الأمان تبقى غير كافية مثيرة بذلك قلق الشركات التى تطلب مقداراً عالياً من الأمان كالشركات المالية والتجارية.أحد أكبر سلبيات استخدام كلمة السر سهولة تعرضها للسرقة ما يمكن السارق من انتحال هوية المستخدم والإضرار به.مشاكل كلمة السر ساهمت بتوجه الشركات إلى استخدام طرق مصادقة أخرى، فأصبحت كلمة السر تستخدم في الأمور التي لا تطلب مستويات مرتفعة من الحماية والأمان، في حال أن الأمور الأكثر حاجة إلى الحماية تتطلب من المستخدم استخدام طريقة مصادقة أخرى.

رمز الأمان (Security token): يعتبر جهاز رمز الأمان من طرق المصادقة الملكية (التي تعتمد على شئ يمتلكه المستخدم). وهو عبارة عن جهاز الكتروني صغير يحصل عليه المستخدم من الجهة التي تمتلك نظام المصادقة لإثبات هويته إلكترونياً. يستخدم بشكل رئيسي لمصادقة المعاملات عبر الانترنت حيث يتم استخدامه كبديل لكلمة السر أو بالإضافة إليها. يعمل الجهاز على انتاج كلمات مرور صالحة لإستخدام واحد من خلال استخدام قيمتين. قيمة ثابتة لكل جهاز، وقيمة متغيرة يدخلها المستخدم حين استخدام الجهاز، ويقوم الجهاز بناءاً على القيمتين بانتاج كلمات السر التي يستخدمها المستخدم فيما بعد للدخول إلى النظام. من سلبيات رمز الأمان أن المستخدم بحاجة إلى اقتنائه في كل مرة يريد تسجيل الدخول إلى النظام ما يجعل استخداماته محصورة في إطار صغير.

الهاتف / الهاتف الخلوي (phone / cell phone):يعتبر جهاز الهاتف من طرق المصادقة الملكية أيضاً. يمكن استخدامه بشكل مشابه لرمز الأمان بحيث يتلقى المستخدم رسالة نصية قصيرة أو مكالمة أوتوماتيكية يحصل من خلالها على كلمة مرور لاستخدام واحد.

بطاقة الدخول (Smart Card): البطاقات الذكية هي شكل آخر من أشكال المصادقة التي تعتمد على شيء تمتلكه (المصادقة الملكية). تحتوي هذه البطاقة على شهادة رقمية بالإضافة إلى معلومات أخرى خاصة بالحامل لها أو الجهة المسئولة عن إصدارها.نظراً لسهولة استخدام هذه التقنية أصبحت مصادقة البطاقة الذكية واسعة الانتشار حيث يمكننا أن نجدها تستخدم لدخول المرافق المختلفة، المباني، والغرف.

رقم التعريف الشخصي (PIN) :يعتبر رقم التعريف الشخصي من طرق المصادقة المعرفية، حيث أن المصادقة تتم باستخدام شئ يعرفه المستخدم. رقم التعريف الشخصي هو كلمة سر رقمية يمكن استخدامها لمصادقة المستخدم تتكون غالباً من أربعة أرقام.

ISSN 2170-0796

يستخدم رقم التعريف الشخصي بشكل كبير في حالتين: – مصادقة المستخدم عند عملية السحب النقدي من أجهزة الصراف الآلي.

– مصادقة المستخدم للوصول إلى محطة GSMفي الهاتف المحمول. بعد عدة محاولات ادخال الرقم بشكل خاطئ يقوم النظام بقفل الحساب.

المصادقة الحيوية: وهي مصادقة من النوع الثالث، حيث يتم فيها استخدام أمور توجد في الإنسان لإجراء عملية التحقق من الهوية. وقد حاز هذا النوع من المصادقة على اهتمام العلماء والمتخصصين على مستوى العالم، وهو النوع الأكثر تطوراً في الوقت الحالي حيث بإمكاننا ذكر العديد من طرق المصادقة الحيوية منها: بصمة الاصبع، حدقة العين، تسلسل الحمض النووي DNA، ملامح الوجه، الصوت، التخطيط الكهربائي للدماغ وغيرها من أشكال المصادقة الحيوية والتي سندرسها بشئ من التفصيل.

المقاييس الحيوية واستخدامها في عملية المصادقة

علم المقاييس الحيوية هو علم الأدلة الجنائية في الأجسام البشرية حيث يضم وسائل التعرف علي هوية الأشخاص علي أساس الصفات الفسيولوجية والتشريحية الخاصة لكل انسان.وبذلك فإن عملية المصادقة الحيوية تعتمد على تحويل المقاييس الحيوية للمستخدمين إلى معلومات رقمية يتم تخزينها في النظام ليتم استخدامها مستقبلاً عند عملية تسجيل دخول المستخدم بحيث يتم مقارنة المقياس الحيوي للمستخدم مع المخزن سابقاً في النظام للتحقق من هويته.إجراء عملية المصادقة يتم باستخدام أجهزة خاصة تقوم بقياس السمات الفريدة للمستخدم كبصمة اليد، ملامح الوجه، الصوت أو حدقة العين.

من أكبر مميزات المصادقة الحيوية:

سهولة الاستخدام: حيث أن عملية المصادقة في هذه الحالة لا تتطلب إلى وجود شئ يمتلكه المستخدم كرمز الأمان أو شئ يحفظه (يعرفه) ككلمة السر، كل ما يلزم المستخدم للقيام بعملية المصادقة هو تواجده أثناء عملية المصادقة.

صعوبة الاستيلاء على عامل المصادقة (العامل الحيوي): حيث أنها تعتمد على شئ يوجد في الإنسان فلا يمكن سرقته. نجد أن المصادقة الحيوية تتغلب في هذا الأمر على أنواع المصادقة الأخرى، فكلمات السر، أرقام PIN، رموز الأمان أو بطاقات الدخول كلها أمور يمكن أن تتعرض للسرقة. بجانب هذه المميزات إلا أن المصادقة الحيوية مازالت تواجه العديد من المعيقات لعل من أبرزها كون إنتاج نظم تعمل بالمصادقة الحيوية أكثر تعقيداً وتكلفةً من النظم التقليدية كالتي تعتمد على كلمات السر أوبطاقات الدخول، ولكن لا شك في أن السنوات القليلة القادمة ستشهد تطوراً كبيراً في هذا المجال واستخداماً أوسع لتقنيات المصادقة الحيوية المختلفة.

قائمة المراجع:

Authentication in an Internet Banking Environment. Federal Financial Institutions Examination Council, 2008, Retrieved 2009-12-31.

A mechanism for identity delegation at authentication level, N Ahmed, C Jensen - Identity and Privacy in the Internet Age, 2009.

"How Can I Easily Authenticate Myself?", Guy Huntington, President of Huntington Ventures Ltd, 2012.

Biometric Recognition: Challenges and Opportunities, Joseph N. Pato and Lynette I. Millett, National Research Council, 2010.

www.authenticationworld.com

http://mymemory.translated.net