9

الفصل التاسع

المتسللون (INTRUDERS)

محتويات الفصل:

اتفقوا على أن يتولى جراهام وضع الاختبار لتشارلز مابليدين. كان الاختبار أن يحصل دراجون على شفرة شتيرن – لا أكثر ولا أقل. فلو كان لديه الـ "in" الموجودة في "Utting" كما يدّعى فسيكون ذلك ممكناً، ولا يمكن أن يحول دون ذلك إلا الولاء لمحطة موسكو المركزية فقط. أما اذا حصل على مفتاح الشفرة فسيثبت ولاءه لمحطة لندن المركزية بدون أدنى شك.

— الحديث إلى رجال غرباء، روث رينديل

النقاط الرئيسة

- يُعدُّ التسلل إلى نظام أو شبكة حاسب واحداً من أخطر التهديدات لأمن أنظمة الحاسب.
- تم تطوير أنظمة اكتشاف التسلل لتوفير الإنذار المبكر عند حدوث تسلل كي يتسنى اتخاذ الإجراءات الدفاعية الكفيلة بمنع الضرر أو تقليله من جرّاء ذلك التسلل.
- يتضمن اكتشاف التسلل الكشف عن أنماط غير عادية من النشاط أو أنماط من النشاط معروف أنها ترتبط بعملية التسلل.
- تُعدُّ إدارة كلمات السر أحد العناصر المهمة لمنع التسلل، وذلك بهدف منع المستخدمين غير المرخّص لهم من الوصول إلى كلمات السر الخاصة بالمستخدمين الآخرين.

من المشكلات الأمنية الكبيرة لأنظمة الشبكات محاولات التسلل المعادية، أو على الأقل غير المرغوب فيها، سواءً من قِبَل مستخدمين أو من قِبَل برمجيات. أما التسلل من قِبَل المستخدمين فقد يأخذ شكل دخول غير مصرّح به (unauthorized logon) إلى أحد الأجهزة، أو – في حالة المُستخدِم المصرّح له – قد يتمثل في حصوله على امتيازات أو قيامه بأعمال تتجاوز تلك المرخّص له بها. أما التسلل من قِبَل البرمجيات فقد يتمثّل في صورة فيروس، أو دودة، أو حصان طروادة.

تتعلق كل تلك الهجمات بأمن الشبكة لأن الدخول إلى النظام يمكن أن يتم عن طريق الشبكة. ومع ذلك، لا تقتصر تلك الهجمات فقط على هجمات أساسها الشبكة. فقد يحاول مستخدم لديه إمكانية للوصول إلى محطة طرفية محلية التسلل إلى النظام دون اللجوء إلى شبكة وسيطة. كما يمكن إدخال فيروس أو حصان طروادة إلى النظام عن طريق قرص مرن. الدودة هي الظاهرة الوحيدة التي ترتبط فقط بالشبكات. وعليه، فإن التسلل إلى النظام يمثل المجال المشترك الذي يلتقي فيه أمن الشبكة مع أمن الحاسب.

نظراً لأن هذا الكتاب يركّز أساساً على أمن الشبكات، فلن نحاول القيام بتحليل شامل لا للهجمات ولا للإجراءات المضادة فيما يتعلق بالتسلل إلى النظام. وبدلاً من ذلك سنُلقي في هذا الباب نظرة عامة واسعة على تلك المخاوف.

يغطي هذا الفصل موضوع المتسللين. سنناقش أولاً طبيعة الهجوم ، ثم نتناول الاستراتيجيات المستخدمة لمنعه، أو اكتشافه إذا تعذر ذلك. بعدها نغطي الموضوع ذا الصلة والمتعلق بإدارة كلمات السر.

9-1 المتسللون

يشكّل المتسللون أحد أشد خطرين يهددان أمن أنظمة الحاسب (الخطر الآخر هو الفيروسات)، ويطلق عليهم بشكلٍ عام القراصنة أو مكسّرو الشفرات. في دراسة مبكرة ومهمة عن التسلل، حدد أندرسون [ANDE80] ثلاث فئات من المتسللين:

- المتنكّر (Masquerader): شخص غير مخوّل له استخدام نظام الحاسب ولكنه يخترق نظام التحكم في الدخول إلى النظام لاستغلال حساب مستخدم شرعي.
- مسيء التصرف (Misfeasor): مستخدم شرعي للنظام ولكنه يصل إلى بيانات أو برامج أو موارد غير مخوّلٍ الوصول إليها، أو أنه مخوّل له الوصول إليها ولكنه يسيء استخدام الصلاحيات المعطاة له.

- المُستخدِم السري (Clandestine user): شخص يستولي على وسائل التحكم الإشرافي على النظام ويستغل ذلك للتهرب من عمليات المراجعة والتحكم في الوصول أو لمنع عمليات جمع سجلات المراجعة.

من المرجّح أن يكون المتنكر شخصاً من خارج النظام، بينما يكون مسيء التصرف عموماً من داخله، أما المُستخدِم السري فقد يكون من الخارج أو من الداخل.

تتفاوت هجمات التسلل من الحميدة إلى الخطيرة. ففي الناحية الحميدة، يوجد كثير من الأشخاص الذين يرغبون ببساطة في مجرد استكشاف شبكات الإنترنت ليرَوا ماذا يقبع على الطرف الآخر هناك. أما في الناحية الخطيرة فهناك أشخاص يحاولون قراءة بيانات خصوصية، أو إجراء تعديلات غير مصرّح بها على البيانات، أو عرقلة عمل النظام.

لقد انتشر الحديث عن تهديدات التسلل، لا سيما إثر حادث قرصان ويلي "Wily Hacker" الشهير في عامي 1986 و1987، والذي قام بتوثيقه كليف ستول [STOL88, 89]. وقد شهد عام 1990 حملة وطنية على قراصنة الحاسب المحظورين تضمنت اعتقالات، وتهماً جنائية، ومحاكمة شهيرة لعدة جلسات، والعديد من الاعترافات، ومصادرة كميات كبيرة من البيانات ومعدات الحاسب [STER92]. وعندئذٍ اعتقد كثيرٌ من الناس أن المشكلة قد تم السيطرة عليها.

في واقع الأمر، لم تتم السيطرة على المشكلة. كمثال واحد على ذلك، أفاد فريق من مختبرات بيل (Bell Labs) [BELL93, BELL92] بوقوع هجمات متكررة وبإصرار على أنظمة الحاسب لديها عبر شبكة الإنترنت على مدى فترة زمنية طويلة ومن مصادر متنوعة. في فترة إعداد تلك التقارير، واجهت مجموعة بيل ما يأتي:

- محاولات لنسخ ملف كلمة السر (والذي سنناقشه لاحقاً)، بمعدّل تجاوز مرة كل يومين.

- نداء إجراء مشبوه عن بُعد (remote procedure call (RPC))، بمعدّل تجاوز مرة كل أسبوع.
- محاولات للاتصال بأجهزة حاسب وهمية تُستخدَم كطُعم (bait)، على الأقل مرة كل أسبوعين.

قد تكون هجمات المتسللين الحميدة مقبولة، ولكنها تستهلك موارد النظام وقد تؤدي إلى إبطاء أداء النظام للمستخدمين الشرعيين. ومع ذلك، لا توجد وسيلة لكي نعرف مسبقاً ما إذا كان هجوم المتسلل سيكون حميداً أو خبيثاً. ومن ثم فحتى بالنسبة للأنظمة التي لا تتضمن موارد حساسة بشكلٍ خاص، هناك مايبرر محاولة السيطرة على تلك المشكلة.

من الأمثلة التي توضّح بشكلٍ كبير حجم التهديد المحتمل، ما حدث في جامعة Texas A&M [SAFF93]. ففي أغسطس 1992 تم إبلاغ مركز الحاسب بالجامعة أن أحد الأجهزة يُستخدم في الهجوم على أجهزة حاسب في مكان آخر عبر الإنترنت. ومن خلال مراقبة النشاط علِم موظفو مركز الحاسب بوجود مجموعة من المتسللين الخارجيين يقومون بتشغيل برامج لفك شفرات كلمات السر على عددٍ من أجهزة الحاسب (يضم الموقع ما مجموعه 12,000 جهاز موصلة فيما بينها بشبكات). وقام المركز بفصل الأجهزة المتضررة وسد الفجوات الأمنية المعروفة ثم استأنف العمل كالمعتاد. وبعد بضعة أيام، اكتشف أحد مديري النظام المحليين أن هجوم التسلل قد استُؤنف. واتضح عندئذٍ أن الهجوم كان أكثر تعقيدا مما كان يُظنّ في البداية. وتم العثور على ملفات تحتوي على المئات من كلمات السر التي تم الاستحواذ عليها، بما في ذلك بعض الكلمات الخاصة بخوادم رئيسة من المُفترض أنها آمنة. وبالإضافة إلى ذلك، كان القراصنة قد اتخذوا من أحد الأجهزة المحلية لوحة إعلانات (bulletin board) خاصة بهم يستخدمونها للاتصال فيما بينهم ولمناقشة الأساليب التي يستخدمونها والتقدم الذي يحرزونه.

تبيّن من تحليل ذلك الهجوم أنه كان هناك بالفعل مستويان من القراصنة. تضمّن المستوى الأعلى المستخدمين المحترفين الذين كانوا على معرفة دقيقة

بالتقنية والأساليب المستخدمة، في حين تضمّن المستوى الأدنى "جنود المشاة" الذين اقتصر دورهم فقط على استخدام برامج تكسير الشفرات دون الحاجة إلى فهم عميق لكيفية عملها. ولقد جمع فريق العمل هذا أخطر سلاحيْن في ترسانة المتسللين: معرفة متطورة بكيفية التسلل من جهة، والاستعداد لقضاء الساعات الطويلة في محاولات "لفتح مقابض الأبواب" بحثاً عن نقاط الضعف من جهة أخرى.

كان من نتائج الوعي المتزايد بمشكلة التسلل إنشاء عدد من فرق الاستجابة لطوارئ الحاسب (computer emergency response teams (CERTs)). تقوم تلك المشاريع التعاونية بجمع المعلومات عن نقاط الضعف في الأنظمة ونشرها بين مديري النظم. وللأسف، يمكن للقراصنة أيضاً الوصول إلى تقارير CERT. وفي حادث جامعة Texas A&M، أظهرت التحاليل التي أُجريت لاحقاً أن القراصنة قاموا بتطوير برامج لاختبار الأجهزة التي تعرضت للهجوم بحثاً عن كل نقاط الضعف تقريبا التي سبق وأُعلن عنها في تقارير CERT. في حال عدم الاستجابة على الفور للتعليمات التي يوصي بها تقرير CERT، حتى ولو على جهازٍ واحدٍ، فإنه يصبح عُرضةً لمثل تلك الهجمات.

بالإضافة إلى تشغيل برامجَ لتكسير كلمات السر، حاول المتسللون تعديل برمجيات التحكم في الدخول (login software) لتمكينهم من الاستيلاء على كلمات السر الخاصة بالمستخدمين أثناء دخولهم إلى النظام. وقد مكّنهم ذلك من حشد مجموعة مُبهرة من كلمات السر التي تمكنوا من الاستيلاء عليها وجعلوها متاحةً على لوحة إعلانات أقاموها على أحد الأجهزة ضمن النظام الضحية.

سنُلقي في هذا الباب نظرةً على الأساليب المستخدمة للتسلل، ثم ننظر في الطرق المختلفة المستخدمة لاكتشاف التسلسل، وأخيراً نتناول أساليب منع التسلسل المبنية على كلمة السر.

9-1-1 أساليب التسلل

يهدف المتسلل إلى الدخول على نظام أو توسيع نطاق الامتيازات المصرّح له بها على النظام. وعموماً، يتطلب ذلك حصول المتسلل على معلومات من المُفترض أن تكون محميَّة. وفي بعض الحالات، تأخذ تلك المعلومات شكل كلمة السر لمستخدم. وبمعرفة كلمة السر لمستخدم شرعي، يتمكّن المتسلل من الدخول على النظام وممارسة جميع الامتيازات الممنوحة لذلك المستخدم. عادةً، يجب أن يحتفظ النظام بملف يربط مابين كل كلمة سر والمُستخدِم الشرعي الذي يستخدمها. إذا كان هذا الملف مُخزّناً بدون حماية، فسيكون من السهل الوصول إليه ومعرفة كلمات السر منه. ويمكن حماية ملف كلمات السر بإحدى طريقتين:

- استخدام دالة أحادية الاتجاه: يخزّن النظام فقط قيمة دالة مبنية على كلمة سر المستخدِم. وعندما يقوم المُستخدِم بإدخال كلمة السر للدخول على النظام، يُحول النظام كلمة السر تلك باستخدام نفس الدالة ويقارن النتيجة بالقيمة المخزنة. عملياً، يستخدم النظام عادةً دالة باتجاه واحد، (أي غير انعكاسية (not reversible) تُستخدم فيه كلمة السر لتوليد مفتاح للدالة ويتم إنتاج مُخرج له طول ثابت.
- التحكم في الوصول للملف: تُقصر صلاحية الوصول إلى ملف كلمات السر على واحد أو عدد قليل جداً من الحسابات على النظام.

إذا استُخدمت إحدى الطريقتين أعلاه أو كلاهما، فسيتطلب الأمر من متسلل حريص بذل بعض الجهد لمعرفة كلمات السر. على أساس دراسة الأدبيات ومقابلات أُجريت مع هواة اكتشاف كلمات السر، يذكر [ALVA90] الأساليب التالية لمعرفة كلمات السر:

1. جرّب استخدام كلمات السر الافتراضية (default) للحسابات القياسية التي تُشحن مع النظام. كثيرٌ من مديري الأنظمة لا يكلّفون أنفسهم عناء تغيير تلك الإعدادات الافتراضية.

2. جرّب بشكلٍ استقصائي جميع كلمات السر القصيرة التي تتكوّن من واحد إلى ثلاثة أحرف.
3. جرّب الكلمات المستخدمة في قاموس النظام على شبكة الإنترنت أو في قائمة كلمات السر المُحتملة. وتوجد أمثلة للكلمات من النوع الأخير متاحة على لوحات الإعلانات الخاصة بالقراصنة.
4. اجمع معلومات عن المستخدمين، كأسمائهم بالكامل، وأسماء الزوج/الزوجة والأطفال، والصور في مكاتبهم، والكتب المتعلقة بالهوايات في مكاتبهم.
5. جرّب استخدام أرقام الهواتف، وأرقام الضمان الاجتماعي، وأرقام الغرف الخاصة بالمستخدمين.
6. جرّب جميع أرقام لوحات السيارات المشروعة في تلك الولاية.
7. استخدم حصان طروادة (سيأتي وصفه في الفصل العاشر) للالتفاف حول القيود المفروضة على الوصول.
8. تنصّت على الخط الواصل بين مستخدم عن بعد والنظام المضيف.

الأساليب الستة الأول هي طرق مختلفة لتخمين كلمة السر. وإذا كان على المتسلل التحقق من صحة تخمينه بمحاولة الدخول يدوياً على النظام، فهذا أمر مُضنٍ ويمكن إحباطه بسهولة. فعلى سبيل المثال، يمكن للنظام ببساطة رفض أي دخول على النظام بعد ثلاث محاولات لإدخال كلمة السر، مما يتطلب من المتسلل إعادة الاتصال بالمضيف لمعاودة المحاولة من جديد. وفي ظل تلك الظروف، ليس من العملي محاولة أكثر من حفنة من كلمات السر. ومع ذلك، فإنه من غير المرجّح أن يحاول المتسلل تلك الأساليب الساذجة. فعلى سبيل المثال، إذا تمكن متسلل بمستوى منخفض من الامتيازات من الوصول إلى ملف مُشفَّر لكلمات السر، فقد تتضمن خطته الاستيلاء على ذلك الملف، ثم استخدام آلية التشفير لذلك النظام وأخذ الوقت الكافي لاكتشاف كلمة سر توفر له امتيازات أكبر.

هجمات تخمين كلمات السر ممكنة، بل قد تكون فعّالة للغاية، إذا أمكن القيام بتجربة عدد كبير من التخمينات آلياً والتحقق من كل تخمين بدون الكشف عن عملية التخمين. ولاحقاً في هذا الفصل، سنورد الكثير عن إحباط هجمات التخمين.

قد يكون من الصعوبة بمكان التمكن من إحباط الأسلوب السابع للهجوم (استخدام حصان طروادة). ويتضمن [ALVA90] مثالاً لبرنامج يمكنه الالتفاف حول القيود المفروضة على الوصول. حيث قام مستخدمٌ ذو امتيازات منخفضة بتطوير برنامج ألعاب ودعا مشغّل النظام لاستخدامه للتسلية في وقت فراغه. وكان البرنامج فعلاً يشغّل لعبة، ولكن في الخلفية كان يتضمن أيضاً كوداً لنسخ ملف كلمات السر الذي كان في هذه الحالة غير مُشفَّر ولكن الوصول إليه كان محمياً. ونظراً لأن برنامج اللعبة كان يتم تشغيله في نمط الامتيازات العالية التي يتمتع بها مشغل النظام، فقد كان بمقدوره الوصول إلى ملف كلمات السر.

يتعلق الهجوم الثامن في القائمة، التنصت على الخط، بمسألة الأمن المادي. ويمكن مواجهته باستخدام أساليب تشفير الوصلة التي تناولناها في الفصل الثاني.

هناك أساليب أخرى للتسلل لا تحتاج لمعرفة كلمة سر. فبوسع المتسللين الدخول على نظام باستخدام هجمات كهجوم فيضان المخزن المؤقت (buffer overflows) على برنامج يعمل بمستوى معين من الامتيازات. كما يمكن للمتسلل محاولة ترقية مستوى الامتيازات المتاحة له بنفس الطريقة.

ننتقل الآن إلى مناقشة النوعين الأساسين من الإجراءات المضادة: الاكتشاف والوقاية. ويعني الاكتشاف العلم بالهجوم، سواءً قبل نجاحه أو بعده. أما الوقاية فهي الغاية الأمنية صعبة التحقيق والتي تمثل تحدياً قائماً في جميع الأوقات. وتكمن الصعوبة هنا في حقيقة أنه في حين يتعين على المدافع محاولة إحباط كل الهجمات الممكنة، يكون للمهاجم الحرية في محاولة للعثور على الحلقة الأضعف في سلسلة الدفاعات ومن ثم الهجوم منها.

9-2 اكتشاف التسلل

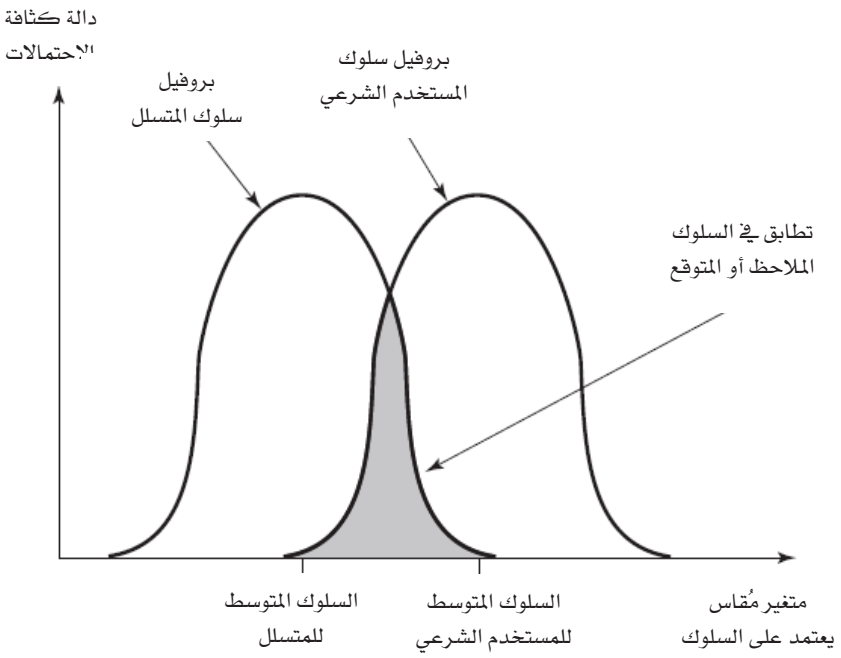
حتى أفضل نظام لمنع التسلل لا بد أن يصاب حتماً بالفشل. ويمثل اكتشاف التسلل خط الدفاع الثاني عن النظام. وكان هذا الموضوع المحور الذي دار حوله كثير من البحوث في السنوات الأخيرة، وكان الدافع وراء ذلك عدة اعتبارات نذكر منها ما يأتي:

1. إذا أمكن اكتشاف التسلل بالسرعة الكافية، فسيتسنى التعرف على المتسلل وطرده من النظام قبل أن يتمكن من إلحاق أي ضرر أو الاستيلاء على أية بيانات أو العبث بها. حتى إذا لم يتم الاكتشاف بسرعة كافية للحيلولة دون حدوث التسلل، فكلما كان الاكتشاف سريعاً، أمكن تقليل الضرر الناجم واستعادة عمل النظام بصورة طبيعية بسرعة أكبر.
2. يمكن أن يكون النظام الفعّال لاكتشاف التسلل بمثابة رادع يسهم في منع عمليات التسلل.
3. يسمح نظام اكتشاف التسلل بجمع المعلومات عن أساليب التسلل التي يمكن أن تُستخدم بدورها لتعزيز قدرة النظام على منع التسلل.

يعتمد اكتشاف التسلل على افتراض أن سلوك المتسلل يختلف عن سلوك المُستخدِم الشرعي من عدة وجوه يمكن تحديدها بشكلٍ كمّي. وبطبيعة الحال، لا يمكننا أن نتوقع أن يكون هناك حد فاصل واضح يميز بالضبط وبشكلٍ قطعي بين هجوم متسلل والاستخدام الطبيعي للموارد من قِبَل مستخدم شرعي. أي أنه يتعين علينا أن نتوقع بعض التماثل.

يوضّح الشكل 9-1، بأسلوبٍ مجرد للغاية، طبيعة المهمة التي تواجه مصممو نظم االكتشاف التسلل. فرغم أن البروفيل (الشكل العام) للسلوك النمطي للمتسلل يختلف عنه للمستخدم الشرعي، فهناك قدرٌ من الشبه بين هذين السلوكين. ومن ثم ، فإن تعريفاً فضفاضاً لسلوك المتسلل سيكون قادراً على كشف عددٍ أكبر من المتسللين، ولكنه في المقابل سيؤدي إلى عدد من الإنذارات الكاذبة أو ما يسمى

بالأخطاء الإيجابية الكاذبة (false positives) حيث سيُصنَّف عددٌ أكبر من المستخدمين الشرعيين على أنهم متسللون. وعلى الجانب الآخر، فإن محاولة الحد من الإنذارات الكاذبة عن طريق تضييق تعريف سلوك المتسلل ستؤدي إلى زيادة عدد المتسللين الذين يفشل النظام في التعرف عليهم كمتسللين ويصنفهم كمستخدمين شرعيين أو ما يسمى بالأخطاء السلبية الكاذبة (false negatives) بطريق الخطأ. ومن ثم تتطلب ممارسة اكتشاف التسلل قدراً من الموازنة والحنكة.



الشكل 9-1 بروفيلات لسلوك المتسللين وسلوك المستخدمين الشرعيين.

في دراسة لأندرسون [ANDE80] افترض فيها أنه يمكن، وبقدر معقول من الثقة، التمييز بين المتنكّر (masquerader) والمُستخدِم الشرعي. فبملاحظة التاريخ الماضي يمكن استنباط أنماط سلوك المستخدمين الشرعيين ، ومن ثم اكتشاف أي انحراف كبير عن تلك الأنماط. وقد ألمح أندرسون إلى أن مهمة كشف مسيء التصرف (misfeasor) (المُستخدِم الشرعي الذي يتصرف بطريقة غير مشروعة) تُعدُّ أكثر صعوبة، حيث إن الفرق بين السلوك الطبيعي والسلوك غير الطبيعي في هذه الحالة قد يكون ضئيلاً. وقد استنتج أندرسون أن مثل تلك الانتهاكات لن يتسنّى اكتشافها من خلال البحث عن السلوك الشاذ فقط. ومع ذلك، فقد يتسنّى اكتشاف سلوك مسيء التصرف عن طريق تعريف ذكي لمجموعة الشروط التي توحي بالاستخدام غير المشروع. وأخيرا فقد خَلُصت الدراسة إلى أن اكتشاف المُستخدِم السري يتجاوز إمكانات أساليب البحث الآلي البحتة. ومن الجدير بالذكر أن هذه الملاحظات التي قُدِّمت في عام 1980 لا تزال صحيحة اليوم.

حدَّد [PORR92] الأساليب الآتية لاكتشاف التسلل:

1. اكتشاف الشذوذ الإحصائي (Statistical anomaly detection): يتضمن ذلك جمع البيانات المتعلقة بسلوك المستخدمين الشرعيين على مدى فترة من الزمن. ثم إجراء اختبارات إحصائية على السلوك الملاحَظ لتحديدإمكانية الجزم ، بدرجة عالية من الثقة، أن ذلك السلوك ليس بسلوك مستخدم شرعي. هناك نوعان من هذا الأسلوب:

   a. الاكتشاف بالعتبة (Threshold detection): يتضمن ذلك تحديد عتبات، لاتعتمد على المستخدم، لمعدلات تكرار وقوع الأحداث المختلفة.

   b. الاكتشاف المبني على البروفيل (Profile based detection): يتم تحضير بروفيل لنشاط كل مستخدم واستخدامه لاكتشاف أي تغيّرات في سلوك حسابات الأفراد.

2. الاكتشاف بناءً على قواعد (Rule-based detection): يتضمن ذلك محاولة التوصل إلى مجموعة من القواعد التي يمكن استخدامها لتقرير ما إذا كان السلوك الملاحَظ صادراً عن متسلل. هناك نوعان من هذا الأسلوب:

a. اكتشاف الشذوذ: تُصمم القواعد بحيث تكشف عن الانحراف الحاصل عن أنماط الاستخدام السابقة.

b. التعرف على نوع الاختراق الناتج: يُستخدم نظام خبير (expert system) للبحث عن السلوكيات المشبوهة.

وباختصار، يمكن القول بأن الطرق الإحصائية تسعى لتحديد السلوك الطبيعي أو المتوقع، في حين تحاول الطرق القائمة على استخدام قواعد تعريف السلوك السليم.

من حيث أنواع المهاجمين المذكورة آنفا، يُلاحظ أن أساليب اكتشاف الشذوذ الإحصائي تُعدُّ فعّالة ضد فئة المتكّرين، حيث يُستبعد أن يقلد هؤلاء أنماط السلوك للحسابات التي استحوذوا عليها. ومن ناحية أخرى، فإن تلك الأساليب قد لا تكون قادرة على التعامل مع مسيئي التصرف. وتكون الأساليب المبنية على استخدام قواعد أكثر قدرةً على كشف هجمات هؤلاء، وذلك بالتعرف على أحداث وسلاسل زمنية معينة قد تؤدي - عند أخذها في السياق الملائم - للكشف عن اختراقات من ذلك النوع. وفي واقع الأمر، قد يجمع نظام اكتشاف التسلل مابين هذين الأسلوبين الأساسيين ليكون فعَّالا ضد تشكيلة واسعة من الهجمات.

9-2-1 سجلات المراجعة (Audit Records)

تُعدُ سجلات المراجعة أداة أساسية لاكتشاف التسلل، حيث يُحتفظ بسجلات عن النشاطات التي يقوم بها المستخدمون على النظام، و تُستخدم تلك السجلات كمُدخل إلى نظام اكتشاف التسلل. في هذا الصدد هناك خطتان أساسيتان:

- سجلات المراجعة المحلية: تتضمن كل أنظمة التشغيل تقريباً التي تدعم عدة مستخدمين برمجيات محاسبة تقوم بجمع معلومات عن نشاط المستخدم. من مزايا استخدام هذه المعلومات أننا لن نكون بحاجة إلى

إضافة برمجيات خاصة لجمع المعلومات. وتكمن المشكلة هنا في أن سجلات المراجعة المحلية قد لا تشمل المعلومات المطلوبة، أو قد لا توفرها بشكلٍ مناسب.

- سجلات المراجعة الخاصة باكتشاف التسلل: يمكن ترتيب آلية لجمع المعلومات وتوفير سجلات مراجعة تتضمّن فقط المعلومات المطلوب إدخالها إلى نظام اكتشاف التسلل. ومن مزايا هذه الطريقة أنه يمكن تصميم تلك الآلية بحيث تكون مستقلة عن المُوَرِّد ومن ثم تركيبها على عدة أنظمة مختلفة. ومن عيوب هذه الطريقة التعقيدات الناتجة عن وجود برنامجيْن للمحاسبة يعملان في الواقع جنباً إلى جنب على كل نظامٍ للحاسب. من الأمثلة الجيدة لأنظمة سجلات المراجعة الخاصة باكتشاف التسلل ذلك النظام الذي قامت بتطويره دوروثي دينج [DENN87]. يتضمن كل سجل مراجعة الحقول الآتية:

- الفاعل (Subject): وهو منشئ الإجراء. وعادةً يكون الفاعل أحد مستخدمي محطة طرفية (terminal user)، أو قد يكون عملية تنفّذ نيابةً عن مستخدم أو عن مجموعة من المستخدمين. تنجم كل الأنشطة عن أوامر يُصدرها الفاعلون. ويمكن تقسيم الفاعلين إلى فئات مختلفة من حيث وصولهم إلى النظام، وقد تتداخل تلك الفئات.

- الفعل (الإجراء) (Action): العملية التي يقوم بها الفاعل أو التي يتم إجراؤها على المفعول به، مثلاً كالدخول على النظام، أوالقراءة، أوالقيام بإدخال/إخراج بيانات أو التنفيذ.

- المفعول به (Object): مُتلقّي الفعل. ومن أمثلة ذلك الملفات والبرامج والرسائل والسجلات والمحطات الطرفية والطابعات، وهياكل البيانات من إنشاء المُستخدِم أو البرامج. عندما يكون متلقّي الفعل هو فاعل آخر، كما في حالة تلقّي رسالة بريد إلكتروني، فإن ذلك الفاعل يُعدُّ في هذه الحالة مفعولاً به. يمكن تصنيف المفعول بهم حسب النوع. قد تختلف درجة خشونة المفعول به (object granularity) حسب نوع المفعول به والبيئة. فمثلاً، قد تتم

مراجعة الإجراءات المتعلقة بقاعدة بيانات على مستوى قاعدة البيانات ككل أو على مستوى السجلات فيها.

- حالة الاستثناء (Exception-Condition): تشير إلى حالة الاستثناء، إن وجدت، التي يتم إعلانها عند العودة في نهاية الإجراء.
- استخدام الموارد: قائمة تضم مجموعة عناصر كمّية يمثل كل عنصر فيها الكمية المستخدمة من بعض موارد النظام (مثلاً، عدد السطور التي تم طباعتها أو عرضها على الشاشة، وعدد السجلات التي تم كتابتها أو قراءتها، ووقت المعالج الذي تم استهلاكه، ووحدات الإدخال/الإخراج التي تم استخدامها، والوقت المنقضي أثناء الجلسة).
- خاتم الوقت (Time-Stamp): خاتم بقيمة فريدة لوقت وتاريخ وقوع الفعل.

تتألف معظم عمليات المستخدمين من عدة أفعال أولية بسيطة. فعلى سبيل المثال، ينطوي أمر "نسخ ملف" على تنفيذ أمر المستخدم، والذي يتضمن تحصيل المصادقة على الوصول للملف والقيام بإعداد النسخة، والقراءة من ملف، بالإضافة إلى الكتابة إلى ملف آخر. لنأخذ في الاعتبار الأمر الآتي:

COPY GAME.EXE TO <Library>GAME.EXE

والصادر من Smith لنسخ الملف التنفيذي GAME من الدليل الحالي (current directory) إلى دليل آخر هو <Library>. قد يتم توليد سجلات المراجعة الآتية:

Smith	execute	<Library> COPY.EXE	0	CPU = 00002	11058721678

Smith	read	<Smith> GAME.EXE	0	RECORDS = 0	11058721679

Smith	execute	<Library> COPY.EXE	write-viol	RECORDS = 0	11058721680

في هذه الحالة، يتم إجهاض عملية نسخ الملف نظراً لأن Smith غير مصرّح له بالكتابة في الدليل <Library>.

هناك ثلاث مزايا لتحليل عمليات المُستخدِم إلى أفعال أولية:

1. لمّا كان المفعول به يمثل الكيانات المفترض حمايتها في النظام، فإن استخدام أفعالٍ أولية يسمح بمراجعة جميع التصرفات التي يمكن أن تؤثر على المفعول به. وهكذا، يمكن للنظام الكشف عن محاولات التلاعب بضوابط الوصول (access controls) (بملاحظة أي مظاهر غير طبيعية في أحوال الاستثناء (exception-conditions) التي يتم الإبلاغ عنها عند العودة من الإجراء، كما يمكنه الكشف عن النجاح في محاولة التخريب بملاحظة مظاهر غير طبيعية في مجموعة كيانات المفعول به التي أصبح بوسع الفاعل الوصول لها.
2. يؤدي استخدام سجلات المراجعة من نوع مفعول به واحد، وفعل واحد (Single-object, single-action) إلى تبسيط النموذج وطريقة التنفيذ.
3. إن الهيكل البسيط والمنتظم لسجلات المراجعة الخاصة باكتشاف التسلل قد يجعل من السهل نسبيا الحصول على تلك المعلومات، أو على الأقل جزءٍ منها، عن طريق مطابقة سجلات المراجعة المحلية الموجودة مباشرةً مع سجلات المراجعة الخاصة باكتشاف التسلل.

9-2-2 اكتشاف الشذوذ الإحصائي

كما ذكرنا آنفاً تنقسم أساليب اكتشاف الشذوذ الإحصائي إلى قسمين أساسيين: أنظمة الاكتشاف بالعتبة (threshold)، والأنظمة المبنية على البروفيل. يتضمن اكتشاف العتبة حساب عدد مرات وقوع حدث من نوع معين خلال فترة زمنية محددة. وإذا تجاوز هذا العدد الحد المقبول المُتوقع حدوثه في الوضع الطبيعي، فإننا نفترض وقوع تسلل.

يُعدُّ تحليل العتبات في حد ذاته طريقةً تقريبيةً وغير فعّالة حتى لاكتشاف هجمات على درجة متواضعة من التعقيد. وينبغي تحديد قيم كلٍّ من العتبة والفترة الزمنية؛ الأمر الذي يؤدي على الأرجح إلى كثير من الأخطاء الإيجابية الكاذبة أو كثير من الأخطاء السلبية الكاذبة نظراً للتباين الشديد عبر المستخدمين. ومع ذلك، قد يفيد استخدام عددٍ من الأنظمة البسيطة للاكتشاف بالعتبة عند توظيفها جنباً إلى جنب مع أساليب أخرى أكثر تطوراً.

يركز اكتشاف الشذوذ المبني على استخدام البروفيل على تحديد خواصٍ تميّز سلوك الأفراد أو مجموعات المستخدمين ذات الصلة واكتشاف الانحرافات الكبيرة عن تلك الخواص بعد ذلك. وقد يتألف البروفيل من مجموعة من المتغيرات، بحيث إن الانحراف في متغير واحد منها فقط قد لا يكون كافيا في حد ذاته لتوليد إنذار بالخطر.

تعتمد هذه الطريقة على تحليل سجلات المراجعة، حيث توفر تلك السجلات مدخلات لعملية اكتشاف التسلل من ناحيتين. أولاً، يجب على مصمم النظام تحديد عدد من المقاييس الكمّية التي يمكن استخدامها لقياس سلوك المستخدم. يمكن عن طريق تحليل سجلات المراجعة تلك على مدى فترة من الزمن تعيين الملامح التي تميّز النشاط المعتاد للمستخدم ومن ثم البروفيل الخاص به. أي أن سجلات المراجعة تُستخدم أولاً في تحديد السلوك النمطي. ثانياً، تُستخدم سجلات المراجعة الحالية بعد ذلك كمُدخلات لاكتشاف التسلل، حيث يقوم نموذج اكتشاف التسلل بتحليل سجلات المراجعة تلك لتحديد مدى الانحراف عن السلوك المعتاد. من أمثلة المقاييس المفيدة للاستخدام في اكتشاف التسلل بناءً على البروفيل ما يأتي:

- عدّاد (counter): وهو عدد صحيح غير سالب يمكن فقط أن يزداد ولكن لا ينقص إلى أن يتم تصفيره من قِبَل الإدارة. عادةً ما يتم حساب قيمة العداد لأنواع معينة من الأحداث على مدى فترة محددة من الزمن. ومن الأمثلة على ذلك عدد مرات محاولة الدخول على النظام من قِبَل مستخدم ما خلال

ساعة، وعدد مرات تنفيذ أمر بعينه خلال جلسة واحدة للمستخدم، وعدد مرات الإخفاق في إدخال كلمة السر خلال دقيقة.

- مقياس (gauge): وهو عدد صحيح غير سالب يمكن أن يزداد أو ينقص، ويُستخدم عادةً لقياس القيمة الحالية لكيانٍ ما. من الأمثلة على ذلك عدد الوصلات المنطقية المخصصة لأحد تطبيقات المستخدم، وعدد الرسائل الصادرة من إحدى عمليات المُستخدِم والتي تنتظر المعالجة.
- موقّت الفترة (Interval timer): وهو طول الفترة الزمنية بين حدثين مرتبطين. من الأمثلة على ذلك طول الفترة الزمنية بين محاولتين متتاليتين للدخول على حساب معيّن على النظام.
- استخدام الموارد (Resource utilization): وهي الكمية المُستَهلَكة من الموارد خلال فترة محددة. من الأمثلة على ذلك عدد الصفحات التي يطبعها مستخدم خلال جلسة، والزمن الكلي الذي يستغرقه تنفيذ برنامج.

باستخدام تلك المقاييس العامة، يمكن القيام بعدة اختبارات لتحديد ما إذا كان النشاط الحالي يقع في نطاق الحدود المقبولة. يسرد [DENN87] الطرق الآتية التي يمكن اتخاذها في هذا الصدد:

- المتوسط والانحراف المعياري.
- النموذج متعدد المتغيرات.
- عملية ماركوف.
- السلسلة الزمنية.
- النموذج التشغيلي.

أبسط اختبار إحصائي يمكن استخدامه هو قياس المتوسط والانحراف المعياري لمتغيرٍ ما على مدى فترة زمنية معينة. يعطي ذلك انطباعاً عن السلوك المتوسط ومدى التغير فيه مع الزمن. يصلح أسلوب المتوسط والانحراف المعياري

للاستخدام مع تشكيلة كبيرة من العدادات والموقّتات ومقاييس استخدام الموارد. غير أن هذه التدابير عادةً ما تكون غير كافية بمفردها لأغراض اكتشاف التسلل.

يعتمد النموذج متعدد المتغيرات على الارتباط بين اثنين أو أكثر من المتغيرات. يمكن توصيف سلوك المتسلل بثقة أكبر عن طريق النظر في علاقات الارتباط تلك (على سبيل المثال، الارتباط بين الوقت المستغل من المعالج واستخدام الموارد، أو معدل الدخول على النظام والوقت المنقضي في الجلسة).

يُستخدم نموذج عملية ماركوف في تحديد قيم احتمالات الانتقال بين مختلف حالات النظام. فمثلاً، يمكن استخدام هذا النموذج لدراسة الانتقالات بين أوامر بعينها.

يركز نموذج السلسلة زمنية على الفترات الزمنية، آخذاً في الاعتبار تسلسل الأحداث التي يمكن أن تقع بشكلٍ أسرع من المعتاد أو أبطأ من المعتاد. يمكن استخدام تشكيلة من الاختبارات الإحصائية لتوصيف التوقيت غير الطبيعي.

وأخيراً، يعتمد النموذج التشغيلي على تقدير ما يُعدّ غير طبيعي، وليس على القيام بالتحليل الآلي لسجلات المراجعة السابقة. وعادةً ما يتم وضع حدود ثابتة ويتم الاشتباه في حدوث تسلل عند ملاحظة سلوك خارج تلك الحدود. وتعمل هذه الطريقة بشكلٍ جيد عندما يكون من الممكن استنتاج سلوك المتسلل من خلال أنواع محددة من النشاط. على سبيل المثال، فإن عدداً كبيراً من محاولات الدخول خلال فترة قصيرة قد ينُم عن محاولة تسلل.

وكمثال على استخدام تلك المقاييس والنماذج المختلفة، يبيّن الجدول 9-1 التدابير المختلفة التي تم اختبارها أو أخذها في الاعتبار ضمن نظام اكتشاف التسلل (IDES) في معهد أبحاث ستانفورد (Stanford Research Institute (SRI)) [DENN87, JAVI91, LUNT88].

الجدول 9-1 المقاييس التي يمكن استخدامها لاكتشاف التسلل.

المقياس	النموذج	أنواع التسلل التي يمكن اكتشافها
أنشطة الدخول على النظام والجلسة		
معدل الدخول على النظام باليوم والوقت	المتوسط والانحراف المعياري	يُحتمل أن يحاول المتسللون الدخول على النظام خارج ساعات الدوام الرسمي
معدل الدخول على النظام في مواضع مختلفة	المتوسط والانحراف المعياري	يُحتمل أن يحاول المتسللون الدخول على النظام من موضع يندر أن يستعمله مستخدم بعينه أولا يستعمله على الإطلاق
الوقت المنقضي منذ آخر دخول على النظام	تشغيلي	اختراق على حسابٍ "ميِّت" (غير فعّال)
الوقت المنقضي أثناء كل جلسة	المتوسط والانحراف المعياري	قد ينم الانحراف الملحوظ عن وجود متنكر
كمية البيانات المُخرَجة إلى موضع	المتوسط والانحراف المعياري	قد ينم إرسال كمية كبيرة من البيانات إلى مواضع بعيدة عن تسريب بيانات حساسة
استخدام الموارد أثناء الجلسة	المتوسط والانحراف المعياري	قد تنم مستويات غير طبيعية من وقت المعالج أو عمليات الإدخال/الإخراج عن وجود متسلل
فشل إدخال كلمة السر أثناء محاولة الدخول على النظام	تشغيلي	محاولة للدخول على النظام عن طريق تخمين كلمة سر
فشل محاولة الدخول على النظام من محطات طرفية معينة	تشغيلي	محاولة اختراق
نشاطات تنفيذ أوامر أو برامج		
معدل التنفيذ	المتوسط والانحراف المعياري	قد يؤدي إلى كشف متسللين يُحتمل أن يحرصوا على استخدام أوامر مختلفة، أو كشف نجاح محاولة اختراق بواسطة مستخدم مشروع تمكّن من التوصل لصلاحية استخدام أوامر ذات امتيازات عالية.
استخدام موارد البرنامج	المتوسط والانحراف المعياري	قد تنم قيمة غير طبيعية عن حقن فيروس أو حصان طروادة في النظام، بما يصحب ذلك من آثار جانبية تتمثل في زيادة معدلات الإدخال/الإخراج واستخدام المعالج.
حجب تنفيذ أوامر	تشغيلي	قد يؤدي لكشف محاولة اختراق بواسطة مستخدم يسعى لتحصيل امتيازات أعلى.

تابع الجدول 9-1 المقاييس التي يمكن استخدم لاكتشاف التسلل.

المقياس	النموذج	أنواع التسلل التي يمكن اكتشافها
نشاطات الوصول إلى ملفات		
معدل عمليات القراءة والكتابة والإنشاء والحذف	المتوسط والانحراف المعياري	قد تنم المظاهر غير الطبيعية في عمليات الوصول للقراءة والكتابة بواسطة المستخدمين عن أعمال تنكّر أو تصفح.
السجلات التي يتم قراءتها وكتابتها	المتوسط والانحراف المعياري	قد تنم المظاهر غير الطبيعية عن محاولة للحصول على بيانات حساسة عن طريق الاستدلال والتجميع.
عدد مرات الفشل في عمليات القراءة والكتابة والإنشاء والحذف	تشغيلي	قد تكشف مستخدمين يصرّون على محاولة الوصول إلى ملفات غير مرخّصة لهم.

تكمن الميزة الأساسية لاستخدام البروفيلات الإحصائية في أننا لا نحتاج لمعرفة مسبقة بالثغرات الأمنية، حيث يقوم البرنامج بنفسه بتعلم ما يُعد سلوكاً "طبيعياً" ثم يبحث عن الانحرافات عن هذا السلوك. ولا تعتمد هذه الطريقة على خواص ونقاط ضعف متعلقة بنظام حاسب بعينه، ومن ثَمَّ، يسهل نقلها واستخدامها على أنواع مختلفة من أنظمة الحاسب.

9-2-3 اكتشاف التسلل بناءً على قواعد (Rule-based Intrusion Detection)

تقوم الأساليب المبنية على قواعد باكتشاف التسلل عن طريق مراقبة الأحداث التي تقع في النظام وتطبيق مجموعة من القواعد للتوصل إلى قرار بشأن ما إذا كان نمط معين من النشاط مشبوهاً. بشكلٍ عامٍ جداً، يمكننا تصنيف كل الطرق المستخدمة هنا إلى طرق تكتشف الشذوذ أو طرق تتعرف على الاختراق، رغم وجود بعض التطابق بين هذين الصنفين.

يشبه اكتشاف الشذوذ بناءً على قواعد اكتشاف الشذوذ الإحصائي من حيث الطريقة التي يستخدمها ونقاط القوة التي يمتاز بها. ففي الأسلوب الذي يعتمد

على قواعد، يتم تحليل سجلات المراجعة التاريخية لتحديد أنماط الاستخدام والقيام آلياً بتوليد قواعد تصف تلك الأنماط. وقد تمثل تلك القواعد أنماط السلوك الماضية للمستخدمين والبرامج والامتيازات والشرائح الزمنية والمحطات الطرفية، وما إلى ذلك. بعد ذلك يتم ملاحظة السلوك الحالي، وتُطابَق كل معاملة إزاء تلك المجموعة من القواعد لتحديد ما إذا كانت تلك المعاملة تتفق مع أي نمط سلوكي تمت ملاحظته تاريخياً.

وكما هو الحال مع اكتشاف الشذوذ الإحصائي، فإن اكتشاف الشذوذ بناءً على قواعد لا يتطلب معرفة نقاط الضعف الأمنية في النظام. فالخطة تقوم على مراقبة السلوك في الماضي، وتفترض في الواقع أن المستقبل سيكون كالماضي. ولكي تكون هذه الطريقة فعّالة، ينبغي أن تضم قاعدة البيانات عدداً كبيراً من القواعد. فعلى سبيل المثال، يستخدم النظام الذي وصفه [VACC89] قاعدة بيانات تضم مابين 10^4 و 10^6 قاعدة.

تتبع نظم التعرف على الاختراق بناءً على قواعد أسلوباً مختلفا للغاية لكشف التسلل يعتمد على تقنية الأنظمة الخبيرة. وتتلخص السمة الرئيسة لتلك النظم في استخدام قواعد للتعرف على اختراقات معروفة أو اختراقات تستغل نقاط ضعف معروفة. ويمكن أيضاً وضع قواعد للتعرف على سلوك مشبوه، حتى لو كان هذا السلوك يقع ضمن حدود أنماط الاستخدام المعتادة. وعادةً ما تكون القواعد المستخدمة في تلك النظم خاصة بنظام حاسب ونظام تشغيل بعينه. كما توضع تلك القواعد من قِبَل "خبراء" آدميين وليس عن طريق التحليل الآلي لسجلات المراجعة. تعتمد الطريقة المعتادة على إجراء مقابلات مع مديري الأنظمة والمحللين الأمنيين لجمع مجموعة من سيناريوهات الاختراق المعروفة والأحداث الرئيسة التي تهدد أمن النظام المستهدف[1]. وهكذا، فإن قوة هذه الطريقة تعتمد على مهارات المشاركين في وضع تلك القواعد.

[1] بل قد تتسع دائرة تلك المقابلات لتشمل القراصنة التائبين أو الذين لم يتوبوا بعد المستعدين لتقاسم خبراتهم نظير أجر [FREE93].

يوجد مثال بسيط لأنواع القواعد التي يمكن استخدامها في هذا الصدد في NIDX، وهو نظام تم تطويره سابقاً ويستخدم قواعد استدلال لامنهجية يمكن استعمالها لتعيين درجة الشك في الأنشطة المختلفة للمستخدمين [BAUE88]. من أمثلة قواعد الاستدلال تلك ما يأتي:

1. لا ينبغي أن يقوم المستخدمون بقراءة الملفات الموجودة في الأدلة الشخصية للمستخدمين الآخرين.
2. لا ينبغي أن يقوم المستخدمون بالكتابة في ملفات المستخدمين الآخرين.
3. المستخدمون الذين يدخلون على النظام بعد ساعات الدوام غالباً ما يصلون إلى نفس الملفات التي استخدموها في السابق.
4. المستخدمون عامةً لا يفتحون أجهزة أقراص التخزين مباشرة ولكنهم يعتمدون في ذلك على برامج خدمة (utilities) ذات مستوى أعلى يوفرها نظام التشغيل.
5. لا ينبغي للمستخدمين الدخول أكثر من مرة في نفس الوقت على نفس النظام.
6. المستخدمون لايسعون للحصول على نسخ من برامج النظام.

يمثل النظام المُستخدَم في IDES للتعرف على الاختراق الاستراتيجية المتبعة عادةً في هذا المجال، حيث يتم فحص سجلات المراجعة بمجرد إنشائها، ومطابقتها بالقواعد الموجودة في قاعدة البيانات. عند وُجود تطابق، فإن معدل الاشتباه في ذلك المُستخدِم يزداد. وفي حال حدوث تطابق مع عدد كافٍ من تلك القواعد، فإن معدل الاشتباه المتزايد قد يجتاز العتبة المحددة مما يؤدي إلى الإبلاغ عن اكتشاف شذوذ عن السلوك الطبيعي.

الجدول 9-2 إجراءات USTAT في مقابل أنواع الأحداث في نظام SunOS.

إجراء USTAT	نوع حدث SunOS
اقرأ (Read)	open_r, open_rc, open_rtc, open_rwc, open_rwtc, open_rt, open_rw, open_rwt
اكتب (Write)	truncate, ftruncate, creat, open_rtc, open_rwc, open_rwtc, open_rt, open_rw, open_rwt, open_w, open_wt, open_wc, open_wct
أنشئ (Create)	mkdir, creat, open_rc, open_rtc, open_rwc, open_rwtc, open_wc, open_wtc, mknod
احذف (Delete)	rmdir, unlink
نفّذ (Execute)	exec, execve
اخرج (Exit)	exit
عدّل المالك (Modify_Owner)	chown, fchown
عدّل التصريح (Modify_Perm)	chmod, fchmod
غيّر الاسم (Rename)	Rename
وصلة صلبة (Hardlink)	link

تعتمد طريقة عمل نظام IDES على فحص سجلات المراجعة. وتُعدُّ قلة المرونة من إحدى نقاط الضعف في هذه الطريقة. فلكل سيناريو اختراق، هناك عدد من التسلسلات البديلة لسجلات المراجعة، تختلف فيما بينها اختلافاتٍ بسيطة أو بشكلٍ غير ملحوظ. وقد يكون من الصعب تضمين تلك الاختلافات في قواعد صريحة. تتلخص إحدى الطرق الأخرى في وضع نموذج على مستوى أعلى بحيث يكون مستقلاً عن أية سجلات مراجعة محددة. ومن الأمثلة على ذلك نموذج انتقال الحالة المعروف بـ USTAT [ILGU93]. يتعامل USTAT مع الإجراءات العامة وليس مع الأفعال التفصيلية المحددة التي تسجلها آلية المراجعة على نظام التشغيل يونيكس. وقد تم تنفيذ USTAT على نظام SunOS الذي يوفر سجلات مراجعة

تشمل 239 حدثاً. تم اختيار 28 حدثٍ فقط من بين تلك الأحداث ليقوم معالج قَبْلي بمقابلتها بعشرة إجراءات عامة، كما بالجدول 9-2. باستخدام تلك الإجراءات العشر فقط مع المتغيرات المرتبطة بكل إجراء أمكن تطوير مخطط لانتقال حالة (state transition diagram) يصف النشاط المشبوه. نظراً لأن عدد الأحداث المختلفة التي يمكن تسجيلها في سجلات المراجعة تقابل عدداً أقل من الإجراءات المختلفة ، فإن عملية إنشاء القواعد تكون أبسط. وعلاوةً على ذلك، يمكن تعديل نموذج مخطط انتقال الحالة لاستيعاب سلوكيات التسلل الجديدة التي يتعلمها النظام.

9-2-4 مغالطة المعدل الأساسي

لكي يكون لنظام اكتشاف التسلل فائدة عملية، ينبغي أن يكون بمقدوره الكشف عن نسبة كبيرة من المتسللين مع الحفاظ على معدل الإنذارات الكاذبة عند مستوى مقبول. إذا كان النظام يكتشف فقط نسبة متواضعة من محاولات التسلل الفعلية فإنه بهذا يعطي إحساساً زائفاً بالأمان. وفي المقابل، إذا كان هذا النظام في كثير من الأحيان يصدر إنذارا بينما لا توجد محاولة تسلل في الواقع (أي إنذار كاذب) فإما أن يبدأ مديرو نظام الحاسب في تجاهل الإنذارات التي يصدرها النظام أو أن وقتاً طويلاً سيضيع في تحليل إنذارات كاذبة.

للأسف، فإنه بسبب طبيعة الاحتمالات التي ينطوي عليها النظام، فإنه من الصعب جداً تلبية المعايير المطلوبة لمعدّلات عالية للاكتشاف مع معدّلات منخفضة للإنذارات الكاذبة في آن واحد. وعموماً، إذا كان العدد الفعلي للاختراقات قليلاً مقارنةً بعدد الاستخدامات المشروعة للنظام، فإن معدل الانذارات الكاذبة سيكون عالياً ما لم يكن الاختبار المُستخدَم للوصول إلى قرار على درجة عالية من التمييز. وتشير دراسة عن أنظمة اكتشاف التسلل الحالية وردت في [AXEL00] إلى أن النظم الحالية لم تتغلب على مشكلة مغالطة المعدل الأساسي. انظر الملحق A-9 للاطلاع على استعراض موجز للخلفية الرياضية لتلك المشكلة.

9-2-5 الأنظمة الموزّعة لاكتشاف التسلل

حتى وقت قريب، انصبّ العمل في مجال اكتشاف التسلل على تطوير أنظمة قائمة بذاتها تعمل على نظام حاسب واحد. غير أن المؤسسات تحتاج عادةً إلى الدفاع عن مجموعة موزّعة من الأنظمة المضيفة ترتبط فيما بينها بشبكة إنترنت أو شبكة محلية. رغم أنه من الممكن توفير ذلك الدفاع عن طريق أنظمة اكتشاف تسلل قائمة بذاتها على كل مضيف، فإن الدفاع سيكون أكثر فعالية إذا تم التنسيق والتعاون بين تلك الأنظمة عبر الشبكة.

يوضّح بوراس المسائل الرئيسة الآتية فيما يتعلق بتصميم نظام موزّع لاكتشاف التسلل [PORR92]:

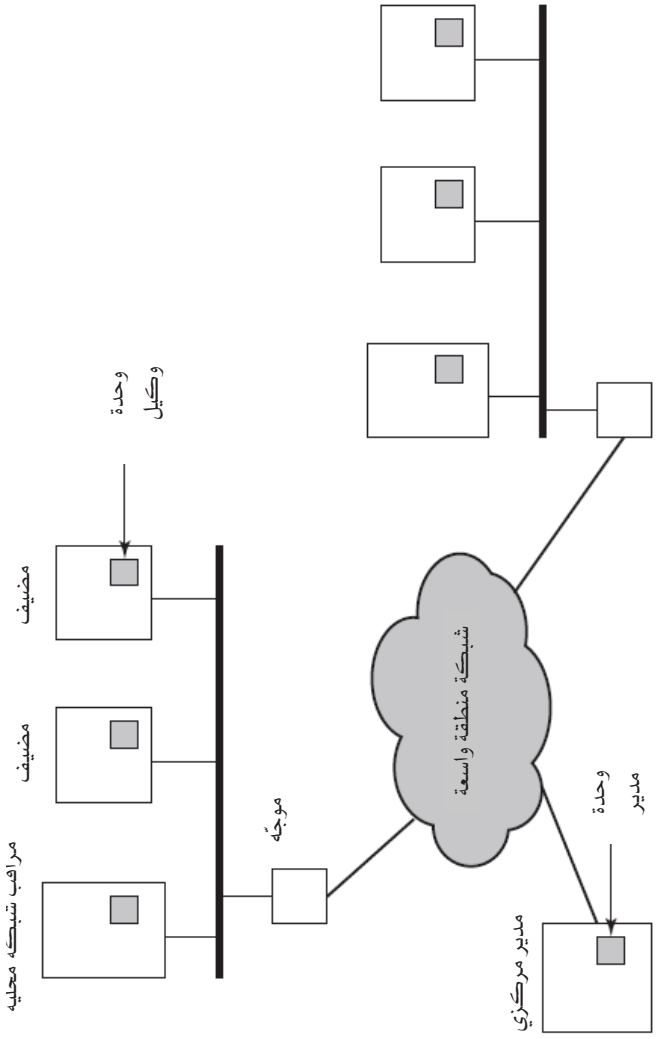
- قد يحتاج النظام الموزّع لاكتشاف التسلل إلى التعامل مع صيغ مختلفة من سجلات المراجعة. وفي بيئة غير متجانسة، سوف تستخدم نظم الحاسب المختلفة أنظمة محلية مختلفة لجمع معلومات المراجعة، وإذا كانت تستخدم أنظمة لاكتشاف التسلل، فقد تستخدم صيغاً مختلفة لسجلات المراجعة المتعلقة بالأمن.
- ستُستخدم عقدة أو أكثر في الشبكة كنقاط لجمع البيانات من الأنظمة الموجودة على الشبكة وتحليلها. وعليه سيتعين إرسال بيانات مراجعة خام أو موجزة عبر الشبكة. ومن ثَمَّ، سيتطلب الأمر ضمان سلامة وسرية تلك البيانات. سلامة البيانات مطلوبة لمنع المتسلل من إخفاء نشاطه عن طريق تغيير بيانات المراجعة المُرسَلة. أما السرية فمطلوبة لأن بيانات المراجعة المرسلة قد تكون ثمينة.
- يمكن استخدام بنية معمارية مركزية أو لامركزية. في حالة البنية المركزية، تكون هناك نقطة مركزية واحدة لجمع كل بيانات المراجعة وتحليلها. رغم أن هذا يُسهِّل مهمة التنسيق واستخلاص العلاقات المشتركة بين التقارير الواردة، فإنه قد يمثل عنق زجاجة كما يمكن أن يؤدي إلى حدوث اختناق أو إلى احتمال تعطّل للنظام بتعطل نقطة واحدة فيه (single

(point of failure). في البنية اللامركزية يوجد أكثر من مركز لتحليل البيانات، ولكن يتعين على تلك المراكز تنسيق أنشطتها وتبادل المعلومات فيما بينها.

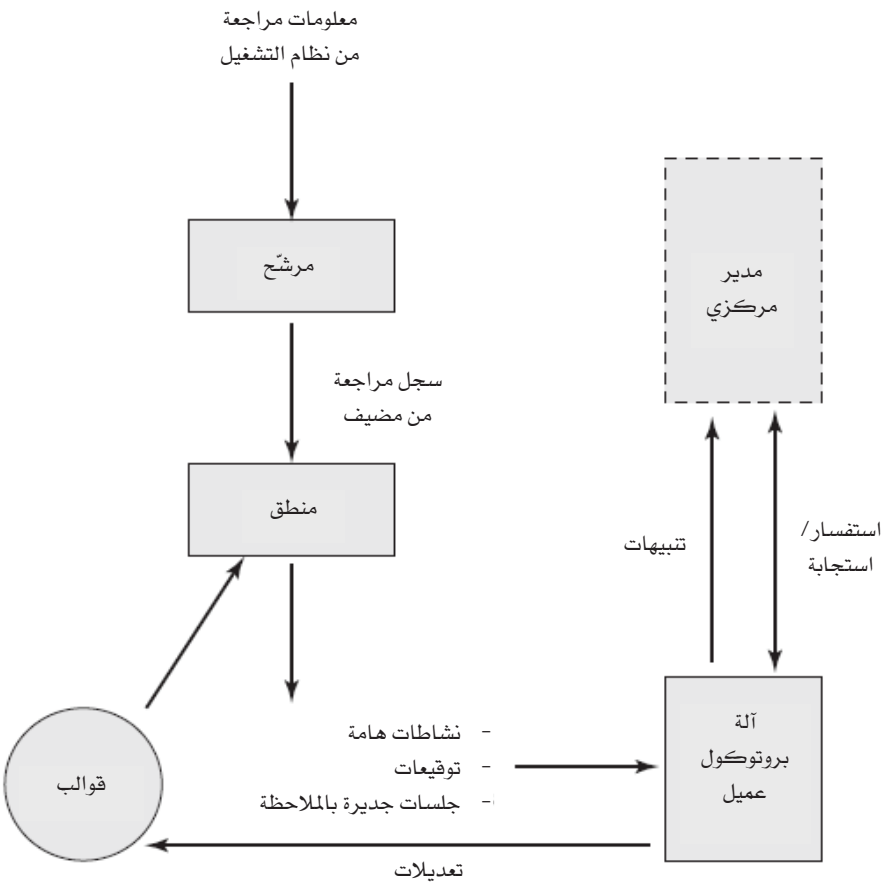
من الأمثلة الجيدة على الأنظمة الموزّعة لاكتشاف التسلل ذلك النظام الذي تم تطويره في جامعة كاليفورنيا في ديفيز [HEBE92, SNAP91]. ويوضّح الشكل 9-2 البنية المعمارية الكلية لذلك النظام، والتي تتألف من ثلاثة عناصر رئيسة هي:

- وحدة وكيل المضيف: وحدة لجمع بيانات المراجعة يجري تشغيلها كعملية بخلفية النظام الذي تجري مراقَبته. تقوم الوحدة بجمع البيانات عن الأحداث المتعلقة بالأمن بالمضيف وإرسالها إلى المدير المركزي.
- وحدة مراقبة الشبكة المحلية: تعمل بنفس طريقة وحدة وكيل المضيف إلا أنها تقوم بتحليل حركة مرور البيانات على الشبكة المحلية وإرسال النتائج إلى المدير المركزي.
- وحدة المدير المركزي: تستقبل التقارير الواردة من وحدات وكلاء مراقبة الشبكة المحلية ووكلاء وعمليات المضيفين وتقوم بالربط بينها بهدف اكتشاف التسلل.

صُمم النظام ليكون مستقلاً عن أيٍّ من أنظمة التشغيل أو أنظمة المراجعة. ويوضّح الشكل 9-3 [SNAP91] النهج العام المتبع. ويقوم الوكيل بالتقاط كل سجل مراجعة ينتجه نظام جمع بيانات المراجعة المحلي ويُستخدم مرشّح للاحتفاظ فقط بالسجلات التي لها علاقة بالأمن. يتم بعد ذلك وضع تلك السجلات في صيغة قياسية موحّدة تُعرف بسجل المراجعة للمضيف ((host audit record (HAR)).



الشكل 9-2 البنية المعمارية لنظام موزّع لاكتشاف التسلل.



الشكل 9-3 البنية المعمارية لوكيل.

تقوم وحدة منطقية مبنية على قالب (template-driven) بتحليل السجلات بحثاً عن أي نشاط مشبوه. في أدنى مستوى، يقوم الوكيل بعملية مسح للسجلات بحثاً عن أحداث بارزة لها أهميتها بصرف النظر عن أي أحداث سابقة. ومن أمثلة ذلك: الفشل في الوصول إلى ملفات، والوصول إلى ملفات النظام، وتغيير ضوابط التحكم في الوصول إلى ملف. وفي أعلى مستوى، يبحث الوكيل عن تسلسلات أحداث،

كأنماط الهجوم المعروفة (التوقيعات). وأخيراً، يبحث الوكيل عن سلوكيات شاذة لمستخدم بعينه على أساس البروفيل التاريخي لذلك المستخدم، كعدد البرامج التي ينفذها، وعدد الملفات التي يصل إليها، وما إلى ذلك.

عند اكتشاف أي نشاط مشبوه، يتم إرسال تنبيه إلى المدير المركزي. يستخدم المدير المركزي نظاماً خبيراً (expert system) يمكّنه من استخلاص النتائج من البيانات الواردة. كما يمكن للمدير أيضاً أن يطلب من مختلف الوكلاء إرسال نسخ من سجلات المراجعة HAR للربط ما بينها وبين السجلات الواردة من وكلاء آخرين.

يقوم وكيل الشبكة المحلية أيضاً بتزويد المدير المركزي بالمعلومات. كما يقوم الوكيل بمراجعة التوصيلات بين الأنظمة المضيفة والخدمات المستخدمة وحجم حركة المرور. ويقوم أيضاً بالبحث عن الأحداث المهمة، كالتغيرات المفاجئة في حِمل الشبكة، واستخدام خدمات متعلقة بالأمن، والأنشطة على الشبكة مثل عمليات الدخول عن بُعد (rlogin).

تُعدُّ البنى المعمارية المبينة في الشكلين 9-2 و9-3 عامةً جداً ومرنة جداً. وهي تمثل الأساس لطريقة مستقلة عن نوع أجهزة الحاسب، ويمكن التوسع فيها ابتداءً من أنظمة قائمة بذاتها لاكتشاف التسلل إلى نظام قادر على الربط مابين الأنشطة على عدد من المواقع والشبكات للكشف عن الأنشطة المشبوهة والتي بدون ذلك كانت ستبقى مخفية.

9-2-6 المصايد الأمنية (Honeypots)

المصايد الأمنية هي وسيلة حديثة نسبياً في مجال تقنيات اكشاف التسلل. تعمل أنظمة المصايد الأمنية كفخاخ بهدف جذب اهتمام المهاجم المحتمل بعيداً عن النظم الأساسية ذات الأهمية المحورية. يتم تصميم تلك المصايد الأمنية لتقوم بما يأتي:

- صرف اهتمام المهاجم بحيث لا يصل إلى النظم المحورية.

- جمع المعلومات عن نشاط المهاجم.
- تشجيع المهاجم على البقاء على النظام لفترة كافية ليتسنى للإداريين التعامل معه.

تمتلئ تلك النظم ببيانات ملفقة صمّمت لتبدو وكأنها معلومات قيّمة ولكنها غير متاحة فلا يمكن الوصول إليها من قِبَل المستخدمين الشرعيين للنظام. وعليه فإن أي وصول إلى المصيدة الأمنية يكون مثار شبهة. يُزوّد النظام بأجهزة مراقبة حساسة ومسجّلات للأحداث للكشف عن أي زيارة للمصيدة وجمع المعلومات عن المهاجم. ونظراً لأن النظام مصمم بحيث يُظهر أي هجوم على المصيدة الأمنية كهجوم ناجح، فإنه سيكون لدى الإداريين الوقت الكافي للتعبئة وتسجيل الهجوم ومتابعة مساره دون الكشف عن النظم الفعلية/الفعّالة.

تضمّنت الجهود الأولية استخدام مصيدة أمنية تتألف من نظام حاسب واحد له عنوان IP مصمم لجذب القراصنة. وقد ركّزت البحوث التي أُجريت مؤخراً في هذا الصدد على بناء شبكات بأكملها من المصايد الأمنية لتبدو كما لوكانت شبكة مؤسسة، وقد تتضمن بيانات وحركة مرور حقيقية أو محاكاة. بمجرد أن يصبح القراصنة داخل الشبكة، يمكن للإداريين مراقبة سلوكهم بالتفصيل وحشد الدفاعات الناجعة ضدهم.

9-2-7 صيغة تبادل البيانات لاكتشاف التسلل

لتيسير تطوير نظم موزّعة لاكتشاف التسلل يمكنها العمل عبر تشكيلة كبيرة من البيئات، ينبغي وضع المعايير اللازمة لدعم العمل المشترك عبر الأنظمة المختلفة. تركّز مجموعة العمل الخاصة باكتشاف التسلل ضمن فريق مهام هندسة الإنترنت (IETF) على تطوير تلك المعايير. والغرض من تشكيل مجموعة العمل تلك هو تحديد صيغ وإجراءات تبادل البيانات للمساعدة في تقاسم المعلومات التي تهم أنظمة الكشف والاستجابة لمحاولات التسلل وكذلك النظم الإدارية التي قد تحتاج للتفاعل مع تلك الأنظمة. تتضمن النتائج المطلوبة من مجموعة العمل ما يأتي:

1. إعداد وثيقة متطلبات تصف الاحتياجات الوظيفية عالية المستوى للاتصال فيما بين أنظمة اكتشاف التسلل، وكذلك متطلبات الاتصال بين أنظمة اكتشاف التسلل ونظم الإدارة، بما في ذلك الأسباب المنطقية لتلك المتطلبات. ولتوضيح تلك المتطلبات سيتم استخدام سيناريوهات متعددة.
2. إعداد مواصفات للغة موحّدة لأغراض اكتشاف التسلل، والتي تصف صيغ البيانات اللازمة لتلبية الاحتياجات المطلوبة.
3. وثيقة إطار تحدد أفضل البروتوكولات الموجودة حالياً لاستخدامها في الاتصال بين أنظمة اكتشاف التسلل وتصف علاقة صيغ البيانات المقترحة بتلك البروتوكولات.

حتى وقت كتابة هذا الجزء، فإن كل تلك الوثائق وصلت إلى مرحلة مسودة وثيقة إنترنت.

9-3 إدارة كلمات السر

9-3-1 حماية كلمة السر

يُعدُّ نظام كلمة السر خط الدفاع الأول ضد المتسللين. حيث تتطلب جميع الأنظمة لعدة مستخدمين تقريباً أن يقوم المُستخدِم بإدخال اسم (أو هوية) المُستخدِم (ID)، وأيضاً بإدخال كلمة سر. والغرض من كلمة السر هو توثيق هوية الشخص للدخول على النظام. وبدورها، توفر هوية المُستخدِم الأمن من الجوانب الآتية:

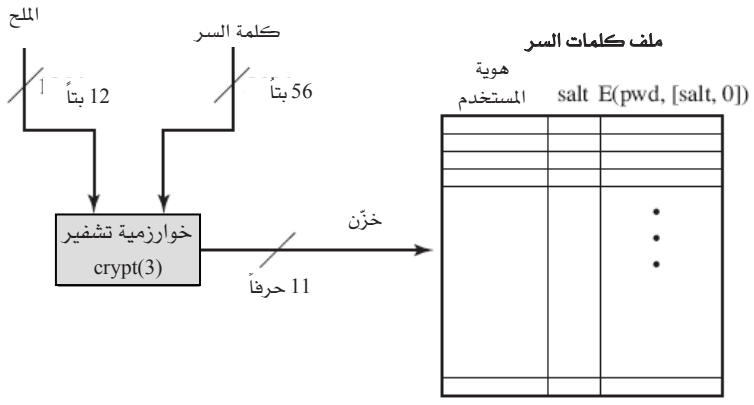
- تُبيّن الهوية ما إذا كان المُستخدِم مرخّصاً له بالدخول على النظام. في بعض النظم، يُسمح بالدخول فقط للأشخاص الذين لديهم فعلاً هوية مخزّنة على النظام.
- تحدّد الهوية الامتيازات الممنوحة للمستخدم. فقد يتمتع قلة من المستخدمين بمرتبة إشرافية (مستخدم متميز) تمكّنهم من قراءة الملفات وأداء المهام التي تتمتع بحماية خاصة من قِبَل نظام التشغيل. وقد توفر بعض الأنظمة

حسابات للضيوف أو حسابات مجهولة الهوية يتمتع مستخدموها بامتيازات محدودة مقارنةً بغيرهم.

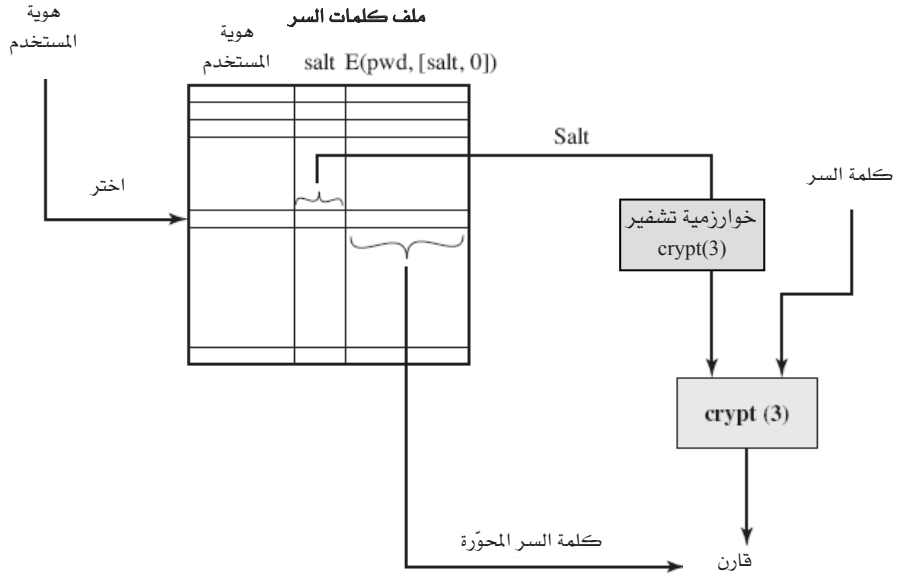
- تُستخدم الهوية فيما يُعرف بالتحكم التقديري في الدخول على النظام (discretionary access control). فعلى سبيل المثال، من خلال نشر قائمة بهويات المستخدمين الآخرين، يمكن لمستخدم أن يسمح لبعضهم بقراءة الملفات التي يملكها .

❖ نقاط الضعف في كلمات السر:

لكي نفهم طبيعة التهديد الذي تتعرض له النظم القائمة على كلمة السر، نأخذ بعين الاعتبار طريقة تستخدم بكثرة على نظام التشغيل يونيكس، حيث لاتخزّن كلمات السر واضحةً أبداً. بدلاً من ذلك، يُستخدم الإجراء التالي (انظر الشكل 9-4 (a)). يختار كل مستخدم كلمة سر تتألف من أحرف قابلة للطباعة بطول أقصى يبلغ ثمانية أحرف. يتم تحويل تلك الكلمة إلى قيمة من 56 بتاً (باستعمال كود آسكي بـ 7 بتات) لتُستخدم كمُفتاح ل لبرنامج التشفير المعروف باسم crypt(3) المبني على خوارزمية DES. يتم تعديل DES باستخدام قيمة تُعرف بالملح طولها 12 بتاً، وعادةً ماتعتمد تلك القيمة على الوقت الذي تم فيه تخصيص كلمة السر للمستخدم. يتم تشغيل خوارزمية DES بإدخال كتلة بيانات تتألف من 64 بتاً كلها أصفار، ويُستخدم ناتج هذه العملية كمُدخل لعملية التشفير التالية. تُكرّر هذه العملية لإتمام عدد كلي من التشفيرات يبلغ 25 تشفيرة، ويُعامل الناتج الذي يتألف من 64 بتاً على أساس أنه يمثل تسلسلاً من 11 حرفاً. بعد ذلك تُخزن كلمة السر المحوّرة (hashed password)، مع نسخة غير مُشفَّرة من قيمة الملح، في ملف كلمات السر مقابل الهوية المناظرة للمستخدم. تم إثبات أن هذه الطريقة آمنة ضد مجموعة متنوعة من هجمات تحليل الشفرة [WAGN00].



(a) تخزين كلمة سر جديدة



(b) التحقق من كلمة سر

الشكل 9-4 منظومة كلمة السر في نظام التشغيل يونيكس.

تخدم قيمة الملح ثلاثة أغراض:

- تمنع ظهور كلمات سر مكررة في ملف كلمات السر. فحتى لو اختار مستخدمان نفس كلمة السر، فإن كلمة السر ستخصص لهما في وقتين مختلفين. ومن ثم فإن كلمة السر "الموسّعة" والمخزنة في الملف ستكون مختلفة لكلٍ منهما.
- تؤدي عملياً إلى زيادة طول كلمة السر للمستخدم بحرفين دون أن يحتاج المُستخدِم إلى تذكّر حرفين إضافيين. وعليه، فإن ذلك يؤدي إلى زيادة عدد كلمات السر الممكنة 4096 مرة، مما يزيد من صعوبة تخمين كلمة السر.
- تمنع استخدام عتاد تنفيذ خوارزمية DES والذي يؤدي، لو استخدم، إلى تقليل صعوبة القيام بهجوم استقصائي لتخمين كلمة السر.

عندما يحاول المُستخدِم الدخول على نظام التشغيل يونيكس فإنه يقوم بإدخال هوية المُستخدِم وكلمة السر. يستخدم نظام التشغيل الهوية كمؤشر إلى كلمة السر في الملف ويسترجع القيمة غير المُشفَّرة للملح وكذلك كلمة السر المُشفَّرة. تُستخدم قيمة الملح وكلمة السر التي أدخلها المُستخدِم كمُدخل لروتين التشفير. إذا تطابقت نتيجة التشفير مع القيمة المخزنة في الملف اعتُبرت كلمة السر مقبولة.

صُمم روتين التشفير بحيث يثبّط من محاولات التخمين. فتنفيذ خوارزمية DES بالبرمجيات أبطأ منه باستخدام العتاد، كما أن تكرار عملية التشفير 25 مرة يضاعف الوقت اللازم للعملية 25 مرة. ومع ذلك فقد طرأ تغييران منذ التصميم الأصلي لتلك الخوارزمية. أولاً، أدت الإصدارات الأحدث من الخوارزمية إلى تنفيذها بشكلٍ أسرع. على سبيل المثال، تمكنت دودة الإنترنت التي نورد وصفاً لها في الفصل العاشر من القيام بتخمين بضع مئات من كلمات السر على الخط مباشرةً في فترة زمنية محدودة باستخدام خوارزمية تشفير أكثر كفاءةً بكثير من النسخة المعيارية المخزنة على أنظمة يونيكس التي كانت عرضةً للهجوم. وثانيا، مع التزايد المضطرد في سرعة أداء أجهزة الحاسب، فإن أي خوارزميات تنفذ بواسطة برمجيات يتم إنجازها أيضاً بشكلٍ أسرع من ذي قبل.

مما تقدم يتضح أن هناك تهديدين لمنظومة كلمة السر على نظام التشغيل يونيكس. أولاً، يمكن للمستخدم الدخول على جهاز عن طريق حساب ضيف أو بأي وسيلة أخرى، ثم يقوم بتشغيل برنامج لتخمين كلمة السر، والذي يُعرف باسم مكسّر كلمات السر (password cracker) على ذلك الجهاز. وسيكون بوسع المهاجم تجربة المئات وربما الآلاف من كلمات السر الممكنة باستخدام كمية ضئيلة من موارد النظام. بالإضافة إلى ذلك، إذا تمكن الخَصْم من الحصول على نسخة من ملف كلمات السر، فسيمكنه تشغيل برنامج للتكسير على رِسْلِه في جهاز آخر. وبهذه الطريقة سيتمكّن الخَصْم من تجربة عدة آلاف من كلمات السر الممكنة خلال فترة معقولة.

كمثال على ذلك، تم الإبلاغ عن مكسّر لكلمات السر على شبكة الإنترنت في أغسطس 1993 [MADS93]. وباستخدام جهاز حاسب بمعالجات من إنتاج شركة Thinking Machines Corporation على التوازي، أمكن تحقيق أداء بلغ 1560 تشفيرة في الثانية لكل وحدة متجه (vector unit). باستخدام أربع وحدات متجه على كل عقدة (وتلك ترتيبة قياسية) يتم إنجاز 800,000 تشفيرة في الثانية على جهاز يضم 128 عقدة (وهو جهاز متواضع الحجم) أو 6.4 مليون تشفيرة في الثانية على جهاز يضم 1024 عقدة.

حتى معدلات التخمين الهائلة تلك لا تجعل من الممكن لمهاجم استخدام الأسلوب الاستقصائي الغبي الذي يجرّب كل تباديل الأحرف الممكنة لاكتشاف كلمة سر. بدلاً من ذلك يعتمد مكسّرو كلمات السر على حقيقة أن بعض الناس يختارون كلمات سر يمكن تخمينها بسهولة.

بعض المستخدمين، عندما يُسمح لهم باختيار كلمة سر خاصة بهم، يختارون كلمة قصيرة للغاية. ويبيّن الجدول 9-3 نتائج دراسة أجريت في جامعة بوردو. راقبت الدراسة خيارات تغيير كلمة السر على 54 جهاز حاسب تمثل حوالي 7,000 حساب مستخدم. تألفت 3% من كلمات السر من 3 أحرف أو أقل. وبوسع مهاجم بدء هجومه بأن يقوم باختبار استقصائي لكل كلمات السر الممكنة بطول 3 أحرف أو

أقل. ويتمثل أحد الحلول البسيطة لتلك المشكلة في أن يرفض النظام اختيار كلمة سر تكون أقل من ستة أحرف مثلاً، أو حتى أن يشترط أن تتكون جميع كلمات السر من ثمانية أحرف بالضبط. ومعظم المستخدمين لن يتضجّر من مثل تلك القيود.

إن طول كلمة السر ليس سوى جزء واحد من المشكلة، فكثير من الناس عندما يُسمح لهم باختيار كلمة سر خاصة بهم، يختارون كلمة سر يمكن تخمينها، كاسم الشخص، أو اسم الشارع، أو كلمة عامة من كلمات القاموس، مما يجعل تكسير كلمة السر مهمة سهلة وبسيطة. فكل مايحتاجه مكسّر كلمات السر هو أن يقوم ببساطة باختبار ملف كلمات السر بحثاً عن قوائم من كلمات السر المحتملة. ولأن كثير من الناس يستخدمون كلمات سر يسهل تخمينها، فإن هذه الاستراتيجية سوف تنجح على جميع النظم.

الجدول 9-3 أطوال كلمة المرور التي تم ملاحظتها في دراسة [SPAF92a].

الطول	العدد	الكسر من المجموع الكلي
1	55	.004
2	87	.006
3	212	.02
4	449	.03
5	1260	.09
6	3035	.22
7	2917	.21
8	5772	.42
المجموع	**13787**	**1.0**

من التجارب التي أكدت فعالية التخمين ما ورد في [KLEI90]. جمع المؤلف، من مصادر مختلفة، ملفات لكلمات السر على نظام يونيكس تتضمن ما يقرب من 14,000 كلمة سر مُشفَّرة. ويبيّن الجدول 9-4 النتيجة، والتي يصفها المؤلف، ومعه حق، بأنها مخيفة. فقد أمكن تخمين الربع من مجموع كلمات السر التي اشتملت عليها الدراسة، وذلك باتباع الاستراتيجية الآتية:

1. جرّب اسم المستخدم، والأحرف الأولى، واسم الحساب، وغير ذلك من المعلومات الشخصية. وقد تم تجربة ما مجموعه 130 تبديلة مختلفة لكل مستخدم.
2. جرّب كلمات من مختلف القواميس. قام المؤلف بتجميع قاموس يضم أكثر من 60,000 كلمة موجودة في عدة مصادر من بينها قاموس النظام نفسه على الإنترنت، وغيره من القوائم المختلفة كما هو مبين في الجدول.
3. جرّب تعديلات مختلفة على الكلمات في الخطوة 2. يشمل ذلك تغيير الحرف الأول إلى حرف كبير (uppercase)، وقلب الكلمة كلها إلى أحرف كبيرة، وعكس ترتيب أحرف الكلمة، وتغيير الحرف "o" إلى الرقم صفر "0"، وهكذا. أضافت تلك التبديلات مليون كلمة أخرى إلى القائمة.
4. تبديلات أخرى تتعلق بجعل الأحرف كبيرة على الكلمات في الخطوة 2 التي لم تؤخذ في الاعتبار في الخطوة 3. أضاف ذلك ما يقرب من 2 مليون كلمة أخرى إلى القائمة.

وهكذا اشتملت التجربة على ما يقرب من 3 مليون كلمة. باستخدام أسرع أجهزة الحاسب من نوع Thinking Machines المذكورة أعلاه، فإن الوقت اللازم لتشفير كل تلك الكلمات باستخدام كل الاحتمالات الممكنة لقيمة الملح سيكون أقل من ساعة. جديرٌ بالذكر أن مثل هذا البحث الدقيق يمكن أن يؤدي إلى نجاح بنسبة 25%، في حين أن النجاح في تخمين كلمة سر واحدة فقط قد يكفي لتحصيل مجموعة كبيرة من الامتيازات على النظام المهاجَم.

❖ **التحكم في الوصول:**

من طرق إحباط الهجوم على كلمة السر منع الخَصْم من الوصول إلى ملف كلمات السر. فإذا جُعل الجزء الخاص بكلمات السر المُشفَّرة من الملف بحيث يمكن الوصول إليه فقط من قِبَل مستخدم متميّز، فلن يتمكن الخَصْم من قراءتها دون أن يعرف بالفعل كلمة السر الخاصة بذلك المستخدم. يشير [SPAF92a] إلى عدد من أوجه القصور في تلك الاستراتيجية:

- يتعرض عدد من النظم – بما في ذلك معظم أنظمة يونيكس – لعمليات اقتحام غير متوقعة. فبمجرد نجاح المهاجم في النفاذ إلى النظام، فإنه يود الحصول على مجموعة من كلمات السر ليستطيع استخدام حسابات مختلفة لجلسات دخول مختلفة وذلك لتقليل خطر انكشافه. أو قد يرغب مستخدم له حساب في استعمال حساب مستخدم آخر للوصول إلى بيانات متميّزة أو لتخريب النظام.
- قد يؤدي حادث يتعلق بالحماية إلى جعل ملف كلمة السر قابلاً للقراءة، ومن ثم تعريض كل الحسابات للخطر.
- بعض المستخدمين لهم حسابات على أجهزة أخرى ضمن مجالات أخرى للحماية وهم يستخدمون نفس كلمة السر لتلك الحسابات. وعليه، فإذا أمكن قراءة كلمات السر من قِبَل أي شخص على أحد الأجهزة، فقد يُصبح جهاز آخر في مكان آخر عُرضةً للخطر.

وهكذا، فإن الاستراتيجية الأكثر فعالية هي إرغام المستخدمين على اختيار كلمات سر يصعب تخمينها.

9-3-2 استراتيجيات اختيار كلمة السر

الدرس الذي يمكن استخلاصه من التجارب التي وصفناها آنفاً (انظر الجدولين 9-3 و 9-4) هو أن المستخدمين إذا تُركوا وشأنهم، فإن كثيراً منهم يختارون كلمة سر قصيرة جداً أو من السهل للغاية تخمينها. وعلى النقيض، إذا تم

تخصيص كلمات سر للمستخدمين تتكون من ثمانية أحرف قابلة للطباعة تُختار عشوائيا فإن كسر كلمات السر يصبح ضرباً من المستحيل عملياً. ولكن في المقابل سيُصبح من المستحيل بنفس القدر تقريباً على معظم المستخدمين تذكُّر كلمات السر الخاصة بهم. لحسن الحظ، حتى لو قمنا بالحد من فضاء كلمة السر لسلاسل أحرف يسهل حفظها بشكلٍ معقول، فإن ذلك الفضاء يبقى كبيراً جداً بحيث لن يسمح بعملية التكسير في الواقع العملي. وهدفنا إذن هو القضاء على كلمات السر سهلة التخمين وفي الوقت نفسه السماح للمستخدم باختيار كلمة سر يسهل تذكرها.

الأساليب الأربعة الأساسية المستخدمة في هذا الصدد هي:

- توعية المستخدم.
- توليد كلمات السر بواسطة الحاسب.
- الفحص التفاعلي لكلمة السر.
- الفحص الاستباقي لكلمة السر.

يمكن أن يُخطَر المستخدمون بأهمية استخدام كلمات سر صعبة التخمين، وأن يتم تزويدهم بمبادئ توجيهية لمساعدتهم في اختيار كلمات سر قوية. ليس من المرجّح أن تنجح مثل تلك الاستراتيجية لتوعية المُستخدِم في معظم المنشآت، ولاسيما حيث يوجد عددٌ كبير من المستخدمين وتكثر عمليات التجديد فيهم. كثير من المستخدمين سيتجاهلون ببساطة المبادئ التوجيهية. البعض الآخر قد لا تتوفر لديه الحكمة الكافية لاختيار كلمة سر قوية. فعلى سبيل المثال، هناك عدد من المستخدمين يعتقدون، وهذا خطأ، أن عكس ترتيب أحرف كلمة السر أو قلب الحرف الأخير منها إلى حرف كبير يجعل كلمة السر غير قابلة للتخمين.

الجدول 9-4 كلمات السر التي أمكن تخمينها من عينة تضم 13,797 حساباً [KLEI90].

نوع كلمة السر	حيز البحث	عدد التطابقات	النسبة المئوية لكلمات السر التي أمكن مطابقتها	نسبة الكلفة/الفائدة[a]
اسم المستخدم/الحساب	130	368	2.7%	2.830
تسلسل أحرف	866	22	0.2%	0.025
أعداد	427	9	0.1%	0.021
صيني	392	56	0.4%	0.143
أسماء أماكن	628	82	0.6%	0.131
أسماء مشهورة	2239	548	4.0%	0.245
أسماء إناث	4280	161	1.2%	0.038
أسماء ذكور	2866	140	1.0%	0.049
أسماء غير مشهورة	4955	130	0.9%	0.026
خرافات وأساطير	1246	66	0.5%	0.053
شيكسبيريات	473	11	0.1%	0.023
مصطلحات رياضة	238	32	0.2%	0.134
خيال علمي	691	59	0.4%	0.085
أفلام ونجوم سينما	99	12	0.1%	0.121
أفلام كرتونية	92	9	0.1%	0.098
مشاهير	290	55	0.4%	0.190
تعبيرات وأنماط	933	253	1.8%	0.271
ألقاب	33	9	0.1%	0.273
مصطلحات بيولوجية	58	1	0.0%	0.017
قاموس النظام	19683	1027	7.4%	0.052
أسماء أجهزة	909	132	1.0%	0.015
اختصارات	14	2	0.0%	0.143
إنجيل الملك جيمس	7525	83	0.6%	0.011
كلمات منوّعة	3212	54	0.4%	0.017
لغة اليديش	56	0	0.0%	0.000
كويكبات	2407	19	0.1%	0.007
المجموع	62727	3340	24.2%	0.053

[a] تُحسب بقسمة عدد التطابقات على حيز البحث. كلما زاد عدد الكلمات التي يتطلب الأمر تجربتها للحصول على تطابق، قلّت نسبة الكلفة/الفائدة.

استخدام كلمات سر من توليد الحاسب له مشاكله أيضاً. إذا كانت كلمات السر عشوائية تماما في طبيعتها، فلن يستطيع المستخدمون تذكّرها. حتى لو كانت كلمة السر يمكن نطقها، فقد يجد المُستخدِم صعوبة في تذكرها، ومن ثَمَّ سيميل إلى كتابتها للاحتفاظ بها. بشكلٍ عام، ارتبطت كلمات السر المولّدة بواسطة الحاسب بتاريخ سيء من حيث قبول المستخدمين لها. تُعرّف الوثيقة FIPS PUB 181 واحداً من أفضل المولدات الآلية لكلمات السر تصميماً. لا تحتوي الوثيقة فقط على وصفٍ للطريقة ولكن تحتوي أيضاً على سردٍ كاملٍ لكود برنامج الخوارزمية بلغة C. تقوم الخوارزمية بتوليد كلمات عن طريق تشكيل مقاطع قابلة للنطق ونظمها في سلسلة لتكوين كلمة السر. وتستخدم الخوارزمية مولد أعداد عشوائية لإنتاج تدفق عشوائي من الأحرف لبناء المقاطع والكلمات.

في استراتيجية الفحص التفاعلي لكلمة السر يقوم النظام دوريا بتشغيل برنامجه الخاص لتكسير كلمات السر بحثاً عن كلمات السر التي يمكن تخمينها. فيقوم النظام بإلغاء كلمات السر التي أمكن تخمينها وإخطار المُستخدِم بذلك. ولهذا الأسلوب عددٌ من المثالب. فهو أولاً يستنزف كثيراً من الموارد لإنجاز المهمة على مايرام. ولأن خَصْماً عنيداً تمكّن من سرقة ملف كلمة السر سيكون بوسعه تكريس وقت المعالج بأكمله للمهمة لساعات أو حتى لأيام، فإن أسلوب الفحص التفاعلي لكلمة السر يعاني من قصور واضح. وعلاوةً على ذلك، فستبقى كلمات السر الضعيفة تمثل نقاط ضعف في النظام إلى أن يكتشفها الفاحص التفاعلي لكلمة السر.

يُعدُّ أسلوب الفحص الاستباقي لكلمة السر من أفضل الاستراتيجيات الواعدة لتحسين أمن كلمات السر. وفي هذه الطريقة، يُسمح للمستخدم باختيار كلمة السر الخاصة به. غير أنه في وقت الاختيار يقوم النظام بفحص كلمة السر لتحديد ما إذا كانت مقبولة، وإلا فإنه يرفضها. ويقوم أسلوب الفحص هذا على الفلسفة التي مؤداها أنه بتوجيهٍ كافٍ من النظام، يمكن للمستخدمين اختيار كلمات سر يسهل تذكرها من فضاء كلمات السر الواسع نسبياً التي يُستبعد تخمينها في هجوم يعتمد على كلمات القاموس.

تكمن الفكرة في الفحص الاستباقي لكلمة السر في تحقيق التوازن بين قوة كلمة السر ومدى تَقبُّل المستخدمين لها. فإذا كان النظام يرفض كثيراً من كلمات السر، فسيشتكي المستخدمون من أنه من الصعب جداً اختيار كلمة سر. وفي المقابل إذا كان النظام يستخدم خوارزمية بسيطة لتحديد ما هو مقبول، فسيوفر ذلك توجيهاً لقراصنة تكسير كلمات السر لمراجعة أساليب التخمين التي يستخدمونها. فيما تبقى من هذا الجزء الفرعي، سنتناول بعض الطرق الممكنة للفحص الاستباقي لكلمة السر.

الطريقة الأولى هي مجرد نظام بسيط لفرض بعض القواعد. فعلى سبيل المثال، يمكن فرض تطبيق القواعد الآتية:

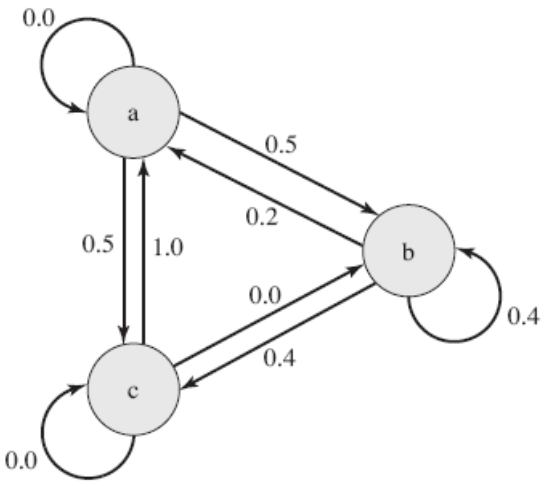
- يجب أن لا يقل طول كلمة السر عن ثمانية أحرف.
- في أول ثمانية أحرف، يجب أن تتضمن كلمة السر واحداً على الأقل من كلٍّ من: الأحرف الكبيرة، والأحرف الصغيرة، والأرقام (من 0 إلى 9)، وعلامات الترقيم.

يمكن أن يصحب تلك القواعد بعض التوجيه للمستخدم. فرغم أن هذه الطريقة تُعدُّ أفضل من مجرد توعية المستخدم، فقد لا تكون كافية لإحباط جهود تكسير كلمات السر. حيث يلفت هذا الأسلوب انتباه قراصنة تكسير كلمات السر إلى الكلمات التي لا ينبغي أن يجربوها، ولكنه مع ذلك قد يسمح بالقيام بتكسير كلمات السر.

من الإجراءات الممكنة أيضاً تجميع قاموس كبير من كلمات السر "السيئة". وعندما يختار مستخدم كلمة سر يقوم النظام بالتأكد من أنها لا توجد في القائمة الممنوعة. هناك مشكلتان في هذه الطريقة:

- الحيز: يتعين أن يكون القاموس كبيراً جداً لتكون الطريقة فعالة. فعلى سبيل المثال، يحتاج القاموس المُستخدَم في دراسة بوردو [SPAF92a] لأكثر من 30 ميجابايت لتخزينه.

- الوقت: الوقت اللازم للبحث خلال قاموس كبير سيكون كبيراً في حد ذاته. وعلاوةً على ذلك، فلفحص التباديل المحتملة لكلمات القاموس، إما أن يتم تضمين تلك التباديل في القاموس، الأمر الذي سيجعله ضخماً بحق، أو أن تكون عملية البحث مصحوبةً بعمليات معالجة مما يستهلك وقتاً إضافياً طويلاً.



حيث: $M = \{3, \{a, b, c\}, T, 1\}$

$$T = \begin{bmatrix} 0.0 & 0.5 & 0.5 \\ 0.2 & 0.4 & 0.4 \\ 1.0 & 0.0 & 0.0 \end{bmatrix}$$

مثال لسلسلة أحرف يُحتمل أن تنتمى لتلك اللغة: abbcacaba

مثال لسلسلة أحرف يُحتمل ألا تنتمي لتلك اللغة: aacccbaaa

الشكل 9-5 مثال لنموذج ماركوف.

هناك أسلوبان واعدان لتطوير نظامٍ للفحص الاستباقي لكلمة السر يقوم على رفض الكلمات الموجودة على قائمة معينة. ويعتمد أحد هذين الأسلوبين على تطوير نموذج ماركوف لتوليد كلمات السر التي يمكن تخمينها [DAVI93]. ويوضّح الشكل 9-5 مثالاً مبسطاً لذلك النموذج والذي يبيّن لغةً تتألف من أبجدية مكونة من ثلاثة أحرف. وتُمثل حالة النظام في أي وقت بآخر حرفٍ تم توليده. وتمثل القيمة المرتبطة بالانتقال من حالة إلى أخرى احتمال كون الحرف التالي يتبع الحرف الحالي في اللغة التي يمثلها النموذج. فكما بالشكل، وبافتراض أن الحرف الحالي هو a فإن احتمال كون الحرف التالي هو b، يساوي 0.5.

بشكلٍ عام، يُمثّل نموذج ماركوف برباعية $[m, A, \mathbf{T}, k]$، حيث m هي عدد الحالات في النموذج، وA هو فضاء (مجموعة set) تلك الحالات، و$\mathbf{T}$ مصفوفة احتمالات الانتقال، و k درجة النموذج . لنموذج من الدرجة k، يعتمد احتمال حدوث انتقال إلى حرف معين على الأحرف الـ k الأخيرة التي تم توليدها. ويبيّن الشكل 9-5 نموذجاً بسيطاً من الدرجة الأولى ($k = 1$).

تناول مؤلفو الدراسة تطوير نموذج من الدرجة الثانية واستخدامه. في البداية يتم إنشاء قاموس من كلمات السر التي يمكن تخمينها. بعد ذلك يتم حساب مصفوفة احتمالات الانتقال كالآتي:

1. قم بتعيين مصفوفة التردد $\mathbf{f}$، حيث $\mathbf{f}(i, j, k)$ هو عدد مرات تكرار ثلاثي الأحرف الذي يشمل الأحرف i وj وk. فعلى سبيل المثال تتضمن كلمة السر parsnips ثلاثيات الأحرف: par، ars، rsn، sni، nip، ips.
2. لكل ثنائي أحرف ij، احسب $\mathbf{f}(i, j, \infty)$ كالعدد الإجمالي لثلاثيات الأحرف التي تبدأ بـ ij. على سبيل المثال، سيمثّل $\mathbf{f}(a, b, \infty)$ العدد الإجمالي لثلاثيات الأحرف: aba ، abb، abc، وهكذا.
3. احسب عناصر $\mathbf{T}$ كالآتي:

$$\mathbf{T}(i, j, k) = \frac{\mathbf{f}(i, j, k)}{\mathbf{f}(i, j, \infty)}$$

والنتيجة هي نموذج يعكس هيكل الكلمات في القاموس. وباستخدام هذا النموذج، فإن السؤال: "هل كلمة السر هذه سيئة؟" ويتحول إلى السؤال: "هل قام نموذج ماركوف هذا بتوليد سلسلة الأحرف تلك (كلمة السر)؟" ولكلمة سر بعينها، يمكن تعيين كل احتمالات الانتقال لكل ثلاثيات الأحرف التي تتضمنها. وبعد ذلك يمكن استخدام بعض الاختبارات الإحصائية القياسية لتحديد ما إذا كان من المرجّح أو من غير المرجّح خضوع كلمة السر تلك لذلك النموذج. ويتم رفض كلمات السر التي يُحتمل توليدها من النموذج. ويذكر مؤلفو الدراسة أنهم حصلوا على نتائج جيدة باستخدام نموذج من الدرجة الثانية. واستطاع النظام الذي طوروه اكتشاف كل الكلمات غير المناسبة في قاموسهم ولم يستبعد كثيراً من كلمات السر الجيدة، مما ينبئ عن أنه سيكون مقبولاً لدى المستخدمين.

أما سبافورد [SPAF92a, SPAF92b] فقد استخدم طريقة مختلفة تماماً تعتمد على استخدام مرشّح بلوم [BLOO70]. في البداية سنشرح طريقة عمل مرشح بلوم. يتألف مرشح بلوم من الدرجة k من عدة دوال تحوير (hash functions) مستقلة عددها k، ولنرمز لها بـ $H_1(x), H_2(x),\ldots, H_k(x)$، حيث تقوم كل دالة بتحويل كل كلمة سر إلى قيمة محوّرة تتراوح مابين 0 و N-1، أي أن:

$$H_i(X_j) = y \qquad 1 \le i \le k; \qquad 1 \le j \le D; \qquad 0 \le y \le N - 1$$

حيث:

X_j = كلمة السر رقم j في قاموس كلمات السر.

D = عدد الكلمات في قاموس كلمات السر.

بعد ذلك يتم تنفيذ الإجراء الآتي على القاموس:

1. يتم تعريف جدول تحوير (hash table) يتكون من N بت، مع وضع كل البتات في البداية عند القيمة 0.
2. لكل كلمة سر، احسب قيم دوال التحوير الـ k لها، وضَع البتات المناظرة لها في جدول التحوير عند القيمة 1. ومن ثَمَّ فإذا كانت قيمة الدالة $H_i(X_j)$

عند (i, j) تساوي 67، فإن البت 67 في جدول التحوير يتم وضعه عند القيمة 1. إذا كانت قيمة ذلك البت 1 بالفعل فإنه يُترك عند القيمة 1.

عندما تَرِد كلمة مرور جديدة للفاحص، يقوم بحساب قيم دوال التحوير لها والتي عددها k. إذا كانت كل البتات المناظرة لقيم تلك الدوال في جدول التحوير لها القيمة 1 فإن كلمة السر تلك يتم رفضها. غير أنه سيكون هناك أيضاً بعض الخطأ الإيجابي الكاذب (false positives) (أي كلمات سر ليست في القاموس ولكنها تؤدي إلى تطابق في جدول التحوير). ولتوضيح ذلك، لنأخذ في الاعتبار نظاماً يستخدم دالَّتَي تحوير. لنفترض أن كلمتي السر *undertaker* و *hulkhogan* موجودتان في القاموس، في حين أن كلمة السر xG%#jj98 ليست في القاموس. لنفترض أيضاً ما يأتي:

H_1(undertaker) = 25	H_1(hulkhogan) = 83	H_1(xG%#jj98) = 665
H_2(undertaker) = 998	H_2(hulkhogan) = 665	H_2(xG%#jj98) = 998

إذا ما قُدمت كلمة السر xG%#jj98 إلى النظام فإنها ستُرفض، رغم أنها ليست في القاموس. وإذا وُجد عدد كبير من الأخطاء الإيجابية الكاذبة تلك سيكون من الصعب على المستخدمين اختيار كلمة السر. ولذلك، نود تصميم دوال التحوير بحيث تقلل الأخطاء الإيجابية الكاذبة لأقل حد ممكن. ويمكننا إثبات أن احتمال حدوث خطأ إيجابي كاذب يُعبّر عنه تقريباً كما يأتي:

$$P \approx (1 - e^{kD/N})^k = (1 - e^{k/R})^k$$

أو ما يكافئ

$$R \approx \frac{-k}{\ln(1 - P^{1/k})}$$

حيث:

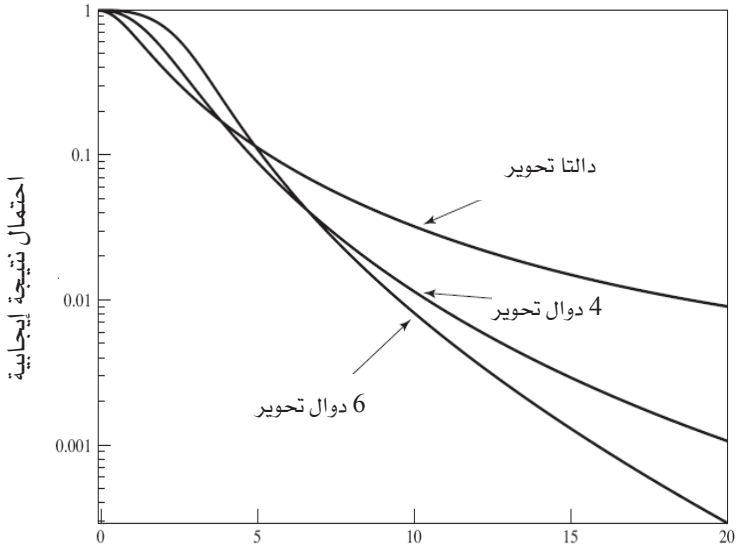
k = عدد دوال التحوير.

N = عدد البتات في جدول التحوير.

D = عدد الكلمات في القاموس.

$R = N/D$ = النسبة بين طول جدول التحوير (بتاً) إلى حجم القاموس (كلمة).

يمثل الشكل 9-6 الاحتمال P مرسوماً كدالة في R عند قيم مختلفة من k. لنفترض أن لدينا قاموساً يضم مليون كلمة ونود أن يكون احتمال رفض كلمة سر غير موجودة في القاموس هو 0.01. إذا اخترنا 6 دوال تحوير تكون النسبة المطلوبة هي $R = 9.6$. وعليه فإننا نحتاج إلى جدول تحوير طوله 9.6×10^6 بتاً، أي حوالي 1.2 ميجابايت من التخزين. وفي المقابل، يتطلب تخزين القاموس كله حيزاً في حدود 8 ميجابايت. وهكذا، فإننا نحقق ضغطاً للبيانات بنسبة تبلغ حوالى 7. وعلاوة على ذلك، ينطوي فحص كلمة السر على حساب ست دوال تحوير بشكلٍ مباشر ولا يعتمد ذلك على حجم القاموس، بينما مع استخدام القاموس الكامل، يحتاج الأمر إلى كمية كبيرة من البحث [2].



الشكل 9-6 أداء مرشّح بلوم.

[2] يتضمن نموذج ماركوف ونموذج مرشح بلوم استخدام أساليب الاحتمالات. في حالة نموذج ماركوف، هناك احتمال قليل أن بعض كلمات السر في القاموس لن يتم اكتشافها واحتمال قليل أن بعض كلمات السر التي ليست في القاموس سيتم رفضها. في حالة مرشح بلوم، هناك احتمال قليل أن بعض كلمات السر التي ليست في القاموس سيتم رفضها. مرة أخرى نرى أن استخدام أساليب الاحتمالات يبسط الحل (على سبيل المثال، انظر الحاشية 1 في الفصل الخامس).

4-9 توصيات للمطالعة

يتضمن كلٌّ من [BACE00] و[PROC01] معالجة شاملة لموضوع اكتشاف التسلل. ومن المقالات المسحية عن الموضوع والتي تُعدُّ مفيدة رغم إيجازها: [KENT00] و[MCHU00]. أما [NING04] فيتضمن مسحاً لجوانب التقدم الذي حدث مؤخراً في تقنيات اكتشاف التسلل. كما يُعدُّ [HONE01] مرجعاً أساسياً عن المصايد الأمنية، حيث يقدم تحليلاً مفصلاً عن أدوات القرصنة وطرقها.

[BACE00] Bace, R. *Intrusion Detection.* Indianapolis, IN: Macmillan Technical Publishing, 2000.

[BACE01] Bace, R., and Mell, P. *Intrusion Detection Systems.* NIST Special Publication SP 800-31, November 2000.

[HONE01] The Honeynet Project. *Know Your Enemy: Revealing the Security Tools, Tactics, and Motives of the Blackhat Community.* Reading, MA: Addison-Wesley, 2001.

[KENT00] Kent, S. "On the Trail of Intrusions into Information Systems," *IEEE Spectrum*, December 2000.

[MCHU00] McHugh, J.; Christie, A.; and Allen, J. "The Role of Intrusion Detection Systems." *IEEE Software*, September/October 2000.

[NING04] Ning, P., et al. "Techniques and Tools for Analyzing Intrusion Alerts." *ACM Transactions on Information and System Security*, May 2004.

[PROC01] Proctor, P., *The Practical Intrusion Detection Handbook.* Upper Saddle River, NJ: Prentice Hall, 2001.

5-9 مصادر للمعلومات على الويب

نوصي بالمواقع الآتية على الويب:

- CERT Coordination Center (مركز سيرت للتنسيق): منظمة نشأت عن فريق الاستجابة لطوارىء الحاسب الذي شكّلته وكالة مشاريع بحوث الدفاع المتقدمة DARPA. يوفر الموقع معلومات جيدة عن تهديدات أمن الإنترنت، ونقاط الضعف، وإحصائيات عن عمليات الهجوم.
- Honeynet Project (مشروع المصايد الأمنية): مشروع بحثي لدراسة أساليب الهجوم التي يستخدمها القراصنة وتطوير منتجات للمصايد الأمنية.
- Honeypots (المصايد الأمنية): مجموعة جيدة من الأوراق البحثية والمقالات الفنية.
- Intrusion Detection Working Group (مجموعة العمل الخاصة باكتشاف التسلل): يضم الموقع جميع الوثائق من إعداد تلك المجموعة.

6-9 مصطلحات رئيسة

audit record	سجل مراجعة
base-rate fallacy	مغالطة المعدل الأساسي
Bayes' Theorem	نظرية بايز
intruder	المتسلل
intrusion detection	اكتشاف التسلل، اكتشاف الاختراق الامني
intrusion detection exchange format	صيغة تبادل البيانات لاكتشاف التسلل
password	كلمة السر، كلمة المرور
rule-based intrusion detection	اكتشاف التسلل بناءً على قواعد
salt	الملح
statistical anomaly detection	اكتشاف الشذوذ الإحصائي
honeypot	مصيدة أمنية

7-9 أسئلة للمراجعة ومسائل

1-7-9 أسئلة للمراجعة

1-9 اذكر وعرّف بإيجاز ثلاث فئات من المتسللين.

2-9 اذكر اثنين من الأساليب المستخدمة بكثرة لحماية ملف كلمات السر.

3-9 اذكر ثلاث فوائد لاستخدام نظم لاكتشاف التسلل.

4-9 ما الفرق بين اكتشاف الشذوذ الإحصائي واكتشاف التسلل بناءً على قواعد؟

5-9 أذكر بعض المقاييس المفيدة في اكتشاف التسلل بناءً على البروفيل.

6-9 ما الفرق بين اكتشاف الشذوذ الإحصائي بناءً على قواعد و التعرف على الاختراق بناءً على قواعد؟

7-9 ما المقصود بالمصيدة الأمنية؟

8-9 ما المقصود بالملح في سياق إدارة كلمات السر بنظام التشغيل يونيكس؟

9-9 اذكر وعرّف بإيجاز أربعة أساليب تُستخدَم لتجنب استعمال كلمات سر يمكن تخمينها.

2-7-9 مسائل

1-9 تسببت سيارة أجرة في حادث مرور مميت ليلاً ثم هربت بعده. وتعمل بالمدينة شركتان لسيارات الأجرة: شركة السيارات الخضراء وشركة السيارات الزرقاء. تنامى إلى علمك المعلومات الآتية:

- 85% من سيارات الأجرة في المدينة خضراء و15% زرقاء.
- ذكر شاهد عيان أن سيارة الأجرة المتورطة في الحادث كانت زرقاء. اختبرت المحكمة موثوقية شهادة الشاهد تحت نفس الظروف السائدة ليلة الحادث واستنتجت أنه كان بوسعه التعرف على اللون الصحيح للسيارة في 80%

من الحالات. ما احتمال أن تكون السيارة المتورطة في الحادث زرقاء وليست خضراء؟.

2-9 بافتراض أن كلمات السر تتألف من تباديل من أربعة أحرف يتم اختيارها من بين 26 حرفاً أبجدياً، وأن الخَصْم قادرٌ على تجربة كلمات السر بمعدل كلمة سر واحدة كل ثانية.

a. فإذا افترضنا أيضاً عدم وجود رد فعل لما يقوم به الخَصْم حتى ينتهي من كل محاولة، ما الوقت المتوقع لاكتشاف كلمة السر الصحيحة؟
b. على افتراض وجود تغذية راجعة على شكل مؤشر يخبر الخَصْم عند إدخال حرف غير صحيح أثناء المحاولة، ما الوقت المتوقع لاكتشاف كلمة السر الصحيحة؟

3-9 بافتراض عناصر مصدر طول كلٍّ منها k خانة يتم مقابلتها بشكلٍ منتظم بعناصر هدف طول كلٍّ منها p خانة. وإذا كانت كل خانة يمكن أن تأخذ قيمة واحدة من بين r قيمة، فإن عدد عناصر المصدر يكون r^k وعدد عناصر الهدف يكون r^p. فإذا عُلم أن عنصر المصدر x_i يقابل عنصر الهدف y_j:

a. ما احتمال أن يقوم خَصْم باختيار عنصر المصدر الصحيح في محاولة واحدة؟
b. ما احتمال أن يقوم الخَصْم باختيار عنصر مصدر مختلف x_k (حيث $x_i \neq x_k$) يُنتج نفس عنصر الهدف y_j ؟
c. ما احتمال أن يقوم خَصْم باختيار عنصر الهدف الصحيح في محاولة واحدة؟

4-9 يقوم مولد كلمات سر باختيار قطعتين عشوائيا لتوليد كلمة سر تتألف من 6 أحرف. CVC (حرف ساكن - حرف متحرك - حرف ساكن) حيث V = <a, e, i, o, u> وC = مكمّل V.

a. ما هو العدد الكلي لكلمات السر الممكنة؟
b. ما هو احتمال أن يتمكن خَصْم من تخمين كلمة سر بشكلٍ صحيح؟

5-9 بافتراض أن كلمات السر تقتصر على استخدام 95 حرفاً بصيغة آسكي قابلة للطباعة، وأن جميع كلمات السر تتألف من 10 أحرف. إذا فرضنا استخدام مكسّر

كلمات سر يقوم بالتشفير بمعدل 6.4 مليون تشفيرة/ ثانية. كم من الوقت يستغرق تجريب كل كلمات السر الممكنة بشكلٍ استقصائي على نظام يونيكس؟

6-9 نظراً للمخاطر المعروفة لمنظومة كلمات السر على نظام التشغيل يونيكس، توصي وثائق نظام التشغيل SunOS-4.0 بإزالة ملف كلمات السر والاستعاضة عنه بملف متاح للقراءة من قِبَل للجمهور يسمّى etc/publickey/. يتألف المُدخل الخاص بالمُستخدِم A في ذلك الملف من معرّف المُستخدِم (ID_A)، والمفتاح العام للمستخدم (PU_a)، والمفتاح الخاص المناظر (PR_a). يتم تشفير ذلك المفتاح الخاص باستخدام خوارزمية DES بمفتاح مستمد من كلمة سر الدخول الخاصة بالمُستخدِم (P_a). وعندما يحاول المُستخدِم A الدخول على النظام، يقوم النظام بإزالة تشفير $E[P_a, PR_a]$ للحصول على المفتاح الخاص للمستخدم (PR_a).

a. يتحقق النظام بعد ذلك من أن كلمة السر التي تم إدخالها صحيحة. كيف؟

b. كيف يمكن لخَصْم الهجوم على هذا النظام؟

7-9 التشفير المُستخدَم لكلمات السر في نظام يونيكس أحادي الاتجاه، ولايمكن عكسه. وعليه، فما مدى دقة القول بأن العملية، في الواقع، تتضمن الحصول على كود تحوير (hash code) لكلمة السر وليس تشفيراً لها؟

8-9 ذكرنا أن استخدام الملح في منظومة كلمة السر على نظام يونيكس يزيد من صعوبة تخمين كلمة السر بمعامل قدره 4096. غير أن قيمة الملح تخزّن واضحةً غير مُشفَّرة في نفس المُدخل مع كلمة السر المناظرة بعد تشفيرها. وعليه، فإن هذين الحرفين يكونان معروفين للمهاجم ولذا لن يحتاج إلى تخمينهما. لماذا أكدنا على أن استخدام الملح يزيد الأمن؟

9-9 إذا كنت قد نجحت في الإجابة على المسألة السابقة وفهمت أهمية استخدام الملح، فهذا سؤال آخر لك. أليس من الممكن إحباط كل هجمات تكسير كلمات السر تماماً عن طريق زيادة كبيرة في حجم الملح، ليصبح، مثلاً 24 أو 48 بتاً؟

10-9 في مرشح بلوم الذي تناولناه في الجزء 9-3 إذا افترضنا أن:

k = عدد دوال التحوير

N = عدد البتات في جدول التحوير

D = عدد الكلمات في القاموس

a. بيّن أن النسبة المتوقعة للبتات التي لها القيمة 0 في جدول التحوير يمكن التعبير عنها على النحو الآتي:

$$\phi = (1 - \frac{k}{N})^D$$

b. بيّن أن احتمال قبول كلمة مُدخلة بطريق الخطأ كأنها كلمة موجودة بالقاموس هو:

$$P = (1 - \phi)^k$$

c. بيّن أن التعبير السابق يمكن تقريبه إلي:

$$P = (1 - e^{-kD/N})^k$$

11-9 قم بتصميم نظامٍ للتحكم في الوصول إلى الملفات يمنح مستخدمين معينين صلاحية القراءة والكتابة في ملف بناءً على معايير الترخيص التي أقامها النظام. ينبغي أن تأخذ التعليمات الشكل:

READ (F, User A): محاولة المُستخدِم A قراءة الملف F

WRITE (F, User A): محاولة المُستخدِم A تخزين نسخة (ربّما معدّلة) من الملف F

لكل ملف سجل ترويسة يتضمن امتيازات الترخيص، أي قائمة بالمستخدمين المرخّص لهم بقراءة الملف وكتابته. وينبغي تشفير الملف بمفتاحٍ غير متاحٍ للمستخدمين ولكنه معروف فقط للنظام.

الملحق A-9

مغالطة المعدل الأساسي

نبدأ باستعراض بعض النتائج المهمة من نظرية الاحتمالات، ثم نقوم بتوضيح مغالطة المعدل الأساسي.

❖ الاحتمالات المشروطة والاستقلال

كثيراً ما نحتاج لمعرفة احتمال مشروط على وقوع حدث بعينه. يؤدي الشرط إلى إزالة بعض النتائج من فضاء العينة. على سبيل المثال، ما هو احتمال الحصول على المجموع 8 عند رمي زهرتين من زهر النرد إذا علمنا أن العدد على وجه زهرة واحدة منهما على الأقل هو عدد زوجي؟ ويمكننا أن نفكّر في الأمر على النحو الآتي: نظراً لأن إحدى الزهرتين زوجية والمجموع زوجي فينبغي أن تكون الزهرة الأخرى أيضاً زوجية. وعليه، فهناك ثلاث نتائج ناجحة لكلٍّ منها نفس القدر من الاحتمال: (2، 6)، (4، 4) (6، 2)؛ وذلك من بين عدد من الاحتمالات يبلغ: [36 - (عدد الأحداث التي تعطي وجهين فرديين)] = 3×3-36 = 27، ومن ثم يكون الاحتمال المطلوب حسابه = 3/27 = 1/9.

ويعرّف الاحتمال المشروط لحدث A رسمياً بافتراض أن حدثاً B قد وقع، ونرمز له بالرمز Pr[A/B]، كما يأتي:

$$\Pr[A \mid B] = \frac{\Pr[AB]}{\Pr[B]}$$

على افتراض أن Pr[B] ليست صفراً.

في مثالنا أعلاه، الحدث A = {المجموع = 8} ، والحدث B = {على الأقل زهرة واحدة تعطي عدداً زوجياً}. تمثل الكمية $\Pr[AB]$ احتمال وقوع الحدثين معاً، أي المجموع = 8 وتعطي زهرة واحدة على الأقل عدداً زوجيا. كما رأينا أعلاه هناك 3 حالات تحقق هذين الشرطين، ومن ثَمَّ فإن $\Pr[AB] = 3/36 = 1/12$. بعد قليل من التفكير سترى أن $\Pr[B] = 3/4$. الآن يمكننا حساب

$$\Pr[A \mid B] = \frac{1/12}{3/4} = \frac{1}{9}$$

وهذا يتفق مع أسلوبنا السابق في الحل.

يُطلق على الحدثين A وB مستقلين إذا كان $\Pr[AB] = \Pr[A]\times\Pr[B]$. ويمكن بسهولة إثبات أنه إذا كان A وB مستقلين فإن $\Pr[A|B] = \Pr[A]$ و$\Pr[B|A] = \Pr[B]$.

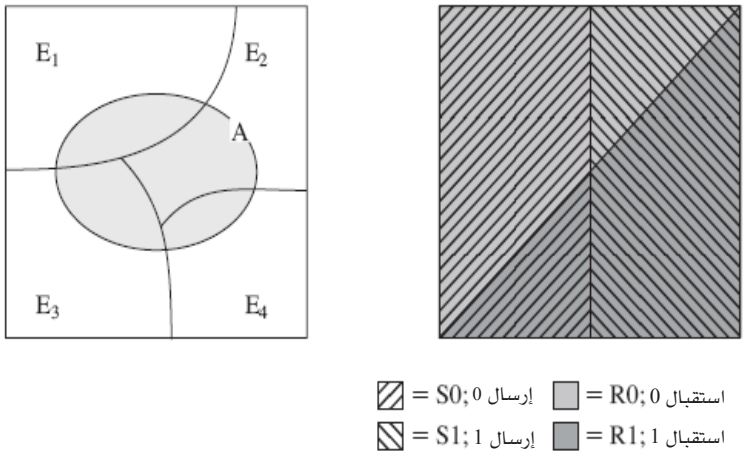
❖ نظرية بايز (Bayes Theorem)

من أهم النتائج لنظرية الاحتمالات ما يعرف بنظرية بايز. نحتاج أولاً لكتابة معادلة الاحتمال الكلي. لنفترض أن لدينا مجموعة من الأحداث المتنافية فيما بينها (mutually exclusive events): $E_1, E_2, \ldots, E_n$ بحيث إن الاتحاد (union) بين تلك الأحداث يغطي كل النواتج الممكنة. بافتراض حدث اعتباطي A، فإنه يمكننا إثبات أن:

$$\Pr[A] = \sum_{i=1}^{n} \Pr[A \mid E_i]\Pr[E_i] \qquad (1\text{-}9)$$

ويمكن التعبير عن نظرية بايز على النحو الآتي:

$$\Pr[E_i \mid A] = \frac{\Pr[A \mid E_i]\Pr[E_i]}{\Pr[A]} = \frac{\Pr[A \mid E_i]\Pr[E_i]}{\sum_{j=1}^{n} \Pr[A \mid E_j]\Pr[E_j]} \qquad (2\text{-}9)$$



(a) شكل لتوضيح المفهوم (b) مثال

الشكل 9-7 مفهوم الاحتمال الكلي ونظرية بايز.

يوضّح الشكل 9-7 (a) مفهوم الاحتمال الكلي ونظرية بايز. تُستخدم نظرية بايز لحساب "الاحتمالات البَعدية" (posterior odds)، أي احتمال أن شيئاً ما واقعٌ بالفعل في ضوء أدلة تؤيد ذلك. فعلى سبيل المثال، لنفترض أننا نرسل سلسلة من البتات بقيم 1 أو 0 على خط لنقل البيانات يعاني من وجود ضجيج (noise). ليكن S0 هو الحدث الذي يمثل إرسال 0 وS1 هو الحدث الذي يمثل إرسال 1 في وقت معيّن. بالمثل، ليكن R0 وR1 هما الحدثان اللذان يمثلان استقبال 0 أو 1 عند المُستقبل، على التوالي. افترض أن الاحتمالات عند المصدر هي: p = Pr[S1] وp -1= Pr[S0]. الآن نراقب الخط لتحديد مدى تكرار حدوث خطأ عند إرسال 1 وعند إرسال 0، ونقوم بحساب الاحتمالات الآتية: p_a = Pr[R0|S1] و p_b = Pr[R1|S0]. إذا تم استقبال 0، فإنه يمكننا حساب الاحتمال المشروط للخطأ، أي الاحتمال المشروط لإرسالنا 1 واستقبالنا 0. باستخدام نظرية بايز:

$$\Pr[S1 \mid R0] = \frac{\Pr[R0 \mid S1]\Pr[S1]}{\Pr[R0 \mid S1]\Pr[S1] + \Pr[R0 \mid S0]\Pr[S0]}$$
$$= \frac{P_a P}{P_a P + (1 - P_b)(1 - P)}$$

يوضّح الشكل 9-7 (b) المعادلة السابقة. ويتم تمثيل فضاء العينة في الشكل بمربع طول ضلعه الوحدة. يمثّل إرسال 0 (S0) بنصف المربع ويمثل إرسال 1 (S1) بالنصف الآخر، وعليه يكون Pr[S0] = Pr[S1] = 0.5. بالمثل، يمثّل استقبال 0 (R0) بنصف المربع ويمثل استقبال 1 (R1) بالنصف الآخر، وعليه يكون Pr[R0] = Pr[R1] = 0.5. في المساحة التي تمثل S0، لاحظ أن ربع تلك المساحة ينتمي للمساحة التي تمثل R1، ومن ثم فإن Pr[R1|S0] = 0.25. يمكن استنتاج بقية الاحتمالات المشروطة من الشكل بنفس الطريقة.

❖ مغالطة المعدل الأساسي

خذ في الاعتبار السيناريو الآتي. أُجرِي لمريض الاختبار الخاص بتشخيص مرضٍ معين، وكانت نتيجة الاختبار إيجابية (أي تشير إلى أن المريض لديه ذلك المرض). تتوافر لديك المعلومات الآتية:

- تبلغ دقة الاختبار 87% (أي اذا كان المريض مصابا بالمرض، فإنه في 87% من الوقت سيشير الاختبار إلى النتيجة الصحيحة، وإذا كان المريض ليس لديه المرض، فإنه في 87% من الوقت سيشير الاختبار أيضاً إلى النتيجة الصحيحة).
- ينتشر ذلك المرض في السكان بنسبة 1%.

إذا وجدنا نتيجة الاختبار إيجابية، فما هو احتمال أن المريض ليس لديه ذلك المرض؟ أي ما هو احتمال أن هذا إنذار كاذب؟ نحن بحاجة إلى نظرية بايز للحصول على الجواب الصحيح:

$$\Pr[well \mid positive] = \frac{\Pr[positive \mid well]\Pr[well]}{\Pr[positive \mid disease]\Pr[disease] + \Pr[positive \mid well]\Pr[well]}$$
$$= \frac{(0.13)(0.99)}{(0.87)(0.01) + (0.13)(0.99)} = 0.937$$

أي أنه في الغالبية العظمى من الحالات، عند اكتشاف حالة مرض باستخدام ذلك الاختبار، تكون النتيجة إنذار كاذب.

عُرضت هذه المشكلة، والتي استُخدمت في الدراسة [PIAT91]، على عدد من الأشخاص. أعطى معظم المشاركين الجواب 13%. أعطت الغالبية العظمى، بما في ذلك عدد من الأطباء، نسبة أقل من 50%. علّق كثيرٌ من الأطباء الذين أعطوا إجابة خاطئة بقولهم: "إذا كنتم على حق، فليس هناك مبرر لإجراء اختبارات سريرية!" يرجع السبب في أن معظم الناس لا يتوصلون إلى الإجابة الصحيحة إلى أنهم لا يأخذون في الاعتبار المعدل الأساسي لوقوع المرض (معدل انتشاره في السكان). يُعرف هذا الخطأ بمغالطة المعدل الأساسي.

كيف يمكن حل هذه المشكلة؟ إذا افترضنا أنه يمكنك تحسين معدل النتيجة الصحيحة للاختبار (سواءً كانت سلباً أو إيجاباً) ليصبح 99.9%. أي افترض القيم الجديدة Pr[postive|disease] = 0.999 وPr[negative|well] = 0.999. بإدخال الرقم الأول في المعادلة أعلاه، نحصل على Pr[well|positive] = 0.09، ومن ثم يقل معدل الإنذارات الكاذبة إلى 9%. هذا أفضل بكثير، ولكنه لا يزال غير مثالي. علاوةً على ذلك ، ومرة أخرى بافتراض 99.9% لدقة الاختبار، افترض الآن أن حالات الإصابة بالمرض تبلغ حالة واحدة فقط في كل 10000 نسمة، أي أن Pr[disease] = 0.0001. في هذه الحالة سنحصل على معدل إنذارات كاذبة يبلغ 91%. في الواقع العملي، وجد [AXEL00] أن الاحتمالات المرتبطة بأنظمة اكتشاف التسلل تُنتج معدلات مرتفعة بشكلٍ غير مُرضٍ للإنذارات الكاذبة.