جمهوريه مصر العربيه
معهد التخطيط القومى

سلسله قضايا التخطيط والتنميه
رقم (١٠٠)

مشروع انشاء قاعدة بيانات الأنشطة البحثية بمعهد التخطيط القومى
(المرحلة الثالثة)

مايو ١٩٩٦

مشروع إنشاء قاعدة بيانات الأنشطة البحثية
بمعهد التخطيط القومى
(المرحلة الثالثة)


بسم الله الرحمن الرحيم

شكر

يود الأستاذ الدكتور محرم الحداد الباحث الرئيسى والمشرف على المشروع تقديم الشكر إلى السادة أعضاء فريق البحث العلميين من داخل المعهد وخارجه والذين قاموا بأعداد وتحليل وتصميم وتنفيذ المرحلة الثالثة من مشروع قاعدة البيانات البحثية بالمعهد ، مؤكدين بذلك الدور الريادى الذى يتميز به معهد التخطيط القومى فى هذا الصدد . كما يمتد الثناء إلى كل من ساهم بالآراء الموضوعية والأفكار البناءة فى سبيل إنجاز هذا العمل .

كما يود الباحث الرئيسى أن يشكر السيدة / معالى السماحى وكذلك الآنسة / نهلة عوض - سكرتارية مركز الأساليب التخطيطية - على مجهوداتهما القيمة التى إنعكست على كتابة هذا البحث فى صورته الأخيرة .

وأتمنى أن يحقق المشروع الهدف المرجو من إعداده ،والله من وراء القصد .

الباحث الرئيسى

(أ.د. محرم الحداد)

فريق البحث لعام ٩٤ /١٩٩٥

أولا : من داخل المعهد :

١- أ٠د٠ محرم الحداد — الباحث الرئيسى

٢- أ٠د٠ أمانى عمر زكى عمر

٣- أ٠د٠ محمد أبو الفتح الكفراوى

٤- أ٠د٠ ماجدة ابراهيم سيد فرج

٥- أ٠د٠ محمد محمود أحمد رزق

٦- السيد / رمضان عبد المعطى

٧- أ٠د٠ محمد ابو الفتح نصار

٨- أ٠ د٠ محمد عبد المجيد الخلوى

٩- أ ٠د٠ عبد الله الدعوشى

١٠ - د٠ حسين محمد صالح

١١- د٠ عبد الفتاح محمد حسين

١٢- د٠ فادية محمد عبد السلام

١٣- د٠ عفاف فؤاد نخلة

١٤- د٠ سهير ابراهيم ابو العنين

١٥- د٠ عزيزة على عبد الرازق

١٦- د٠ نفيسة ابو السعود

١٧- د٠ زينات طبالة

١٨- د٠ سلوى مرسى

١٩ د٠صالح العدوى

٢٠- السيدة / أمانى الريس

٢١- السيد / خالد عبد العزيز

ثانيا : من خارج المعهد :

أ٠د٠ شوقى حسن

أ٠د٠ حسن شحاته

د٠ محمد السعيد خشبه

الفصل الأول

مقترح لنظام أمنى

لقاعدة بيانات الأنشطة البحثية بالمعهد

المحتويات

مقدمة

بعد إتمام المرحلة الأولى من مشروع بناء قاعدة بيانات الأنشطة البحثية بالمعهد وفيها مرت القاعدة بعدة مراحل مختلفة، منها مرحلة التخطيط ثم مرحلة التحليل والتصميم ثم مرحلة تنقيح مبدئية ثم مرحلة التنفيذ وتشغيل القاعدة على بيانات الأنشطة البحثية المختلفة الصادرة فى الفترة من ١٩٨٩ إلى ١٩٩٣ تقوم المجموعة البحثية بالعمل على إنجاز المرحلة الرابعة وهى المرحلة الخاصة بإستكمال القاعدة لفترة عشر سنوات، وذلك بإضافة بيانات خمس سنوات جديدة، بجانب العمل على إنجاز الأهداف الأخرى التى دعت إلى أنشاء قاعدة البيانات البحثية من حيث تسويق النظام، ربط النظام بقواعد وشبكات معلومات أخرى خارجية، ومن هنا كان من الضرورى تصميم نظام أمنى يضمن سلامة وحماية بيانات القاعدة.

وقد يصبح من الضرورى بدء دورة جديدة لتطوير القاعدة ونظام المعلومات الخاص بها فى المستقبل بناءا على التطورات التكنولوجية التى ستصاحب السنوات المقبلة . وسوف نتناول فى هذا الجزء أهمية وجود نظام أمنى لقواعد البيانات وطرق تحقيق سلامة وأمن المعلومات من خلال نظام أمنى مقترح .

١_١ أهمية وجود نظام أمنى لقاعدة معلومات

تلعب نظم المعلومات الإلكترونية دورا هاما وحيويا فى العديد من جوانب الحياة المختلفة، حيث يتم التعامل مع البيانات المخزنة آليا من أجل الحصول على المعلومات المختلفة والمتباينة والعديدة والتى تعتبر موردا رئيسيا تعتمد عليه الكثير من القرارات الهامة فى شتى مجالات الحياة والتطبيقات الحيوية . ومن هنا تظهر أهمية الحفاظ على سلامة وأمن قواعد البيانات وضرورة دراسة الطرق والأساليب التى تؤدى إلى حماية فعالة لها من أى مشاكل أو تهديدات قد تؤدى إلى خلل النظام أو تؤثر على كفاءة أدائه أو كفاءة مستويات السرية به . ولذا يجب أن يصحب مراحل التشغيل المتعددة أنواع متعددة ومختلفة من عمليات

الرقابة وكذا إحاطة البيانات وإحاطة طرق وعمليات تشغيلها بإجراءات أمنية تضمن سلامة وأمن النظام ككل . ويمكن القول إن الكثير من جرائم الكمبيوتر المتزايدة بشكل خطير فى الآونة الأخيرة تعتبر إحدى نتائج عدم وجود نظام أمنى فعال يقوم بعمليات الرقابة المحكمة على قاعدة البيانات والنظام ككل ،ولا يخفى أن العبث بمعلومات مخزنة على قاعدة بيانات بحثية له أثره الخطير على صلاحية الدراسات التى ستعتمد على تلك المعلومات المسترجعة من هذه القاعدة المخربة، ففقدان بعض المعلومات عن طريق الحذف مثلا قد يؤدى إلى تكرار نقاط البحث فى دراسات أخرى تالية وكذلك فإن أى تغير فى محتوى البحوث سواء أكان عن طريق الخطأ أوطريق العمد قد يؤدى إلى التغير فى النتائج المستنبطة بتلك الأبحاث وهذا يؤدى بدوره إلى إستنباط نتائج خاطئة ومضللة فى الدراسات التى سترتبط وتعتمد على تلك الدراسات، كما أن بكل نظام معلومات مستويات سرية مختلفة لابد والحفاظ عليها وعدم الإفصاح عنها لأسباب قد تكون مادية أو معنوية أو إستراتيجية. ومن هنا تظهر أهمية نظم حماية وأمن قواعد المعلومات، وبإنشاء نظام أمنى لقاعدة البيانات البحثية للأنشطة العلمية بالمعهد يصبح الباحث المستفيد من القاعدة وكذا إدارة المعهد والمتصلين بالقاعدة عن طريق الشبكة فى المستقبل واثقين كل الثقة فى مخرجاتها ومحتوياتها المخزنة .

١_٢ طرق الإخلال بأمن قواعد المعلومات

عندما نتحدث عن أمن قاعدة بيانات فإن ذلك لابد وأن يشمل كل عناصر المخاطر والخلل الذى قد يصيب القاعدة بداية من الأمن المادى لمكونات الأجهزة والحواسب الخاصة بالقاعدة إلى أمن برامج التشغيل مرورا بحماية البيانات والمعلومات المخزنة وكذلك الوقاية من فيروسات الحاسب . لذا يمكن تعريف أمن نظام معلومات على أنه حماية المستخدمين والبيانات والأجهزة والآلات وبرامج التشغيل وشبكة الإتصالات بالقواعد الخارجية من الخلل والحوادث الطبيعية أو المتعمدة. ومن الناحية النظرية فإن عددا غير محدود من الموارد وأساليب التأمين يمكن أن تؤدى إلى الوصول إلى مستويات أمن محكمة وكفء وفعالة ، ولكن من الناحية التطبيقية يعتبر من الغير مفيد جمع موارد كثيرة وأساليب معقدة للوصول إلى مستويات عليا من الأمن على حساب التكلفة أو مستويات الأداء، ولذا يجب تحديد قدر من الموارد والأساليب بهدف الوصول إلى درجة جيدة ومقبولة من الأمن للنظام بقدر مقبول من التكلفة . وعموما تتعدد المخاطر التى قد تتعرض لها بيانات أى قاعدة ولكن يمكن إجمال هذه

المخاطر فى ست مخاطر، بعضها يمكن أن يحدث مصادفة بينما البعض الآخر يمكن أن يكـون متعمدا من حيث تغيير فى البيانات أو حذفها أو الإفصـاح عنهـا أو بعـض منهـا.أى أن الإخـلال بهيكل البيانات يمكن أن يكون على النحو التالى:

مصادفة	أو	متعمدا
أ. تغير فى البيانات		د . تغيير فى البيانات
ب. حذف بعض البيانات أو فقدها كلية .		هـ. حذف بعض البيانات أو كلها .
ج . الإفصاح عن البيانات		و. الإفصاح عن بيانات

وهذه المخاطر الست التى تحيط بالبيانات يمكن أن تحدث كما سـبق القـول مصادفـة أو عن قصد . ويعتبر الإخلال بالبيانات الذى يحدث بمحض الصدفة أكثر خطورة من الإخـلال المتعمد، وذلك لأن الأخطاء بمحض الصدفة عادة ما تتكرر كثيرا دون التنبه إليها ولوجودها.

وتسمى الأحداث الغير مرغـوب فيهـا والتـى تهـدد أمـن أى نظـام معلومـات أو قـاعدة بيانات " بالتهديدات "، ويمكن تقسيم تهديدات أمن قاعدة معلومات إلى نوعين رئيسيين :

- تهديدات تنتج عن الكوارث الطبيعية .
- تهديدات تنتج عن أفعال ضارة متعمدة من بعض المخربين .

ويلاحظ أن النوع الأول من التهديدات يتمثل فى أثر الكوارث الطبيعية وهى تهديـدات رغم ندرة حدوثها إلا أن أضرارها خطيرة وحدوثها يهدد أمن البيانات وبرامج التشغيل وسـلامة النظام ككل . أما التهديدات التى تنتج من أفعال المخربين فلهـا طـرق وأسـاليب وقايـة عديـدة سنذكر بعض منها فيما يلى :

وجدير بالذكر أن موضوع الأمن لنظام معلومات لا يرتبط بالجوانب الفنية فحسب، أى البيانات والبرامج والأجهزة ومكونات الحاسب، بل يرتبط أيضا بالسلوك النفسـى والإجتمـاعى للأشخاص الذين يتعاملون مع القـاعدة والنظـام، وهـذا يجعـل موضـوع الأمـن موضوعـا معقـدا

متشعب الأبعاد ومن ثم فإنه لا يوجد نظام أمنى يمنع كل الأخطار منعا تاما ولكن المقصود فقط هو تقليل إحتمالات هذه الأخطار إلى أقل حد ممكن .

١-٣_ بعض طرق وأساليب حماية البيانات وبرامج تشغيل قاعدة معلومات

المقصود هنا ببرامج التشغيل هو مجموعة البرامج المعدة للتعامل مع البيانات المخزنة فى القاعدة والتى تتفاعل مع الأجهزة والحواسب والشبكات لإسترجاع المعلومات المطلوبة والمستهدفة من بناء القاعدة، أما البيانات فهى مجموعة الأرقام والحروف والأشكال المخزنة بالقاعدة .

ويمكن ذكر أربع وسائل شائعة الإستعمال لحماية البيانات وهى :

- التحكم فى الدخول إلى البيانات Access Control
- التحكم فى محاولات الإستنتاج Inference Control
- التحكم فى تدفق البيانات Flow Control
- تشفير البيانات Cryptographic Control

وسنتناول ثلاث من هذه الطرق بالشرح فيما يلى :

١-٣-١ وسائل التحكم فى الدخول إلى البيانات

يتم التحكم فى الدخول إلى البيانات عن طريق تحديد الأشياء المسموح بالدخول إليها بواسطة كل مستوى من المستخدمين . ولذا قبل الدخول إلى قاعدة البيانات من قبل المستخدم يجب على المتعامل مع القاعدة أن يطلب ذلك وبالتالى يجب أن يتصرف نظام القاعدة على المتعامل معه وأن يتحقق من شخصيته قبل أن يسمح له بإستخدام أى من مكونات النظام. والتعرف على المستخدم يعتبر أول خطوة فى سبيل منح المستخدم حق الدخول إلى القاعدة . والمقصود به الإسم الذى يعرف به المستخدم . وهذا التصرف ليس كافيا لحماية البيانات

ومكونات القاعدة بل يجب التحقق من شخصية المستخدم والتأكد من أن المستخدم هو صاحب الإسم الذى تم إدخاله . وتوجد وسائل عديدة للتحقق من شخصية المتعامل مع النظام منها :

- إستخدام خواص مميزة للمستخدم مثل الصوت أو بصمات الأصابع .
- إستخدام أشياء يمتلكها المستخدم مثل الكروت الممغنطة .
- إستخدام كلمات المرور (Password)
- إستخدام المصافحة .

والوسيلة الأولى هى أكثر الوسائل حماية للبيانات ولأجزاء النظام المختلفة إلا إنها غير شائعة الإستعمال حيث أنها تتطلب أجهزة وحاسبات متقدمة، أما الوسيلة الثانية فتستخدم بصفة خاصة فى النظم التى تتطلب درجة عالية من الحماية والأمن مثل البنوك أو قواعد البيانات العسكرية ، أما الوسيلة الثالثة فهى أكثر الوسائل إستخداما لحماية وصيانة بيانات نظم المعلومات. وكلمة المرور هى عبارة عن مجموعة من الحروف والأرقام والأشكال الخاصة المتتالية التى يقوم المتعامل مع القاعدة بإدخالها إلى الحاسب ليتمكن من الدخول إلى القاعدة، ثم يقوم برنامج خاص بالحاسب بفحص تكويدة الحروف والأرقام هذه ومطابقتها مع الكلمات المخزنة بالحاسب فإذا وجدت متطابقة مع أى منها يسمح للمستخدم بالدخول إلى النظام . ومن البديهى إنه كلما زاد عدد حروف كلمة المرور كلما قل إحتمال إكتشافها بالتخمين من قبل المتطفلين والمخربين . وقد حدد بعض الباحثين الوقت اللازم لإكتشاف كلمة مرور بالمعادلة الآتية :

وقت إكتشاف كلمة مرور = عدد محاولات الوصول إلى كلمة المرور x الوقت اللازم لإدخال كل كلمة

فمثلا إذا كانت "س" هى عدد حروف كلمة المرور و "ن" هى عدد الحروف التى يتم إختيار الكلمات منها فإن :

عدد المحاولات المطلوبة للوصول إلى كلمة المرور = ن س

فإن كان زمن إدخال الكلمة للحاسب هو ثانية واحدة ، و ن = ٢٦ حرف و س = ٦ حروف ،

فإن عدد المحاولات = $(٢٦)^{٦}$ و

زمن إكتشاف كلمة المرور = $(٢٦)^{٦}$ x ١ ثانية≈٩ سنوات

ومن الواضح أن عدد حروف كلمة المرور عامل مؤثر على الوقت اللازم لإكتشافها ، إلا أن كثرة عدد حروف كلمة المرور يزيد من صعوبة تذكرها ، وتشير الخبرة إلى أن العدد المثالى لكلمة المرور يتراوح ما بين خمسة إلى ستة حروف، فالكلمة فى هذه الحالة تكون سهلة التذكر بالنسبة للمستخدم وصعبة التخمين بالنسبة للمتطفل .

وهناك عدة طرق لإدخال كلمات المرور منها طريقتين شائعتين وهما إدخال حروف معينة من كلمة المرور وكلمات المرور الوقتية .

والطريقة الأولى ، أى إدخال حروف معينة من كلمة المرور ، تتيح للمستخدم إدخال حروف معينة وتعتبر هذه الحروف فى كل مرة يحاول فيها المستخدم الدخول إلى القاعدة . وبهذه الطريقة لا يمكن الدخول إلى القاعدة فى كل مرة بواسطة شخص آخر غير الشخص صاحب كلمة المرور حتى إذا إستطاع الدخول إليها فى إحدى المحاولات .

أما الطريقة الثانية فهى تتيح للمستخدم إستعمال مجموعة من كلمات المرور وتحديد فترة زمنية لإستخدام كل كلمة ، وعيب هذه الطريقة هى صعوبة تذكر المستخدم لكلمات المرور المختلفة المخصصة له .

وجدير بالذكر أن هناك قواعد عامة وطرق مختلفة لحماية كلمات المرور منها :

- إن كلمات المرور المخزنة بالحاسب يجب أن تكون مشفرة.
- عدم ظهور كلمة المرور على الشاشة (شاشة الحاسب) أثناء كتابتها.
- تغيير كلمة المرور من آن لآخر، حيث أن إستخدام كلمة مرور واحدة لمدة طويلة يزيد من إحتمال إكتشافها .

أما وسيلة المصافحة (Hand Shaking) فتعتبر من الوسائل التى توفر درجة عالية نسبيا لأمن البيانات، ففى هذه الطريقة يتم إعطاء المستخدم دالة تحويل خاصة (د) تكون معروفة للنظام وعندما يريد المستخدم الدخول إلى النظام فإن الحاسب يعطيه رقما عشوائيا وليكن (م) ثم ينتظر الحاسب الإجابة من المستخدم ، ولذا يقوم المستخدم بإيجاد قيمة الدالة د (م) عند القيمة م ثم يدخل الناتج إلى الحاسب ، وعندئذ يسمح نظام القاعدة للمستخدم بالدخول إلى

القاعدة إن كان بيان الناتج الذى أدخل للحاسب صحيحا، وفى هذه الحالة يصعب الدخول إلى القاعدة دون معرفة دالة التحويل (د) .

وبعد التأكد من شخصية المستخدم نصل إلى مستوى آخر من مستويات الأمن وهو أمن الوصول إلى البيانات والبرامج Security of Data Access ، وهنا يجب التأكد إن كان طلب الدخول إلى برنامج معين أو إستخدام معلومة معينة مسموح به لهذا المستخدم أم لا . وفيما يلى نستعرض طريقتين من طرق الرقابة على الدخول إلى القاعدة للحصول على بعض المعلومات، وهما طريقة مصفوفة الدخول Access Matrix وطريقة " جداول السلطات " Authorization Lists .

١_٣_١_١ جداول السلطات Authorization Lists

جدول السلطات هو عبارة عن قائمة تضم أسماء وفئات المستخدمين للنظام مع توضيح إمتيازات كل فئة أو إسم بالنسبة لحق الدخول إلى أجزاء النظام المختلفة . ولكل مكون من مكونات القاعدة، والجدول التالى يوضح فكرة جداول السلطات بصفة عامة :

فئة المستخدمين	الإمتيازات
فئة (١)	قراءة وكتابة
فئة (٢)	قراءة فقط
فئة (٣)	قراءة ونسخ
.....	.....
وهكذا	

وتعتبر طريقة واسلوب جداول السلطات من الأساليب المثالية لحماية برامج وملفات النظام عموما .