الفصل السابع

إدارة الوصول للمعلومات[١] وأمن المعلومات

يتناول هذا الفصل موضوعين مرتبطين بعضهما ببعض، وهما: طرق ضبط عملية التداول من قبل من لهم حق الوصول إلى مقتنيات المكتبات الرقمية، وأساليب الأمن التي تتوافر في شبكات الحاسبات الآلية.

وتعد الجوانب الاقتصادية من أهم مبررات ضبط عملية الوصول للمعلومات، ومن ثم فإن الناشرين الذين يتوقعون تحقيق عائد مادي مما ينتجون من مواد، يمنحون حق الوصول للمعلومات فقط للمستفيدين الذين دفعوا الرسوم المطلوبة. وقد يرى البعض أن لا حاجة لفرض قيود على إدارة الوصول للمعلومات إلا عندما يكون العائد المادي هو الأساس. غير أن هناك أسباباً أخرى تدعو إلى ضبط عملية تداول مقتنيات المكتبات الرقمية، فقد يقيد استخدام بعض المواد بشروط معينة يفرضها الذين أهدوا هذه المواد (كأن يقيد الاستخدام بحياة هؤلاء أو وفاتهم)، كما قد لا ترغب بعض الجهات في تداول مجموعاتها لما تتضمنه من معلومات ذات طابع سري، كالأسرار التجارية وسجلات الشرطة أو وثائقها، والمعلومات الحكومية المصنفة

---

(١) يستخدم مصطلح "إدارة الوصول للمعلومات" في هذا الكتاب ليصف عملية التحكم في الوصول إلى مقتنيات المكتبات الرقمية وتداولها، وإن كانت هناك مصطلحات أخرى تشير إلى المعنى نفسه، مثل "الضوابط والشروط"، ومن الملاحظ أن ثمة مصطلحًا غريبًا يشيع استخدامه في مجال النشر حيث التركيز على العائد المادي، وهو مصطلح "إدارة الحقوق". وبالرغم من عدم وجود تفاوت واضح بين هذه المصطلحات، فإن لكل واحد منها جانبًا من التركيز لا يتوافر لغيره.

classified government information. كما أنه ليس من السهولة وضع حدود فاصلة بين عوالم الفن والإسفاف وانتهاك خصوصية الآخرين، وحتى عندما يكون تداول المجموعات أو الوصول إليها مفتوحاً أو متاحاً، فإن أساليب ضبط عمليات الإضافة والتغيير والحذف لمحتويات هذه المجموعات وما وراء البيانات الخاصة بها، يعد مطلباً له ما يبرره. وتحرص الإدارة الجيدة للمكتبة الرقمية على الاحتفاظ بسجل يضم جميع التغيرات حتى يمكن إعادة اختزان تلك المجموعات في حالة حدوث أية أخطاء أو تلف يصيب ملفات الحاسب الآلي.

إن إدارة الوصول للمعلومات يحيطها شيء من عدم وضوح الرؤية، حيث يفترض من لديهم خلفية في الحاسب الآلي أنه من الممكن في بعض الأحيان إن يتم عنونة كل كائن رقمي بمجموعة ما وراء البيانات التي تضم قائمة حقوق الاستخدام وتصاريحه، والعوامل الأخرى المتصلة بإدارة الوصول للمعلومات. هذا في الوقت الذي يعلم فيه من لهم خلفية في مجال المكتبات، وخاصة المسؤولين عن المجموعات التاريخية والأرشيفية، أن تجميع مثل هذه المعلومات عادة ما يكون مضيعة للوقت، بل أحياناً ما يكون ضرباً من المستحيل. إن مشروعات كمشروع الذاكرة الأمريكية الذي تتبناه مكتبة الكونجرس، تسعى إلى تحويل الملايين من المواد من المجموعات التاريخية، ويبدو من الطبيعي في حالة تلك المواد القديمة افتراض انتهاء فترة حماية حقوق التأليف الخاصة بها، وبالتالي إزالة كل القيود على تداول هذه المواد، غير أن ذلك أبعد ما يكون عن الحقيقة. فانقضاء فترة حماية حقوق التأليف للمواد المنشورة مرتبط بوفاة صاحبها، وهو أمر يصعب تحديده أو التكهن

به، كما أن المكتبات غالباً لا تعرف ما إذا كان قد تم نشر مادة بعينها أم لا.

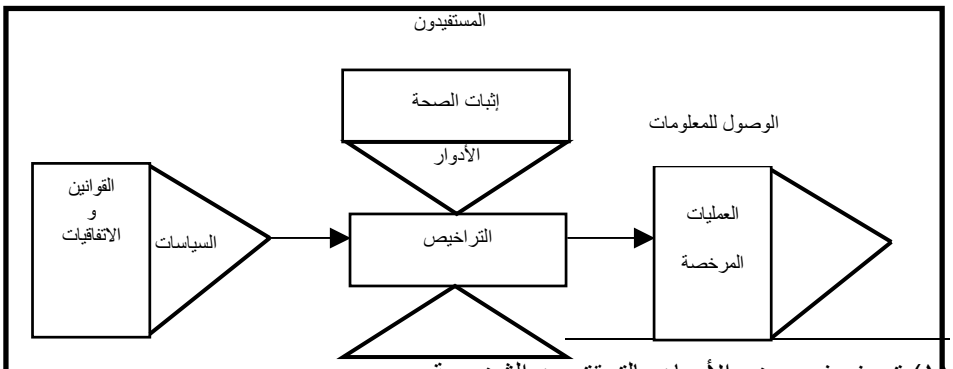
وكما أوضحنا في الفصل السادس، فإن كثيراً من القوانين التي تحكم عمل المكتبات الرقمية، مثل قوانين حقوق التأليف، ليس لها حدود واضحة، ومن ثم فإن السياسات الخاصة بإدارة الوصول للمعلومات، والتي تستند إلى تلك القوانين يحيطها الغموض نفسه، وإذا قدر أن تتضح هذه المعالم من خلال ما يستجد من قوانين أو معاهدات أو إجراءات قانونية، فإن تلك السياسات ستتغير تبعاً لذلك.

عناصر إدارة الوصول للمعلومات :

يوضح الشكل رقم (٧-١) نظامًا يفيد في عملية التفكير بإدارة الوصول للمعلومات؛ حيث يظهر على اليمين من الشكل مديرو المعلومات الذين يضطلعون بمهام وضع السياسات الخاصة بالوصول للمعلومات التي تربط بدورها المستفيدين (في قمة الشكل) بالمواد الرقمية (في أسفل الشكل)، هذا في الوقت الذي يتمركز فيه الترخيص بالاستخدام (في وسط الشكل) محدداً أساليب الوصول للمعلومات (على اليسار من الشكل). ويحتاج كل جانب من هذه الجوانب إلى إيضاح؛ فلا بد أن يضع مديرو المعلومات في اعتبارهم عند وضعهم للسياسات والقوانين المتصلة بذلك، الاتفاقيات الموقعة مع الآخرين (مثل التصاريح الممنوحة من أصحاب حقوق التأليف)، كما يجب التثبت من هويات المستفيدين أو شخصياتهم، وأن يحدد دورهم في الوصول لهذه المواد، كذلك يجب أن تعرف المواد الرقمية في المجموعات أو تحدد، فضلاً عن التثبت من هوية تلك المواد، وعلى الطرف الآخر فإن الوصول لهذه المواد لا يتم إلا عبر العمليات المرخص بها.

وعندما يطلب المستفيد إتاحة فرصة الوصول لمادة رقمية، فإن طلبه يمر عبر إجراءات عملية إدارة الوصول للمعلومات، وبعد التثبت من شخصية المستفيد من خلال عمليتي "التثبت من الهوية [١] Authentication والترخيص بالاستخدام Authorization"، تقوم هذه الإجراءات بمنح هذا المستفيد حق تنفيذ عمليات محددة أو منعه من ذلك.

إن مسؤولية التعامل تقع عادة على الطرف الذي يتولى إدارة المواد الرقمية، وقد يكون هذا المدير مكتبة ما، أو ناشراً، أو مدير أحد المواقع على مدير الويب webmaster، أو منتج المعلومات نفسها، ويمكن أن يفوض جزءًا من هذه المسؤولية لطرف آخر. وإذا كان هذا الطرف إحدى المكتبات التي تتحكم في المواد وتتيحها للمستفيدين، فإنها تضع السياسات وتعمل على تطبيقها، وعادة ما يحكمها في ذلك القيود الخارجية، كالضوابط القانونية، أو التراخيص الممنوحة من قبل الناشرين، أو الاتفاقيات مع المتبرعين. وإذا قام أحد الناشرين بإتاحة المواد، ورخص بتداولها، فإن هذا الناشر يصبح هو المسؤول عن إدارتها (المدير)، ويمكنه في هذه الحالة أن يفوض آخرين في صلاحيات الأنشطة الأساسية كالترخيص للمستفيدين.



(١) تعرف في بعض الأحيان بالتحقق من الشخصية .

التعريف والتثبت في الهوية
المادة الرقمية

الشكل رقم (٧ - ١) إدارة الوصول للمعلومات

المستفيدون :

التحقق من الهوية Authentication :

ثمة أساليب كثيرة ومتنوعة تستخدم في التثبت من هويات المستفيدين، منها ما يتميز بالبساطة - وإن كان يعيبه سهولة الاختراق، ومنها ما يتمتع بقدر كبير من الأمان، لكن يعيبه التعقيد. ويمكن تقسيم هذه الأساليب إلى أربع فئات رئيسة على النحو التالي :

- ما الذي يعرفه المستفيد؟

من الأساليب القياسية وشائعة الاستخدام للتثبت من هويات المستفيدين، أن يمنح كل مستفيد اسمًا مميزًا للدخول وكلمة سر. وبالرغم من سهولة هذا الأسلوب فإنه عرضة لإساءة الاستخدام، كما أن من السهولة سرقة كلمات السر؛ لأن المستفيدين غالباً ما يختارون كلمات سهلة التذكر، ومن ثم تخمينها بسهولة.

- ما الذي يمتلكه المستفيد؟

هناك نوعان من بطاقات التثبت من هوية المستفيد، هما: البطاقات المشفرة مغناطيسياً magnetic encoded cards كالتي تستخدم في أجهزة الصراف الآلي، "والبطاقات الذكية الرقمية digital smartcards" التي تنفذ برنامج التثبت. وبشكل عام تعد هذه البطاقات الذكية من أفضل نظم التثبت،

حيث تتمتع بدرجة عالية من الأمان فضلاً عن سهولة الاستخدام.

- أين يتواجد المستفيد؟

من نماذج التثبت شائعة الاستخدام : عنوان الحاسب على الشبكة، حيث يمكن التثبت من أي شخص لديه إمكانية الوصول لحاسب معين له عنوان معتمد مبني على بروتوكول الإنترنت، وعلى ذلك فإن البيانات المحملة على كثير من الحاسبات الشخصية لا تتوافر لها الحماية عادة إلا من قبل صاحب الجهاز، أي أن كل من له الحق في استخدام الحاسب يمكنه قراءة تلك البيانات.

- ما السمات الشخصية للمستفيد؟

يستخدم أسلوب التثبت من هوية المستفيد عن طريق سماته الشخصية، كنبرات الصوت على سبيل المثال، في القليل من التطبيقات السرية، غير أن استخدام هذا الأسلوب في مجال المكتبات الرقمية لا يزال ضعيفاً.

الأدوار Roles :

نادراً ما تحدد سياسات إدارة الوصول للمعلومات المستفيدين عن طريق أسمائهم، لأنها مرتبطة عادة بفئات المستفيدين أو بدور كل مستفيد على حدة. وقد يكون للمستفيد عدة أدوار؛ حيث يمكن للمستفيد نفسه أن يستخدم المكتبة الرقمية في أوقات مختلفة لأغراض التدريس أو للقراءة الحرة، أو لأغراض العمل الجزئي غير المتفرغ. وتبعاً لذلك فإن المكتبة الرقمية قد يكون لها سياسات مختلفة تجاه هذا المستفيد نفسه، بحيث تتفاوت بتفاوت كل دور من تلك الأدوار. ومن أهم الأدوار في هذا السياق ما يلي :

- **عضوية إحدى المجموعات:** فقد يكون المستفيد أحد أعضاء المعهد (الأوروبي) للفيزياء على سبيل المثال، أو قد يكون طالباً في الأكاديمية البحرية الأمريكية.

- **موقع المستفيد:** فقد يستخدم المستفيد حاسباً في مكتبة جامعة كارنيجي في بتسبرج، أو في مكان ما من نيوزيلندا.

- **مدى اشتراك المستفيد:** فقد يكون المستفيد مشتركاً اشتراكاً ساري المفعول في مجلة جمعية حرفيي استخدام الحاسبات، أو أحد منسوبي إحدى الجامعات التي تمتلك الترخيص لاستخدام جميع مجموعات جستور JOSTR.

- **برنامج التكشيف الآلي:** فقد يكون المستفيد أحد مستخدمي برنامج متصفح الويب أو أي برنامج آلي آخر.

- **أسلوب تسديد الرسوم:** فقد يكون للمستفيد حساب ائتمان مع خدمة ليكزيس Lexis[1]، وأنه ممن يدفعون عشرة دولارات مقابل الوصول للمواد.

إن معظم مستخدمي- أو بالأحرى مستفيدي- المكتبات الرقمية هم عناصر بشرية يستخدمون حاسبات شخصية، إلا أن المستفيد قد يكون حاسباً آلياً يعمل بدون شخص يشغله، أو أحد برامج تكشيف صفحات الويب، أو

(١) إحدى الشركات الرائدة في تقديم المعلومات القانونية النصية الكاملة على الخط المباشر (المترجمان).

أحد برامج المطابقة Mirroring [١] التي تقوم باستنساخ المجموعة بأسرها أو تكرارها، وهناك من المواقع ما يحظر ضمنياً إتاحة الوصول عن طريق برامج آلية أو عن طريق منحها صلاحيات عالية higher privileges.

المادة الرقمية :

تعريف المواد والتثبت من هوياتها:

يجب تعريف المواد الرقمية بوضوح من أجل تحقيق متطلبات إدارة الوصول إليها وتداولها، ويتم ذلك من خلال إعطاء كل وحدة من وحدات تلك المواد اسمًا أو محددًا معينًا. وهذا موضوع رئيسي بالنسبة لكل من المكتبات الرقمية والنشر الإلكتروني.

والتثبت من هوية المواد الرقمية يضمن لكل من المستفيد ومدير المجموعات عدم حدوث أي تغيير في مضمون تلك المواد. وهي مسألة بالغة الأهمية في بعض المواقف؛ فقد سبق لي أن عملت مع بعض الزملاء لدى وزارة التجارة الأمريكية في تجميع عدد من الوثائق ذات العلاقة بالشؤون الخارجية كالمعاهدات والاتفاقيات التجارية، وبدت لنا هنا مدى أهمية دقة الصياغة في تلك الوثائق؛ فلو أن وثيقة ما- على سبيل المثال- ذكر أنها هي التي تتضمن النص الدقيق لاتفاقية التجارة الحرة لأمريكا الشمالية، لوجب على كل من يتعامل مع هذه الوثيقة أن يثق في صحة صياغتها ودقة نصها، وكم من مرة أثارت نصوص غير دقيقة في صياغتها- سواء أكان ذلك عن قصد أو عن غير قصد- أزمات دولية.

(١) نظام آلي يحتوي على نسخة مكررة من المعلومات المختزنة في نظام آخر (المترجمان).

ويحدث في معظم المكتبات الرقمية ألا يتم التثبت من مدى صحة موادها بشكل دقيق، وحيثما يكون مستوى الثقة عالياً وتكلفة الأخطاء قليلة، فليس هناك حاجة أو مبرر لعملية رسمية للتثبت من الهوية، وإذا كانت التغييرات المتعمدة قد تبدو نادرة، كما أن الأخطاء عادة ما يكون من السهولة كشفها. فإن وجود تلك الأخطاء يعد أمراً خطيراً، وخاصة في بعض المجالات الحيوية كالطب على سبيل المثال، وبناء على ذلك فإن على المكتبات الرقمية في مثل هذه الحالات، أن تعيد النظر بشكل جاد في استخدام الطرق الرسمية للتثبت من هوية موادها.

ولضمان دقة كائن معين، فإنه يمكن ربطه بتوقيع رقمي خاص بها (سنتناول في نهاية هذا الفصل الأساليب الفنية للقيام بذلك)، بحيث يكفل هذا التوقيع عدم تغيير أي ملف، أو أية أجزاء من مكوناته بعد وضعه. وتبين اللوحة رقم (٧-١) كيفية استخدام التوقيعات الرقمية في مكتب حماية حقوق التأليف الأمريكي.

وثمة مجموعة من وسائل التثبت من هوية المواد يشار إليها بالمصطلح "الدمغ بالعلامات المائية Watermarking"، وهي وسائل دفاعية يستخدمها الناشرون لتتبع عمليات النسخ غير القانونية وردعها. وتكمن الفكرة الأساسية لهذه الأساليب في دمغ رمز (أو علامة) ما في المادة بطريقة دقيقة ماكرة لا يدركها المستفيد، ولكن يمكن استعادتها لإثبات الملكية تماماً مثلما تفعل شركات الإعلان عندما تضيف شعاراً لإعلان تليفزيوني ليكشف مصدر الصورة إذا ما تم تقليدها. وقد يكون من المستحيل على المستفيد كشف

العلامات المائية الرقمية، لكن من المؤكد أن إزالتها تكاد تكون مستحيلة، وإذا ما تم ذلك فيصبح ذلك أمراً مكشوفاً للعيان.

اللوحة رقم (٧-١)

التسجيل الإلكتروني والإيداع التزاماً بقانون حقوق النشر

يعد المكتب الأمريكي لحقوق النشر إحدى الإدارات المستقلة التابعة لمكتبة الكونجرس، ولمكتبة الكونجرس - حسب القانون الفيدرالي- حق اقتناء نسختين من كل عمل ينشر في الولايات المتحدة الأمريكية. وفي الوقت الذي نجد فيه أن إيداع الأعمال المنشورة أمر إلزاميّ، نلاحظ أن تسجيل الأعمال الخاضعة للحماية القانونية لم تكن مطلباً في قانون حق المؤلف الصادر عام ١٩٧٨م، رغم أن هناك تشجيعاً لعملية التسجيل لما لها من فوائد كبيرة.

وطريقة التسجيل لأغراض حماية حقوق المؤلف بسيطة وواضحة، إذ يقوم مالك هذه الحقوق بإرسال نسختين من عمله إلى مكتب حق المؤلف مع نموذج التسجيل والرسوم اللازمة، بعد ذلك يتم دراسة الطلب والعمل المقدم، وإذا أُقر ذلك صدرت للعمل شهادة تسجيل، بعدها يرسل العمل لمكتبة الكونجرس لكي تقرر ما إذا كان يستحق الإضافة لمجموعاتها، أو وضعه ضمن قائمة التبادل مع المكتبات الأخرى.

وفي عام ١٩٩٣م شرع كل من مكتب حقوق التأليف ومؤسسة مبادرة البحوث الوطنية، في استحداث نظام لتسجيل الأعمال الإلكترونية وإيداعها، عرف باسم كوردس Copyright Office Electronic Registration, Recording and Deposit System (CORDS). ويعكس هذا النظام الإجراءات التقليدية المتبعة، فالطلب نموذج متاح على الويب، بالإضافة إلى نسخة رقمية من

العمل تتاح بشكل آمن على الإنترنت، أما الرسوم فتدفع بشكل منفصل. ويتم استخدام التوقيعات الرقمية في التعرف إلى الطلبات المقدمة لتسجيل حق المؤلف؛ حيث يقدم صاحب الطلب مستخدماً مفتاحاً خاصاً به طلباً موقعاً، إضافة إلى العمل نفسه، والتوقيع الرقمي، والمفتاح العام، والشهادات ذات الصلة بالموضوع. ويعمل التوقيع الرقمي على إبلاغ مكتب حقوق التأليف بوصول الطلب بشكل صحيح وتأكيد صحة بيانات هوية صاحب الطلب. وبناء على ذلك وفي حالة حدوث أي نزاع في المستقبل حول العمل، يرجع إلى التوقيع الرقمي للتثبت من صحة الادعاء ومن العمل المسجل.

سمات المادة الرقمية Attributes of Digital Library :

غالباً ما تتعامل سياسات إدارة الوصول للمعلومات مع المواد المختلفة بطرق وأساليب متنوعة حسب سمات تلك المواد وخصائصها، ويمكن تشفير تلك الخصائص باعتبارها "ما وراء بيانات إدارية administrative metadata" يتم اختزانها مع الكائن نفسه، أو أن هذه الخصائص يمكن أخذها من مصدر آخر. كذلك يمكن لبعض السمات أن تحسب، كما هو الحال بالنسبة لحجم الكائن حيث يمكن قياسه. وفيما يلي بعض الأمثلة على ذلك :

- **التقسيم إلى مجموعات فرعية:** غالباً ما تُقسَمُ المجموعات إلى مواد متاحة بدون قيود، ومواد مقيدة الاستخدام؛ حيث يفصل الناشرون نصوص المقالات الكاملة عن غيرها من الكشافات والمستخلصات والمواد الإعلانية الأخرى، كما تتيح بعض المواقع على الويب حرية الدخول إليها للجميع، في حين تقيد بعض المواقع الأخرى استخدامها بفئة محددة من المستفيدين كأعضاء المؤسسة التابع لها هذا الموقع.

- **الترخيص والالتزامات الخارجية الأخرى:** قد تقتني المكتبة الرقمية مواد مرخصاً بها من قبل ناشريها، أو مواد تخضع لضوابط وشروط تحكم تداولها، كتلك المواد التي تودع في مكتبة الكونجرس تنفيذاً لقانون حق المؤلف.

- **الخصائص المادية والمؤقتة:** ربما يكون للمكتبات الرقمية سياسات تستند إلى عامل الفترة الزمنية، وهو تاريخ النشر، أو على الخصائص المادية كالحجم، حيث تتيح بعض الدوريات حرية التداول المجاني لبعض مقالاتها وذلك فور صدورها، في حين تطلب ترخيصاً لتداول تلك المقالات بعد مضي فترة زمنية على نشرها.

- **أنواع الوسائط:** قد تعتمد المكتبة الرقمية على سياسات تستند إلى شكل المادة، أو على نوع الوسيط حيث يمكن - على سبيل المثال - أن تعامل الوسائط السمعية المرقمنة والمواد النصية وبرامج الحاسب والصور بأساليب مختلفة بناءً على اختلاف طبيعة كل وسيط من هذه الوسائط.

ومن الضروري تناول خصائص المواد الرقمية بطرق متفاوتة granularity، لأنه لو توافرت لجميع المواد في مجموعة معينة الخصائص نفسها لكان من المناسب وصفها وصفاً واحداً، وعلى النقيض من ذلك تماماً، حيث نجد في بعض الأوقات أن أجزاءً معينة من المواد تنفرد بسمات خاصة بها. كما أن الحقوق المتعلقة بالصور تختلف في الغالب عن تلك الحقوق المتعلقة بالنص الذي تلحق به تلك الصور، ومن ثم فلا بد من التمييز بين

هذين الشكلين، ويمكن لشخص ما أن يهدي إحدى المكتبات مجموعة من الرسائل ويسمح بإتاحتها للتداول باستثناء مواد محددة منها يقيد تداولها بشروط معينة. وبناء على ذلك، فإن على المكتبات الرقمية أن تسعى إلى ربط الخصائص بالمجموعات الكلية، أو بالمجموعات الفرعية، أو بمواد معينة في المجموعة، بل بعناصر محددة في تلك الكائنات.

العمليات :

غالباً ما تحدد أو تقيد سياسات إدارة الوصول العمليات وغيرها من الممارسات المختلفة الأخرى التي يسمح للمستفيد القيام بها حيال مواد المكتبة، وهناك نوعان من العمليات هما:

- **العمليات الحاسوبية:** هناك بعض العمليات التي توصف بمصطلحات حاسوبية، مثل: كتابة البيانات على الحاسب الآلي، أو تنفيذ البرنامج، أو تراسل البيانات عبر الشبكة، أو عرض البيانات على شاشة الحاسب، أو طباعة البيانات أو نسخها من جهاز إلى جهاز آخر.
- **حدود الاستخدام:** حيث يسمح للمستفيد باقتباس مواد معينة من إحدى قواعد البيانات، ولكن لا يسمح له بنسخ قاعدة بيانات بأكملها.

ويمكن ضبط العمليات المشار إليها سابقاً بالوسائل الفنية، لكن هناك كثيراً من السياسات التي قد يقررها مدير المعلومات ويستحيل تنفيذها من الناحية الفنية، ومن هذه السياسات ما يلي:

* **العمل أو الغرض:** حيث يمكن أن يشير تفويض المستفيد إلى سبب

القيام بعملية ما، وتشمل الأمثلة على ذلك الاستخدامات التجارية والتعليمية والحكومية.

* **العمليات الفكرية:** فقد تحدد العمليات الاستخدام الفكري لمادة من المواد، وهنا تظهر أهمية القواعد التي تضبط عملية اشتقاق عمل جديد يقوم على محتوى عمل آخر، أي أن المعايير لابد أن تضع في اعتبارها هدف الاستخدام ومداه.

الاستخدام اللاحق [غير المباشر] Subsequent Use :

ينبغي على نظم إدارة الوصول أن تراعي كلاً من العمليات المباشرة direct operations، والاستخدام اللاحق للمواد. ويقصد بالعمليات المباشرة تلك العمليات التي يتولاها الجهاز الخازن repository، أو أي نظام آلي آخر يعمل كوكيل لمدير المجموعة. أما الاستخدام اللاحق فيشمل جميع العمليات التي يمكن أن تحدث بمجرد خروج المادة عن سيطرة المكتبة الرقمية، ويشمل ذلك جميع سبل النسخ (بدءاً من عمليات استنساخ ملفات الحاسب إلى عمليات تصوير المستندات). ومن منظور فكري يمكن أن يتراوح الاستخدام اللاحق بين عمليات اقتباس أجزاء قصيرة، وإيجاد أعمال قائمة على أعمال سابقة، وانتهاءً بالانتحال الصريح للمحتوى الفكري.

وعندما يتم إرسال مادة معينة، أو جزء من إحدى المواد إلى حاسب شخصي، يصعب من الناحية الفنية منع المستخدم من نسخ ما أرسل إليه أو اختزانه أو توزيعه إلى الآخرين، وهو أمر يشبه عملية تصوير المستندات. وإذا كانت المعلومات متاحة للبيع، زادت احتمالات الاستخدام اللاحق لها. والواقع

أن الناشرين تزعجهم فكرة قيام القراء بتوزيع نسخ من المواد دون موافقة منهم على ذلك، وإذا ما تتبعنا الفكرة في أسوأ احتمالاتها وجدنا أنه لو قام أحد الناشرين ببيع نسخة واحدة من إحدى المواد، ثم حدث أن وزعت تلك المادة عبر الإنترنت توزيعاً موسعاً، فقد ينتهي به الحال إلى عدم بيع نسخ أخرى من العمل غير تلك النسخة الوحيدة الأولى؛ وتحسباً لهذه المخاوف تسمح المكتبات الرقمية غالباً لقرائها بتداول تسجيلات فردية أو استخدامها، دون تقديم أية وسائل تكفل لهم نسخ مجموعات كاملة، ومع أن هذا لا يحول دون ضياع قدر ضئيل من العائد المادي من صاحب المادة، فإنه يقف عائقاً أمام كل من يحاول تقويض المصالح الاقتصادية للناشر من خلال نسخ العمل برمته.

السياسات :

يشير التعريف الرسمي لكلمة "السياسة policy" إلى أنها القاعدة التي سنّها مدير المعلومات لتحدد من له حق القيام بعمل أو فعل معين تجاه مادة معينة، ومن السياسات الشائعة في المكتبات الرقمية ما يلي :

- أن يكون لأحد المطبوعات سياسة تحدد إتاحتها؛ بمعنى أن يتاح لأي شخص إمكانية قراءة المادة فقط، في حين يخول أعضاء تحرير هذا العمل الحق في إجراء أي تغييرات عليه.

- أن يكون لناشري الدوريات على الخط المباشر سياسة تسمح للمشتركين دون غيرهم بالوصول إلى هذه الدوريات أو قراءتها، في حين لا تسمح لغيرهم إلا بقراءة صفحة المحتويات، أو المستخلصات، بمعنى أن حق التعامل مع الدورية بمحتوياتها كاملة لا يخول إلا لمن يدفعون رسوماً نظير

استخدامهم تلك الدوريات.

- تقوم بعض الجهات الحكومية بتصنيف المواد (مثل المواد السرية للغاية)، ويكون لها سياسات مشددة حول من له حق الوصول لهذه المواد وتداولها، والظروف التي يسمح له فيها بذلك، وطبيعة ذلك التداول.

وتجدر الإشارة إلى أن تلك السياسات نادراً ما تكون بالبساطة التي عرضنا لها في الأمثلة السابقة، فمجلة المكتبات الرقمية D.L. magazine على سبيل المثال، لها سياسة الإتاحة الحرة للجميع، غير أن مؤلفي مقالات هذه المجلة يحتفظون بحقوق تأليف مقالاتهم هذه. أي أن سياسة الوصول هذه تسعى إلى تشجيع الجميع على قراءة المقالات وطباعتها للاستخدامات الشخصية، أما الاستخدامات اللاحقة (كتأليف عمل معتمد على العمل الأصلي، أو بيع نسخ بقصد الربح)، فيتطلب إذناً بذلك من صاحب حق التأليف.

ونظراً لأن سياسات إدارة الوصول قد تكون معقدة، فقد تطلب الأمر إيجاد بعض الوسائل الرسمية لصياغتها بهدف تبادل المعلومات بين أنظمة الحاسب الآلي، وربما يعد أكثر الأعمال شمولاً في هذا الصدد ما قام به "مارك ستيفكMark Stefik" من شركة زيروكس، حيث طرح مارك ما يعرف بـ "لغة حقوق الملكية الرقمية The Digital Property Rights Language"، وهذا العمل يعتبر لغة تعبر عن حقوق استخدام الأعمال الرقمية، وضوابط ذلك، ورسومه. كما تسعى هذه اللغة إلى تحديد خصائص المواد الرقمية، وسياسات تداولها، بما في ذلك الاستخدام اللاحق لها.

وبموجب هذه اللغة يكون بمقدور مدير المجموعة وضع ضوابط وشروطًا لعمليات نسخ هذه المواد وإرسالها ونقلها وطباعتها وغيرها من العمليات الأخرى المشابهة. وتنص اللغة المقترحة على إيجاد رسوم تُحدد بعد ذلك نظير أي عملية، كما أنها تضع تصوراً للروابط مع آليات الدفع الإلكتروني. أما بالنسبة لنظام الرمز المستخدم في هذه اللغة فهو يعتمد على لغة معالجة القوائم Lisp (١)، وهي لغة تستخدم لمعالجة اللغة الطبيعية، ويرى البعض أن من الأفضل لنظام الرموز في المكتبات الرقمية أن يستخدم لغة التهيئة الموسعة XML (٢). غير أن المحك الحقيقي ليس في نظام الرمز بقدر ما هو في مدى فاعلية اللغة ونجاحها في إثبات وجودها واستخدامها على نطاق واسع.

تنفيذ سياسات إدارة الوصول :

ليست عملية إدارة الوصول مجرد مسألة وضع سياسات ملائمة، بل العبرة ـ كما يريد مديرو المعلومات-في تطبيق تلك السياسات، وهو أمر يتطلب شيئاً من الإلزام.

---

(١) Lisp (list procssing) لغة معالجة القوائم، إحدى لغات البرمجة صممها جون مكارثر في عامي ١٩٥٩- ١٩٦٠م، واستعملت أساساً لتناول قوائم البيانات بالتعديل والترتيب، وقد استعملت هذه اللغة على نطاق واسع في دوائر الأبحاث والدوائر الأكاديمية، حيث تعتبر اللغة المعيارية لأبحاث الذكاء الاصطناعي (المترجمان).

(٢) إصدارة مبسطة من اللغة المعيارية الموحدة لتهيئة النصوص SGML، ولغة XML هذه خاصة بالوثائق المعروفة على الويب تساعد المستخدمين على إضافة مهام للوثيقة غير موجودة في لغة HTML (المترجمان).

إن بعض السياسات يمكن تطبيقها بشكل إلزامي من الناحية الفنية، لكن ذلك ليس ممكنًا مع جميع السياسات؛ فهناك مثلاً وسائل فنية واضحة لتطبيق سياسة معينة مع من يصرح له بتغيير مادة ما في مجموعة معينة، أو بالبحث في مستودع الوثائق. لكن ليس هناك وسائل فنية لمكافحة الانتحال، أو انتهاك الخصوصية أو ضمان استخدام المواد للأغراض التعليمية دون غيرها من المجالات. فمثل هذه السياسات- وبرغم ما تتمتع به من بعد منطقي- تبدو غاية في الصعوبة عند تنفيذها بالوسائل الفنية، ولا سبيل إلى تنفيذها إلا بالوسائل القانونية والاجتماعية.

وهناك علاقة عكسية بين دقة التنفيذ ومدى رضا المستفيدين؛ فالوسائل الفنية لتنفيذ السياسات قد تسبب لهم إزعاجاً؛ فقليلون هم أولئك الذين يعترضون على كتابة "كلمة مرور password" عند بداية الدخول إلى الشبكة، لكن الجميع لا يرغبون في إعادة كتابة كلمة المرور أو غيرها من إجراءات أخرى للتحقق من الهوية عدة مرات. وقد يقرر مديرو المعلومات في بعض الأحيان تخفيف قيود عملية تطبيق السياسات من أجل إرضاء المستفيدين، على اعتبار أن إرضاءهم يسهم في نمو السوق حتى ولو ضاع جزء من العائد بسبب المستفيدين غير المصرح لهم بالدخول. وكما يحرص الناشرون الذين يتحمسون كثيراً لتطبيق السياسات على سعادة المستفيدين، وغالباً ما تكون عائداتهم أكبر من عائدات غيرهم من الناشرين. وكما يبدو من اللوحة رقم (٧-٢)، فإن هذه تعد الاستراتيجية المتبعة الآن في الغالبية العظمى من برمجيات الحاسبات الشخصية. وهو التوجه نفسه الذي يعمد إليه بعض ناشري الدوريات الإلكترونية، ومثال ذلك دار نشر هاي وير High wire Press.

وإذا ما أخذ التراخي مأخذه من الوسائل الفنية، فيمكن للضغوط الاجتماعية والقانونية أن تؤدي دورها، ومن بين الأهداف الاجتماعية تدريب المستفيدين على السياسات المطبقة على المجموعات وإقناعهم باتباعها، أو حتى ملاحظتهم بذلك، وتحتاج هذه الأهداف إلى سياسات يسهل فهمها وبالتالي إتباعها. كما ينبغي إحاطة المستفيدين بالسياسات وإعلامهم بطبيعة التصرفات السليمة. ومن الوسائل المفيدة أن تظهر على الشاشة "عبارات إرشادية" بمجرد الوصول إلى المادة، وهذه العبارة بمثابة نصوص تحدد بعض السياسات، مثل: "من أجل الحفاظ على حقوق التأليف" يحظر استخدام هذه المادة لأغراض تجارية. وهناك من الوسائل غير الفنية في مجال تطبيق السياسات ما هو أكثر حزماً، مثل إقدام الناشر على إلغاء الترخيص الذي يمنحه لأعضاء إحدى المؤسسات إذا ما دأبوا على انتهاك اتفاقية الترخيص، أو أساءوا استخدام السياسات التي ينبغي عليهم احترامها والالتزام بها، أما أشد الإجراءات قسوة فهو اللجوء للقضاء، وعندها يمكن القول: إن قضية واحدة يحسن أصحابها الدعاية لها، قد تقنع الكثيرين بالتحلي بالمسؤولية إزاء التعامل مع المواد.

اللوحة رقم (٧-٢)

سياسات إدارة الوصول للبرمجيات

تقدم التجارب المبكرة في برمجيات الحاسبات الشخصية نموذجاً لما يحدث عندما لا تلقى محاولات تطبيق السياسات قبولاً من المستفيدين.

ومن المعتاد أن البرامج يرخص بها لحاسب واحد، كما تغطي رسوم الترخيص استخدام البرمجية في حاسب واحد، لكنه من السهل نسخ مثل هذه

البرمجيات، وعادة ما يخسر منتجو البرامج العائد من هذه البرمجيات المنسوخة، وخاصة إذا تم توزيعها على نطاق واسع.

وقد حاول منتجو البرمجيات في بدايات استخدام الحاسبات الشخصية أن يضبطوا عملية الاستنساخ غير المرخص للبرمجيات بأساليب فنية، منها أن تحمل البرمجيات على أقراص لا يمكن نسخها بسهولة، وهو ما يعرف باسم "الحماية ضد النسخ copy protection"، وفي كل مرة يريد المستفيد تشغيل البرنامج عليه أن يضع الأسطوانة الأصلية، وقد كان لهذا أثره الواضح على سوق النشر، وهو ما لم يكن يطمح إليه منتجو البرمجيات، ولم يكن مناسباً للمستفيدين المرخص لهم باستخدام البرنامج الذي اشتروه، كما كانت عملية تنصيب القرص الصلب وحفظ البرنامج تتسم بالصعوبة، وقد اعترض المستفيدون على ذلك، وكانت النتيجة أن موردي البرامج الذين كانوا من دعاة حمايتها، قد خسروا مبيعات كثيرة وذهبت أرباحها لأولئك الذين طرحوا برامج غير محمية ضد النسخ.

وقد كانت شركة "مايكروسوفت" إحدى الشركات التي أدركت أن التنفيذ بأساليب فنية ليس هو الخيار الوحيد، وكسبت الشركة مكاسب خرافية من جراء بيع منتجات ليست محمية ضد النسخ من الناحية الفنية، وقد اجتهدت الشركة في حث المستفيدين على الالتزام بالسياسات وذلك من خلال وسائل غير فنية. وقد شجعت حوافز التسويق كدعم المستفيدين وتطوير أجهزتهم بتكلفة منخفضة - المستفيدين على شراء تراخيص الاستخدام. وفي هذا السياق كذلك،تم اللجوء إلى الضغوط الاجتماعية لتثقيف المستفيدين، كما لوح باستخدام القنوات القضائية لترهيب من ينتهك سياسات الشركة.

ولا تزال عمليات النسخ غير المرخص بها تكلف منتجي البرمجيات مبالغ طائلة، إلا أن الشركات التي تركز جهودها على إرضاء المستفيدين المسؤولين تستطيع التكيف مع ظروف السوق وتحقيق الانتعاش.

إدارة الوصول على المستودع أو الجهاز الخازن Repository :

تطبق معظم المكتبات الرقمية سياسات على مستوى الجهاز الخازن، أو على مستوى المجموعات. ورغم الاختلاف في التفاصيل، فإن جميع الوسائل تتبع النمط الموضح في الشكل رقم (٧-١). ومن المعروف أن المكتبات الرقمية هي نظم آلية لا مركزية أو موزعة، تتدفق فيها المعلومات من حاسب إلى آخر، وإذا كانت هناك إدارة للتعامل على مستوى الجهاز الخازن، فإنه يمكن إنجاح عملية التعامل هذه محلياً، وما أن تخرج المادة من حدود الجهاز الخازن، حتى تقل فرص التحكم فيها من الناحية الفنية.

وقد سبق لنا تناول قضية الاستخدام اللاحق، وهي تتلخص في أنه ما أن يتلقى الحاسب أي معلومة، حتى يصعب على المدير الأصلي للمكتبة الرقمية أن يسيطر عليها سيطرة فاعلة دون التعرض للمستخدم المرخص له باستخدامها. ومع وجود الشبكات، أخذت المسألة بعداً جديداً، وهو أن النسخ العديدة للمادة الموجودة على الحاسبات المرتبطة بالشبكة بما فيها الذاكرة المخبأة caches والذاكرة المطابقة mirrors والخوادم الأخرى، تكون خارج نطاق سيطرة الجهاز الخازن المحلي.

وقد اكتفت معظم المكتبات الرقمية، وإلى يومنا هذا، بتوفير إدارة الوصول للمعلومات على مستوى الجهاز الخازن مع اعتمادها على الضغوط

الاجتماعية والقانونية لضبط عملية الاستخدام اللاحق، وعادة ما تكون مثل تلك الضغوط في محلها، غير أن بعض الناشرين منزعجون من أن الافتقار إلى السيطرة الكاملة [على مواد المكتبات الرقمية] قد يأتي على عائداتهم المالية، من هنا جاء الاهتمام بالوسائل الفنية التي تضبط عملية النسخ والاستخدام اللاحق، حتى ولو كانت المادة قد خرجت من حدود الجهاز الخازن. وتنقسم هذه الوسائل إلى فئتين، هما: النظم الموثوق بها، والحاويات الآمنة.

– النظم الموثوق بها Trusted Systems :

الجهاز الخازن هو مثال للنظم الموثوق بها، حيث يتوافر لدى مديري المكتبة الرقمية ثقة في أن المكونات المادية للحاسبات الآلية والبرمجيات والإجراءات الإدارية تتمتع جميعها بمستوى ملائم من الأمن والسلامة لاختزان المعلومات القيمة وتوفير ضمانات الوصول إليها. وقد يكون هناك نظم أخرى مرتبطة بهذا الجهاز الخازن وتتمتع بالدرجة نفسها من الثقة. ويمكن للمكتبات الرقمية في داخل شبكة النظم الموثوق بها أن تستخدم وسائل تنفيذ للسياسات تشبه تلك المستخدمة مع الجهاز الخازن الواحد، ويمكن تمرير السمات والسياسات فيما بين النظم مع توفر الثقة من أنها ستلقى معالجة فعالة.

إن تجهيز وعمل شبكات مكونة من نظم موثوق بها ليس بالأمر الهين؛ لإن مكونات النظم الفردية لابد أن تكفل مستوى عالياً من الأمن، وكذلك الحال مع العمليات التي يتم بها تمرير المعلومات فيما بين الحاسبات المختلفة؛ ولهذه الأسباب فإن هذه النظم الموثوق بها تستخدم فقط في مواضع محددة أو في حاسبات مخصصة لأغراض محددة. ولو أن جميع عمليات

تشغيل الحاسبات كانت تتم من المجموعة نفسها أو من قبل مجموعات تعمل في ظل قوانين صارمة، لتضاءلت بالطبع كثير من المشكلات الإدارية. ومن أمثلة النظم الضخمة الموثوق بها شبكة الحاسبات التي تدعم ماكينات الصرف الآلي التابعة للبنوك.

ويمكن القول بأنه لا يمكن التسليم بطبيعة الحاسبات الشخصية للمستفيدين وكيفية إدارتهم لها، ومن المعقول حقاً عدم الثقة بها، ولهذا السبب كان طبيعياً أن تقتصر التطبيقات المبكرة للنظم الموثوق بها في المكتبات الرقمية على الأجهزة المخصصة لأغراض محددة مثل البطاقات الذكية، أو الطابعات الآمنة، أو تقتصر على حاسبات خادمة تستعمل برمجيات شديدة الإحكام.

- الحاويات الآمنة Secure Containers :

ما دامت الشبكات غير آمنة، وطالما يصعب تنفيذ النظم الموثوق بها، فإن مجموعات متعددة تعكف على تطوير حاويات آمنة لنقل المعلومات عبر شبكة الإنترنت، حيث يتم من خلالها نقل المادة الرقمية للمستفيد في حزمة تشتمل على البيانات وما وراء البيانات الخاصة بسياسات الوصول للمواد. وعادة ما تكون جميع المعلومات أو بعضها مشفراً. كما أن الوصول للمعلومات يتطلب مفتاحاً رقمياً يمكن تسلمه من نظام دفع آلي أو من أي نظام آخر من نظم التحقق من الهوية. ومن ميزات هذه الطريقة أنها توفر قدراً كبيراً من ضبط عملية الاستخدام اللاحق، كما أن الحزمة المرسلة (البيانات وما وراء البيانات) يمكن نسخها وتوزيعها إلى طرف ثالث، لكن ليس من الممكن الوصول إلى مضمون هذه الحزمة دون ذلكم المفتاح، وتقدم لنا اللوحة رقم (٧-٣) وصفاً

لواحد من هذه النظم.

وبالرغم من ذلك فهناك عائق في تقبل نظم الحاويات الآمنة؛ حيث تنعدم جدواها بالنسبة للمستفيد ما لم يتمكن المستفيد من الحصول على المفاتيح السرية المطلوبة للوصول إليها، ومن ثم الإفادة من محتوياتها. وهو أمر يتطلب نشراً واسعاً لخدمات الأمن ولوسائل الدفع الإلكتروني. وإلى وقت قريب كان انتشار مثل هذه الخدمات محدوداً، لذلك لم يجد الناشرون سوقاً رائجة للمعلومات التي يتم توزيعها عبر تلك الحاويات الآمنة.

اللوحة رقم (٧- ٣)

الشيفرات **Cryptolopes**

يُستخدم نظام شركة آي بي إم لتشفير الحاويات الآمنة ليتيح للمستفيدين بيع وشراء محتويات المواد من خلال الإنترنت بأسلوب آمن، ويعطينا الرسم الذي يظهر في هذه اللوحة فكرة عن بنية المعلومات في نظام التشفير.

فالمعلومات ترسل في مظروف مشفر يسمى بالحاوية، ويوقع موردو المعلومات على معلوماتهم هذه بالحاوية، ولا يمكن لمن يتلقى هذه المعلومات أن يفتح تلك الحاوية إلا بعد أن يفي بكل المتطلبات التي تفرضها سياسة إدارة الوصول، كأن يدفع مبلغاً مالياً مقابل استخدامه أو إفادته من لتلك المعلومات. ومن الملاحظ أن المحتوى لا يمكن فصله عن عملية إدارة الوصول ومعلومات الدفع في المظروف، أي أنه من الممكن إرسال المظروف لاحقاً إلى الآخرين الذين سيتوجب عليهم الدفع إذا أرادوا فتحه (مع ملاحظة أنه يجب على كل مستفيد أن يحصل على الشيفرة التي تُمكنه من فتح المظروف).

وإضافة إلى المحتوى المشفر، فقد تتضمن الحاويات المشفرة مستخلصاً ذا نص واضح يقدم وصفاً للمستفيدين عن المادة، وتشتمل المعلومات التي يتضمنها هذا المستخلص على ملخص للمادة وتعريفاً بمصدرها ومؤلفها وآخر تحديث لها وحجمها، وسعرها وشروط بيعها. وما أن يقرر المستفيد فتح محتوى هذه الحاوية المشفرة، حتى يصدر له مفتاح رقمي يمكنه من فتحها. ولمشاهدة أحد مفردات هذه المواد بشكل مجاني، ما على المستفيد سوى الضغط على المستخلص، وبالتالي تظهر له المعلومات على سطح المكتب، فإذا أراد مشاهدة المحتوى الذي لابد من دفع مقابل مادي له، على المستفيد الموافقة على شروط استخدام الحاوية المشفرة كما هو موضح في المستخلص.

ويمكن أن تكون محتويات الحاوية المشفرة مركبة أو غير ثابتة dynamic، لأن النظام به إمكانية تغطية خطوط جافا وبرامج جافا وغيرها من البرامج التي تُسكّن المحتوى في حاويات آمنة. وفي سياق الاهتمام بالتوصيف في هذا المجال، رخصت شركة آي بي إم لغة حقوق الملكية الرقمية التي وضعتها شركة زيروكس لتحديد القواعد التي تحكم استخدام المحتوى وتسعيره.

بيان بالمواد	
نص واضح	
تعليمات بصمة الأصابع والدفع بالعلامات المائية المشفرة	
جزء مشفر من الوثيقة	تسجيلة أساسية
جزء مشفر من الوثيقة	تسجيلة أساسية
جزء مشفر من الوثيقة	تسجيلة أساسية

الشروط والضوابط
حماية السلامة والتوقيعات

أمن المكتبات الرقمية Security of Digital Library:

نتناول فيما تبقى من هذا الفصل بعض الوسائل الأساسية لأمن المعلومات التي تستخدم في نظم الحاسبات بالشبكة، وهي وسائل لا يقتصر استخدامها على المكتبات الرقمية، بل يتجاوزها لمجالات أخرى، إلا أن المكتبات الرقمية لها حاجات خاصة بسبب أهمية الشبكات اللامركزية المتناهية لكل من موردي المعلومات والمستفيدين منها.

وتبدأ عملية الأمن من إداريي النظم، وهم أولئك الذين يقومون بتجهيز وإدارة الحاسبات الآلية والشبكات التي تترابط فيما بينها. وينبغي أن تكون أمانة هؤلاء فوق كل الشبهات لأن لديهم صلاحية الدخول على بطائن النظام، ويعمل إداريو النظم البارعين على تنظيم الشبكات وملفات النظام حتى يتمكن المستفيدون من الوصول إلى المعلومات المناسبة، كما أن عليهم إدارة كلمات المرور وإعداد ما يعرف "بالجدران النارية firewalls" لعزل أجزاء الشبكات، وتشغيل البرامج التشخيصية تحسباً للمشاكل، وعليهم كذلك عمل نسخ احتياطية من المعلومات حتى يمكن إعادة بناء النظام في حالة حدوث خلل ما، مثل أعطال التجهيزات، أو نشوب حريق، أو حدوث اختراق لإجراءات الأمن.

إن شبكة الإنترنت ليست آمنة؛ إذ يستطيع الكثيرون التلصص ومراقبة المعلومات المتوافرة، وقد يحدث هذا الدخول بشكل مشروع من أجل حل

مشكلة ما، لكنه يمكن أن يحدث لأغراض لا تمت للأمانة والنزاهة بصلة. والسؤال هنا بوجه عام عن الأمن هو:كيف يمكن بناء تطبيقات آمنة عبر هذه الشبكة غير الآمنة ؟

وطالما أن الإنترنت لا تتوافر لها ضمانات الأمن الكافية؛ فإن أمن المكتبات الرقمية يبدأ من الحاسبات التي تشكل بنية هذه المكتبات، ومن المعلومات الموجودة بها، مع تركيز الاهتمام على إجراءات الاتصال بين تلك الحاسبات والشبكات المحلية. وبالنسبة لكثير من الحاسبات الشخصية ليس هناك من سبيل للأمن إلا بتقييد عدد من يستخدمونها، ولبعض الحاسبات الأخرى برامج حماية لا تزيد عن وضع كلمات مرور وأسماء مستخدمين مبسطة، وعندما يشترك أكثر من مستخدم في استعمال الحاسبات يجب اتخاذ إجراءات تحكم لتحديد من يقرأ ومن يكتب في كل ملف.

والخطوة التالية في عملية الحماية تتمثل في ضبط إجراءات الاتصال بين الشبكات المحلية وشبكة الإنترنت الموسعة، وتوفير حاجز في وجه المتطفلين من الخارج، والحاجز الأكمل هو العزل أو الفصل isolation ، أي منع أية اتصالات خارجية بالشبكة. وهناك وسيلة أكثر جدوى في هذا الصدد، وهي أن يتم وصل الشبكة المحلية أو الداخلية بالإنترنت عبر حاسب ذي هدف مخصص يسمى "بالجدار الناري أو جدار الحماية firewall"، الذي يعمل على مراقبة كل حزمة معلومات تحاول المرور عبر الشبكة، ومنع أولئك الذين يحاولون انتهاك إجراءات الأمن. و جدران الحماية هذه يمكنها كذلك منع المحاولات الخارجية للاتصال بالحاسبات

داخل المنظمة أو الشركة، أو أنها تستطيع أن ترفض الحزم التي لا تتفق وقائمة البروتوكولات المعتمدة، ويمكن لهذه الجدر النارية إذا ما أحسن إداراتها أن تكون على درجة عالية من الفعالية في إيقاف المتطفلين عند حدودهم.

ولقد كانت الجامعات في صدارة المؤسسات التي استخدمت شبكات الحاسبات منذ عدة سنوات مضت، ورغم كثرة المستفيدين وتنوعهم، فقد نجحت في وضع نظم آمنة لتأمين شبكات الحاسبات داخل المدن الجامعية campus network التي تضم آلاف الحاسبات، صحيح قد تحدث بعض الانتهاكات وسلوكيات الاستخدام غير السوي في كل جامعة، لكن من النادر أن يحدث عطل كامل في شبكة الحاسبات.

وإذا روعي الحرص والاهتمام في إدارة الشبكات، فإن الحاسبات المرتبطة بإحدى الشبكات يمكن أن يتوافر لها قدر كبير من دواعي الأمن، إلا أن هناك عدة طرق يمكن أن يحتال بها من يريد انتهاك إجراءات الأمن. وفي الجامعات تأتي معظم المشاكل ممن يعملون بها من موظفين ساخطين على أوضاعهم، أو من بعض الطلبة الذين يعملون على سرقة أسماء المستخدمين وكلمات المرور الخاصة ببعض المستفيدين، أما طرق الانتهاك الأكثر فاعلية فهي تتم عن طريق برامج حاسبات خاصة بذلك، ومع أن لكل نظام تشغيل إجراءات الأمن المثبتة معه، فإن المشكلات قد تحدث بسبب الأخطاء في التصميم أو في البرمجة. وهناك برامج هامة جداً للمكتبات الرقمية كالبريد الإلكتروني وخوادم الويب يصعب تأمينها على الوجه الأكمل، ولهذه الأسباب ينبغي على من ينشئ مكتبة رقمية أن يسلم بأن ضمانات الأمن أمر بعيد

المنال، لكن مع الإصرار يمكن تحجيم هذه المخاطر، مع بقاء احتمالات الخطأ. وينبغي على مديري المكتبات الرقمية أن يتخذوا موقفاً متوازناً نحو قضية الأمن، صحيح أن ضمانات الأمن الكاملة مستحيلة، إلا أن تحقيق قدر كبير منها في نظم شبكات الحاسبات دون تكلفة باهظة أمر غير مستحيل، وإن احتاج ذلك بعض الجهد والتركيز.

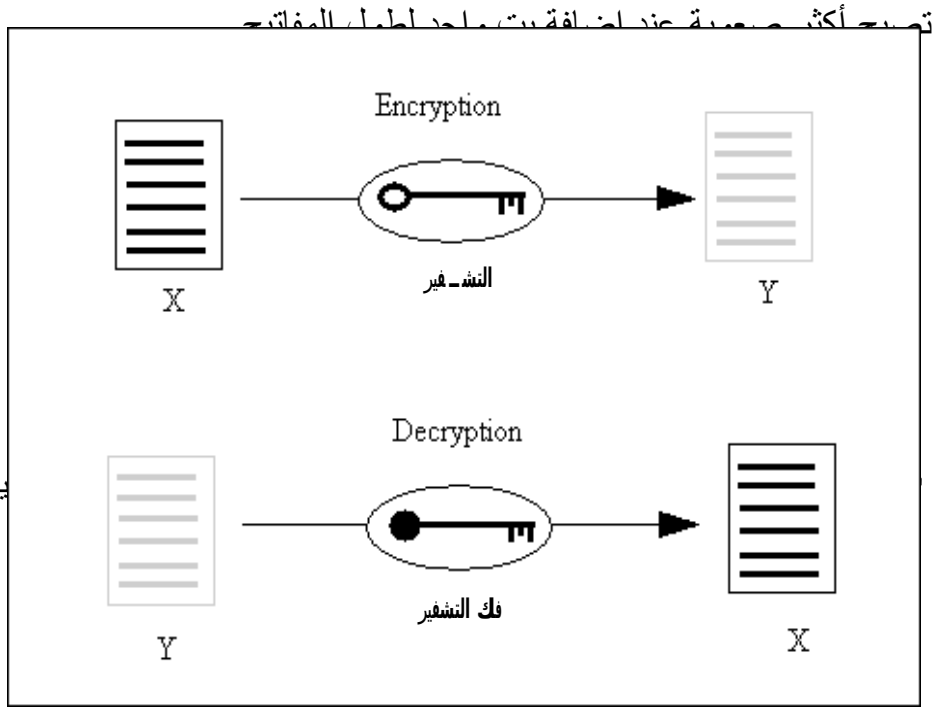
التشفير Encryption :

" التشفير" يقصد به مجموعة الأساليب الفنية المتبعة في تخزين وبث المعلومات الخاصة بطريقة مشفرة تجعلها تبدو في صورة مبعثرة أو غير منتظمة تماماً إلى أن يتم تحويلها عن طريق الإجراءات اللازمة. وحتى لو تمكن شخص غير مصرح له من الاطلاع على هذه المعلومات فلن يتمكن من تغييرها أو العبث بها. ويستخدم التشفير في المكتبات الرقمية في نقل المعلومات السرية عبر الإنترنت، وقد تبلغ بعض المعلومات مستوى من السرية يتحتم معه تشفيرها في كل مكان يتم اختزانها فيه، وتعد كلمات المرور مثالاً واضحاً للمعلومات التي يجب تشفيرها على نحو دائم سواء أكانت مختزنة في الحاسبات أم كانت مبثوثة عبر الإنترنت. وفي كثير من المكتبات الرقمية تعد كلمات المرور هي المعلومات الوحيدة التي يجب تشفيرها.

ويظهر الشكل رقم (٧-٢) الفكرة الأساسية لعملية التشفير، حيث يتم إدخال البيانات المفترض إبقاؤها سرية، والتي يرمز لها بالرمز (X)، في عملية تشفير تنطوي على تحويلات رياضية لتخرج لنا في صورة مشفرة، والتي يرمز لها بالرمز (Y)، وينبغي أن يكون لتلك البيانات التي تم تشفيرها (

Y) العدد نفسه من وحدات البتات التي كانت للبيانات الأصلية غير المشفرة. وقد تبدو هذه البيانات على أنها مجموعة غير منتظمة من الوحدات، لكن يمكن عكس العملية عن طريق مجموعة من الإجراءات المخصصة لذلك بحيث يتم استعادة البيانات في صورتها الأصلية (X)، وكلتا العمليتين - التشفير encryption وفك التشفير decryption- يمكن أن يتم تنفيذهما عن طريق برامج آلية، أو عن طريق أجهزة مخصصة لهذا الغرض.

يتم التحكم في الوسائل شائعة الاستخدام في عملية التشفير عبر زوجين من الأرقام يعرفا "بالمفاتيح keys"، يستخدم أحدهما لأغراض التشفير، ويستخدم الآخر لفك التشفير. وتتنوع وسائل التشفير من حيث الطريقة التي تختار بها المفاتيح. صحيح أن الأشكال الرياضية للعمليات ليست سراً، لكن معايير الأمن تكمن في المفاتيح ذاتها. فالمفتاح عبارة عن سلسلة من البتات التي تتروح ما بين ٤٠ إلى ١٢٠بتاً، لكنها قد تتجاوز هذا الرقم في بعض الأحيان. ومن البدهي أن تكون المفاتيح المطولة أكثر أمناً من المفاتيح القصيرة؛ لأن أي محاولة لانتهاك إجراءات الأمن من خلال تخمين المفاتيح تصبح أكثر صعوبة عند إضافة بت واحد لطول المفاتيح



الشكل رقم (٧-٢)
الفكرة الأساسية لعملية التشفير

وقد اقتصر استخدام التشفير من الناحية التاريخية على قدرات الحاسب؛ فجميع الخطوات تتطلب عمليات حاسوبية كثيرة لمزج المعلومات وإعادة ترتيبها، و قد تطلبت التطبيقات المبكرة لمعيار تشفير المعلومات DES. كما هو موضح في اللوحة رقم (٧-٤) - جهازاً خاصاً يلحق بكل حاسب آلي، أما اليوم وفي ظل وجود الحاسبات ذات السرعات العالية، فلم تعد هذه مشكلة كبيرة، غير أن الوقت المبذول في عملية التشفير وفك التشفير لا يزال أمراً ملحوظاً. وبشكل عام يمكن القول إن أساليب التشفير تثمر عن نتائج جيدة مع الرسائل القصيرة (مثل كلمات المرور)، أو الرسائل بالغة السرية التي تأتي بين حين وآخر، لكنها لا تؤدي النتيجة نفسها مع البيانات الكثيرة، وخاصة عندما يكون لسرعة الرد أهميتها البالغة.

التشفير باستخدام المفتاح الخاص .Private-key Encryption :

التشفير باستخدام المفتاح الخاص هو مجموعة أساليب يستخدم فيها المفتاح لتشفير البيانات وفك تشفيرها مع ضرورة الإبقاء على ذلك سراً. وتعرف هذه العملية أيضاً بالتشفير باستخدام المفتاح الواحد single-key encryption، أو التشفير باستخدام المفتاح السري secret - key encryption. وتقدم اللوحة رقم (٧-٤) وصفاً لمعيار تشفير البيانات الذي يعد من أكثر الأساليب استخداماً.

ولا تبدو جدوى التشفير باستخدام المفتاح الخاص إلا إذا أحاط الأمن بجميع خطواتها، فإذا أراد أحد الحاسبات إرسال معلومة مشفرة لحاسب بعيد، ينبغي عليه أن يجد الطريق الآمن تماماً لتوصيل المفتاح للحاسب

البعيد. لذلك يتم استخدام التشفير بالمفتاح الخاص على نطاق واسع في التطبيقات التي تتولى مهام تبادل المعلومات فيها تلك المرافق أو الخدمات الموثوق بها trusted services.

اللوحة رقم (٧-٤)

معيار تشفير البيانات

The Data Encrytion Standard

معيار تشفير البيانات هو وسيلة تشفير باستخدام المفتاح الخاص، طورته شركة آي بي إم، وأصبح معياراً أمريكياً منذ عام ١٩٧٧م. والواقع أن العمليات الحسابية التي يقوم بتنفيذها هذا المعيار تتسم بالبطء عندما تستخدم في برمجية حاسوبية، لكنها تكون ذات سرعة كافية للعديد من التطبيقات. وحالياً يمكن لأي حاسب شخصي أن يشفر نحو مليون بايت في الثانية الواحدة.

ويستخدم معيار تشفير البيانات مفاتيح مكونة من ٥٦ بتاً. حيث يقوم بتقسيم مجموعة البيانات إلى وحدات، كل منها مكونة من ٦٤بتاً، ويقوم بتشفير كل منها على حدة، ومن المفتاح ذي الـ ٥٦ بتاً يتولد ستة عشر مفتاحاً صغيراً، ويعتمد أساس الخوارزمية على ست عشرة عملية تحويل متتابعة للوحدات ذات الـ٦٤بتاً مستخدماً هذه المفاتيح الصغيرة بالتتابع، ويستخدم التشفير المفاتيح الستة عشر الصغيرة نفسها لتنفيذ التحويلات الراجعة في الاتجاه المعاكس، وقد يبدو هذا وكأنه عملية خوارزمية بسيطة، لكن ثمة فروقاً بسيطة، أهمها أن أنماط البتات المتولدة عن عملية التشفير تبدو عشوائية تماماً وخالية من أية إشارة تدل على البيانات أو على المفتاح.

ويذهب من يغالون في هذه المسألة إلى أن المفاتيح ذات الـ ٥٦ بتاً يمكن كسرها ببساطة عن طريق إجراء عملية التجريب لكل مفتاح يمكن معرفته، لكن هذه مهمة صعبة، والواقع أن معيار تشفير البيانات يناسب تطبيقات المكتبات الرقمية بشكل كاف.

التشفير باستخدام المفتاح المزدوج Dual-key Encryption :

عندما يتم استخدام "التشفير باستخدام المفتاح الخاص" عبر إحدى الشبكات، ينبغي أن يكون هذا المفتاح معلوماً لكل من الحاسب المرسل والحاسب المستقبل. وهو ما يمثل لغز كيفية عمل طرف منهما إذا لم يفلح جهاز الطرف الآخر في إرسال المفتاح إليه بطريقة سرية. ومن هنا جاء " التشفير باستخدام المفتاح المزدوج " ليتيح إرسال جميع المعلومات عبر الشبكة؛ ولهذا السبب اكتسب اسماً آخر، وهو "التشفير باستخدام المفتاح العام public-key encryption"، الذي تظل فيه المعلومات المشفرة حتى لو حدث اعتراض أو رصد لكل رسالة.

وتعد طريقة ريفست - شامير- أولمان Rivest-shamir-Adleman من أشهر طرق التشفير باستخدام المفتاح المزدوج. وهي تتطلب وجود مفتاحين : أحدهما عام والآخر سري، فإذا افترضنا أن شخصاً ما (وليكن (أ)) يريد أن يرسل معلومة مشفرة لشخص آخر (وليكن (ب))، فعليه أن يشفرها مستخدماً المفتاح العام للطرف (ب)، وعندما يتسلم الأخير تلك المعلومة، عليه أن يفك شفرتها مستخدماً المفتاح الخاص والذي لا يعلمه أحد سواه.

يمتاز التشفير باستخدام المفتاح المزدوج هذا بمزايا عديدة، غير أن له عيباً واحداً، وهو أن الأمر يتطلب التأكد من أن المفتاح هو فعلاً المفتاح العام

لشخص بعينه، والحل المعتاد لهذه المشكلة أن تقوم "هيئة تصديق أو إصدار شهادات الترخيص[١] certification authority " موثوق بها بعمل جميع المفاتيح والتثبت من هوياتها أو صحتها، على أن تقوم بعد ذلك بإصدار شهادات certificates عبارة عن رسائل موقعة تحدد هوية كل شخص ومفتاحه العام. وهذه الطريقة لا غبار عليها طالما لم يحدث انتهاك لإجراءات الأمن الخاصة بهيئة إصدار شهادات الترخيص هذه.

التوقيعات الرقمية Digital Signature :

كما سبق أن أسلفنا فإن التوقيع الرقمي يمكن الاستفادة منه في التأكد من عدم العبث بملف معين من ملفات الحاسب، وتعتمد التوقيعات الرقمية على فكرة " دالة المزج أو التمويه، أو القيمة الاختبارية hash function"، وهي دالة رياضية يمكن تطبيقها على بايتات "bytes" أحد ملفات الحاسب لتوليد رقم ثابت الطول.

ومن دوال المزج أو التمويه أو القيم الاختبارية شائعة الاستخدام ما تعرف بـ"إم دي فايف MD5" وهي تقوم بتحويل خاص لبتات bits أحد الملفات لتنتهي إلى ١٢٨بتاً عشوائية تماماً، ويمكن تطبيق هذه الطريقة على ملفات مختلفة الأطوال. وإذا اختلف ملفان ولو في بت واحد، انعكس ذلك الاختلاف على عملية تحويلها، والعكس لو كان هناك ملفان لهما القيمة الاختبارية نفسها hash فإن احتمالات عدم تطابقهما لا يمكن حدوثها تحت أي ظرف. ولذلك فإن من أبسط طرق التأكد من عدم العبث بأحد الملفات هي حساب " القيمة الاختبارية

(١) هناك من يسميها سلطة منح الشهادات الرقمية (المترجمان) .

MD5 hash" الخاصة به عند إنشائه، ثم يعاد بعدها بفترة معينة حساب ذلك ومقارنته بالبيانات الأصلية لرصد أي تغيير طرأ على الملف، فإذا لم تتضح أية اختلافات بين القيمتين، فهذا يعني أن الملف لا يزال كما هو دون حدوث أية تغيرات أو تدخلات.

ولطريقة دالة التحويل إم بي فايف MD5 هذه عدة مزايا منها: أنها الأسرع في حساب الملفات الكبيرة، إلا أنها - شأنها في ذلك شأن أية وسيلة أخرى من وسائل الأمن- تتعرض دائماً لاحتمال قيام مستفيد بارع بكشف طريقة عملها، وإنشاء ملف له قيمة اختبارية hash value محددة. وقد كثر الحديث أثناء إعداد هذا الكتاب عن إمكانية اختراق تلك الطريقة، وإن بقيت لها وظائف أخرى.

ولا تكشف القيمة الاختبارية عن المصدر الذي قام بحسابها، لكن التوقيع الرقمي يخطو خطوة أبعد من ذلك نحو ضمان موثوقية أي كائن بالمكتبة، فعندما يتم حساب القيمة المزجية لكائن ما، فإنها تشفر عن طريق استخدام المفتاح الخاص بصاحب المادة، وهذا ما ينشئ التوقيع الرقمي، إلى جانب المفتاح العام وجهة التصديق. وقبل أن يتأكد المستفيد من القيمة الاختبارية، يقوم بفك شيفرة التوقيع الرقمي مستخدماً المفتاح العام، فإذا تطابقت النتائج دل ذلك أن المادة لم يطرأ عليها أي تغيير، وأن التوقيع الرقمي تم إنشاؤه باستخدام المفتاح الخاص المعني بذلك.

وبرغم كل ذلك، فإن التوقيعات الرقمية ليست مجردة من النقائص، فمع أن المستفيدين من المكتبات الرقمية يرغبون في التأكد من عدم حدوث عبث

في المواد، إلا أنهم لا ينشغلون بدقائق الأمور، بل بمضمون المادة فحسب. فمكتب حق المؤلف في الولايات المتحدة على سبيل المثال يركز اهتمامه الأساسي على المحتوى الفكري، مثل كلمات النص، لكنه لا يعير اهتماماً بما إذا كان الحاسب قد أضاف بعض معلومات الحماية لأحد الملفات أم لا، أو ما إذا كان قد حدث تغيير البنط المستخدم في كتابة النصوص. لكن الفشل الذريع للتوقيع الرقمي يبدو عندما يتغير بت واحد في الملف، وحتى الآن لم تطرح طريقة ناجحة لضمان صحة المضمون وأمنه سوى التأكد من بتاته.

انتشار التشفير باستخدام المفتاح العام :

قد يتوقع المرء أن يكون التشفير باستخدام المفتاح العام قد انتشر منذ سنوات عديدة بحكم أن العمليات الرياضية الأساسية التي اعتمد عليها هذا الأسلوب معروفة منذ عشرين سنة مضت، إلا أن ذلك ليس هو الواقع - مع الأسف الشديد- فلما تزل هناك قضايا فنية هامة يتعلق كثير منها بإدارة المفاتيح وكيفية إنشائها، وكيفية تخزين المفاتيح الخاصة، وما الاحتياطات التي يمكن اتخاذها إذا ما انتهكت إجراءات الأمن في الجهة المسؤولة عن المفاتيح. ومع ذلك ينبغي أن تراعى الأسباب الرئيسية للتأجيل في نشرها بشيء من التصرف الدبلوماسي أو السياسي.

فهناك أولاً مشكلة براءات اختراع البرمجيات (وهو ما سبق تناوله في الفصل السادس). فلا خلاف بين معظم علماء الحاسب الآلي على أن مجال التشفير باستخدام المفتاح العام هو أحد المجالات القليلة في عالم الحاسب الآلي الذي شهد ابتكارات حقيقية. يضاف إلى ذلك أن وسائل التشفير ليست

واضحة، وأن مخترعيها يستحقون المكافأة على اختراعهم، ومع الأسف فإن أصحاب براءات الاختراع ووكلاءهم قد انتهجوا سياسات محدودة في منح التراخيص والتي قلصت من سرعة انتشارها.

لكن العائق الأكبر خطراً تمثل في تدخل الجهات الحكومية الأمريكية، إذ تدعي وكالة الاستخبارات المركزية أن تقنية التشفير تدخل في إطار الأسرار العسكرية، ومن ثم فإن تصديرها للخارج يهدد الأمن القومي للولايات المتحدة الأمريكية، كما يدعي مكتب التحقيقات الفيدرالية أن الأمن العام يعتمد على قدرته في تفسير وقراءة أي رسالة على الإنترنت عند تخويله بذلك. وفيما يخص تصدير التقنيات فإنه من الصعب التسليم بها في ظل الانتشار الواسع لوسائل التشفير في أنحاء العالم، وفي ظل قيام شركات أوربية ويابانية لها وزنها بتسويق منتجات التشفير. أما مسألة الحفاظ على الأمن العام فهي لا تقل تعقيداً، لكن الذي يهون من شأنها أن الشعب الأمريكي لا يثق في القدرات الفنية لوكالة الاستخبارات المركزية وغيرها من هيئات الشرطة ولا في إجراءاتهم الإدارية، ولا هم للناس سوى أنهم يريدون إرسال معلوماتهم السرية دون أن يراقبها أحد.

ومن المناسب أن يختتم هذا الفصل بإشكالية تعكس كيف تقوض مصاعب السياسة قدرات الحلول الفنية. وهو ما يعكس فكرة تتردد في مجال المكتبات الرقمية، ولها أهميتها الخاصة في إدارة الوصول إلى مواد تلك المكتبات، وهي الارتباط الوثيق بين الناس أو المستفيدين من جهة، والتقنية من ناحية ثانية، والإجراءات الإدارية من ناحية ثالثة. والمكتبات الرقمية الناجحة هي التي تجمع بين جوانب جميع هذه الأطراف الثلاثة ولا تعتمد على التقنيات

وحدها.