11

الفصل الحادي عشر

الجدران النارية

محتويات الفصل:

"تعتمد قوة الموقع على جعل قوي الحماية المحيطة به غير قابلة للاختراق بشكلٍ عمليّ" – من كتاب "عن الحرب"، لكارل فون كلاوزفيتز.

"في اليوم الذي تصبح فيه قائداً، سُدّ معابر الحدود، وحطّم السجلات الرسمية، وأوقف مرور جميع المبعوثين" – من كتاب "فن الحرب" لصن تزو.

النقاط الأساسية:

- يُشكل الجدار الناري (جدار الحماية) حاجزاً لحركة المرور بالشبكة في الاتجاهات المختلفة، حيث يقوم بالسماح أو عدم السماح بالمرور طبقاً للسياسة الأمنية لهذا الجدار.
- يمكن تصميم الجدار الناري للعمل كمرشح على مستوى رزم بروتوكول الإنترنت (IP packets)، أو للعمل على أيٍّ من الطبقات العليا للبروتوكولات.
- يتكون النظام الموثوق من جهاز حاسب ونظام تشغيل يمكن التحقق من تنفيذهما لسياسة أمنية معينة. وعادةً، يركِّز مثل هذا النظام على عملية التحكم في الوصول (access control)، وذلك تبعاً لسياسة تُحدِّد المستخدمين الذين يُسمح لهم بالوصول لكل خدمة من الخدمات المتاحة.
- المعايير المشتركة لأمن المعلومات هي مبادرة دولية لتحديد مجموعة مشتركة من متطلبات الأمن ووسائل محدَّدة ومنضبطة لتقييم المنتجات على أساس تلك المتطلبات.

يمكن للجدران النارية أن تكون وسائل فعَّالة لحماية نظام محلي أو شبكة نظم من التهديدات الأمنية المتعلقة بالشبكات، كما توفر في نفس الوقت إمكانية الاتصال بالعالم الخارجي عن طريق الشبكات واسعة النطاق وشبكة الإنترنت.

سوف نبدأ هذا الفصل بلمحة عامة عن وظائف الجدران النارية ومبادئ تصميمها، ثم نعالج بعدها قضية أمن الجدار الناري نفسه، وبصفة خاصة مفهوم الأنظمة الموثوقة، أو أنظمة التشغيل الآمنة.

1-11 مبادئ تصميم الجدران النارية

لقد شهدت نظم المعلومات في الشركات والوكالات الحكومية والمنظمات الأخرى تطوراً مستمراً تَمثَّل في المراحل الآتية:

- مرحلة النظام المركزي لمعالجة البيانات: يتكون من حاسب مركزي أساسي يدعم عدداً من المحطات الطرفية المتصلة به مباشرةً.
- مرحلة الشبكات المحلية (LANs): تربط أجهزة الحاسب الشخصية والمحطات الطرفية بعضها ببعض كما تربطها أيضاً بالحاسب المركزي.
- مرحلة شبكة المنشآت (Premises network): تتألَّف من عدد من الشبكات ذات النطاق المحلي، لربط الحاسبات الشخصية مع الأنظمة الخادمة وربما مع حاسب مركزي أو حاسبين مركزيين.
- مرحلة شبكة المؤسسة (Enterprise-wide network): تتألَّف من عدة شبكات منشآت موزعة جغرافيا ومرتبطة ببعضها عن طريق شبكة خاصة واسعة النطاق (WAN).
- مرحلة الارتباط بالإنترنت: يتم فيها ربط جميع شبكات المنشآت بشبكة الإنترنت. يُمكِن أيضاً أن تكون تلك الشبكات مرتبطة فيما بينها من خلال شبكة خاصة واسعة النطاق بالإضافة إلى ارتباطها عن طريق الإنترنت.

لم يعد الارتباط بالإنترنت أمراً اختيارياً بالنسبة للمؤسسات أو الشركات، حيث أصبحت المعلومات والخدمات المتاحة على الإنترنت ضرورية لأي مؤسسة. وعلاوةً على ذلك يرغب المستخدمون بتلك المؤسسات في الاتصال بالإنترنت، وإن لم يتوفر لهم ذلك عبر شبكاتهم المحلية، فسيقومون باستخدام الاتصال الهاتفي من حاسباتهم الشخصية إلى أي موفر لخدمة الإنترنت (ISP). وبالرغم من أن الارتباط بالإنترنت يوفر فوائد للمؤسسات، فإنه يُمكِّن العالم الخارجي من الوصول إلى مكوِّنات الشبكة المحلية والتفاعل معها مما يشكل تهديداً لتلك المؤسسات. في

حين أنه من الممكن تجهيز كل محطة عمل خادم على الشبكة الخاصة بخصائص أمنية قوية – كالحماية ضد الاختراق – فإن هذا لا يُعدُّ أمراً عملياً. وإذا اعتبرنا شبكة تتألَّف من المئات أو حتى الآلاف من الأنظمة، وتعمل وفقَ مزيجٍ من الإصدارات المختلفة لأنظمة تشغيل مختلفة مثل يونيكس (UNIX) أو ويندوز، فإن أي ثغرة أمنية يتم اكتشافها تستدعي القيام بتحديث كل أنظمة التشغيل التي يُحتمل تأثرها بتلك الثغرة حتى يتم علاجها. أما العلاج البديل لذلك – والذي يلاقي قبولاً متزايداً – فهو الجدار الناري، ويتم وضعه بين الشبكة الخاصة والإنترنت كوصلة يمكن التحكم فيها وللعمل بمثابة سياج أمني خارجي. الهدف من ذلك هو حماية الشبكة الخاصة من هجمات الإنترنت والعمل كنقطة تفتيش يمكنها فرض الأمور الأمنية ومراجعتها. قد يتكون هذا الجدار الناري من جهاز حاسب واحد أو عدد من الأجهزة (اثنين أو أكثر) التي تتعاون فيما بينها لأداء تلك الوظيفة.

في هذا الجزء من هذا الفصل، سنستعرض الخصائص العامة للجدران النارية، ثم على أنواع الجدران النارية الأكثر استخداماً في الوقت الحالي، وأخيراً سنقوم بفحص بعض إعدادات الجدار الناري الأكثر شيوعاً.

1-1-11 خصائص الجدار الناري

حدد المرجع [BELL94b] قائمة الأهداف الآتية للتصاميم المختلفة للجدار الناري:

1. المرور من داخل الشبكة إلى خارجها، والعكس بالعكس، لابد وأن يكون عبر الجدار الناري. ويتم ذلك عن طريق منع الوصول إلى الشبكة المحلية إلا من خلال الجدار الناري. وكما سيتضح لاحقاً يمكن إنجاز ذلك بأشكال متعددة.
2. تحدّد السياسة الأمنية المحلية ما يُسمح له وما لا يُسمح له بالعبور من خلال الجدار الناري، كما سيتم إيضاحه لاحقاً في هذا الجزء. هناك أنواع متعددة من الجدران النارية تنفذ أنماطاً مختلفة من السياسات الأمنية.

3. ينبغي أن يكون الجدار الناري ذاته محصَّناً ضد الاختراق، مما يعني ضرورة استخدام نظام حاسب موثوق مع نظام تشغيل آمن؛ وسنتناول هذا الموضوع في الجزء 11-2.

حدَّد المرجع [SMIT97] أربعة أساليب عامة تستخدمها الجدران النارية للتحكم في الوصول (النفاذ) ولفرض السياسة الأمنية للموقع. كان تركيز الجدران النارية بالدرجة الأولى على التحكم في الخدمات، لكنها تطورت منذ ذلك الحين للقيام بالمهام الأربعة الآتية:

- التحكم في الخدمات: يحدد أنواع خدمات الإنترنت – الداخلية منها والخارجية – التي يمكن الوصول إليها. وقد يقوم الجدار الناري بفلترة حركة المرور على أساس عنوان بروتوكول الإنترنت (IP address)، ورقم منفذ TCP (بروتوكول التحكم في الإرسال)؛ كما قد يقوم بدور الخادم المفوَّض (البروكسي) الذي يستقبل كل طلب خدمة ويفسره قبل تمريره؛ كما قد يقوم باستضافة برامج خادمات أخرى كخدمة الويب والبريد الإلكتروني.
- التحكم في الاتجاه: يحدد اتجاه كل طلب من طلبات الخدمة ليتم بدؤها والسماح بتدفقها عبر الجدار الناري.
- التحكم في المستخدم: يتحكم في الوصول إلى خدمةٍ ما حسب المستخدم الذي يحاول الوصول لتلك الخدمة. و عادة ما تطبق هذه الخاصية على المستخدمين داخل محيط الجدار الناري (المستخدمين المحليين). كما يمكن تطبيقها على طلبات الخدمة الواردة من المستخدمين الخارجيين؛ وهذا يتطلب إحدى تقنيات التوثيق الآمنة مثل التي يتم توفيرها في بروتوكول الإنترنت الآمن (IPSec) (انظر الفصل السادس).
- التحكم في السلوك: يتحكم في الكيفية التي يمكن بها استخدام خدمات معينة. فعلى سبيل المثال، يمكن للجدار الناري ترشيح (فلترة) البريد الإلكتروني للقضاء على رسائل الدعاية الإلكترونية (spam)، أو قد

يمكنه السماح للمستخدمين الخارجيين بالوصول إلى بعض أجزاء من المعلومات الموجودة على خادم الويب المحلي.

قبل الشروع في تفاصيل أنواع الجدار الناري وتكويناته، فإنه من المفيد تلخيص ما يمكن للمرء أن يتوقعه من الجدار الناري كما يأتي:

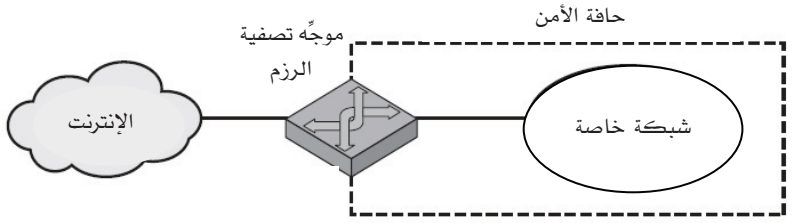
1. يُحدِّد الجدار الناري نقطة اختناق (choke point) تمنع المستخدمين غير المصرّح لهم من دخول الشبكة المحميَّة، وتحظر على الخدمات الحساسة الدخول أو الخروج من الشبكة، كما توفر الحماية ضد جميع أنواع التحايل على عناوين بروتوكول الإنترنت (IP spoofing) وهجمات التوجيه (routing attack) المختلفة. إن استخدام نقطة اختناق واحدة يُبَسِّط عملية الإدارة الأمنية لأن القدرات الأمنية مدموجة على حاسب واحد أو عدد محدود من الحاسبات.
2. يوفر الجدار الناري موقعاً لرصد العمليات المتعلقة بالأمن. كما يمكن تنفيذ عمليات التدقيق والمراجعة بالإضافة إلى الإنذار على نظام الجدار الناري.
3. يُمثِّل الجدار الناري منصَّة ملائمة للعديد من وظائف الإنترنت غير المتعلقة بالأمن، والتي تشمل مترجم عنوان الشبكة، والذي يترجم العناوين المحلية لعناوين الإنترنت المقابلة، وكذلك وظيفة إدارة الشبكة التي تدقق أو تسجل استخدامات الإنترنت.
4. يمكن للجدار الناري أن يكون بيئةً ملائمةً لبروتوكول الإنترنت الآمن (IPSec)، وذلك باستخدام نمط النفق (tunnel mode) الموصوف بالفصل السادس، كما يمكن أيضاً استخدام الجدار الناري لتنفيذ الشبكات الخاصة الافتراضية ((Virtual Private Networks (VPNs).

للجدران النارية حدودٌ لا تتعداها، فمثلاً:

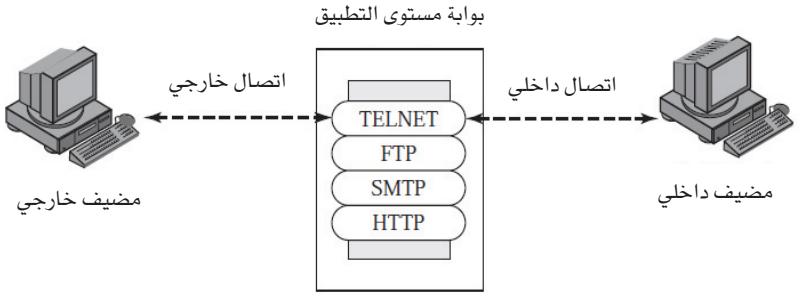
1. لا يمكن للجدار الناري توفير الحماية ضد الهجمات التي تتخطاه. فمثلاً قد يتوفر للنظم الداخلية إمكانية الاتصال الهاتفي بموفر خدمة الإنترنت (ISP)، وقد تدعم الشبكة المحلية الداخلية وحدة لأجهزة المودم التي توفر إمكانية الاتصال بالشبكة من الخارج للموظفين المسافرين.
2. لا يوفر الجدار الناري حمايةً ضد التهديدات الداخلية، مثل الموظف الساخط أو الموظف الذي يتعاون عن غير قصد مع أحد المهاجمين الخارجيين.
3. لا يمكن للجدار الناري الحماية ضد نقل برامج أو ملفات محمَّلة بالفيروسات. فنظراً لتنوع أنظمة التشغيل والتطبيقات البرمجية المعتمدة داخل محيط هذا الجدار، فإنه من غير العملي وربما من المستحيل على الجدار الناري فحص كافة الملفات الواردة ورسائل البريد الإلكتروني للتأكد من خلوها من الفيروسات.

11-1-2 أنواع الجدران النارية

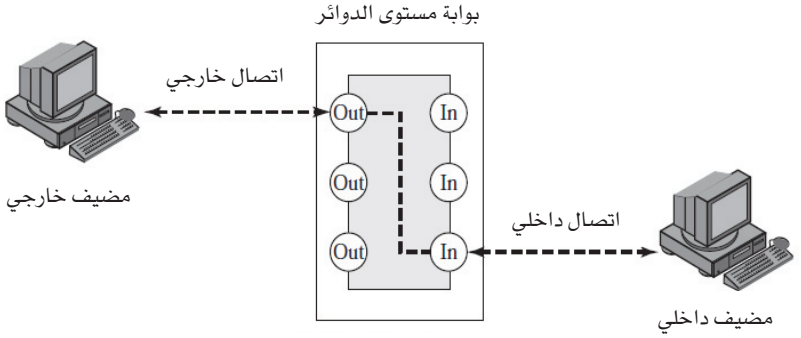
يوضِّح الشكل 11-1 ثلاثة أنواع شائعة من الجدران النارية: مرشحات الرزم (مصفيات أو فلاتر)، وبوابات مستوى التطبيق، وبوابات مستوى الدوائر. وسوف نتناول هذه الأنواع بالترتيب.



(a) موجِّه تصفية الرزم



(b) بوابة مستوى التطبيق



(c) بوابة مستوى الدوائر

الشكل 11-1: أنواع الجدران النارية.

❖ مرشحات الرزم (Packet Filters):

يطبِّق موجِّه ترشيح الرزم مجموعة من القواعد على كل رزمة من رزم بروتوكول الإنترنت قادمة أو مغادرة ومن ثَمَّ يقوم بتمريرها أو التخلص منها. ويتم عادةً تهيئة الموجِّه لترشيح الرزم في كلا الاتجاهين (من الشبكة الداخلية وإليها). تستند قواعد الترشيح على المعلومات المتضمَّنة في الرزمة:

- عنوان بروتوكول الإنترنت (IP address) للمصدر: عنوان بروتوكول الإنترنت للنظام الذي أنشأ تلك الرزمة (على سبيل المثال: 192.178.1.1).
- عنوان بروتوكول الإنترنت (IP address) للوجهة: عنوان بروتوكول الإنترنت للنظام الذي تحاول تلك الرزمة الوصول إليه (على سبيل المثال: 192.168.1.2).
- عنوان مستوى النقل (transport-level address) للمصدر والوجهة: رقم منفذ بروتوكول طبقة النقل (مثل: TCP أو UDP)، والذي يحدد نوعية تطبيقات الشبكة مثل SNMP أو TELNET.
- حقل بروتوكول الإنترنت: ويحدد بروتوكول النقل.
- الواجهة: بالنسبة لموجِّه ذي ثلاثة منافذ أو أكثر، هي واجهة الموجِّه التي تأتي منها الرزمة أو تتجه إليها.

وعادةً ما تتم تهيئة مرشح الرزم بتحديد قائمة من القواعد المبنيَّة على تطابقات مع حقول بترويسة بروتوكول الإنترنت أو ترويسة TCP. فإذا وُجد تطابق مع أحد تلك القواعد، فإنه وتبعاً لتلك القاعدة يتم تمرير الرزمة أو التخلص منها. وإذا لم يوجد تطابق مع أي من القواعد، فيتم اتخاذ إجراء مفترض. ويمكن اتباع إحدى سياستين مفترضتين:

- الإجراء المفترض = التخلص من الرزمة (اسقاطها): فالذي لا يُنص صراحةً على السماح له يُحظر.
- الإجراء المفترض = تمرير الرزمة: فالذي لا يُنص صراحةً على حظره يُسمح له.

الجدول 11-1: أمثلة لترشيح الرزم.

(A)

الإجراء	مضيفنا	المنفذ	مضيفهم	المنفذ	التعليق
ممنوع	*	*	SPIGOT	*	لا نثق بهؤلاء الناس
مسموح	OUR-GW	25	*	*	الاتصال بمنفذ SMTP الخاص بنا

(B)

الإجراء	مضيفنا	المنفذ	مضيفهم	المنفذ	التعليق
ممنوع	*	*	*	*	افتراضي

(C)

الإجراء	مضيفنا	المنفذ	مضيفهم	المنفذ	التعليق
مسموح	*	*	*	25	الاتصال بمنفذ SMTP الخاص بنا

(D)

الإجراء	المصدر	المنفذ	الوجهة	المنفذ	الأعلام	التعليق
مسموح	مضيفاتنا	*	*	25		رزمنا لمنفذ SMTP الخاص بهم
مسموح	*	25	*	*	ACK	ردودهم

(E)

الإجراء	المصدر	المنفذ	الوجهة	المنفذ	الأعلام	التعليق
مسموح	مضيفاتنا	*	*	*		اتصالاتنا الصادرة
مسموح	*	*	*	*	ACK	الردود على اتصالاتنا
مسموح	*	*	*	> 1024		حركة المرور لغير الخادمات

التخلص من الرزمة كإجراء مفترض هي السياسة الأكثر تحفظاً. فبدايةً يتم حظر كل شيء حيث تُضاف الخدمات الواحدة تلو الأخرى كلٌ حسب حالتها. وهذه السياسة هي الأكثر وضوحاً للمستخدمين الذين يرون الجدار الناري عائقاً. أما سياسة تمرير الرزمة كإجراء مفترض فهي أكثر سهولةً بالنسبة للمستخدمين ولكنها أقل أمناً؛ حيث يجب على مسؤول الأمن التعامل السريع مع كل تهديد جديد للأمن بمجرد اكتشافه.

يعطي الجدول 11-1 – المأخوذ من [BELL94b] – أمثلةً على بعض مجموعات قواعد ترشيح الرزم. يتم تطبيق القواعد في كل مجموعة بالترتيب من أعلاها إلى أسفلها. يستخدم الرمز "*" في حقل ما كرمز عام يتطابق مع كل شيء. وسنعتبر هنا أن الإجراء المفترض هو التخلص من الرزمة.

A. يُسمح للبريد الوارد بالنفاذ (منفذ 25 لواردات SMTP)، ولكن فقط لبوَّابة المضيف (gateway host). ولكن يمكن حظر الرزم الواردة من مضيف خارجي معين SPIGOT نظراً لوجود سوابق عديدة لهذا المضيف في إرسال ملفات ضخمة من خلال رسائل البريد الإلكتروني.

B. هذا بيان صريح للسياسة المفترضة. وتحوي جميع مجموعات القواعد هذه القاعدة بشكلٍ ضمني كقاعدتها الأخيرة.

C. تهدف مجموعة القواعد هذه إلى النص على أن أي مضيف داخلي يمكنه إرسال بريد إلى الخارج. فأي رزمة TCP تقصد منفذ 25 يتم توجيهها إلى خادم بروتوكول SMTP الخاص بحاسب الوجهة (destination machine). ولكن المشكلة في هذه القاعدة هو أن استخدام المنفذ 25 لاستلام SMTP يتم فقط كوضع مفترض؛ بمعنى أنه من الممكن تهيئة حاسب آخر خارجي لربط تطبيقات أخرى بالمنفذ 25. وبما أن هذه قاعدة مكتوبة، فإنه يمكن للمهاجمين النفاذ إلى الحاسبات الداخلية عن طريق إرسال رزم برقم 25 لمنفذ مصدر TCP.

D. تحقق مجموعة القواعد هذه النتيجة المرجوَّة التي لم تتحقق في (C). وتستفيد هذه القواعد من أحد خصائص وصلات الـ TCP. فبمجرد إنشاء

اتصالٍ ما، يتم ضبط مؤشر ACK لقطعة TCP في الوضعية 1 للإشعار باستلام القطع المرسلة من الطرف الآخر. ومن ثَمَّ فإن مجموعة القواعد هذه تقضي بالسماح لرزم بروتوكول الإنترنت التي يكون عنوان بروتوكول الإنترنت للمصدر فيها هو أحد المضيفات الداخلية ورقم منفذ الـ TCP للوجهة فيها هو 25. كما تقضي أيضاً بالسماح بمرور الرزم الواردة والتي يكون رقم منفذ الـ TCP للمصدر فيها هو 25 والتي يكون مؤشر ACK لقطعة TCP بها في الوضعية 1. لاحظ أننا عيَّنَّا نظامي المصدر والوجهة صراحةً لتحديد هذه القواعد بشكلٍ واضح.

E. مجموعة القواعد هذه هي نهج لمعالجة توصيلات FTP. ففي حالة توصيلات FTP، يتم استخدام توصيلتي TCP: توصيلة تحكم للتجهيز لنقل الملف، وتوصيلة بيانات للنقل الفعلي للملف. وتستخدم توصيلة البيانات رقم منفذ مختلفاً يتم تعيينه بطريقة ديناميكية لعملية النقل. ومعظم الأنظمة الخادمة، ومن ثَمَّ معظم أهداف الهجوم، تعمل على منافذ لها أرقام منخفضة؛ وفي المقابل تميل معظم المكالمات الصادرة إلى استخدام المنافذ ذات الأرقام العالية (عادةً أكبر من 1023). ولذا فإن مجموعة القواعد هذه تسمح بما يأتي:
   - الرزم التي تنشأ داخلياً.
   - رزم الرد على اتصال أنشئ عن طريق حاسب داخلي.
   - رزم متجهة لمنافذ عالية الرقم بأيٍّ من الحاسبات الداخلية.

   يتطلب هذا المخطط تهيئة النظم بحيث تسمح باستخدام المنافذ ذات الأرقام المناسبة فقط.

تشير مجموعة القواعد (E) إلى صعوبة التعامل مع التطبيقات التي تعمل على مستوى ترشيح الرزم. وهناك طريقة أخرى أيضاً للتعامل مع بروتوكول نقل الملفات (FTP) والتطبيقات المماثلة باستخدام بوَّابة مستوى التطبيق (application-level gateway) وسنتناولها لاحقاً في هذا الجزء.

أحد أهم مزايا موجِّه ترشيح الرزم (packet-filtering router) هو بساطته الشديدة. وعادةً ما تكون مرشحات الرزم شفافةً للمستخدمين وعالية السرعة. ويذكر المَرجع [WACK02] القائمة التالية لنقاط الضعف (الثغرات) الموجودة بالجدران النارية الخاصة بمرشحات الرزم:

- لا تقوم مرشحات الرزم بفحص بيانات الطبقات العليا، ولذا لا تستطيع منع الهجمات التي تستغل نقاط ضعف أو وظائف تطبيقات محدّدة. فعلى سبيل المثال، لا يمكن لجدار ناري يعمل مرشحاً للرزم عرقلة أوامر تطبيق محدَّد؛ لأنه إذا سمح ذلك الجدار الناري لتطبيق معين، فإن جميع الوظائف المتاحة في هذا التطبيق يكون مسموحاً بها أيضاً.
- نظراً لقلة المعلومات المتاحة للجدار الناري لترشيح الرزم ، فإن وظيفة التسجيل/التدوين (logging) الموجودة بهذه الجدران النارية محدودة للغاية، وعادةً تحتوي سجلات مرشح الرزم على نفس المعلومات التي تُستخدم عادةً في اتخاذ قرارات التحكم في الوصول (عنوان المصدر، وعنوان الوجهة، ونوع حركة المرور).
- معظم الجدران النارية لترشيح الرزم لا تدعم الأساليب المتقدمة لتوثيق المستخدمين. ومرةً أخرى، فإن هذا العيب في الغالب ناتجٌ عن عدم توفر وظائف الطبقات العليا بالجدار الناري.
- كما أن الجدران النارية عموماً عرضة للهجمات والإساءات التي تستغل المشكلات الموجودة بمواصفات ورصَّة بروتوكولات TCP/IP، مثل تزييف عنوان طبقة الشبكة. الكثير من الجدران النارية لترشيح الرزم لا يمكنها الكشف عن رزم الشبكات التي تم بها تغيير معلومات العنونة الخاصة بطبقة OSI الثالثة. وعموماً يتم استخدام هجمات الانتحال (التحايل وتزييف العناوين) من قبل الدخلاء من أجل تجاوز الضوابط الأمنية المنفَّذة بالجدار الناري.
- أخيراً، ونظراً لعدد المتغيرات القليلة المستخدمة في اتخاذ قرارات التحكم في الوصول، فإن الجدران النارية لترشيح الرزم عرضة للخروقات الأمنية

الناجمة عن تهيئتها بطريقة خاطئة. وبعبارة أخرى، من السهل تهيئة الجدران النارية لترشيح الرزم بصورة خاطئة غير متعمدة مما يسمح بمرور أنواع معينة من حركة المرور أو المصادر أو الوجهات التي ينبغي أن تُحظَر وفقاً لسياسة أمن المعلومات الخاصة بتلك المنظمة.

وفيما يلي بعض الهجمات التي يمكن أن تستهدف موجِّهات ترشيح الرزم والتدابير المضادة المناسبة:

- انتحال عنوان بروتوكول الإنترنت (IP address spoofing): وفيه يُرسِل الدخيل (المهاجم) رزماً من الخارج مع حقل عنوان IP للمصدر يحتوي على عنوان مضيف داخلي، ويأمل المهاجم في أن يسمح استخدام العنوان المزيف باختراق النظم التي تستخدم احتياطات أمنية بسيطة تعتمد على عنوان المصدر ويتم فيها قبول الرزم القادمة من المضيفات الداخلية الموثوقة. والتدبير المضاد في هذه الحالة هو التخلص من الرزم التي لها عنوان مصدر داخلي إذا وصلت هذه الرزم عن طريق واجهة خارجية.
- هجمات توجيه المصدر (source routing attacks): يقوم المصدر بتحديد المسار الذي ينبغي أن تتخذه الرزمة في عبورها خلال شبكة الإنترنت، أملاً في تجاوز الإجراءات الأمنية التي لا تقوم بتحليل معلومات توجيه المصدر. والتدبير المضاد في هذه الحالة هو التخلص من كافة الرزم التي تستخدم هذا الخيار.
- هجمات التجزئة الدقيقة (tiny fragment attacks): يستخدم الدخيل خيار تجزئة بروتوكول الإنترنت لإنشاء رزم جزئية صغيرة جداً، ويجعل معلومات ترويسة TCP في جزئية رزمة منفصلة. يصمم هذا الهجوم بطريقة تتحايل على قواعد الترشيح التي تعتمد على معلومات ترويسة TCP. فى العادة يقوم مرشح الرزم باتخاذ قرار الترشيح اعتماداً على الجزئية الأولى من الرزمة، ثم يتم ترشيح جميع الجزئيات اللاحقة من تلك الرزمة على أساس أنها تشكل جزءاً من الرزمة التي تم رفض جزئيتها الأولى. لكن في هذا الهجوم يأمل المهاجم أن يقوم موجِّه الترشيح بفحص الجزئية الأولى فقط وتمرير

الجزئيات المتبقية. يمكن التغلب على هجمات التجزئة الدقيقة بفرض قاعدة تنص على أنه يجب أن تحتوي الجزئية الأولى من الرزمة على قدرٍ محدّدٍ مسبقاً من ترويسة النقل كحدٍ أدنى. وإذا تم رفض الجزئية الأولى، فإنه يمكن للمرشح تذكُّر الرزمة ونبذ جميع جزئياتها اللاحقة.

❖ جدران تفتيش الحالة (Stateful Inspection Firewalls):

يتخذ مرشح الرزم التقليدي قرار الترشيح لكل رزمة على حدة بدون أن يأخذ في الاعتبار أي سياق للطبقات العليا. نحتاج للنظر في بعض خلفيات هذا الموضوع؛ لفهم ما هو المقصود من السياق، ولفهم سبب محدودية قدرة مرشح الرزم التقليدي فيما يتعلق بالسياق. تتبع معظم التطبيقات القياسية المبنية على بروتوكول TCP نموذج الزبون/الخادم. فعلى سبيل المثال، بالنسبة لبروتوكول نقل البريد البسيط (SMTP)، يتم نقل البريد الإلكتروني من نظام الزبون إلى نظام الخادم حيث يقوم نظام الزبون بإرسال رسائل بريد إلكتروني جديدة – الصادرة عادةً من المستخدمين – ويقوم نظام الخادم بدوره بنقل الرسائل ووضعها في صناديق بريد المُرسَل إليهم. يعمل بروتوكول نقل البريد الإلكتروني من خلال إقامة اتصال TCP بين الزبون والخادم، ويكون فيه رقم منفذ خادم TCP الذي يحدد تطبيق خادم بروتوكول SMTP هو 25. أما رقم منفذ بروتوكول TCP لزبون بروتوكول SMTP، فيقع بين 1024 و65535 ويتم إنشاؤه من قبل زبون بروتوكول SMTP.

بصفة عامة عندما يُنشئ تطبيق من التطبيقات التي تستخدم TCP جلسةً مع مضيف بعيد، فإنه يُنشئ اتصال TCP يكون فيه رقم منفذ TCP للتطبيق البعيد (الخادم) هو عدد أقل من 1024، ويكون رقم منفذ TCP للتطبيق المحلي (الزبون) هو عدد بين 1024 و65535. تخصَّص أرقام المنافذ الأقل من 1024 وهي الأرقام "المعروفة جيداً" (well-known) بشكلٍ دائم لتطبيقات محدّدة (كرقم 25 لخادم بروتوكول SMTP). أما الأرقام التي تقع بين 1024 و65535 فيتم توليدها ديناميكياً وتخصيصها بصفة مؤقتة فقط خلال فترة اتصال TCP.

يجب أن يسمح الجدار الناري البسيط لترشيح الرزم بمرور ما يَرِدُ إلى جميع المنافذ عالية الترقيم لضمان سلامة حركة المرور المبنية على TCP؛ مما يخلق ضعفاً يمكن استغلاله من قبل المستخدمين غير المخوَّلين.

أما جدار تفتيش الحالة فيقوم بالتشديد على قواعد حركة مرور TCP من خلال إنشاء دليل لاتصالات TCP الصادرة، كما هو مبين بالجدول رقم 11-2، ويخصص في هذا الدليل مُدخلاً لكل اتصال فعَّال، ثم يقوم هذا الجدار الناري بالسماح لرزم حركة المرور الواردة إلى المنافذ عالية الترقيم فقط التي تتوافق مع أحد مُدخلات هذا الدليل.

الجدول 11-2: مثال لدليل حالة الاتصال لجدار تفتيش الحالة.

عنوان المصدر	منفذ المصدر	عنوان الوجهة	منفذ الوجهة	حالة الاتصال
192.168.1.100	1030	210.9.88.29	80	مؤسَّس
192.168.1.102	1031	216.32.42.123	80	مؤسَّس
192.168.1.101	1033	173.66.32.122	25	مؤسَّس
192.168.1.106	1035	177.231.32.12	79	مؤسَّس
223.43.21.231	1990	192.168.1.6	80	مؤسَّس
219.22.123.32	2112	192.168.1.6	80	مؤسَّس
210.99.212.18	3321	192.168.1.6	80	مؤسَّس
24.102.32.23	1025	192.168.1.6	80	مؤسَّس
223.212.212	1046	192.168.1.6	80	مؤسَّس

❖ بوَّابة مستوى التطبيق (Application-Level Gateway):

تعمل بوَّابة مستوى التطبيق – وتسمَّى أيضاً بالخادم المفوّض (proxy server) – كمُرَحِّل لحركة المرور على مستوى التطبيقات (الشكل 11-1 (b)). يقوم المستخدم بالاتصال بالبوَّابة باستخدام أحد تطبيقات TCP/IP، مثل Telnet أو بروتوكول نقل الملفات (FTP). تطلب البوَّابة من المستخدم اسم المضيف البعيد المطلوب الوصول إليه.

عندما يستجيب المستخدم ويوفر هويَّة المستخدم الصالحة ومعلومات التوثيق المطلوبة، تتصل البوَّابة بالتطبيق الذي يكون على المضيف البعيد وتُرَحِّل قطع بيانات TCP التي تتضمن بيانات التطبيق بين الطرفين. إذا لم تنفِّذ البوَّابة كود المفوّض لتطبيق معين، فلن تتوفر هذه الخدمة ولن يُسمح بتمريرها عبر جدار الحماية. فضلاً عن ذلك، يمكن ضبط البوَّابة لدعم سمات محدّدة فقط لتطبيق ما يعتبرها مدير الشبكة مقبولة مع رفض جميع السمات الأخرى.

غالباً ما تكون بوابات مستوى التطبيق أكثر أمناً من مرشحات الرزم؛ فبدلاً من محاولة التعامل مع كثير من التوليفات الممكنة التي يتم السماح لها أو منعها على مستوى TCP أو IP، تقوم بوَّابة مستوى التطبيق بفحص القليل فقط من التطبيقات المسموح بها. هذا بالإضافة إلى أنه من السهل تسجيل ومراجعة كافة أنواع حركة المرور الواردة على مستوى التطبيق.

العيب الرئيس لهذا النوع من البوابات هو المعالجة الإضافية التي تُجرَى لكل اتصال. وفعلياً يمكن اعتبار أن هناك اتصالين منقسمين بين المستخدمين الطرفيين؛ تكون فيهما البوَّابة هي نقطة الانقسام، حيث يجب على البوَّابة أن تفحص وتمرر حركة المرور في كلا الاتجاهين.

❖ بوَّابة مستوى الدائرة (Circuit-Level Gateway)

هناك نوع ثالث من الجدران النارية هو بوَّابة مستوى الدائرة (الشكل 11-1 (c)). يمكن أن يكون هذا النوع نظاماً بذاته أو أن يكون وظيفة خاصة يتم تشغيلها لصالح تطبيقات معينة من قِبَل بوَّابة مستوى التطبيقات. لا تسمح بوَّابة مستوى الدائرة بإجراء اتصال TCP من طرف لطرف؛ بل تُنشئ اتصالي TCP: واحداً بينها وبين مستخدم TCP لمضيف داخلي، وآخر بينها وبين مستخدم TCP لمضيف خارجي. وبمجرد إنشاء الاتصالين، تقوم البوَّابة عادةً بنقل قطع بيانات TCP من وصلة إلى أخرى دون فحص محتوياتها. هنا تكون وظيفة الأمن عبارة عن تحديد الاتصالات التي يمكن السماح بها.

في الاستخدامات المعتادة لبوابات مستوى الدائرة يثق مدير النظام (system administrator) بالمستخدمين الداخليين. هنا يمكن تهيئة البوَّابة لدعم الاتصالات الواردة على مستوى التطبيقات أو خدمات المُفَوِّض، بالإضافة إلى دعم الوظائف على مستوى الدوائر للاتصالات الصادرة. في هذا الوضع، قد تتكبد البوَّابة عبئاً إضافياً للتفتيش عن أية عمليات محظورة قد توجد ببيانات التطبيقات الواردة، أما في حالة البيانات الصادرة فلا تتكبد البوَّابة شيئاً من هذا العبء.

أحد الأمثلة العملية على بوابات مستوى الدائرة هو حزمة بروتوكول SOCKS [KOBL92]؛ وقد تم توصيف الإصدار 5 من SOCKS في طلب التعليقات رقم 1928 الذي يعرِّف SOCKS كما يأتي:

> "البروتوكول الموصوف هنا مصممٌ لتوفير إطار عمل لتطبيقات الزبون/الخادم في مجالي TCP وUDP لاستخدام خدمات الجدران النارية بسهولة وبشكلٍ آمن، وهذا البروتوكول من حيث المفهوم هو "طبقة حشوة" بين طبقة التطبيق وطبقة النقل، وعلى هذا فإنه لا يوفر خدمات البوَّابة لطبقة الشبكة، كتمرير رسائل ICMP."

تتألَّف حزمة SOCKS من العناصر الآتية:

- خادم SOCKS: يعمل على جدار ناري بنظام تشغيل يونيكس.
- مكتبة زبون SOCKS: تعمل على المضيفات الداخلية المحميَّة من قِبَل الجدار الناري.
- إصدارات تدعم SOCKS لكثير من برامج الزبون القياسية مثل بروتوكول نقل الملفات (FTP) وTELNET. وعادةً ما تتضمن تنفيذات SOCKS إعادة ترجمة (recompilation) أو إعادة ربط (relinking) لتطبيقات الزبون المبنية على TCP لكي تستخدم إجراءات التغليف (encapsulation) المناسبة بمكتبة SOCKS.

عندما يرغب زبون TCP في تأسيس اتصال مع كائن معين يمكن الوصول إليه فقط عبر جدار الحماية ، لا بد من فتح اتصال TCP إلى منفذ SOCKS مناسب على نظام خادم SOCKS. تقع خدمة SOCKS على منفذ TCP رقم 1080. إذا نجح طلب الاتصال هذا، فإن الزبون يتفاوض على أسلوب التوثيق الذي سيتم استخدامه، والذي على أساسه تتم عملية التوثيق، ومن ثمَّ يُرسِل الزبون طلب الترحيل. ويقوم خادم SOCKS بتقييم الطلب وبناءً عليه يُنشئ وصلة مناسبة أو يُهمِل الطلب. ومن الجدير بالذكر أن التعامل مع تبادلات UDP يتم بطريقة مماثلة؛ حيث يتم فتح اتصال TCP لتوثيق المستخدم من أجل إرسال قطع بيانات UDP واستقبالها، ومن ثم يتم تمريرها طالما ما زال اتصال TCP مفتوحاً.

❖ مضيف المَعقِل (Bastion Host)

مضيف المَعقِل هو نظام محدّد من قبل مسئول الجدار الناري كنقطة حرجة بشدة في أمن الشبكة. وعادةً ما يعمل مضيف المَعقِل بمثابة منصَّة لبوَّابة على مستوى الدائرة، أو على مستوى التطبيق. ومن السمات الشائعة لمضيف المَعقِل ما يأتي:

- يقوم مضيف المَعقِل بتنفيذ نسخة آمنة من نظام التشغيل بواسطة مكوِّناته المادية (hardware)، مما يجعل هذا النظام نظاماً موثوقاً.
- يتم فقط تنصيب الخدمات التي يعتبرها مدير الشبكة أساسية على مضيف المَعقِل. وتشمل هذه الخدمات تطبيقات المفوَّض مثل TELNET، وDNS، وFTP، وSMTP، وتوثيق المستخدم.
- قد يطلب مضيف المَعقِل توثيقاً إضافياً قبل أن يسمح للمستخدم بالوصول إلى خدمات المفوَّض. بالإضافة إلى ذلك، قد تطلب كل خدمة من خدمات المفوَّض توثيقاً خاصاً بها قبل السماح للمستخدم بالنفاذ.
- يتم ضبط كل مفوَّض لدعم مجموعة محدودة من الأوامر القياسية للتطبيقات.

- يتم ضبط كل مفوَّض بحيث يسمح بالوصول فقط إلى مجموعة محدّدة من الأنظمة المضيفة؛ وهذا يعني أن المجموعة المحدودة للأوامر المسموح بها يمكن تطبيقها فقط على هذه المجموعة المحدّدة من الأنظمة على الشبكة المحميَّة.
- يحتفظ كل مفوَّض بمعلومات مراجعة تفصيلية عن طريق تسجيل كل حركة مرور وكل اتصال ومدته. إن تسجيل مثل تلك المعلومات ضروري لاكتشاف هجمات الدخلاء وإنهائها.
- كل وحدة مفوَّض هي عبارة عن حزمة صغيرة من البرامج المصمَّمة خصيصاً لأمن الشبكة. وبسبب بساطتها النسبية، فمن السهل التحقق من العيوب الأمنية لهذه الوحدات. فمثلاً يحتوي تطبيق بريد يونيكس الإلكتروني عادةً على أكثر من 20,000 سطر من التعليمات البرمجية، في حين أن مفوَّض البريد قد يحتوي على أقل من 1000 سطر.
- يكون كل مفوَّض مستقلاً عن المفوَّضين الآخرين على مضيف المَعقِل. فإذا حدثت مشكلةٌ ما في تشغيل أي مفوَّض، أو إذا تم اكتشاف ضعف أمني به، فمن الممكن إلغاء تثبيته دون أن يؤثر ذلك على تشغيل تطبيقات المفوَّضين الآخرين. وأيضاً إذا كانت مجموعة المستخدمين تتطلب دعماً لخدمة جديدة، فإنه يمكن لمسئول الشبكة تثبيت المفوَّض المطلوب بسهولة على مضيف المَعقِل.
- عموماً لا يحتاج المفوَّض في عمله للنفاذ إلى القرص الصلب إلا عند قراءة ملف التهيئة (الإعدادات) الأوَّليّ (initial configuration file)؛ وهذا مما يصعِّب على الدخلاء تثبيت برامج أحصنة طروادة لالتقاط الرزم أو غيرها من الملفات الخطرة على مضيف المَعقِل.
- كل مفوَّض يعمل كمستخدم بدون امتيازات (صلاحيات privileges) في دليل خاص ومؤمَّن على مضيف المَعقِل.

3-1-11 تهيئة الجدار الناري

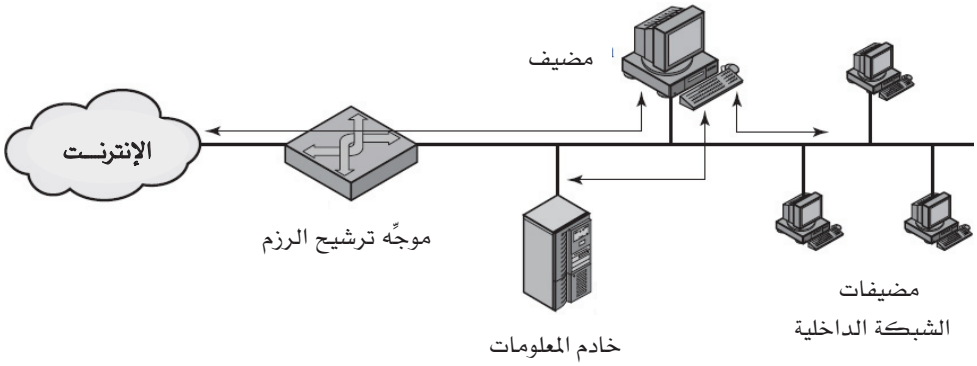
يمكن استخدام تهيئة بسيطة تتكون من نظام واحد، مثل موجِّه واحد لترشيح الرزم أو بوَّابة واحدة (كما بالشكل 11-1)، كما أنه من الممكن أيضاً استخدام تهيئات أكثر تعقيداً بل وأكثر شيوعاً. يوضِّح الشكل 11-2 ثلاثاً من تهيئات الجدار الناري الشائعة التي سنقوم بدراسة كلٍّ منها.

في جدار حماية المضيف المنتقى بتشكيل المَعقِل أحادي المقر (screened host firewall, single-homed bastion) (الشكل 11-2 (a))، يتألف الجدار الناري من نظامين: موجِّه ترشيح رزم، ومضيف المَعقِل. عادةً يتم تهيئة الموجِّه على النحو الآتي:

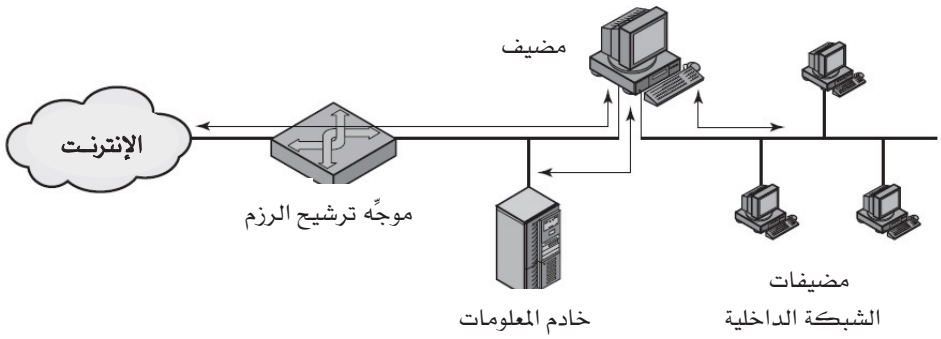
1. بالنسبة لحركة المرور من الإنترنت: يتم السماح لرزم بروتوكول الإنترنت المتجهة إلى مضيف المَعقِل فقط.
2. بالنسبة لحركة المرور من الشبكة الداخلية: يتم السماح لرزم بروتوكول الإنترنت القادمة من مضيف المَعقِل فقط.

يُنفِّذ مضيف المَعقِل مهام التوثيق ووظائف المفوَّض. تمتلك هذه التهيئة قدراً أكبر من الأمن مقارنةً مع مجرد استعمال موجِّه لترشيح الرزم أو مجرد بوَّابة على مستوى التطبيقات، وذلك لسببين:

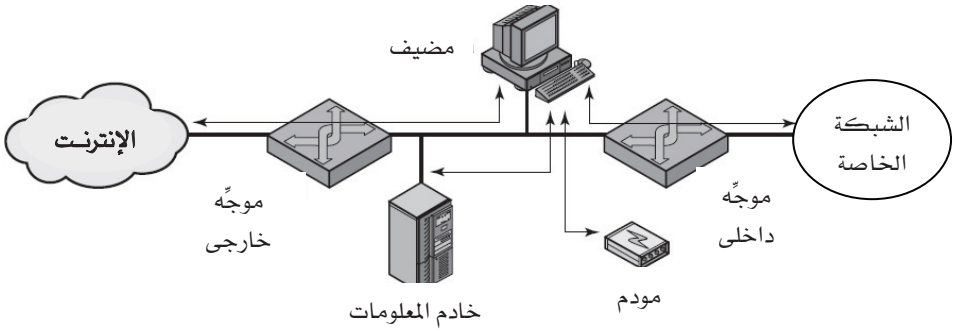
- قيام هذه التهيئة بعمل ترشيحين أحدهما على مستوى الرزمة والآخر على مستوى التطبيق، مما يسمح بقدر كبير من المرونة في تحديد السياسة الأمنية.
- أن على الدخلاء عموماً اختراق نظامين منفصلين قبل أن يتعرض أمن الشبكة الداخلية للخطر.



(a) جدار حماية المضيف المنتقى بتشكيل المعقل أحادي المقر.



(b) جدار حماية المضيف المنتقى بتشكيل المعقل ثنائي المقر



(c) تشكيل جدار حماية الشبكة الفرعية المنتقاة

الشكل 11-2: تهيئات الجدران النارية.

يمتاز هذا الشكل أيضاً بالمرونة في توفير الوصول المباشر إلى شبكة الإنترنت، فعلى سبيل المثال قد تشتمل الشبكة الداخلية على خادم معلومات عامة – مثل خادم الويب – والذي لا يتطلب قدراً عالياً من الأمن. وفي هذه الحالة، يمكن تهيئة جهاز التوجيه ليسمح بحركة مرور مباشرة بين خادم المعلومات والإنترنت.

في تشكيل المَعقِل أحادي المقر الموصوف للتوّ، إذا أصبح أمن موجِّه ترشيح الرزم مخترقاً أو منعدماً، عندها يمكن أن تتدفق حركة المرور مباشرةً خلال الموجِّه الواقع بين الإنترنت والأنظمة المضيفة الأخرى على الشبكة الخاصة. أما جدار حماية المضيف المنتقى بتشكيل المَعقِل ثنائي المقر (screened host firewall, dual-homed bastion) فيقوم بمنع مثل هذا الاختراق الأمني بشكلٍ مادي (الشكل 11-2 (b)). تتوفر في هذا التشكيل نفس مزايا الطبقات الأمنية المزدوجة المتوفرة في التشكيل السابق. ومرةً أخرى، فإنه يمكن السماح لخادم المعلومات أو الأنظمة المضيفة الأخرى بالاتصال المباشر مع الموجِّه إذا كان هذا متوافقاً مع السياسة الأمنية.

يُعد تشكيل جدار حماية الشبكة الفرعية المنتقاة (screened subnet firewall) كالمُبيَّن بالشكل 11-2 (c) الأكثر أماناً مقارنةً بجميع النظم السابق عرضها. ففي هذا التشكيل، يتم استخدام موجِّهين لترشيح الرزم، يقع أحدهما بين مضيف المَعقِل والإنترنت ويقع الآخر بين مضيف المَعقِل والشبكة الداخلية. يُنشئ هذا التشكيل شبكة فرعية معزولة قد تتكون ببساطة من مضيف المَعقِل فقط كما قد تضم أيضاً واحداً أو أكثر من خادمات المعلومات وأجهزة المودم من أجل توفير قدرة الاتصال الهاتفي (dial-in). عادةً ما يمكن لشبكة الإنترنت والشبكة الداخلية الوصول إلى الأنظمة المضيفة على الشبكة الفرعية المنتقاة، لكن يتم حظر حركة المرور عبر تلك الشبكة الفرعية. يوفر هذا التشكيل عدداً من المزايا:

- يوجد الآن ثلاثة مستويات من الدفاع تهدف إلى إحباط الدخلاء.

- يقوم الموجِّه الخارجي بالإعلان (على شبكة الإنترنت) فقط عن وجود شبكة فرعية منتقاة، ولذلك تصبح الشبكة الداخلية غير مرئية بالنسبة لشبكة الإنترنت.
- وبالمثل، فإن الموجِّه الداخلي يعلن (على الشبكة الداخلية) فقط عن وجود شبكة فرعية منتقاة، ولذلك لا يمكن للنظم على الشبكة الداخلية بناء مسارات مباشرة إلى شبكة الإنترنت.

11-2 الأنظمة الموثوقة

إحدى الطرق لتعزيز قدرة النظام على الدفاع ضد الدخلاء والبرمجيات الخبيثة هي تنفيذ تقنية النظم الموثوقة. ويعطي هذا الجزء لمحةً موجزةً عن هذا الموضوع. وسنبدأ بالنظر في بعض المفاهيم الأساسية للتحكم في الوصول إلى البيانات.

11-2-1 التحكم في الوصول إلى البيانات

بعد الوصول الناجح للشبكة، يحق للمستخدم النفاذ إلى أحد الأنظمة المضيفة والتطبيقات (أو إلى مجموعة منها). وعادةً لا يُعد هذا كافياً لنظام يتضمن بيانات حساسة في قاعدة بياناته. ويمكن أن يتم تعريف المستخدم للنظام من خلال إجراءات التحكم في الوصول للنظام وذلك بأن يحتفظ النظام بملف تعريف لكل مستخدم يحدد العمليات المسموح له بها والملفات التي يمكنه الوصول إليها، ويقوم نظام التشغيل بإعمال قواعد تستند إلى ذلك الملف. ومع ذلك يجب على نظام إدارة قواعد البيانات التحكم في الوصول إلى سجلات محدّدة أو حتى إلى أجزاء من بعض السجلات. فعلى سبيل المثال، قد يكون من المتاح لأي فرد في الإدارة الحصول على قائمة موظفي الشركة، لكن يُسمح فقط لأفراد معدودين بالوصول إلى معلومات الرواتب. وهذه المسألة هي أكثر من مجرد مستوى آخر من التفاصيل. ففي حين أن نظام التشغيل قد يمنح الإذن لمستخدمٍ ما بالوصول إلى ملف أو استخدام تطبيق معين بدون الحاجة لمزيد من التدقيق الأمني بعد ذلك، فإن نظام إدارة قواعد البيانات لا بُدّ وأن يقرر السماح من عدمه بشأن كل محاولة للحصول على بيانات جديدة.

وقرار كهذا لا يعتمد فقط على هويَّة المستخدم ولكن أيضاً على أجزاء البيانات التي يريد الحصول عليها، بل وحتى على المعلومات التي سبق أن حصل عليها.

وهناك نموذج عام للتحكم في الوصول كالنظام المستعمل من قبل نظم إدارة قواعد البيانات والملفات ألا وهو مصفوفة الوصول (access matrix) (انظر الشكل 3-11 (a))، والعناصر الأساسية لهذا النموذج هي كما يأتي:

- الفاعل (Subject): وهو كيانٌ قادرٌ على الوصول إلى الأشياء. وعموماً، فإن مفهوم الفاعل يكافئ مفهوم العملية (process). وفي الواقع أي مستخدم أو تطبيق لا يصل إلى كائنٍ ما إلا من خلال العملية التي تمثل ذلك المستخدم أو التطبيق.
- الكائن (Object): أي شيء يتم التحكم في الوصول أو النفاذ إليه؛ كالملفات أو أجزاء منها ، والبرامج، وقطاعات الذاكرة.
- حق الوصول (Access right): الطريقة التي يمكن للفاعل (subject) النفاذ بها لكائن ما (object)؛ كالقراءة (read)، والكتابة (write)، والتنفيذ (execute).

يمثل أحد محوري المصفوفة الفاعل الذي قد يحاول الوصول إلى البيانات. ويشمل ذلك عادةً، آحاد المستخدمين أو مجموعاتهم، بالرغم من إمكانية فرض عملية التحكم في الوصول على المحطات الطرفية والأنظمة المضيفة أو التطبيقات بدلاً من أو بالإضافة إلى المستخدمين. أما المحور الآخر فيعدِّد الكائنات التي يمكن الوصول إليها. وبتفصيل أكثر، قد تكون تلك الكائنات حقول بيانات فردية، أو قد تكون أيضاً مجموعات أكبر مثل السجلات (records) والملفات أو حتى قواعد بيانات بأكملها. يبين كل مُدخل في المصفوفة حقوق وصول فاعل معين لكائنٍ ما.

	البرنامج 1	...	القطعة A	القطعة B
العملية 1	قراءة وتنفيذ		قراءة وكتابة	
العملية 2				قراءة
. . .				

(a) مصفوفة الوصول

قائمة التحكم في الوصول للبرنامج 1:
العملية 1 (قراءة، تنفيذ)
قائمة التحكم في الوصول للقطعةA:
العملية 1 (قراءة، تنفيذ)
قائمة التحكم في الوصول للقطعة B:
العملية 2 (قراءة)

(b) قوائم التحكم في الوصول

قائمة الصلاحيات للعملية 1:
البرنامج 1 (قراءة، تنفيذ)
القطعة A (قراءة، كتابة)
قائمة الصلاحيات للعملية 2:
القطعة B (قراءة)

(c) قائمة الصلاحيات

الشكل 11-3: هياكل التحكم في الوصول.

عادةً ما تكون معظم مُدخلات مصفوفة الوصول خاوية (مصفوفة متناثرة sparse matrix)، ويتم تنفيذها عملياً بتقسيمها بأحد طريقتين. فيمكن تقسيم المصفوفة بحسب الأعمدة مما يولد عدداً من قوائم التحكم في الوصول (access control lists (ACLs)) (الشكل 11-3 (b)). ومن ثَمَّ، يكون لكل كائن قائمة خاصة به تحدد لكل مستخدم الحقوق المسموح له بها. وقد تحتوي قائمة التحكم هذه على مُدخل عام أو افتراضي، مما يسمح للمستخدمين غير المذكورين صراحةً بمجموعة حقوق افتراضية (default). ويمكن أن تشمل عناصر هذه القائمة آحاد المستخدمين أو مجموعاتهم.

كذلك يمكن تقسيم المصفوفة بحسب الصفوف مما يولد عدداً من تذاكر الإمكانات (capability tickets) (الشكل 11-3 (c)). وتحدد تذكرة الإمكانات الكائنات والعمليات المخولة لكل مستخدم والذي يكون لديه عدد محدّد من التذاكر، وقد يُخوَّل للمستخدم إقراض هذه التذاكر أو إعطائها لآخرين. ولأن التذاكر قد تكون متناثرة في جميع أنحاء النظام، فإنها تمثل مشكلة أمنية أكبر من مشاكل قوائم التحكم في الوصول؛ فبالتحديد يجب أن تكون التذكرة غير قابلة للتزوير. وإحدى الطرق لتحقيق ذلك أن يمسك نظام التشغيل بجميع التذاكر نيابةً عن المستخدمين وأن يتم تخزينها في منطقة من الذاكرة لا يحق للمستخدمين الوصول إليها.

11-2-2 مفهوم النظم الموثوقة

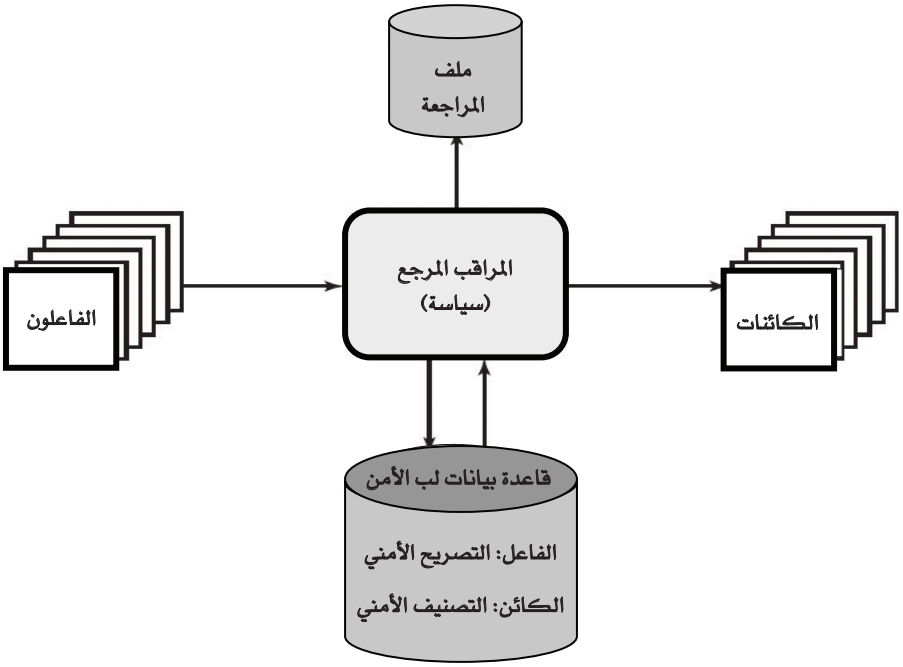
معظم ما ناقشناه حتى الآن معنيٌّ بحماية رسالة معينة أو عنصرٍ ما من هجمات سلبية (passive attacks) أو نشطة (active) من قِبَل مُستخدِم معين. وهناك متطلبٌ مختلفٌ نوعاً ما ولكنه مطلوبٌ على نطاق واسع ألا وهو حماية البيانات أو الموارد بدرجات أمنية متفاوتة. وهذا الأمر شائع في المجال العسكري، حيث يتم تصنيف المعلومات على أنها معلومات متاحة (U)، أو خاصة (C)، أو سرية (S)، أو سرية للغاية (TS)، أو ما هو أشد. وينطبق هذا المفهوم أيضاً في مجالات أخرى، والتي يمكن تنظيم المعلومات فيها إلى فئات إجمالية حيث يُمنح المستخدمون تصاريح

وصول إلى فئات معينة من تلك البيانات. فعلى سبيل المثال، يمكن تخصيص المستوى الأعلى من الأمن لوثائق وبيانات التخطيط الاستراتيجي للشركات، والتي يمكن الوصول إليها فقط من قِبَل مسئولي الشركة ومساعديهم؛ ويلي ذلك البيانات المالية وشئون الموظفين الحساسة، والتي يمكن الوصول إليها فقط من قبل إدارة شئون الموظفين ومسئولي الشركة، وهلم جرا.

يشار إلى المتطلبات التي يُراد فيها تصنيف البيانات إلى فئات أو مستويات متعددة بالأمن متعدد المستويات (multilevel security). والنص العام لمتطلب الأمن متعدد المستويات هو أن الفاعل الموجود بمستوى عالٍ لا يصح له نقل معلومات إلى كائن بمستوى أدنى أو مستوى غير مماثل إلا إذا كان تدفق المعلومات هذا يعكس بدقة إرادة مستخدم مخوّل له. أما لأغراض التنفيذ، فيمكن صياغة هذا المتطلب كشرطين ينبغي لنظام الأمن متعدد المستويات الالتزام بهما، وهما:

- ممنوع القراءة لأعلى (No read up): يمكن للفاعل فقط قراءة كائن ذي مستوى أمن مساوٍ أو أدنى، ويشار إلى ذلك بخاصية الأمن البسيط (Simple Security Property).
- ممنوع الكتابة لأسفل (No write down): يمكن للفاعل فقط الكتابة في كائن ذي مستوى أمن مساوٍ أو أعلى. ويشار إلى ذلك بخاصية * (خاصية النجمة)[1].

[1] النجمة '*' لا تعني شيئاً محدداً. حيث لم يأت أحد باسم مناسب لتلك الخاصية حتى كتابة أول تقرير لهذا النموذج. فاستُخدِمت النجمة في المسودة حتى يمكن تبديلها بسرعة بمجرد الاتفاق على اسمٍ للخاصية. وحيث أنه لم يتم الاتفاق على اسم ما فقد تم طبع التقرير كما هو بدون تبديل النجمة.



الشكل 11-4: المراقب المَرجع.

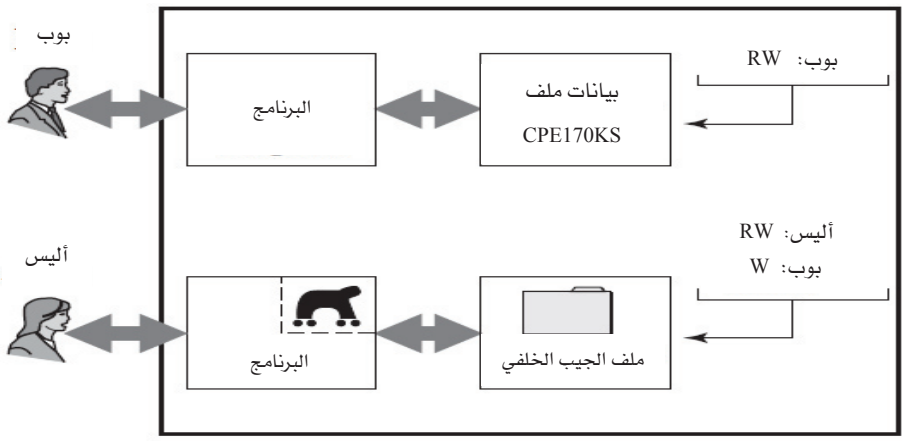
وهاتان القاعدتان إذا طبقتا على النحو الصحيح، فإنهما توفران الأمن متعدد المستويات. وبالنسبة لنظم معالجة البيانات، فإن النهج المتّبع الذي كان هدفاً لكثير من البحث والتطوير يستند إلى مفهوم المراقب المَرجع (reference monitor) كما هو موضح بالشكل 11-4. والمراقب المَرجع هو جزء بالمكوِّنات المادية ونظام التشغيل بجهاز الحاسب يقوم بالتحكم وتنظيم وصول فاعل ما إلى الكائنات على أساس المتغيرات الأمنية للفاعل والكائنات. ويمتلك المراقب المَرجع حق الوصول إلى الملف المعروف باسم لب قاعدة بيانات الأمن (security kernel database) والذي يسرد امتيازات الوصول (التصريح الأمني security clearance) لكل فاعل، وسمات الحماية (مستوى التصنيف classification level) لكل كائن. يفرض المراقب المَرجع

القواعد الأمنية (ممنوع القراءة لأعلى وممنوع الكتابة لأسفل)، كما يمتلك الخصائص الآتية:

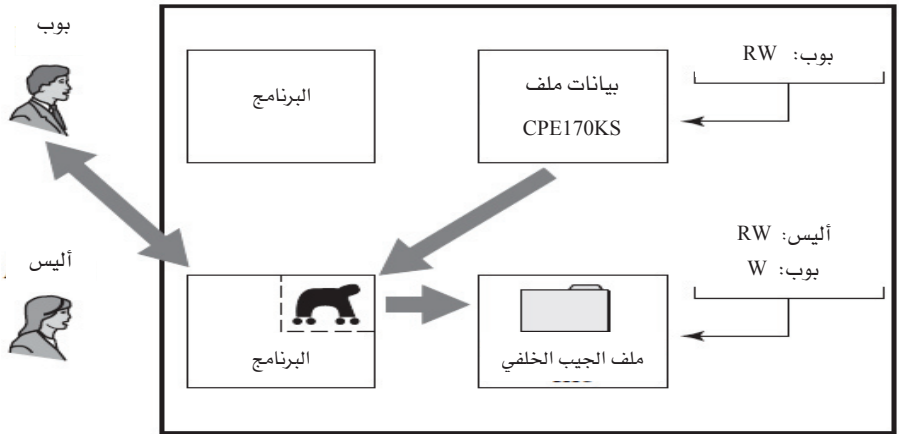
- الوساطة الكاملة: يتم تطبيق القواعد الأمنية على كل وصول (نفاذ)، وليس فقط – على سبيل المثال – عند فتح الملف.
- العزل: يتم حماية المراقب المَرجِع وقاعدة البيانات من أي تعديل غير مصرّح به.
- التحقق: يجب توفر إمكانية إثبات صحة المراقب المَرجِع؛ أي أنه يجب أن يكون من الممكن رياضياً إثبات أن المراقب المَرجِع يفرض القواعد الأمنية ويوفر الوساطة الكاملة والعزل.

وهذه شروط جامدة لا مرونة فيها. فشرط الوساطة الكاملة مثلاً يعني أن الوساطة لابد أن تتحقق في أي حالة وصول إلى البيانات سواءً كانت داخل الذاكرة الرئيسة أو على القرص الصلب أو غيره. وتنفيذ عمل مثل هذا كبرمجيات فقط يُشكِّل عبئاً كبيراً جداً في الأداء ليكون عملياً، ولهذا ينبغي تنفيذه على الأقل جزئياً كمكوِّن مادي (hardware). كما يعني شرط العزل أنه يجب أن لا يكون من الممكن للمهاجم، مهما كان ذكياً، أن يغير منطق المراقب المَرجِع أو محتويات لب قاعدة بيانات الأمن. وأخيراً، فشرط الإثبات الرياضي يُعدُّ تحدياً هائلاً لنظامٍ معقد مثل الحاسب متعدد الغرض (general-purpose computer). فالنظام الذي يمكنه أن يقدم مثل هذا التحقق يشار إليه بأنه نظام موثوق.

وثمة عنصر أخير مبين في الشكل 11-4 ألا وهو ملف المراجعة (audit file)؛ حيث يتم تخزين كل الأحداث الأمنية المهمة، وكل الخروقات الأمنية المكتشفة، وكل التغييرات في لب قاعدة بيانات الأمن المصرّح بها، في هذا الملف.

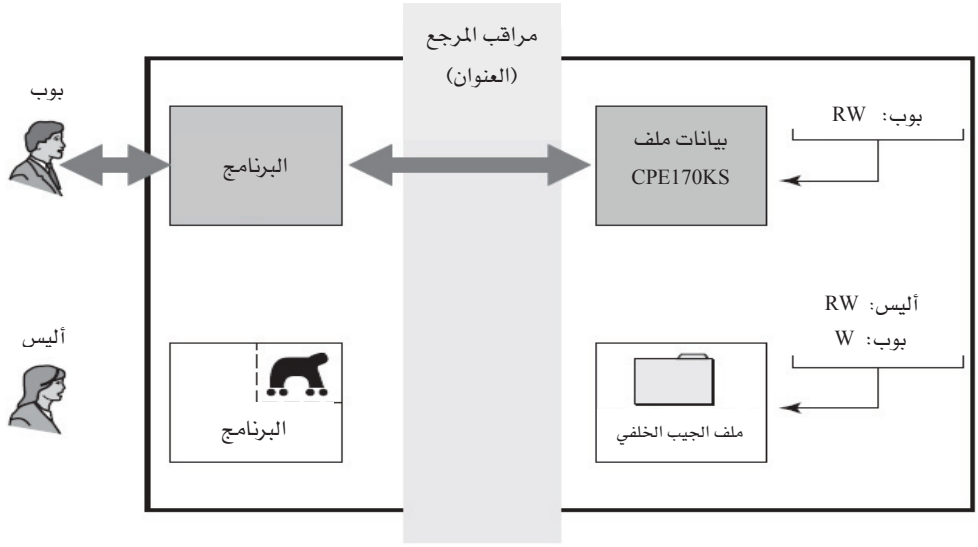


(a)

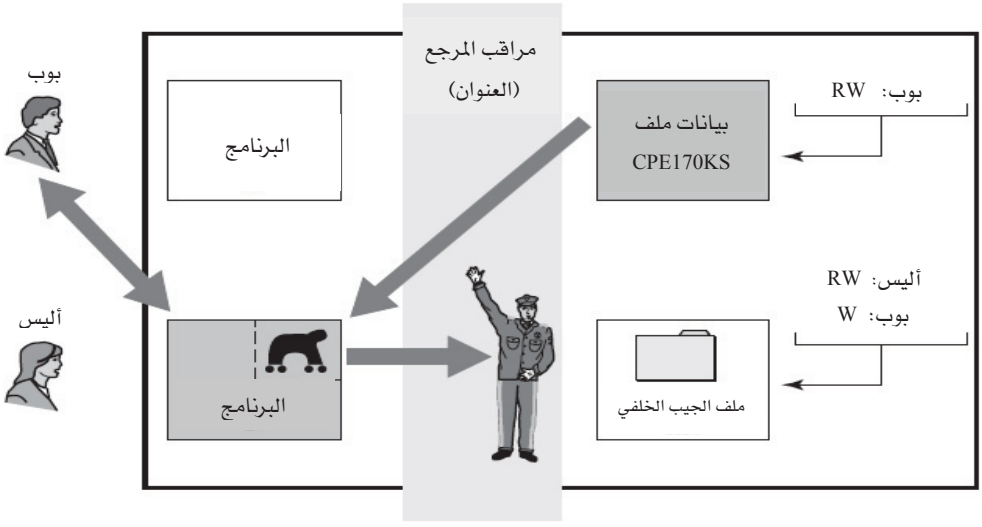


(b)

الشكل 11-5: حصان طروادة و نظام التشغيل الآمن.



(c)



(d)

تابع الشكل 11-5: حصان طروادة و نظام التشغيل الآمن.

أنشأت وزارة الدفاع الامريكية في عام 1981 – في محاولة لتلبية احتياجاتها الخاصة، وكخدمة عامة – مركزاً لأمن الحاسب داخل وكالة الأمن القومي (NSA) وذلك بهدف تشجيع توافر نظم الحاسب الموثوقة على نطاق واسع. وتحقق هذا الهدف عن طريق "برنامج تقييم المنتج التجاري" الخاص بالمركز. وبشكلٍ أساسي يحاول المركز تقييم المنتجات المتاحة تجارياً وتصنيفها من حيث استيفائها للمتطلبات الأمنية سالفة الذكر. حيث يُصنَّف المركز المنتجات المقيَّمة وفقاً للسمات الأمنية المتوفرة بها. وهذه التقييمات ضرورية لمشتريات وزارة الدفاع ولكن يتم نشرها وإتاحتها للجميع مجاناً. ولذلك فهي تعمل بمثابة إرشادات للعملاء الراغبين في شراء مثل تلك المنتجات المتاحة تجارياً.

11-2-3 الدفاع ضد حصان طروادة

هناك طريقة واحدة للتأمين ضد هجمات حصان طروادة ألا وهي استخدام نظام تشغيل آمن وموثوق. ويوضِّح الشكل 11-5 مثالاً على ذلك. في هذه الحالة، يُستخدم حصان طروادة للالتفاف حول آلية الأمن المعيارية والتي تستخدمها معظم أنظمة إدارة الملفات ونظم التشغيل: قائمة التحكم في الوصول. ففي هذا المثال، يتفاعل المستخدم بوب من خلال برنامجٍ ما مع ملف بيانات يحتوي على سلسلة الحروف الحساسة "CPE170KS". ثم يقوم المستخدم بوب بإنشاء ملف مع حقوق وصول "قراءة/كتابة" يسمح بها فقط للبرامج العاملة لحسابه: بمعنى أن العمليات (processes) التي يملكها بوب هي الوحيدة التي يمكنها الوصول إلى الملف.

يبدأ هجوم حصان طروادة عندما تستطيع مستخدمة مُعادية – تدعى أليس – الوصول بطريقة شرعية إلى النظام وتقوم بتثبيت برنامج حصان طروادة مع ملف خاص لاستخدامه في الهجوم كـ "جيب خلفي". تعطي أليس حق "قراءة/كتابة" لنفسها لهذا الملف، كما تعطي بوب حق "الكتابة" فقط (الشكل 11-5 (a)). وتدفع أليس بوب لاستحضار برنامج حصان طروادة – ربما عن طريق الإعلان عنه كأداة مفيدة – وعندما يكتشف البرنامج أنه يجري تنفيذه حالياً من قبل بوب، فإنه يقوم

بقراءة سلسلة الحروف الحساسة "CPE170KS" من ملف بوب، ونسخها إلى ملف جيب أليس الخلفي (الشكل 11-5 (b)). وتتوافق كلٌّ من عمليات القراءة والكتابة مع القيود التي تفرضها قوائم التحكم في الوصول. وحينئذٍ تستطيع أليس الوصول إلى ملف الجيب الخلفي في وقتٍ لاحقٍ لقراءة قيمة السلسلة.

إذا ما تم استخدام نظام تشغيل آمن في هذا السيناريو (الشكل 11-5 (c))، حيث تحدد مستويات الأمن عند الوصول إلى النظام على أساس بعض المعايير، مثل المحطة الطرفية التي تم الوصول منها إلى جهاز الحاسب، ومثل المستخدم كما تحدده كلمة المرور وهويَّة المستخدم. وفي هذا المثال هناك نوعان من مستويات الأمن: المستوى الحساس والمستوى العام، والمستوى الحساس هو الأعلى. فالعمليات (processes) التي يملكها بوب وملف بياناته خصِّص لها المستوى "الحساس" كمستوى للأمن. أما ملفات أليس وعملياتها فقد خصص لها المستوى "العام" كمستوى للأمن. عندما يستحضر بوب برنامج حصان طروادة (الشكل 11-5 (d))، فإن هذا البرنامج يحصل على نفس مستوى أمن بوب. ولذلك يصبح قادراً، تحت خاصية الأمن البسيط، على مراقبة سلسلة الحروف الحساسة. وعند محاولة البرنامج تخزين السلسلة في ملف عام (ملف الجيب الخلفي)، يُعدُّ ذلك انتهاكاً لخاصية *، ولذا يتم منع المحاولة من قِبَل المراقب المَرجِع، ويتم رفض محاولة الكتابة في ملف الجيب الخلفي على الرغم من أن قائمة التحكم في الوصول سمحت بها؛ لأن السياسة الأمنية لها الأسبقية على آلية قائمة التحكم بالوصول.

11-3 المعايير المشتركة لتقييم أمن تقنية المعلومات

العمل الذي قامت به وكالة الأمن القومي وغيرها من الوكالات الحكومية الأمريكية لتعريف صفات التقييم ومعاييره للنظم الموثوقة تم محاكاته بأعمال مماثلة في بلدان أخرى. والمعايير المشتركة (Common Criteria (CC)) لتقييم أمن تقنية المعلومات هي مبادرة دولية من قِبَل الهيئات المعنية بوضع المعايير في عدد من البلدان لتطوير معايير دولية، وتحديد المتطلبات الأمنية، ووضع معايير للتقييم.

11-3-1 المتطلبات

تُحدِّد المعايير المشتركة (CC) مجموعة عامة من المتطلبات الأمنية المتوقعة لاستخدامها في التقييم. ويشير مصطلح هدف التقييم (Target of Evaluation-TOE) إلى الجزء من المنتج أو النظام الخاضع للتقييم. وتصنَّف المتطلبات إلى نوعين:

- متطلبات وظيفية: تحدِّد السلوك الأمني المرجوّ. تعرِّف وثائق CC مجموعة من المكوِّنات الوظيفية الأمنية التي توفر وسيلة معيارية للتعبير عن المتطلبات الوظيفية للأمن لهدف التقييم (TOE).
- متطلبات التأمين: تشكِّل أساساً لاكتساب الثقة بأن المقاييس الأمنية المذكورة فعَّالة ومنفَّذة بشكلٍ صحيح. وتعرِّف وثائق CC مجموعة من مكوِّنات التأمين التي توفر طريقة موحدة للتعبير عن متطلبات التأمين لهدف التقييم (TOE).

الجدول 11-3: المتطلبات الوظيفية للمعايير المشتركة للأمن.

الصنف	الوصف
المراجعة	يتضمن إدراك المعلومات المتعلقة بالأنشطة الأمنية وتسجيلها وتخزينها وتحليلها. ويتم إنتاج سجلات المراجعة من قِبَل هذه الأنشطة، ويمكن دراستها لتحديد مدى أهميتها الأمنية
دعم التشفير	يُستخدَم عندما ينفَّذ هدف التقييم وظائف التشفير. وقد يُستخدَم، على سبيل المثال، لدعم الاتصالات ،وتحديد الهويَّة، والتوثيق ، أو فصل البيانات
الاتصالات	يوفر اثنين من العائلات المعنيّة بعدم التنصل من قِبَل المنشئ ومتلقي البيانات
حماية بيانات المستخدم	تحديد المتطلبات المتعلقة بحماية بيانات المستخدم ضمن هدف التقييم خلال الاستيراد، والتصدير، والتخزين، إضافة إلى السمات الأمنية المتصلة ببيانات المستخدم
التحقق والتوثيق	تضمن التحقق – دون أي لبس – من المستخدمين الموثقين والارتباط الصحيح للسمات الأمنية مع المستخدمين والموضوعات.
إدارة الأمن	تحدّد إدارة السمات الأمنية، والبيانات، والوظائف
الخصوصية	توفر للمستخدم الحماية ضد الانكشاف، وإساءة استخدام هويته من قِبَل المستخدمين الآخرين
حماية وظائف هدف التقييم الأمنية	تركّز على حماية بيانات TSF (وظائف هدف التقييم الأمنية TOE security functions)، وليس بيانات المستخدم. ويتعلق هذا الصنف بسلامة وإدارة آليات TSF والمعلومات.
استخدام المصادر	تدعم توافر المصادر اللازمة، مثل قابلية المعالجة وسعة التخزين. وتتضمن متطلبات تحمُّل الخطأ (fault tolerance)، والأولوية في تخصيص المصادر والخدمات.
وصول هدف التقييم	تحدّد المتطلبات الوظيفية، بالإضافة إلى تلك المحدّدة للتحقق والتوثيق، من أجل التحكم في إنشاء جلسة عمل مستخدم. وتعرض متطلبات توجيه وصول هدف التقييم، مثل أمور الحد من عدد ونطاق جلسات المستخدم، تاريخ الوصول وتعديل متغيرات الوصول.
المسارات/القنوات الموثوقة	تُعنى بمسارات الاتصالات الموثوقة بين المستخدمين والـ TSF وبين مجموعات من TSF.

يتم تقسيم كلٌّ من المتطلبات الوظيفية ومتطلبات التأمين إلى فئات. والفئة هي عبارة عن مجموعة من المتطلبات التي تشترك في رؤية مشتركة أو مقصد واحد. يُعرِّف الجدولان 11-3 و11-4 بصورة مختصرة الفئات الخاصة بالمتطلبات الوظيفية ومتطلبات التأمين. تحتوي كلٌّ من هذه الفئات على عدد من العائلات، وتضم كل عائلة متطلبات تشترك في الأهداف الأمنية ولكنها تختلف في شدتها أو صرامتها. فعلى سبيل المثال، تحتوي طبقة المراجعة على ست عائلات تتعامل مع الجوانب المختلفة لعملية المراجعة (مثل: توليد بيانات المراجعة، وتحليل بيانات المراجعة، وتخزين أحداث المراجعة). وتحتوي كل عائلة بدورها على واحد أو أكثر من المكوِّنات. يصف المكوّن مجموعة معينة من المتطلبات الأمنية ويمثل أصغر وحدة متطلبات أمنية يمكن اختيارها لإدراجها في الهياكل المعرفة في CC.

فعلى سبيل المثال، تشمل فئة دعم التشفير الخاصة بالمتطلبات الوظيفية عائلتين هما: عملية التشفير، وإدارة مفاتيح التشفير. وتحتوي عائلة إدارة مفاتيح التشفير على أربعة مكوِّنات تُستخدَم لتحديد ما يأتي: خوارزمية توليد المفاتيح مع طول المفتاح، وأسلوب توزيع المفاتيح، وأسلوب الوصول إلى المفاتيح، وأسلوب إتلاف المفاتيح.

يوجد لكل مكوّن معيار يُرجَع إليه لتحديد المتطلبات. فمثلاً عائلة عملية التشفير تتضمن مكوّن واحد يحدد الخوارزمية وطول المفتاح بناءً على المعيار المحدّد.

ويمكن جمع بعض المكوِّنات الوظيفية ومكوِّنات التأمين معاً في حزمة (package) واحدة يمكن إعادة استخدامها، وعادةً ما تكون تلك الحزم مفيدة في إنجاز الأهداف المرغوبة. ومن الأمثلة على تلك الحزم؛ المكوِّنات الوظيفية المطلوبة للأدوات التقديرية للتحكم في الوصول (Discretionary Access Controls).

الجدول 11-4: متطلبات ضمان المعايير المشتركة للأمن.

الفئة	الوصف
إدارة التهيئة	تتطلب المحافظة على سلامة هدف التقييم بدرجة كافية. وعلى وجه التحديد، توفر إدارة التهيئة الثقة بأن هدف التقييم والوثائق المستخدمة في عملية التقييم هي تلك التي أعدَّت للتوزيع.
التوصيل والتشغيل	يُعنى بالتدابير والإجراءات والمعايير الخاصة بتأمين عملية التسليم والتركيب والاستخدام العملي لهدف التقييم؛ وذلك لضمان أن الحماية الأمنية التي يوفرها هدف التقييم لا يتم تعرضها للخطأ خلال هذه الأحداث.
التطوير	يُعنى بضبط هدف التقييم من المواصفات المحدّدة في الهدف الأمني إلى التطبيق، وبترجمة المتطلبات الأمنية إلى مستويات التمثيل الدنيا.
وثائق الإرشاد	يُعنى بالاستخدام العملي الآمن لهدف التقييم من قِبَل المستخدمين والإداريين.
دعم دورة الحياة	يُعنى بدورة حياة هدف التقييم، ويشمل تعريف دورة الحياة، وأساليب وأمن تطور البيئة، ومعالجة نقاط الضعف المكتشفة من قِبَل مستخدمي هدف التقييم .
الإختبارات	يُعنى بالبرهنة على أن هدف التقييم يلتقي مع متطلباته الوظيفية. وتُعنى العائلات بمسائل الشمول، وعمق اختبار المُطَوِّر، ومتطلبات الاختبارات المستقلة.
تقييم نقاط الضعف	يُحدِّد متطلبات التعرف على نقاط الضعف القابلة للاستغلال، والتي قد تنتج عن عمليات الإنشاء أو التشغيل، أو الاستخدام غير الصحيح، أو التهيئة الخاطئة لهدف التقييم. والعائلات المحدّدة هنا هي المعنية بتحديد نقاط الضعف من خلال تحليل القنوات السرية، أو تحليل تهيئة هدف التقييم، أو اختبار قوة آليات الوظائف الأمنية، أو تحديد العيوب الناتجة خلال تطوير هدف التقييم. وتغطي العائلة الثانية التصنيف الأمني لعناصر هدف التقييم. وتشمل الثالثة والرابعة تحليل التغيرات للتأثيرات الأمنية، وتقديم أدلة على أن هذه الإجراءات يجري اتباعها. وهذه الفئة توفر لبنات البناء لتأسيس مخططات صيانة الضمان.
صيانة الضمان	يُحدِّد المتطلبات المراد تطبيقها بعد اعتماد هدف التقييم بناءً على المعايير المشتركة. تهدف هذه المتطلبات إلى ضمان أن هدف التقييم سيواصل الوفاء بأهدافه الأمنية مع دوام عمليات التغيير في هدف التقييم أو بيئته.

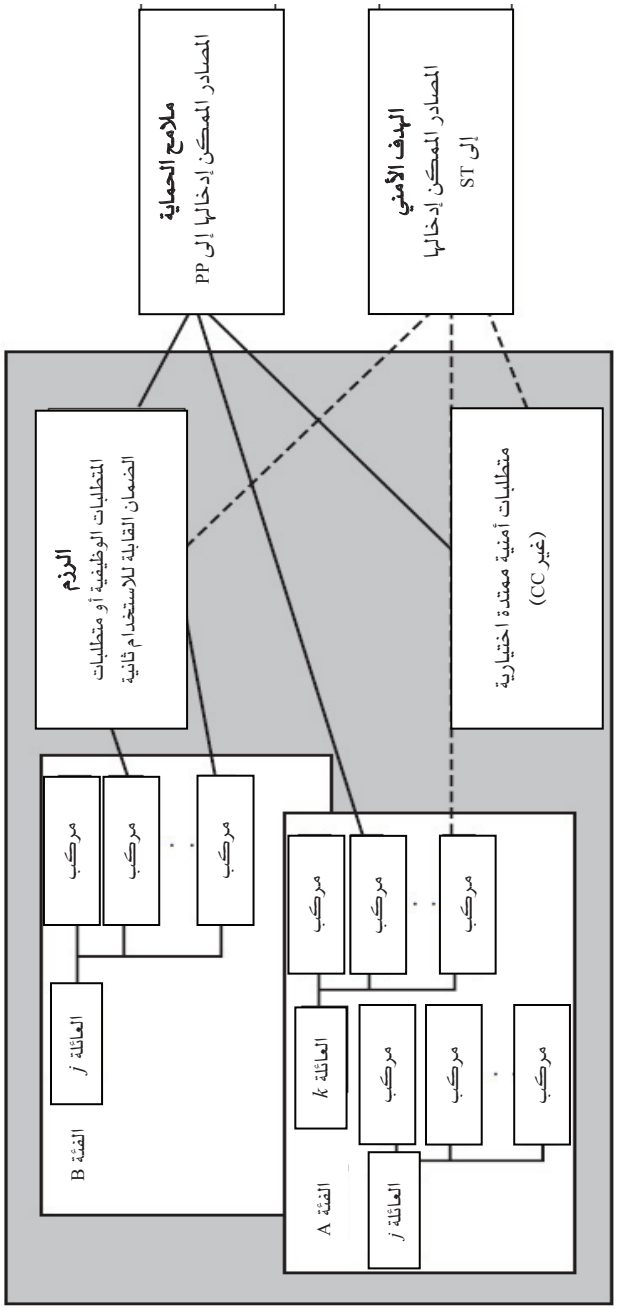
11-3-3 الملامح والأهداف

تحدِّد المعايير المشتركة (CC) أيضاً نوعين من الوثائق التي يمكن إنتاجها باستخدام المتطلبات المعرَّفة في CC.

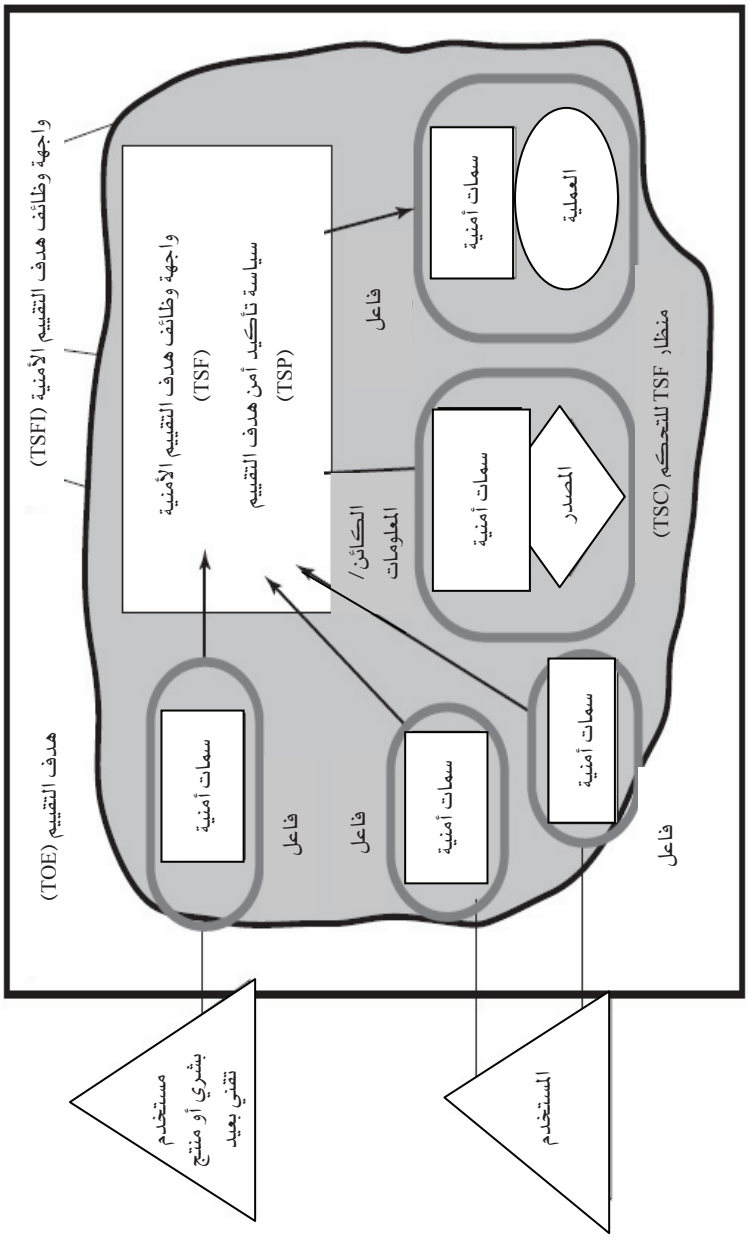
- ملامح الحماية ((Protection profiles (PPs): تحدِّد مجموعة من المتطلبات والأهداف الأمنية لا تعتمد على أسلوب التنفيذ لأحد أصناف المنتجات أو النظم التي تلبي احتياجات المستهلكين المتشابهة لأمن تقنية المعلومات. تستهدف ملامح الحماية أن تكون قابلة لإعادة الاستخدام، وأن تكون مفيدة وفعَّالة في تحقيق الأهداف التي تم تحديدها. وقد تم تطوير مفهوم ملامح الحماية لدعم تعريف المعايير الوظيفية، وكعامل مساعد في صياغة مواصفات الاقتناء. تعكس ملامح الحماية المتطلبات الأمنية للمستخدم.
- الأهداف الأمنية ((Security targets (STs): تتضمن الأهداف والمتطلبات الأمنية لتقنية المعلومات المحدّدة لهدف تقييم معين، كما تحدِّد المقاييس الوظيفية ومقاييس التأمين المقدَّمة من قِبَل هدف التقييم (TOE) المحدّد، لتلبية المتطلبات المنصوص عليها. وقد تتوافق الأهداف الأمنية مع واحد أو أكثر من الملامح الأمنية، كما تشكل أساساً للتقييم. ويتم دعم الأهداف الأمنية من قِبَل البائع أو المطور.

يوضِّح الشكل 11-6 العلاقة بين المتطلبات من جهة والملامح والغايات من جهة أخرى. وبالنسبة لملامح الحماية، يمكن للمستخدم اختيار عدد من العناصر لتحديد متطلبات المنتج المطلوب. كما يمكن للمستخدم أيضاً الاستعانة بالحزم المُعرَّفة مسبقاً التي تضم عدداً من المتطلبات التي تجتمع معاً عادةً في إطار وثيقة متطلبات المنتج. وبالمثل، يمكن للبائع أو المصمم أن يحدد عدداً من المكوِّنات والحزم لتحديد الأهداف الأمنية.

يبين الشكل 11-7 ما يشار إليه في وثائق CC كنموذج متطلبات الأمن الوظيفية. وجوهرياً، يستند هذا التوضيح إلى مفهوم المراقب المَرجع ولكن باستخدام المصطلحات وفلسفة التصميم الخاصة بالأهداف الأمنية.



الشكل 11-6: نظام و ترتيب متطلبات المعايير المشتركة.



الشكل 11-7: نموذج متطلبات الأمن الوظيفي.

4-11 توصيات للمطالعة

يقدم [CHAP00] شرحاً تقليدياً للجدران النارية. وهناك مرجع تقليدي آخر تم تحديثه مؤخراً هو [CHES03]. أما [LODI98]، و[OPPL97]، و[BELL94b] فهي مقالات جيدة تقدم استعراضاً عاماً للموضوع. أيضاً [WACK02] يقدم استعراضاً جيداً لتقنية الجدار الناري وسياساته. ويقدم [AUDI04] و[WILS05] مناقشات مفيدة للجدران النارية. كما يتضمّن [GASS88] دراسة شاملة لنظم الحاسب الموثوقة، ويوفر [PFLE03] و[GOLL99] أيضاً تغطية للموضوع. أما [FELT03] و[OPPL05] فقد قدما مناقشات مفيدة للحاسوبية الموثوقة.

[AUDI04] Audin, G. "Next-Gen Firewalls: What to Expect," *Business Communications Review*, June 2004.

[BELL94b] Bellovin, S., and Cheswick, W. "Network Firewalls," *IEEE Communications Magazine*, September 1994.

[CHAP00] Chapman, D., and Zwicky, E. *Building Internet Firewalls.* Sebastopol, CA: O'Reilly, 2000.

[CHES03] Cheswick, W., and Bellovin, S. *Firewalls and Internet Security: Repelling the Wily Hacker*. Reading, MA: Addison-Wesley, 2003.

[FELT03] Felten, E. "Understanding Trusted Computing: Will Its Benefits Outweigh Its Drawbacks?" *IEEE Security and Privacy*, May/June 2003.

[GASS88] Gasser, M. *Building a Secure Computer System*. New York: Van Nostrand Reinhold, 1988.

[GOLL99] Gollmann, D. *Computer Security.* New York: Wiley, 1999.

[LODI98] Lodin, S., and Schuba, C. "Firewalls Fend Off Invasions from the Net," *IEEE Spectrum*, February 1998.

[OPPL97] Oppliger, R. "Internet Security: Firewalls and Beyond," *Communications of the ACM*, May 1997.

[OPPL05] Oppliger, R., and Rytz, R. "Does Trusted Computing Remedy Computer Security Problems?" *IEEE Security and Privacy*, March/April 2005.

[PFLE03] Pfleeger, C. *Security in Computing*. Upper Saddle River, NJ: Prentice Hall, 2003.

[WACK02] Wack, J.; Cutler, K.; and Pole, J. *Guidelines on Firewalls and Firewall Policy*. NIST Special Publication SP 800-41, January 2002.

[WILS05] Wilson, J. "The Future of the Firewall."*Business Communications Review*, May 2005.

5-11 مصادر للمعلومات على الويب

- Firewall.com: يضم الكثير من الروابط لمراجع عن الجدار الناري وبعض الموارد البرمجية.
- Trusted Computing Group: مجموعة موردين لتطوير معايير الحاسب الموثوقة وتبنيّها. ويحتوي الموقع على أوراق بيضاء (white papers) ومواصفات وبعض روابط للموردين.
- Common Criteria Portal: الموقع الرسمي لمشروع المعايير المشتركة.

6-11 مصطلحات رئيسة

access control list (ACL)	قوائم التحكم في الوصول
access matrix	مصفوفة الوصول
access right	حق الوصول
application-level gateway	بوَّابة مستوى التطبيق
bastion host	مضيف المَعقِل
capability ticket	تذكرة الإمكانات
circuit-level gateway	بوَّابة مستوى الدوائر
common criteria (CC)	المعايير المشتركة
multilevel security	الأمن متعدد المستويات
object	كائن
packet-filtering router	موجِّه ترشيح الرزم
reference monitor	المراقب المَرجع
stateful inspection firewall	جدران تفتيش الحالة
subject	الفاعل
trusted system	النظام الموثوق

7-11 أسئلة للمراجعة ومسائل

1-7-11 أسئلة المراجعة

1-11 عَدِّد ثلاثة أهداف تصميم للجدار الناري.

2-11 عَدِّد أربع تقنيات تستخدمها الجدران النارية للتحكم في الوصول وتنفيذ السياسة الأمنية.

3-11 اذكر المعلومات التي يستخدمها موجِّه ترشيح الرزم.

4-11 اذكر بعض نقاط الضعف في موجِّه ترشيح الرزم.

5-11 ما الفرق بين موجِّه ترشيح الرزم والجدار الناري لتفتيش الحالة؟

6-11 ما المقصود ببوَّابة مستوى التطبيقات؟

7-11 ما المقصود ببوَّابة مستوى الدوائر؟

8-11 ما الفوارق بين التشكيلات الثلاثة بالشكل 11-2؟

9-11 في سياق التحكم في الوصول، ما الفرق بين الفاعل والكائن؟

10-11 ما الفرق بين قائمة التحكم في الوصول وتذكرة الإمكانات؟

11-11 اذكر القاعدتين اللتين يفرضهما المراقب المَرجِع؟

12-11 ما الخصائص اللازمة للمراقب المَرجِع؟

13-11 ما المقصود بالمعايير المشتركة (CC) للأمن؟

2-7-11 مسائل

1-11 كما ذكرنا في الجزء 11-1، إحدى الطرق للتغلب على هجمات التجزئة الدقيقة هي بفرض حد أدنى لطول ترويسة النقل التي يجب أن تَرِد في الجزئية الأولى من رزمة بروتوكول الإنترنت. وإذا تم رفض الجزئية الأولى، يمكن أن يتم رفض جميع الجزئيات اللاحقة. ومع ذلك، فإن طبيعة بروتوكول الانترنت هي أن هذه الجزئيات قد تصل بدون ترتيب. ولذا قد تمر جزئية متوسطة عبر المرشح قبل رفض الجزئية الأولى. كيف يمكن التعامل مع هذا الوضع؟

2-11 في رزمة IPv4، حجم الحمولة في الجزئية الأولى (بالبايتات) =

الطول الكلي - (4×IHL). وإذا كانت هذه القيمة أقل من الحد الأدنى المطلوب (8 بايتات لـ TCP)، فسيتم رفض هذه الجزئية وبقية الرزمة برمَّتها. اقترح طريقة بديلة لتحقيق نفس النتيجة باستخدام حقل إزاحة الجزئية فقط.

3-11 يصف طلب التعليقات RFC 791 الخاص ببروتوكول IPv4 خوارزمية إعادة التجميع التي تُنتِج جزئيات جديدة تحل محل الجزئيات السابقة. في حال وجود هذا البرنامج لإعادة التجميع، يمكن للمهاجم بناء سلسلة من الرزم بحيث تحتوي الجزئية الأولى فيها (ذات الإزاحة الصفرية أي العنوان النسبي = صفر) على بيانات غير ضارة (ومن ثَمَّ يتم تمريرها عن طريق مرشحات الرزمة الإدارية)، وتتداخل فيها بعض الرزم اللاحقة (إزاحتها غير صفرية) مع معلومات ترويسة TCP (منفذ الوجهة، على سبيل المثال)، وتتسبب في تعديلها. ومعظم التنفيذات المختلفة للمرشحات ستقوم بتمرير الرزمة الثانية لأنها ليست صفرية الإزاحة. اقترح طريقة يمكن استخدمها من قِبَل مرشح الرزم للتصدي لهذا الهجوم.

4-11 إن ضرورة قاعدة " ممنوع القراءة لأعلى" لنظام آمن متعدد المستويات واضحةٌ تماماً، فما هي أهمية قاعدة " ممنوع الكتابة لأسفل"؟

5-11 في الشكل 11-5 هناك وصلة واحدة من حصان طروادة "انسخ - ولاحظ - لاحقاً" مكسورة. هناك زاويتان أُخْرَيان يمكن لـ "دريك" (Drake) الهجوم منهما. بعد نفاذ دريك للنظام يحاول قراءة السلسلة مباشرةً، أو أن يعين مستوى أمن الحساسية لملف الجيب الخلفي. هل يمنع المراقب المَرجِع هذه الهجمات؟