الجامعة الافتراضية السورية

SYRIAN VIRTUAL UNIVERSITY

أمن الحواسب

Books

أمن الحواسب

من منشورات الجامعة الافتراضية السورية

الجمهورية العربية السورية 2018

Computer Security

Publications of the Syrian Virtual University (SVU)

Syrian Arab Republic, 2018

الفهرس

الفصل الأول: أساسيات أمن الحاسب

1. مقدمة

يهدف هذا المقرر إلى تحديد المشاكل الأمنية لنظام معلومات ما. ومن ثم التوجيه إلى كيفية العمل على حل هذه المشاكل. لذلك سنعمل أولاً على تحديد ملامح مصطلح الأمن وتعريفه.

النظام الحاسوبي computer system: هو أي شيء يمكنك أن تفكر به: نظام متشارك **shared system**، مخدم ويب، مصرف **ATM**....وهكذا.

عندما تعمل على تحقيق الأمن لكل حالة مما سبق عليك:

1. تحديد السياسة الأمنية بمعنى تحديد الأهداف المطلوبة. فمثلاً في النظم المتشاركة يجب السماح بدخول الأشخاص المرخص لهم الدخول، وفي مخدم الويب يجب أن يدفع الزبائن الداخلين إليه رسم، وهكذا.....
2. بعد أن تحدد السياسة الأمنية يجب أن تختار الآليات الأمنية التي تحتاجها. بمعنى أن تحدد الأدوات التي تجعلك متأكداً من وصولك إلى أهدافك الأمنية. مثلاً ستوفر آلية كلمات المرور دخول المستخدمين المرخص لهم فقط إلى النظام المتشارك، وسيتأكد بروتوكول تسديد النفقات **payment protocol** من دفع الزبائن المستخدمين لخدمة الويب.
3. بعد أن تضع آليات الأمن عليك أن تراجعها لتحدد نقاط الضعف **vulnerabilities** الممكنة في النظام والتي يمكن أن تترك النظام معرض للهجمات.
4. إذا حددت نقاط الضعف، يجب أن تبني آليات صيانة وتقوم بإجراءات مضادة للحد من نقاط الضعف الأمني في النظام.

2. أهداف أمن الحاسب

لأمن الحاسب أهداف ثلاثة أساسية تدعى بـ الثلاثية **CIA** وهي:

1. الخصوصية **confidentiality**.
2. السلامة **integrity**.
3. الإتاحة **availability**.

يجب أن تحقق متحكمات الأمن واحدة أو أكثر من هذه الأهداف الثلاث الأساسية. وعادة ما تقيم متحكمات الأمن بكونها تحقق الأهداف الثلاث السابقة أم لا.

كما تقيم نقاط الضعف **vulnerabilities**، والمخاطر **risks**، بناء على تلبيتها تهديدها لواحدة أو أكثر من الثلاثية **CIT**.

1. الخصوصية Confidentiality

معنى أن الآلية الأمنية تقدم الخصوصية (السرية)، هو أن هذه الآلية تقدم مستوى عالي من الثقة بأن البيانات، الأغراض، أو الموارد ليست معرضة للاختراق من أي مصدر غير مصرح له.
هناك نوعين من اختراقات السرية:

- اختراقات تعتمد على هجوم مباشر متعمد. مثل: التقاط حركة مرور على الشبكة ، وسرقة ملف كلمات المرور ، و **social engineering، port scanning، shoulder surfing، eavesdropping، sniffing .**
- اختراقات بسبب أخطاء بشرية، أو إهمال، أو سوء تصرف. مثلاً: عدم تعمية البيانات المتبادلة بشكل تام وصحيح، ترك نقاط دخول أمنية مفتوحة، تمكين برامج خبيثة تؤمن أبواب خلفية، أو حتى الابتعاد عن طرفية حاسوبية أثناء عرض بيانات على شاشتها.

وبشكل عام يمكن أن تحدث اختراقات السرية بسبب فعاليات المستخدمين، أو مدير النظام، كما يمكن أن تحدث بسبب عدم تطبيق السياسة الأمنية، أو عدم تنفيذ إجرائياتها بشكل جيد.

يوجد العديد من الاحتياطات الممكن اتخاذها لتقوية السرية ضد التهديدات الممكنة. مثل: التعمية، استخدام الحشو في حركة المرور على الشبكة، تحكم قوي بالدخول، إجراءات تصريح صارمة، تصنيف البيانات، وتدريب مكثف للمستخدمين.

2. السلامة Integrity

تعني السلامة أن تحافظ الأغراض **objects** على صحتها ولا تغير بشكل متعمد إلا من قبل مخولين **authorized** (مستخدمين، خدمات). وعليه نقول إن الآلية الأمنية تقدم السلامة، عندما تقدم مستوى عالي من الثقة بأن البيانات، الأغراض، والموارد لم تعدل عن حالتها الأصلية المحمية.

يمكنك أن تختبر السلامة من وجهات نظر ثلاث:

- يجب أن تمنع غير المخولين (مستخدمين، خدمات) من بإجراء تعديلات.

- يجب أن تمنع المخولين (مستخدمين، خدمات) من إجراء تعديلات غير مرخص لهم إجراءها.
- يجب أن تكون الأغراض مترابطة داخلياً وخارجياً بحيث تكون بياناتها صحيحة وتعطي انعكاس صحيح للعامل الحقيقي وأن تكون أي علاقة مع أغراض أبناء أو آباء أو نظراء هي علاقة صحيحة ومترابطة ومحققة.

هناك نوعين من اختراقات السلامة:

1. اختراقات سلامة تعتمد على هجوم مباشر متعمد. مثل: الفيروسات، قنابل منطقية **logic bombs**، دخول غير مرخص **unauthorized access**، أخطاء في البرامج **coding** والتطبيقات، تعديلات خبيثة، تبديلات عدوانية، وأبواب خلفية في النظام.
2. اختراقات سلامة بسبب أخطاء بشرية، أو إهمال، أو سوء تصرف. مثل: حذف ملفات خطأً، إدخال بيانات غير صحيحة، تعديل تهيئة (**configuration**)، أخطاء في الأوامر، أو في الترميزات **codes**، أو في الخطاطات **scripts**، إدخال فيروسات ، أو تشغيل برامج خبيثة **Trojan horse**.

يوجد العديد من الإجراءات الاحتياطية التي يمكنك أن تتخذها لتأكيد قوة السلامة أمام المهددات الممكنة. مثل: تحكم قوي بالدخول، إجراءات تصريح صارمة، نظم كشف للاقتحام ، اختبار وظائف الإدخال **input/function checks**، تدريب مكثف للمستخدمين.

3. الإتاحة Availability

معنى الإتاحة أن يتمكن المخولون من الوصول إلى الأغراض المرخص لهم الوصول لها بدون أي مقاطعة وفي الأوقات المرخصة لهم. عندما تضمن الآلية الأمنية الإتاحة فهذا يعني أنها تقدم مستوى عالي من الثقة بأنه يمكن للمخولين الدخول إلى البيانات، الأغراض، والموارد المرخص دخولهم إليها وفي الأوقات المرخصة لهم.

تقسم اختراقات الإتاحة إلى:

- اختراقات إتاحة تعتمد على هجوم مباشر متعمد. مثل: هجمات حجب الخدمة **denial of service**، تدمير غرض، مقاطعات الاتصالات.
- اختراقات إتاحة بسبب أخطاء بشرية، إهمال، أو سوء تصرف. مثل: حذف ملفات خطأً، استخدام أجزاء العتاد أو البرامج بشكل مبالغ فيه (**overutilizing a hardware or software component**)، **under-allocating resources**، عدم توزيع أو تصنيف الأغراض بالشكل المطلوب.

يوجد العديد من الاحتياطات التي من الممكن أن تتخذها لتأكيد قوة الإتاحة أمام المهددات المحتملة. مثل: تصميم أنظمة تسليم وسيطة ملائمة، استخدام متحكمات دخول مؤثرة ، مراقبة الأداء وحركة مرور الشبكة، استخدام جدار النار والموجهات لمنع هجمات **DoS**، توظيف **redundancy** للأنظمة الحساسة، صيانة واختبار نظم التخزين الاحتياطي.

3. آليات أمن الحاسب

1. توعية المستخدم

وذلك عن طريق تثقيف المستخدم وتدريب المستثمر ورفع درجة إدراكه لأهداف النظام ، والأخطار المحتملة.
وتجدر الإشارة إلى أن المستخدم غير المؤهل يشكل النسبة الأعظم من حالات الخروقات المكتشفة في الأنظمة الحاسوبية.

2. الأمن الفيزيائي

يهدف الأمن الفيزيائي إلى الوقاية من المهددات الفيزيائية مثل: النار والدخان، الماء، الزلازل والبراكين، العواصف، التخريب أو التدمير المتعمد، الانفجارات، انهيار المبنى، المواد السامة ، تعطل المعدات، نقص المستخدمين. فمهما حاولت تحقيق الأمن لنظامك لن تصل إليه بدون أن تراعي موضوع الأمن الفيزيائي الذي يمكنك من حماية نظامك من الأخطار السابقة.
يوجد العديد من العناصر في بناء الأمن الفيزيائي والمحافظة عليه. أحد أهم هذه العناصر هو اختيار وتصميم الموقع الذي سيحوي البنية التحتية لتكنولوجيا المعلومات و للتطبيقات في مؤسستك.
يمكن أن نقسم متحكمات الأمن المستخدمة لإدارة الأمن الفيزيائي إلى ثلاث مجموعات أساسية:

1. **متحكمات الأمن الفيزيائي الإدارية:** تتضمن بناء واختيار موقع، إدارة الموقع التحكم بالمستخدمين، التدريب والإطلاع، الاستجابة في حالات الطوارئ والإجراءات.
2. **متحكمات الأمن الفيزيائي التقنية:** وتتضمن متحكمات الدخول، كاشفات المقتحمين ، الإنذارات، المراقبة التلفزيونية **closed-circuit television (CCTV)**، المراقبة، التدفئة، التهوية، تكييف الهواء (يرمز للأربعة الأخيرة بـ **HVAC**)، مزودات الطاقة، كاشفات الحريق ومخمداتها.

3. **متحكمات الأمن الفيزيائي الفيزيائية:** الأسيجة، الإضاءة، الأقفال، مواد البناء، الأفخاخ، الكلاب، الحراس الأمنيين.

3. التعمية

تقدم التعمية مستويات إضافية من الأمن إلى البيانات خلال المعالجة، التخزين، والاتصالات.

1. تعريفات ومفاهيم أساسية:

1. تدعى عملية تحويل النص الصريح إلى نص غير صريح (مبهم) بـ" التعمية " **encrypt** وتتم هذه العملية باستخدام معلومات إضافية خاصة تدعى مفتاح التعمية **encrypt key**.
2. يدعى النص قبل تعميته بالنص الصريح **plaintext**.
3. يدعى النص بعد تعميته بالنص المعمى **ciphertext**.
4. تدعى عملية نقل النص من الشكل المعمى إلى النص غير المعمى بفك التعمية **decrypt**.
5. تدعى الخوارزمية المستخدمة لتعمية وفك تعمية النص بالمعمية **cipher**.
6. يدعى علم بناء المعميات بعلم التعمية **cryptography**.
7. يدعى العلم الذي يعمل على فك التعمية بفك التعمية **cryptosystems**.
8. الفرق بين مرمز **code** ومعمي**cipher**. غالباً ما تستخدم كلمتي مرمز **code** و معمي **cipher** بشكل متبادل. لكن تقنياً يوجد فرق مهم بين المفهومين. فالمرمزات هي أنظمة تعمية للرموز بحيث تعيد تمثيل الكلمات والعبارات. وهي سرية أحياناً لكنها غالباً ليست معنية بتوفير السرية.بينما يقوم المعمي بإخفاء المعنى الحقيقي للرسالة.

وفيما يلي أهم أنواع المعميات من حيث كيفية عملها:

1. **معميات الترتيب Transposition Ciphers:** تستخدم خوارزميات تقوم بإعادة ترتيب حروف النص الصريح لتنتج النص المعمى.
2. **معميات الاستبدال Substitution Ciphers:** تستخدم خوارزميات تقوم باستبدال كل محرف أو بت من النص الصريح بمحرف (بت) معين لتشكل النص المعمى.
3. **حشو المرة الواحدة One-Time Pads:** تستخدم خوارزميات تقوم باستبدال كل محرف أو بت من النص الصريح بمحرف (بت) (مختلف لكل نص صريح) لتشكل النص المعمى.

من ناحية أخرى يمكن تقسم المعميات من حيث حجم النص الصريح المعالج كما يلي:

1. **المعميات الجدولية:** هي معميات تعمل على كل حرف أو بت من النص الصريح على حدى، وبحيث محرف (بت) في كل مرة.
2. **المعميات الكتلية: و**هي تعمل على كتل من النص الصريح، وبحيث تطبق الخوارزمية على كل كتلة النص في نفس الوقت. يمكن اعتبار معميات الترتيب مثال على المعميات الكتلية.

2. أهداف التعمية وأسسها:

السرية: وهي المحافظة على خصوصية الرسالة أثناء تراسلها بين طرفين أو أكثر، يوجد نوعين أساسيين من نظم التعمية التي تقدم السرية: نظم التعمية بالمفتاح السري، ونظم التعمية بالمفتاح العام.

السلامة: وهي المحافظة على الرسالة بدون تعديل أثناء تراسلها. يمكنك أن تفرض السلامة بتوقيع الرسالة رقمياً عند إرسالها ثم يقوم المستقبل بالتحقق من صحة التوقيع الالكتروني. يمكن إجراء التوقيع الالكتروني باستخدام نوعي نظم التعمية (المفتاح السري، المفتاح العام).

الاستيقان: وهو التحقق من هوية المستخدم الذي يريد الدخول إلى النظام. وهو الهدف الأساسي لنظم التعمية.
مثلاً لنفرض أن **A** يريد فتح جلسة اتصال مع **B** علماً أنهما شريكين في نظام اتصالات يعتمد المفتاح السري المتشارك. ليتأكد **A** أنه يتخاطب مع **B** فعلاً، يمكنه ن يستخدم تقنية تحدي-إجابة استيقان **challenge-response authentication**. وهي عبارة عن رسالة ترسل من **A** إلى **B** الذي يقوم بدوره بفك تعميتها باستخدام المفتاح المتشارك والرسالة الواردة مع الرسالة الأصلية وفي حال المطابقة فإن **A** متأكد من هوية **B** ذلك أنه الوحيد الذي يعلم بالمفتاح المتشارك.

التبرأ Nonrepudiation: وتفيد التأكيد بأن الرسالة المستقبلة فعلاً تم إرسالها من قبل المرسل المفترض وليس من قبل شخص آخر تنكر بشخصية المرسل. وهي تمنع المرسل من التنكر لرسالته. وبشكل عام لا يمكن استخدام نظم تعمية بالمفتاح السري لتقديم التبرأ وهي تتم فقط باستخدام نظم التعمية بالمفتاح العلني.

3. التعمية الحديثة وأنواعها:

تستخدم نظم التعمية الحديثة خوارزميات حاسوبية معقدة ومفاتيح تعمية طويلة لتلائم أهداف التعمية:

- السرية.
- السلامة.
- الاستيقان.
- التبرأ.

حيث يعتبر طول المفتاح من أهم عوامل قوة المعمية وبسبب تزايد قوة الحاسبات يمكنك أن تستخدم مفاتيح ذات طول أكبر لتزيد من مصاعب كسر نظام تعميتك.

في البداية، كان أحد أهم مبادئ الأمن هو " الأمن عبر الغموض". حيث اعتبر العلماء أن إخفاء خوارزمية التعمية يزيد في أمنها. بينما نجد في التعمية الحديثة أن خوارزميات التعمية لمعظم نظم التعمية الحديثة هي خوارزميات معروفة التفاصيل ومنشورة على الانترنت. حيث يزيد هذا النشر من أمن الخوارزمية بسبب التحليل الواسع الذي تتعرض له والذي يكشف نقاط ضعف الخوارزمية.

وبدل الاعتماد على إخفاء المعمي، تعتمد نظم التعمية الحديثة على إخفاء مفتاح تعمية أو أكثر وذلك لإضفاء الخصوصية على الخوارزمية لأجل مؤسسة ما.

خوارزميات المفتاح المتماثل:

تعتمد هذه الخوارزميات على المفتاح التعمية السري المتشارك والذي يوزع إلى كل العناصر المتشاركين في الاتصال حيث يستخدم المفتاح نفسه في التعمية وفك التعمية.

لهذا النوع من الخوارزميات عدد من نقاط ضعف منها:

1. عملية توزيع مفتاح التعمية السري مسألة صعبة ومهمة.
2. لا تستطيع خوارزميات المفتاح المتماثل أن تقدم التبرأ.
3. من الصعب استخدام هذه الخوارزميات لتعمية الاتصالات بين مجموعة كبيرة من الأطراف وإنما فقط بين شريكين اثنين وذلك لصعوبة توزيع مفتاح التعمية.
4. غالباً يجب إعادة توليد مفاتيح التعمية دورياً.

من أشهر خوارزميات التعمية بالمفتاح المتماثل:

1. **Data Encryption Standard (DES).**
2. **Triple DES (3DES).**
3. **International Data Encryption Algorithm (IDEA).**
4. **Blowfish.**
5. **Skipjack.**
6. **the Advanced Encryption Standard (AES).**

خوارزميات المفتاح غير المتماثل:

وتدعى أيضاً خوارزميات المفتاح العام، يقدم هذا النوع من الخوارزميات حلاً لنقاط الضعف في خوارزميات المفتاح المتماثل.

في هذا النوع من الخوارزميات يملك كل مستخدم مفتاحين أحدها عام والآخر خاص (سري).

حيث يستخدم المفتاح العام للتعمية ويستخدم المفتاح الخاص لفك التعمية.

لهذا النوع من الخوارزميات عدد من الميزات التي تعتبر نقاط قوة فيها منها:

1. عند إضافة مستخدم جديد لا نحتاج إلى أكثر من توليد زوج مفاتيح (خاص/عام).
2. يمكن حذف أي مستخدم من النظام ببساطة بدون أي تأثير على بقية النظام.
3. لا نحتاج لإعادة توليد المفتاح إلا عندما يكشف المفتاح الخاص لأحد المستخدمين.
4. يؤمن هذا النوع من الخوارزميات التبرأ.
5. عملية توزيع المفاتيح عملية بسيطة.

من أشهر خوارزميات هذا النوع:

7. خوارزمية **El Gamal**.
8. خوارزمية المنحنيات الاهليلجية.
9. **RSA** التي تعتبر العمود الفقري لمعظم تطبيقات التعمية ومنتجاتها.

خوارزميات تبادل المفاتيح:

كما ذكرنا فإن عملية تبادل المفاتيح في نظم المفتاح المتماثل هي مسألة صعبة لذلك توجد عدد من الطرق المتبعة لإنجاز هذه العملية منها:

1. **توزيع offline:** وهي من أبسط الطرق حيث يتم توزيع المفتاح عن طريق قطعة ورق مكتوب فيها المفتاح أو أي وسيط آخر من وسائط التخزين. ولكن يجب ضمان أمنية هذا التبادل بطريقة فيزيائية.

2. **التعمية بالمفتاح العام:** حيث تستخدم خوارزميات المفتاح العام لإنجاز تبادل المفاتيح في بداية جلسة الاتصال ثم ينتقل المستخدمان إلى نمط التعمية المتماثلة.
3. **خوارزمية Diffie-Hellman:** تستخدم هذه الخوارزمية على نطاق واسع و هي مفيدة عندما لا يمكن لطرفي الاتصال تبادل أي مواد فيزيائية بينهما ولا يوجد بينهما بنية تمكنهم من استخدام خوارزمية مفتاح عام.

خوارزميات الاختصار Hash:

لهذه الخوارزميات هدف بسيط فهي تأخذ رسالة طويلة وتنتج قيمة وحيدة مشتقة من محتوى الرسالة. تدعى هذه القيمة موجز الرسالة **message digest**.

يوجد خمسة متطلبات في خوارزميات المزج هي:

1. يمكن أن يكون الدخل من أي طول.
2. للخرج طول محدد ثابت.
3. من السهل حساب دالة المزج لأي دخل.
4. دالة المزج هي دالة وحيدة الاتجاه.
5. لا يمكن حدوث تعارض في دالة المزج (أي أن ينتج نفس الخرج لدخلين مختلفين).

4. التحكم بالدخول وتقنياته:

يعتمد التحكم بالدخول على أربعة عناصر أساسية:

الموضوع subject أو المفهوم principle وهو الكائن الفعال الذي سيقوم باستخدام الدخول إلى كائن خامد ندعوه **غرض object** من خلال **عملية دخول access operation** يمكن أن يسمح بها أو يمنعها **مراقب مرجعي reference monitor**.

عادة ما يستخدم المصطلحان **موضوع ومفهوم** لنفس الغرض في نظم التشغيل التجارية. لكنهما فعلياً مختلفان. فالموضوع محدود بالمفهوم.

مثال عن المفهوم: هو المستخدم في نظام التشغيل.

مثال عن الموضوع: عملية معالجة **prosses** تعمل ضمن مستخدم ما (مفهوم).

تتم عملية التحكم بالدخول إلى غرض ما بالمراحل التالية:

- **التعريف Identification:** وهي العملية التي بموجبها يصرح بها الموضوع عن هويته. فالمستخدم يقدم اسمه أو رقم تعريـف شخـصي **personal identification number (PIN)** .
- **الاستيفان:** هي عملية التحقق من الهوية التي ادعاها الموضوع.
- **التخويل:** تهدف إلى التأكد من أن الموضوع الذي تم الاستيقان منه في المرحلة السابقة مخول لأن ينفذ عملية الدخول للغرض الذي يريده وما هي الأعمال الأخرى المخول له القيام بها.
- **المحاسبة والتدوين:** تبدأ هذه العملية منذ لحظة إنهاء عملية التعريف حيث تسجل كل فعل يقوم به الموضوع.

1. تقنيات التعريف والاستيفان:

يوجد العديد من تقنيات التعريف والاستيقان من أهمها:

1. كلمات السر.
2. **Biometrics**.
3. علامات **Tokens**.
4. التذاكر **Tickets**.
5. التوقيع لمرة واحدة **Single Sign On (SSO)**.

1. كلمات السر:

وهي التقنية الأكثر انتشاراً برغم كونها الأضعف لعدة أسباب:

- عادة يختار المستخدمين كلمات يسهل عليهم حفظها وبالتالي يسهل أن يخمنها المهاجمين.
- كلمات السر المولدة عشوائياً يصعب حفظها لذلك لابد من تخزينها وهذا يعرضها للسرقة.
- غالباً ما يتشارك المستخدمون كلمات المرور مما يسهل كشفها.

يوجد العديد من الاحتياطات الممكن اتخاذها لرفع أمن تقنية كلمات المرور:

- استخدام أقوى شكل ممكن من التعمية وحيدة الاتجاه (دوال المزج) عند تخزين كلمات المرور.
- لا تسمح أبداً بانتقال كلمات المرور عبر الشبكة.
- استخدم أدوات تحقق **verification** و **cracking** لملفات قاعدة بيانات كلمات السر.
- إلغاء حسابات المستخدمين غير المستخدمة لفترة معينة.

- درب المستخدمين ليحافظوا على سرية كلمات المرور واختيارها قوية.
- استخدام كلمات المرور المعرفية وهي عبارة عن أجوبة محددة لعدة أسئلة يطرحها النظام.
- التغيير الدوري لكلمات المرور.
- اختيار تركيب معقد لكلمة المرور يحتوي على محارف عادية وخاصة وأرقام و لها طول معقول.

2. Biometrics:

تعتمد هذه التقنية على اختيار صفة سلوكية أو فيزيولوجية تكون معرفة للموضوع بشكل وحيد وتتخذ كطابع مميز له. مثل: بصمة الإصبع، بصمة العين،.....

3. علامات Tokens:

هي أداة تولد كلمات المرور يحملها الموضوع معه. يمكن أن:

- تولد كلمة مرور واحدة ثابتة مثلاً بالاعتماد على **PIN**.
- أو تولد بشكل مستمر وعندها تكون كالآلة الحاسبة في كل مرة تستخدمها تولد كلمة مرور جديدة.

4. التذاكر Tickets:

تعتمد هذه التقنية على وجود طرف ثالث يقوم بتعريف واستيقان الموضوع.

من أشهر نماذج الأمن التي تستخدم هذه التقنية نجد نموذج **Kerberos**.

5. التوقيع لمرة واحدة Single Sign On (SSO):

هي آلية تسمح بأن يتم استيقان الموضوع لمرة واحدة. ويسمح باستخدام هذه التقنية فقط في حال استخدام كلمات مرور قوية جداً.

2. عمليات الدخول:

عند تعاملك مع عمليات الدخول ستجد أنها تختلف من نظام لآخر وهناك مجموعات نموذجية لعمليات الدخول منها:

1. أنماط الدخول:

وهي تقسيم لعمليات الدخول في أبسط شكل له وهي نمطين:

- **نمط الإطلاع observe:** وهنا يخول الموضوع فقط بالإطلاع على محتوى الغرض.
- **نمط التعديل alter**: وفيه يخول الموضوع بتعديل الغرض.

2. حقوق الدخول لنمط Bell-LaPadula:

وهنا يكون التقسيم على مستوى أكثر تعقيداً فنجد أربعة أنواع من حقوق الدخول:

- التنفيذ.
- القراءة.
- الإلحاق **append** (يسمى أحياناً الكتابة العمياء).
- الكتابة الذي يحتوي حق القراءة.

وفيما يلي جدول يوضح العلاقة بين حقوق الدخول في النمطين الأساسيين:

	التنفيذ	الإلحاق	القراءة	الكتابة
الإطلاع			X	X
التعديل		X		X

3. حقوق الدخول في نظم التشغيل الحالية:

في نظام التشغيل **UNIX** توجد ثلاث أنواع من العمليات:

- القراءة.
- التنفيذ.
- الكتابة والذي لا يحتوي حق القراءة.

نظام تشغيل **2000** فيه العمليات التالية:

- القراءة.
- الحذف.
- الكتابة **ADCL** (تعديل قائمة التحكم بالدخول).
- كتابة المالك (تعديل مالك المصادر).
- المزامنة **synchronize** (للمزامنة بين البرامج متعددة المسالك).

3. المالك ownership:

عند الحديث عن التحكم بالدخول علينا أن نحدد من يضع السياسة الأمنية، وفي هذا المجال يوجد خيارين أساسيين:

- نمط التحكم **discretionary**: وفيه يعرف مالك لكل غرض وهذا المالك يحدد سماحية الدخول وسماحيات استخدام الأغراض المملوكة من قبله.

- النمط الإلزامي **mandatory**: وفيه تحدد سياسة النظام بشكل عام سماحية الدخول.

علماً أن معظم أنظمة التشغيل تدعم مفهوم المالك.

4. بنى التحكم بالدخول:

عليك اختيار بنية ما تطبق من خلالها العمليات المختلفة التي عرفناها سابقاً و تحقق أهداف سياستك الأمنية.

يوجد العديد من البنى التي تنظم وفقها عمليات حقوق الدخول منها:

- مصفوفة التحكم بالدخول.
- القدرات **capabilities**.
- قوائم التحكم بالدخول.

مصفوفة التحكم بالدخول:

يمكن تعريف حقوق الدخول لكل موضوع على كل غرض بشكل مستقل في مصفوفة تسمى مصفوفة السماحيات.

مثال:

لنأخذ مستخدمين وثلاثة ملفات:

1. الملف **a.doc** يمكن لـ **B** أن يقرأه ويكتب فيه بينما لا يملك **A** أي حقوق دخول عليه.
2. الملف **e.exe** يمكن أن ينفذ من قبل كل من **A** و**B** ولا يملكان أي حقوق أخرى عليه.
3. الملف **f.com** يمكن أن ينفذ ويقرأ ن قبل المستخدمان، لكن فقط **B** يستطيع الكتابة فيه.

	b.doc	e.exe	f.com
A	-	تنفيذ	تنفيذ - قراءة
B	قراءة - كتابة	تنفيذ	تنفيذ – قراءة - كتابة

هذا النوع من البنى فعال في حالة عدد محدود من المستخدمين لكن مع ازدياد العدد يصبح توظيف هذه البنية صعب ومعقد ويحتاج إلى مستويات وسيطية إضافية من متحكمات الأمن.

القدرات capabilities:

يمكنك أن تحتفظ بحقوق الدخول في المواضيع أو في الأغراض.

في الحالة الأولى، يعطى الموضوع قدرة **capability** تمثل حقوق الدخول التي يملكها . وبهذا الشكل فهي تمثل الأسطر في مصفوفة التحكم في الدخول.

فمثلاً يمكن أن نعبر عن قدرات المستخدمين في المثال السابق كما يلي:

قدرات A: **e.exe**: تنفيذ؛ **f.com**: تنفيذ، قراءة.

قدرات B: **b.doc**:قراءة، كتابة؛ **e.exe**: تنفيذ؛ **fun.com**: تنفيذ، قراءة، كتابة.

ترتبط القدرات عادة بنمط التحكم التمييزي **discretionary**، فعندما يقوم موضوع ما بإنشاء غرض جديد، يمكن أن يعطي (الموضوع) الموضوعات الأخرى حقوق دخول على هذا الغرض الجديد بإعطائهم القدرات المناسبة.

تعتبر هذه البنية من المفاهيم الجديدة التي لم تعتمد بعد في نظم التشغيل التجارية بسبب تعقيدها الكبير وبالتالي صعوبة توظيفها.

قوائم التحكم بالدخول:

ويرمز لها بـ **ACL** تخزن حقوق الدخول إلى غرض ما في الغرض نفسه. وهي بذلك تمثل الأعمدة في مصفوفة التحكم بالدخول.

ففي المثال السابق تكون الـ **ACL** كما يلي:

ACL للملف (غرض) b.doc: **B**: قراءة، كتابة.

ACL للملف e.exe: **A**:تنفيذ؛ **B**: تنفيذ.

ACL للملف f.com: **A**: تنفيذ، قراءة؛ **B**: تنفيذ، قراءة، كتابة.

غالباً ما تستخدم بنية قوائم التحكم في البنية الأمنية لنظم التشغيل التجارية.

5. المتحكمات الوسيطة:

هي طبقات وسيطة بين المستخدمين والأغراض لتنفيذ السياسة الأمنية بشكل أكثر مرونة وفاعلية.

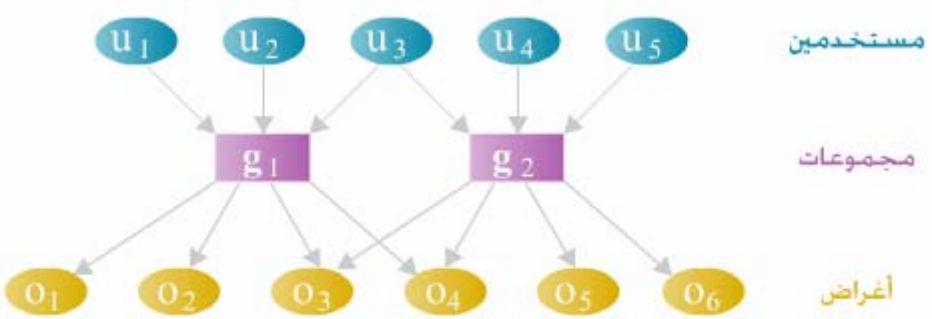
سوف ندرس:

- السماحية السلبية.
- المجموعات.
- الامتيازات **privileges**.
- حلقات الحماية.
- أدوار التحكم بالدخول**role-based access control (RBAC)**.

1. المجموعات:

هي مجرد تبسيط لتعريف سياسات التحكم بالدخول. حيث يجمع المستخدمين الذين لهم حقوق تحكم متطابقة في مجموعة وتعطى لهذه المجموعة سماحيات دخول للأغراض.

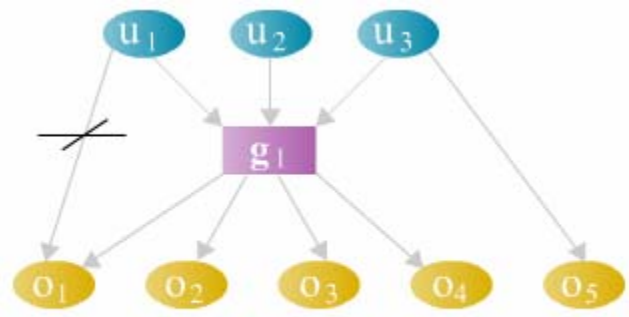
بعض السياسات الأمنية تفرض انضمام المستخدم إلى مجموعة واحدة فقط بينما تسمح سياسات أخرى بانضمام المستخدم إلى أكثر من مجموعة.



مجموعات تعمل كقائمة وسيطية للتحكم بالوصول

2. السماحية السلبية:

هي إحدى القيم في بنية تحكم الدخول تحدد العمليات الغير المسموح للمستخدم إجراءها من قبل المستخدم.



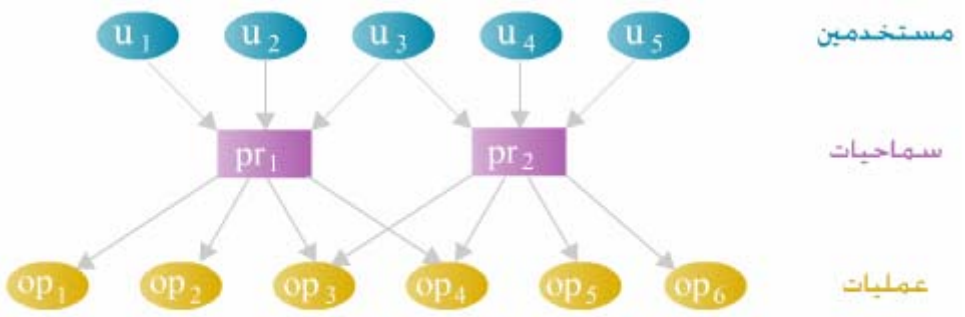
تحكم بالوصول بسماحيات سلبية

السماحية السلبية المعطاة للمستخدم u_1 المتعارضة مع السماحية الإيجابية للمجموعة g_1 تمثل إحدى حالات **تضارب السياسة الأمنية.**

3. الامتيازات privileges:

يمكنك أن تجمع حقوق إجراء عدد من العمليات في امتياز **privilege**.

وعادة ما ترتبط الامتيازات بعمليات نظام التـشغيل و فعالياته مثل إدارة النظام ، التخزين الاحتياطي، دخول البريد، ودخول الشبكة.



توضع الامتيازات كطبقة وسيطية بين المواضيع و العمليات

4. أدوار التحكم بالدخول(role-based access control (RBAC:

يدعى تطبيق مجموعة محددة من العمليات بـ "دور". غالباً ما يستخدم مفهوم **RBAC** في نظم إدارة قواعد البيانات.

5. حلقات الحماية:

هي من الأمثلة البسيطة عن الطبقة الوسيطية من متحكمات الدخول على مستوى العتاد.

كل موضوع (عملية معالجة **process**) وكل غرض تربط برقم يعتمد على أهميتها.

تحدد هذه الأهمية بالاعتماد على السياسة الأمنية وأهدافها.

مثال:

(**0**) نواة نظام التشغيل.

(**1**) نظام التشغيل.

(**2**) الأدوات.

(**3**) عمليات معالجة المستخدم.

مع الأخذ بعين الاعتبار أن الحلقة المركزية تعطي أعلى مستوى من الحماية. وعليه إذا ارتبطت عملية المعالجة **process** برقم **i** تجري في الحلقة **i**.

5. نماذج الأمن:

تعريف: نموذج الأمن هو توصيف معياري للسياسة الأمنية وكائناتها وقواعدها بلغة مفهومة معيارية قابلة للقراءة والفهم.

يوجد العديد من نماذج الأمن. من أهمها نموذج **Bell-LaPdula**.

سوف ندرس:

1. نماذج آلة الحالة.
2. نموذج **Bell-LaPdula BLP**.
3. نموذج **Biba**.
4. نموذج **Clark-Wilson**.

1. نماذج آلة الحالة:

تعريف: آلة الحالة هي أداة شائعة تستخدم لنمذجة العديد من مفاهيم نظم الحاسبات. وبالتالي فهي من أهم الأسس التي تبنى عليها نماذج الأمن.

يعتمد هذا النموذج على مفهومين:

الوضع state: هو المفهوم الأساسي في هذا النوع من النماذج ويمكن تعريفه بأنه تمثيل دقيق للنظام (من الوجهة التي نسعى لدراستها في النظام) في لحظة زمنية محددة.

تحولات الوضع state transition: يمكن تمثيله بدالة دخلها الوضع الحالي و خرجها الوضع في اللحظة التالية.

2. نموذج Bell-LaPdula (BLP):

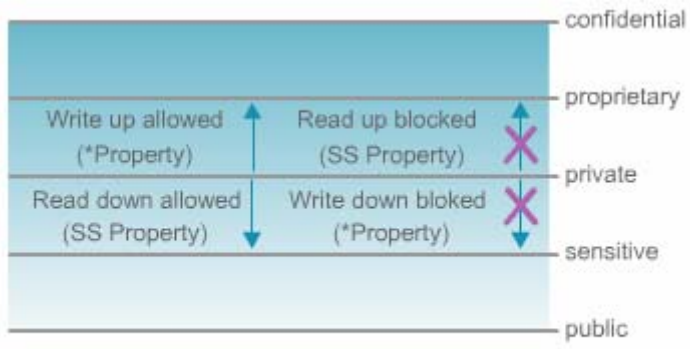
هو النموذج الأشهر بين نماذج الأمن وقد صمم في إطار الجهود لتصميم أنظمة تشغيل متعددة المستخدمين وآمنة.

هذا النموذج مؤسس على مجموعة من المبادئ هي:

- هو معني بالسياسة الأمنية المتعددة المستويات. لذلك تعرف سماحيات الدخول من خلال مصفوفة التحكم بالدخول ومستويات الأمن.
- تمنع السياسة الأمنية تدفق المعلومات من مستويات الأمن الأعلى إلى مستويات الأمن الأخفض.
- يعتبر هذا النموذج أن المعلومات تتدفق فقط عندما يقوم موضوع بمراقبة أو تعديل غرض.

يمكن توصيف الوضع في نموذج **BLP** بصفتين أو وفق قاعدتين:

1. **خاصة الأمن البسيط Simple Security Property (SS Property):** تحدد أن الموضوع في مستوى أمني معين لا يستطيع قراءة البيانات المصنفة بمستوى أمني أعلى ويصطلح على تسمية هذه القاعدة بـ "عدم قراءة الأعلى" **no read up**.
2. **خاصة النجمة Security Property (*):** تحدد أن الموضوع في مستوى أمني محدد لا يستطيع كتابة البيانات إلى مستوى أمني أخفض. ويصطلح على تسمية هذه القاعدة بـ "لا كتابة في الأسفل" **no write down** .



نموذج Bell-La Pdula

يوجد استثناء في نموذج **BLP** حيث أن المواضيع الموثوقة **trusted subject** غير مقيدة بالخاصية نجمة. وتعرف المواضيع الموثوقة بأنها أغراض مضمون أنها لن تقوم بأي تحويل يخرق أمن المعلومات حتى لو كان ذلك ممكناً. وهذا يعني أن المواضيع الموثوقة مسموح لها خرق الخاصة نجمة بمعنى أنه يمكنها الكتابة إلى الأسفل.

بالرغم من أن **BLP** يقدم إدارة جيدة للسرية **confidentiality** إلا أنه يفشل في تحديد أو إدارة عدد كبير من المفاهيم:

1. لا يعالج السلامة، أو الإتاحة.
2. لا يعالج إدارة التحكم بالدخول، ولا يقدم طريقة لتحديد أو تغيير مستوى أمن غرض أو موضوع.
3. لا يمنع القنوات المغطاة (هي وسائل تمكن من تراسل البيانات خارج نطاق الطرق العادية أو المتوقعة أو المكشوفة).
4. هو لا يعالج مفهوم مشاركة الملفات وهو مفهوم حيوي في النظم الشبكية.

3. نموذج Biba:

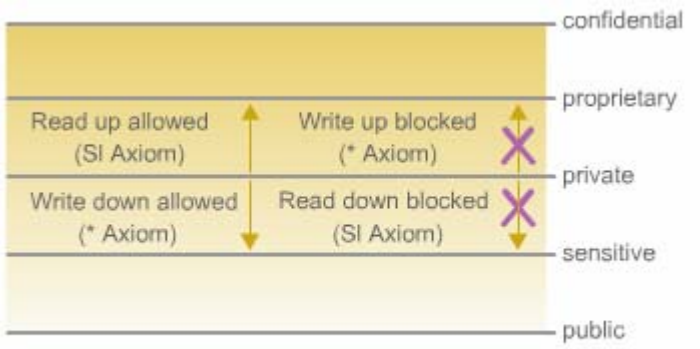
تعتبر السلامة أكثر أهمية من السرية لمعظم المؤسسات الغير عسكرية. لذلك يوجد عدد من النماذج التي ركزت على السلامة مثل نموذج **Biba** ونموذج **Clark-Wilson**.

يعتبر نموذج **Biba** أيضاً نموذج آلة حالة يتبع النمط الإلزامي والشعري **lattice**، صمم ليعالج ثلاثة مفاهيم حول السلامة:

- يمنع تعديل الأغراض من قبل مواضيع غير مخولة (مرخصة).
- يمنع التعديلات الغير مرخصة من قبل المواضيع المخولة.
- يحمي التماسك الداخلي والخارجي للأغراض.

يعتمد نموذج **Biba** على فرضيتين:

1. **فرضية السلامة البسيطة (Simple Integrity Axiom (SI Axiom:** تقول هذه الفرضية لا يمكن لموضوع من مستوى أمني معين قراءة بيانات من مستوى أمني أدنى . و غالباً ما يصطلح على تسمية هذا الوضع بـ **no read down**.
2. **فرضية السلامة نجمة:** تقول هذه الفرضية لا يمكن لموضوع من مستوى أمني معين أن يكتب بيانات ذات مستوى أمني أعلى. وغالباً ما يصطلح على تسمية هذا الوضع بـ **no write up**.



نموذج Biba

يوجد في نموذج **Biba** بعض نقط الضعف مثل:

1. هو معني فقط بالسلامة ولا يهتم بالسرية أو الإتاحة.
2. يركز فقط على حماية الأغراض من المهددات الخارجية، فهو يفترض أنه يتم الاهتمام بالمهددات الداخلية برمجياً.
3. هو لا يعالج إدارة التحكم بالدخول، ولا يقدم طريقة لتحديد أو تغيير مستوى أمن غرض أو موضوع.
4. لا يمنع القنوات المغطاة.

4. نموذج Clark-Wilson:

هو أيضاً نموذج حماية السلامة. لكنه يعالج السلامة من منظور مختلف عن نموذج **Biba**. فهو لا يستخدم البنية الشعرية وإنما يعتمد على علاقة ثلاثية **للموضوع_برنامج_غرض** والتي تدعى ثلاثية.

لا تملك المواضيع إمكانية دخول مباشر إلى الأغراض. فالأغراض يمكن الدخول لها فقط من قبل البرامج.

يعتمد هذا النموذج على مفهومين – إجراءات مصاغة بشكل جيد ومهام منفصلة.

1. **تأخذ الإجراءات المصاغة جيداً شكل البرامج:** هذه البرامج تستخدمها المواضيع لتدخل إلى الأغراض. لكل برنامج حدود تقيده بما يمكنه أن يفعله أو لا يفعله بالغرض . و هذا يقيد استطاعة المواضيع. فإذا صممت البرامج بشكل جيد يمكن للعلاقة الثلاثية أن تقدم وسائل حماية لسلامة الغرض.

2. **فصل المهام:** وهي فصل الوظائف الحرجة (المهمة) إلى جزأين أو أكثر يجب إنجاز كل جزء منها من قبل موضوع مختلف. هذا يمنع المواضيع المخولة من إجراء تعديلات غير مرخصة على الأغراض. وهذه حماية أخرى لسلامة الأغراض.

يمكن أن ندعو نموذج **Clark-Wilson** أيضا بنموذج الواجهات المقيدة **restricted interface model**. حيث يستخدم قيود مصنفة ليقدم فقط المعلومات والوظائف المرخصة لموضوع معين. ففي مستوى تصنيف معين سيرى الموضوع مجموعة واحدة من البيانات و يملك دخول إلى مجموعة واحدة من الدوال، بينما يرى موضوع آخر في مستوى تصنيفي آخر سيرى مجموعة مختلفة من البيانات وسيدخل إلى مجموعة مختلفة من الدوال.

الفصل الثاني: أمن الشبكة

1. مقدمة

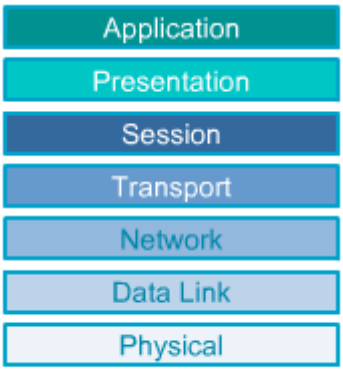
شبكات الحواسب هي البنية التحتية لاتصالات المعطيات والمستخدمة لتبادل البيانات بين العقد والحواسيب في الأنظمة الشبكية الموزعة. حيث تجهز البيانات التي سترسل من تطبيق معين في عقدة ما، فترسل على شكل متتالية من إشارات الكترونية أوضوئية ثم تجمع وتقدم إلى التطبيق في العقدة المستقبلة.

وعلى الشبكة أن:

- تجد الطريق من المرسل إلى المستقبل.
- تتعامل مع ضياع أوتلف البيانات.
- أيضاً التعامل مع انقطاع الاتصال.

لذلك من الجيد إنجاز كل مهمة من هذه المهام على حدى وبشكل مستقل عن باقي المهام وبالتالي استخدام بنية طبقية تكون فيها التطبيقات في الأعلى والبروتوكولات التي ترسل المعلومات المرمزة فيزيائياً في الأسفل.

لذلك وجد ما يدعى ببنية **ISO/OSI** المعيارية التي تقسم الشبكة وبروتوكولاتها إلى سبعة طبقات كما في الشكل التالي:



بنية ISO\OSI

تعرف بنية **ISO/OSI** (**International Organization for Standardization**) عدة خدمات أمنية **security services** لمعالجة مهددات أمن الشبكة. والتي هي غالباً أدوات أمنية تعمل على تقنيات التعمية. مثل: التعمية والتوقيع الالكتروني، ودوال اختبار السلامة.

تتمتع الحماية بالتعمية بصفة جيدة: إذ لا يمكن كسر بروتوكول أمني يعمل في الطبقة **N** حتى لوكان يعمل فوق بروتوكول غير آمن. ويوجد استثناء واحد لهذه القاعدة، هوعندما يكون هدفك

مجهولاً وأنت تحتاط لتخفي كائنات الشركاء في الطبقة الواحدة، عندئذ ستظل البيانات المضافة من بروتوكولات الطبقات الأدنى حول عنوان مرسل ومستقبل الرسالة مكشوفة.

على كل حال لا يمكن حل كل مشاكل أمن الشبكة باستخدام التعمية. هناك طرق حماية أخرى مثل:

- أدوات التحكم بالدخول (جدار النار **firewall**).
- نظم كشف الاختراقات.

نماذج المهددات:

يمكن أن يأخذ مهاجم الشبكة أحد شكلين:

- مهاجم تفاعلي نشط **active** .
- أو مهاجم غير تفاعلي مستتر **passive**.

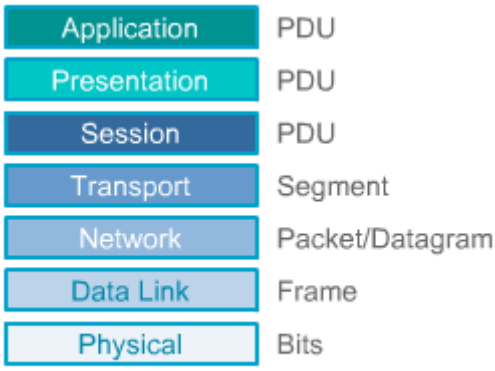
يكتفي المهاجم غير التفاعلي بالتنصت على حركة المرور. يمكن للمهاجم التفاعلي أن يعدل الرسالة، أو أن ينشئ رسائل جديدة، أوأن يفسد معلومات إدارة الشبكة مثل المقابلة بين الأسماء في خدمة **DNS** وعناوين بروتوكول الانترنت **IP**. كما يمكن أن يحاول المهاجم أن يحصل على معلومات عن شبكتك الداخلية ويستفيد من هذه المعلومات في إجراء الهجمات.

من أهم نماذج المهددات:

- محلل حركة المرور **Traffic analysis**: يحاول أن يحدد أنماط الاتصالات وعندما لا يتمكن المهاجم من قراءة رسائل مستقلة فإنه يحاول تحديد الرسائل القادمة من نفس المصدر أوأن يكتشف هوية المتصلين. وفي حالة خدمة المحمول ربما يهتم المهاجم بتحديد مواقع المستخدمين.
- ندعوالمهاجم الذي يهتم بمحتوى الرسالة بمسترق السمع **eavesdropping**، أو المتنصت **wiretapping**، أوالشمام **sniffing**.
- هجمات الرسائل المزيفة **spoofing attacks** حيث تصل رسائل لها عناوين مرسل مزيفة.
- في هجمات الطوفان **flooding** يوجه عدد كبير من الرسائل إلى الضحية بنفس الوقت.
- في هجمات الاحتلال **squatting** يحاول المهاجم أخذ مكان الضحية.

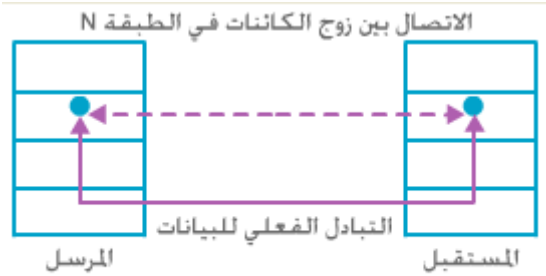
2. مبادئ تصميم البروتوكول

تعتبر الطبقات السبع التي تقدمها البنية **ISO/OSI** اختصار مفيد لمناقشة أمن الشبكة.
حيث نلاحظ بشكل عام أن الخدمات الأمنية المقدمة في الطبقة العليا تكون مخصصة لتطبيق محدد بينما تقوم الخدمات الأمنية المقدمة في الطبقات الدنيا بتقديم الأمن لأي حركة المرور باتجاه أي من الطبقات الأعلى منها.



نموذج الطبقات السبع ISO/OSI

في هذا النموذج، تتصل أزواج (بين المرسل والمستقبل) الكائنات في الطبقة **N**، باستخدام البروتوكول **N**. بينما ترى البروتوكولات في الطبقة **N+1** اتصال وهمي في الطبقة **N**. بالطبع فإن بروتوكول الطبقة **N** مبني على بروتوكولات من الطبقات الدنيا. ويوجد معيار عام لتمرير البيانات إلى الطبقات الدنيا.



الاتصال الافتراضي في الطبقة N

تدعى الرسائل في البروتوكول **N** بوحدات بيانات البروتوكول **N** **N-protocol data units (PDUs)**.

يقوم البروتوكول **N** بإرسال **N-PDU** باستخدام مسهلات **invoking facilities** المتوفرة في الطبقة **N-1**.

في هذه المرحلة، يمكن أن تجزأ الـ **N-PDU** أوتعالج. ثم تجهز بترويسات وتذييلات لتنتج **(N-1)-PDU**.

حيث سيستخدم المستقبل لهذه الـ **(N-1)-PDU** معلومات الترويسة والتذييل لإعادة تجميع **N-PDU**.

يوجد مفهومان رئيسيان لتوظيف الخدمات الأمنية في الطبقة**N-1** التي تستدعى ببرتوكول الطبقة **N**:

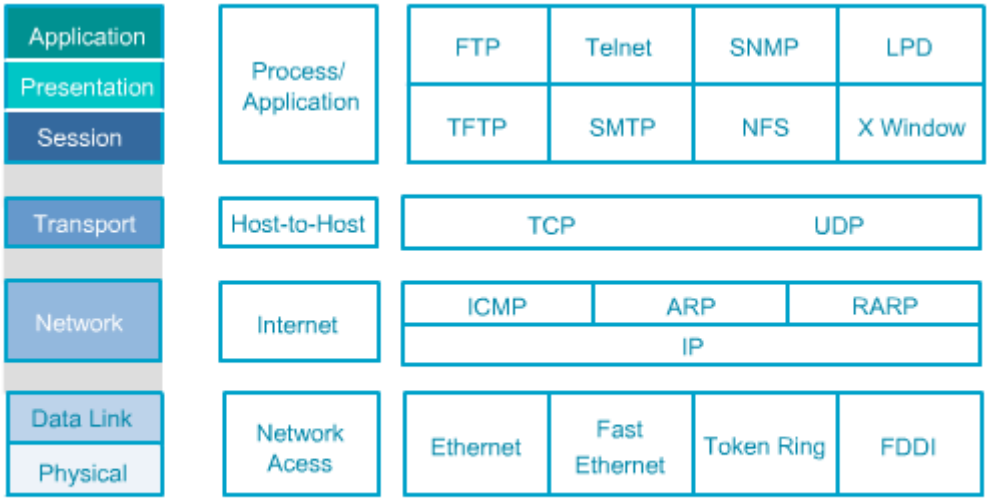
يمكن أن تكون الطبقة العليا مطلعة على الخدمات الأمنية في الطبقة الأدنى أو يمكن أن تكون شفافة. في الحالة الأولى، يجب على بروتوكول الطبقة العليا أن يغير استدعاءاته بحيث تصبح تشير إلى المسهلات الأمنية المقدمة. أما في الحالة الثانية، فليس على بروتوكول الطبقة العليا أن يتغير أبداً. في الحالتين، يتلاءم مكان ترويسات **(N-1)-PDU** لتخزين البيانات الأمنية ذات العلاقة.

يوجد أربعة طبقات في رزمة بروتوكول الانترنت:

1. **طبقة التطبيق:** ومن بروتوكولاتها:**telnet, ftp, http,** ،
smtp (Simple Mail Transfer Protocol), Set (Secure Electronic Transaction) .
2. **طبقة النقل:** ومن بروتوكولاتها: **TCP (Transport Control Protocol)**
UDP (User Datagram Protocol).
3. **طبقة الانترنت:** بروتوكولاتها: بروتوكول **IP**.
4. **طبقة الربط link (والفيزيائية):** بروتوكولات هذه الطبقة تحددها تقنية الشبكة.

يستخدم بروتوكولي **TCP** و**UDP** أرقام البوابات **ports** لتحديد بروتوكول طبقة التطبيق الذي أتت منه الرزم الـ**PDU**، ومن أهم أرقام المنافذ الشائعة: المنفذ رقم 21 للبروتوكول **ftp**، المنفذ

رقم 23 للبروتوكول **telnet**، 25 للبروتوكـول **smtp** (إرسال البريد الالكتروني)، 110 بروتوكول **pop3** (جمع البريد الالكتروني).....



طبقات الشبكة و بروتوكولاتها

تعتبر بروتوكولات **TCP** و**IP** و**UDP** مع بروتوكول الإدارة **ICMP** **قلب الانترنت**. وقد صممت لأجل المستخدمين المتعاونين (غير المؤذيين) العاملين على شبكة غير موثوقة. لذلك فالأمن لم يكن بالحسبان أبداً. لكن مع التوسع الكبير في استخدام **TCP/IP** ظهرت الحاجة إلى تثبيت المفاهيم الأمنية واستخدامها.

أصبح الآن يوجد عدد كبير من بروتوكولات الأمن في طبقتي النقل والانترنت، كما يتم حالياً تطوير العديد من البروتوكولات المعيارية لنفس الهدف.

3. أمن بروتوكول IP (IP Security)

يعمل بروتوكول **IP** دون الانتباه والتحسس لحالة الشبكة **connectionless** لذلك فإنه يدعى بـ "عديم الحالة" **stateless**، لهذا السبب فإن كل رزمة تعامل بشكل منفصل عن أي رزمة أخرى. فلا يوجد ضمانة توصيل للرزم، ولا توجد آلية لإصلاح ترتيب الرزم ولا أي حماية أمنية.

عرضت البنية الأمنية لبروتوكول **IP** (**IPsec**) في معايير **RFC 2401**. وهي اختيارية لإصدار **IP4** لكنها إجبارية لإصدار **IP6**.

يحتوي **IPsec** آليتين أمنيتين أساسيتين:

- ترويسة الاستيقان **AH** الموصوفة في المعيار **RFC 2402**.
- الحمولة الأمنية المغلفة **Encapsulating Security Payload (ESP)** والمعتمدة بالمعيار **RFC 2406**.

علماً أن بنية **IPsec** لا تملك آليات تمنع تحليل حركة المرور.

1. ترويسة الاستيقان AH

تقوم ترويسة الاستيقان **IP AH** بحماية سلامة وأصالة رزم **IP** لكن لا تحمي السرية.

وقد طرح هذا البروتوكول لأسباب سياسية (قوانين حظر تصدير خوارزميات التعمية الصادر عن الحكومة الأمريكية).

حالياً يفضل استخدام آلية **ESP** فقط لتسهيل توظيف **IPsec**.

2. حمولات الأمن المغلفة ESP

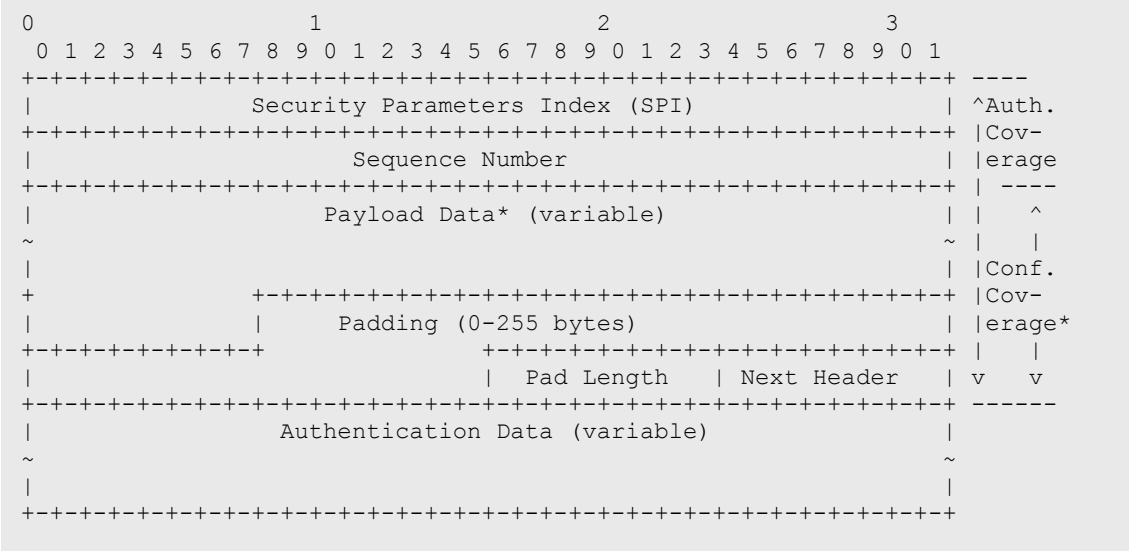
يمكن استخدام **ESP** ل:

- تقديم الأمن والاستيقان من مصدر البيانات.
- سلامة البيانات.
- سرية محدودة لتدفق حركة مرور.
- منع عملية إعادة الاستخدام **replay protection**.

تحتوي رزمة **ESP** على الحقول التالية:

1. فهرس معاملات الأمن **Security Parameter Index (SPI)**: هي حقل من **32** بت. يوصف الرابط الأمن **security association SA** بشكل وحيد لكل رزمة عابرة وعنوان **IP** المستقبل وبروتوكول الأمن **(ESP)**.
2. **رقم تسلسلي:** هوحقل **unsigned** طوله **32** بت يحوي قيمة عداد يزداد برتابة. توضع هذه القيمة من قبل المرسل لكنها تعالج من قبل المستقبل.
3. **حمولة البيانات:** هوحقل متغير الطول يحوي **PDU** طبقة النقل.
4. **البطانة:** هو حقل اختياري يحتوي بيانات بطانة لأجل خوارزميات التعمية ، يجب أن يكون طول البيانات التي ستعمى من مضاعفات حجم كتلة المعميات.
5. طول البطانة.
6. **الترويسة التالية:** هوحقل يبين نوع **PDU** لطبقة النقل.

7. **بيانات الاستيفان:** هي عدد متغير من كلمات طولها **32** بت تحوي قيمة اختبار السلامة **integrity check value (IVC)** المحسوبة على رزمة الـ **ESP** مطروح منها بيانات الاستيقان.



الشكل العام لترويسة

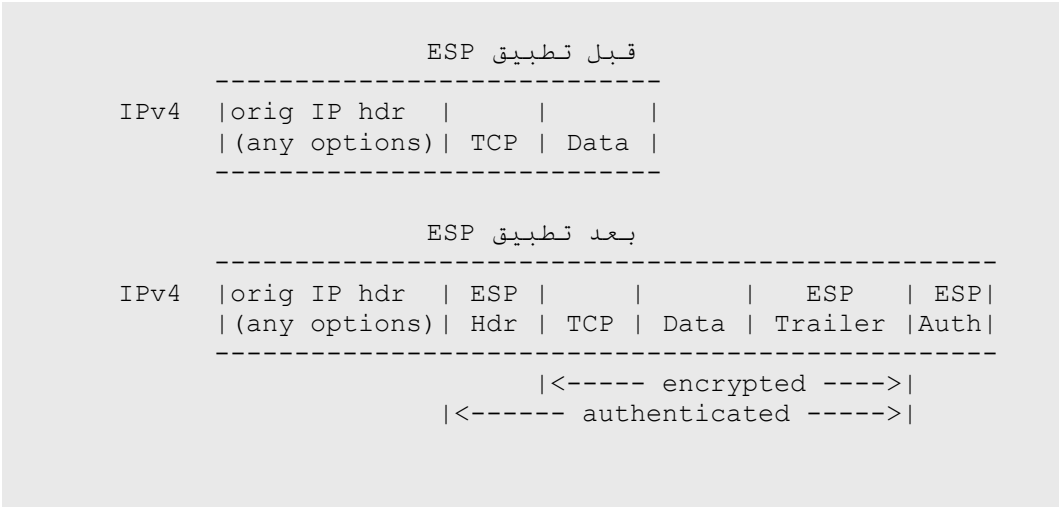
يشكل **SPI** والرقم التسلسلي ترويسة **ESP**. بينما تشكل الحقول التي بعد الحمولة تذييل **ESP**.

يمكن استخدام **ESP** في نمطين أساسيين:

1. **نمط النقل transport mode:**

حيث يغلف الإطار **frame** القادم من الطبقة الأعلى (**TCP**أو**UDP**) بـ**ESP**. ولا تعمى ترويسة **IP**.

يوفر نمط النقل حماية نقطة - نقطة للرزم المنتقلة بين عقدتين **hosts**.وعلى كلتا العقدتين أن تدركا **IPsec** (بمعنى أن تعدا مسبقاً للتعامل مع **IPsec**).



توضع ترويسة ESP في نمط النفق

2. نمط النفق:

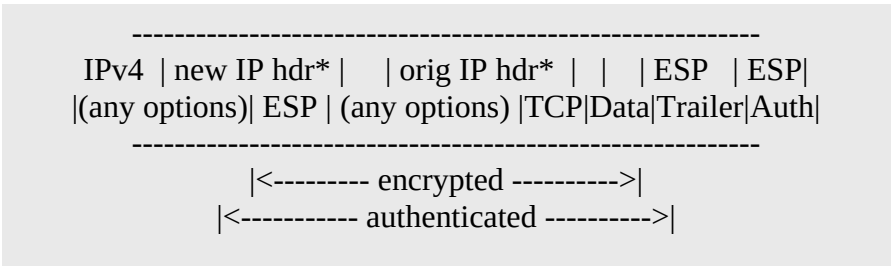
تعامل كل الرزم وحقول الأمن على أنها حمولة جديدة لرزم **IP** الخارجية. بينما تغلف رزم **IP** الأصلية الداخلية بالرزم **IP** الخارجية.

وبالتالي يمكن أن نصف نمط النفق بأنه رزم **IP** ضمن رزم **IP** أخرى.

يمكن استخدام هذا النمط عندما تجرى معالجة **IPsec** على بوابات أمنية في طرف العقد. حيث لا تحتاج العقد الوسيطة أن تكون مدركة لـ **IPsec**.

يمكن أن تكون البوابة جدار نار **firewall** أوموجه **router** . وبالتالي فهذا النمط يقدم أمن بوابة لبوابة بدلاً من أمن عقدة لعقدة.

من جهة أخرى نحصل على خصوصية لحركة المرور لأن الـرزم الداخليـة ليـست مرئيـة للموجهات الوسيطة وعنواني الهدف والمصدر مخبئان.



توضع ترويسة ESP في نمط النفق

3. الرابط الآمن

لكي يستطيع نظام ما أن يولد أوأن يفك تعمية، أوأن يتحقق من رزمة **ESP** يجب أن يعلم الخوارزمية المستخدمة وأي مفتاح يجب أن يستخدم. تخزن كل هذه المعلومات فيما يسمى الرابط الآمن **security association SA**.

وهي الحالة العامة **state** لعقدتين يتصلان باتجاه واحد. بشكل عام يحتاج الاتصال بين حاسبين باتجاهين إلى رابطتين آمنتين واحدة في كل اتجاه. لذلك فعادة ما تنشأ الروابط الآمنة كأزواج.

تحدد الرابطة الآمنة بشكل وحيد باستخدام فهرس معاملات الأمن **SPI** (التي تحمل في ترويسات **AH** و**ESP**)، وعنوان **IP** الهدف، وبروتوكول الأمن المستخدم (**ESP** أو**AH**).

وهي تحتوي البيانات المتعلقة بالتعمية مثل محددات الخوارزمية والمفاتيح وزمن حياة المفتاح ومحتمل أن تحتاج إلى أشعة ابتدائية **IVs**، كما يمكن أن تحتوي رقم عداد تسلسلي، ونافذة منع الإعادة **anti-replay window**. بالإضافة إلى أن الرابطة الآمنة تحدد أي من نمطي الاتصال يتم استخدامه نفق، أونقل.

بشكل عام تخزن الروابط الآمنة الفعالة في قاعدة بيانات تدعى **SAD** **Security Association Data base**.

يمكن أن تدمج الروابط الآمنة كما في حالة وجود مستويات متعددة لأنفاق **IPsec**. وعندها يبدأ كل نفق وينتهي في بوابات **IPsec** مختلفة على طول الطريق.

4. بروتوكول تبادل مفاتيح الانترنت

يمكن إنشاء رابطة آمنة يدوياً عندما يكون عدد العقد صغير نوعاً ما لكن لأجل شبكة كبيرة يصبح الخيار اليدوي صعباً لذلك يوجد ما يسمى بروتوكول تبادل مفاتيح الانترنت **IKE**.

لهذا البروتوكول العديد من الأهداف الأمنية، أهمها:

- الاستيقان من الكائنات.
- تأسيس قيم سرية حديثة ومتشاركة تكون بذرة توليد مفاتيح سرية مشتركة أخرى.
- إنجاز المفاوضات السرية لكل خوارزميات التعمية مثل: طرق الاستيقان وطرق تبادل المفاتيح وخوارزميات التعمية ورمز استيقان الرسائل **Message Authentication code MAC** وخوارزميات الاختزال وتستخدم هذه الآلية لإيجاد مقاومة لهجمات رفض الخدمة.

يقدم **IPsec** مجموعة مرنة من آليات تأسيس المفاتيح لها عدة خيارات وعدة معاملات. ذلك أن **IPsec** يحتاج إلى عدد كبير من المفاتيح السرية. فكل جلسة آمنة تحتاج مفتاح حيث توجد جلسة لكل ثلاثية من الجداء التالي: **{ESP, AH}×{tunnel, transport}×{sender, receiver}.**

يعمل **IKE** على مرحلتين:

1. **في المرحلة الأولى:**

تعدّ الرابطة الآمنة لتكون قناة آمنة لحمل بقية مفاوضات **SA** ولإدارة حركة المرور.

تتضمن هذه المرحلة أعمال الاستيقان، وتبادل المفتاح.

يوجد للمرحلة الأولى نمطان مختلفان كلياً:

- النمط الأول: بطيء ويدعى النمط الرئيسي**main mode** (ست رسائل) فيه ضمانات أمنية كبيرة.
- النمط الثاني: سريع يدعى النمط الهجومي **aggressive mode** (أربعة رسائل).

يعطي كلا النمطان اختيار آلية الاستيقان مثل الاستيقان المعتمد على التوقيع و المفاتيح المتشاركة مسبقاً وهاتان الآليتان موظفتان بالفعل في تطبيقات **IPsec** بينما الاستيقان باستخدام التعمية بالمفتاح العلني هي جزء من المعايير لكنها غير موظفة فعلياً.

2. **في المرحلة الثانية:**

يتم التفاوض على الروابط الآمنة للاستخدام العام. حيث تتم هذه المفاوضات بسرعة باستخدام الجلسة الآمنة التي تم تأسيسها في المرحلة الأولى. ويمكن أن تؤسس عدة جلسات آمنة عامة (المرحلة الثانية) باستخدام جلسة آمنة واحدة من المرحلة الأولى.

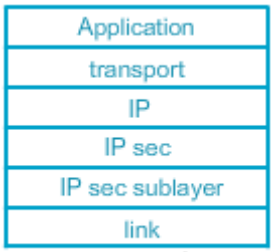
يقدم بروتوكول **IPsec** خدمات الاستيقان والتعمية بشكل مستقل عن بروتوكولات تبادل المفاتيح التي تعد الجلسات الآمنة ومفاتيح الجلسة.

5. سياسات IPsec

تحدد سياسات بروتوكول **IPsec** المعالجة الأمنية التي ستطبق على رزم بروتوكول **IP**.

وتحتوي كل عقدة مشاركة بفعالية ببروتوكول **IPsec** على قاعدة بيانات سياسة أمنية **SPD** **Security Policy Data base** تستشار لأجل كل رزمة داخلة أوخارجة من هذه العقدة.

حيث تقارن الحقول المعنية في **IP** رزمة مع حقول السياسة الأمنية. تعتمد هذه المقارنات على حقول عنواني المصدر والهدف وبروتوكول طبقة النقل وأرقام المنفذ...وتحدد النتيجة جلسة آمنة أومجموعة جلسات أمنية أوربما الحاجة إلى تأسيس جلسة آمنة جديدة.....الخ.



أمن IP

6. مميزات IPsec

- يقدم خدمات أمنية لكل من يستخدم بروتوكول **IP**.
- لا تحتاج الطبقات الأعلى أن تكون مدركة لعملية المعالجة الأمنية في طبقة **IP** والتي تتم باستخدام **IPsec**.
- يقدم **IPsec** خدمات أمنية بشكل عقدة – عقدة وليس مستخدم - مستخدم أو تطبيق – تطبيق.
- لا يشترط **IPsec** استخدام بروتوكول تبادل مفاتيح محدد وإنما تتفق العقد التي تتراسل وفق **IPsec** على بروتوكول تبادل مفاتيح لتستخدمه.

4. بروتوكول الأمن على طبقة النقل\الأمن على طبقة المقابس secure socket layer SSL / Transport Layer Security TLS

يعتبر بروتوكول **connection-oriented TCP** بمعنى انه يقوم بمتابعة الرزم ويتحسس لضياع إحدى الرزم حيث يقوم بإعادة إرسال الرزم الضائعة. ويقوم بروتوكول **TCP** بإنجاز الاستيقان بناء على عنوان الكائنات عند بدء تكوين جلسة بين عقدتين. لكن ينقص بروتوكول **TCP**، استيقان قوي مبني على التعمية وسلامة البيانات وسريتها. لذلك تقدم هذه الخدمات في بروتوكول **SSL** المستخدم في تطبيق **Netscape**. ليحمي وبشكل رئيسي حركة المرور على الشبكة العالمية (الانترنت)**World Wide Web**، بمعنى تقديم الخدمات الأمنية للاتصالات بين مخدّم الويب ومستعرض الانترنت لدى الزبون.

لكن يوجد بروتوكول آخر هو**Transport Layer Security TLS** يعتبر توأم بروتوكول **SSL** لذلك اصطلح على إدراج التسمية **SSL/TLS**. يتوضع **SSL** بين طبقتي التطبيق و**TCP** في رزمة بروتوكول الانترنت. لهذا يمكنه الاعتماد على خصائص **TCP**. فمثلاً لا يهتم بروتوكول **TCP** بمسألة التسليم الموثوق **reliable delivery**.

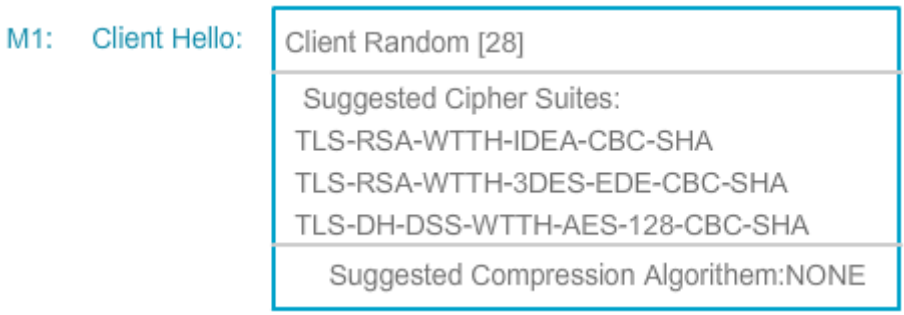
يتصف بروتوكول **SSL** بأنه **connection oriented** ومعتمد على الحالة. يخزن حالة جلسة **SSL session state** على المعلومات اللازمة لتنفيذ خوارزميات التعمية مثل: معرف الجلسة ومواصفات المعمية والمفاتيح السرية المتشاركة والشهادات والقيم العشوائية المستخدمة في بروتوكولات مثل **Diffi – Hellman**. يمكن لجلسة **SSL** واحدة أن تحتوي عدة اتصالات و ذلك لتفادي الحمل المتولد من إدارة البروتوكولات مثال: جلسة **http 1.0** بين مخدّم وزبون حيث يتم إنشاء اتصال جديد لنقل كل جزء من وثيقة مركبة. وعندها يتغير جزء فقط من معلومات الحالة لأجل كل اتصال جديد.

يتألف بروتوكول **SSL** بشكل رئيسي من جزأين أساسيين: طبقة سجل **SSL** وطبقة مصافحة **SSL Handshake**.تأخذ ***طبقة سجل SSL*** الرزم من بروتوكولات الطبقة الأعلى، ثم تجزأ هذه الرزم إلى سجلات نص بسيط لـ **SSL** ثم تطبق عليها خطوات التعمية المعرفة في مواصفات المعمية المخزنة في الوضع الحالي للجلسة.

بشكل أساسي فان طبقة سجل **SSL** تقدم خدمة شبيهة لخدمة **IPsec**، والتشابه بين جلسات **IPsec** وجلسات **SSL** ليس مصادفة.

يقوم بروتوكول **مصافحة *SSL*** بإعداد معاملات التعمية لوضع الجلسة. ولشرح هذا البروتوكول سنتابع خطوات استيقان زبون من مخدّم.

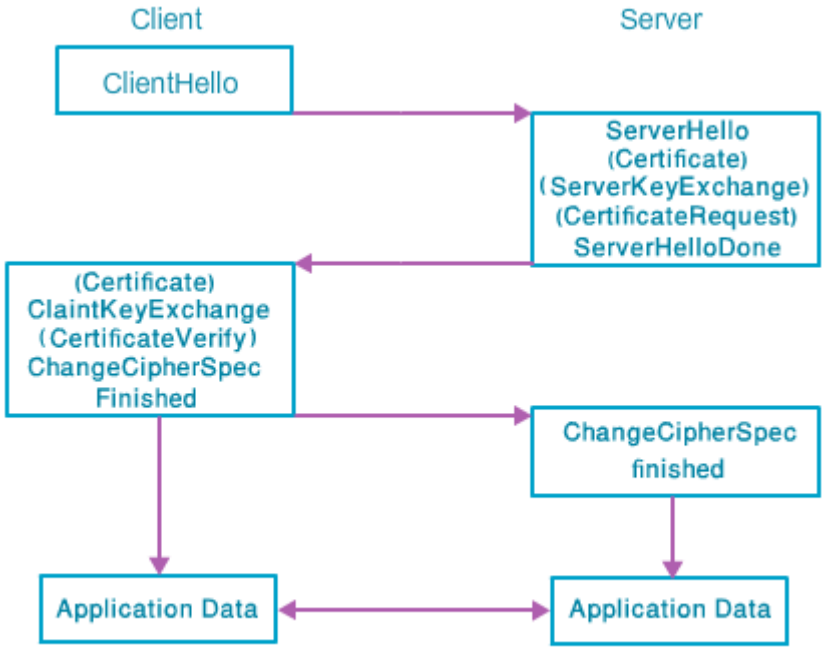
يبدأ الزبون البروتوكول برسالة **ClientHello**. وهي تحتوي رقم عشوائي و قائمة بالمعميات المقترحة مرتبة حسب أفضليتها عند الزبون وخوارزمية الضغط المقترحة.



يختار المخدّم المجموعة المعمية

مثال:

TLS-RSA-WITH-3DES-EDE—CBC-SHA من المجموعات المقترحة.حيث ستستخدم **RSA** لتبادل المفاتيح، وتستخدم **3DES** في النمط **CBC** للتعمية، وتستخدم **SHA** كخوارزمية الضغط . يرد المخدّم برسالة **ServerHello** وسلسلة شهادة.



بروتوكول مصافحة SSL

M2: ServerHello:	**ServerRandom[28]**
	Use Cipher Suite: TLS.RSA>WITH-3DES-EDE-CBC-SHA
Certificates:	**Session ID:0xa00372d4xs**
	subjectAltName: SuperStoreVirtualOutlet PublicKey:0x521aa593….. Issuer: SuperStoreHQ
Server	**subjectAltName: SuperStoreVirtualHQ PublicKey: 0x9f400682….. Issuer: Verisign**
	NONE

الرسالة الثانية

في مثالنا لم يطلب من الزبون شهادة، يتحقق الزبون من سلسلة الشهادة التي تشير إلى توسيعات الاسم الإضافي للموضوع **subject alternative name** في الشهادات ثم ينشأ محلياً قيمة عشوائية طولها **48** بايت تدعى السر الأساسي **PreMasterSecet**.

تعريف: السر الأساسي هوالبايتات الـ**48** الأولى مما يدعى **PRF**.

تعريف: الاختصار**PRF(PreMasterSecet،"master secret"** ،

(CleantRandom||ServerRandom يرمز إلى لدالة معقدة جداً مبنية على **MD5** و**SHA** التي تأخذ دخلاً لها: السر وعلامة وبذرة. حيث يستخدم السر الأساسي كدخل في بناء رزمة المفتاح كما يلي:

. CleantRandom||ServerRandom)، "key expansion"،PRF(MasterSecet

يستخرج من رزمة المفتاح كل المفاتيح اللازمـة لعمليتـي **MAC** و التعمية لأجل الزبون والمخدم.تختلف المفاتيح التي تحمي الاتصال من المخدم إلى الزبون عن المفاتيح التي تحمي الاتصال من الزبون إلى المخدم. لذا يستطيع طرفي الاتصال التمييز بسهولة بين الرسائل التي المرسلة والرسائل المستقبلة وبالتالي لن تكون هناك إمكانية لهجوم الانعكاس **reflection attack** الذي ترد فيه الرسالة إلى مرسلها.

يرسل الزبون الآن **PreMasterSecet** إلى المخدم، باستخدام خوارزمية تبادل المفتاح التي تم تحديدها في مجموعة الخوارزميات المختارة والمفتاح العام المعتمد للمخدم (على الزبون تدمير **PreMasterSecet** مباشرة بعد إرساله).

نشاط: في مثالنا حدد خوارزمية تبادل المفاتيح والمفتاح العام.

تعني رسالة تغيير مواصفات المعمية **ChangeCipherSpec** انه سيتم حماية السجلات المرسلة لاحقاً باستخدام مجموعة الخوارزميات والمفاتيح التي تم التفاوض عليها تواً.

ثم يقوم الزبون بربط الرسالة الثالثة إلى الاثنتين السابقتين من خلال اخنزالين مبنيين بواسطة **MD5** و**SHA**.

M3:	**A: ClientKeyExchange**	**RSA_Encryption (ServerPublicKey,PreMasterSecret)**
	B: ChangeCipherSpec	**NONE**
	C: Finished	**MD5(M1 || M2 || M3A)** **SHA(M1 || M2 || M3A)**

الرسالة الثالثة

يفك المخدم تعمية **PreMasterSecet** ويحسب من خلاله **MasterSecet**، ورزمة المفتاح، وكل المفاتيح السرية المشتقة الفعالة في هذه الجلسة مع الزبون.
يتحقق المخدم الاختزال المضاف إلى رسائل الزبون ويرد بـ :

M4:	**A: ChangeCipherSpec**	**NONE**
	B: Finished	**MD5(M1 || M2 || M3A || M3C)** **SHA(M1 || M2 || M3A ||M3C)**

الرسالة الرابعة

يتحقق الزبون من الاختزال في رسائل المخدم. ويكون عندها كلا الطرفين قد أسس مفاتيح سرية متشاركة والتي يمكن استخدامها لحماية اتصالات التطبيقات.

5. DNS

غالباً ما تتعرف التطبيقات على الكائنات من خلال الأسماء الخاص بها وتسمى بنظام أسماء النطاقات **DNS (Domain name system)**. بينما نحتاج عناوين الانترنت المقابلة لأسماء الـ **DNS** في الاتصالات. تقدم هذه الخدمة من قبل مخدمات **DNS**. حيث تقدم خدمة البحث **DNS lookup** بإعطاءعناوين الانترنت لأسماء **DNS** وبالعكس تقدم خدمة البحث العكسي **reverse lookup** أسماء **DNS** المقابلة لعناوين الانترنت.
قد يقوم المهاجم بإفساد هذه المعلومات وبالتالي يوجه المستخدمين إلى مواقع مزيفة . و جعل بعض المواقع تظهر وكأنها غير فعالة مسبباً الكثير من الفوضى. ويمكن أن تتفاقم المشكلة إذا قامت مخدمات **DNS** أخرى بتحديث بياناتها بالمعلومات الخاطئة.
يستخدم برتوكول **DNS lookup** الأصلي طريقة بسيطة لأجل منع التزييف **spoofing prevention**. ويجري العمل
حالياً على تطوير خدمة **DNS** آمنة.

6. جدران النار

تحمي آليات التعمية سرية وسلامة البيانات أثناء الإرسال. وتقوم بروتوكولات الاستيقان بالتحقق من مصدر البيانات. أما جدران النار فتستخدم للتحكم بحركة المرور المسموح بدخولها إلى نظامنا (مرشحات الدخول) أوبخروجها من نظامنا (مرشحات الخروج).

تعريف: جدار النار هي آلة أمنية شبكية تتحكم بتدفق حركة المرور بين جزأين من الشبكة.

غالباً ما تتوضع جدران النار بين الشبكة العامة للمؤسسة والانترنت. لكن يمكن أيضا استخدامها في الشبكة الداخلية للمؤسسة الانترانت لحماية الأقسام المختلفة.

يجب أن تتحكم جدران النار بكل حركة المرور من وإلى الشبكة المقصود حمايتها. لذلك يجب أن تمر كل الحركات من خلال جدار النار ليكون فعالاً.

لكن يوجد بعض أنواع الشبكات التي تعتبر نقاط دخول إضافية خلف جدار النار مثل الشبكات اللاسلكية وشبكات الدخول الهاتفية **dial- in**.

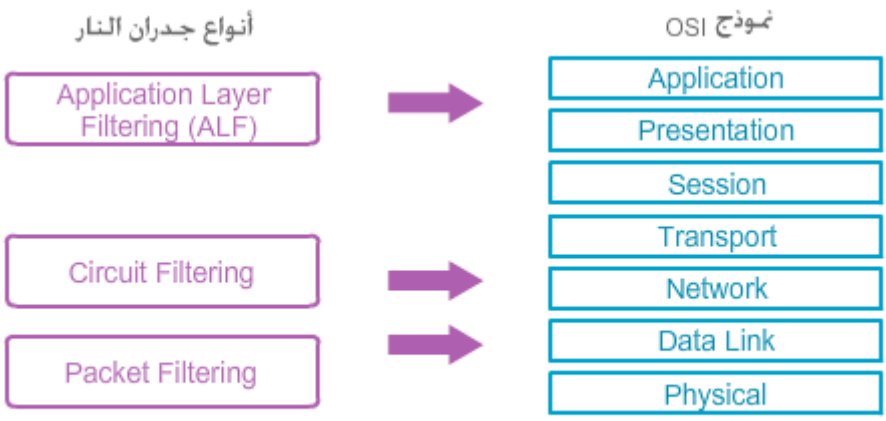
يمكن لجدار النار أن يمنع الولوج إلى الخدمات أوأن يسمح للمستخدمين أوالآليات بذلك بعد أن يستيقن منها. كما يراقب حركة المرور من وإلى الشبكة.

يدافع جدار النار عن الشبكة ضد من يحاول الولوج إلى الخدمات التي يجب أن تكون فقط متاحة داخلياً من خارج الشبكة. أيضاً يمكن أن يقيد الولوج إلى الخدمات الخارجية التي ليست ضرورية للمؤسسة أويمكن أن تسبب ضرراً لها وذلك من داخل الشبكة. كما يمكن لجدار النار أن يقرر توجيه حركة المرور الحساسة إلى شبكة خاصة افتراضية **virtual private network (VPN)**.

تؤمن الشبكة الخاصة الافتراضية الـ **VPN** اتصال آمن بين بوابات شبكات المؤسسة الفرعية التي لا تتصل ببعضها مباشرة. بحيث تتم حماية كل الاتصالات بين هذه البوابات بآليات تعمية تزيد من أمنها.

يمكن لجدار النار أيضا أن يقوم بترجمة عنوان الشبكة **(NAT)**. حيث تتم تخبئة الحواسيب الداخلية بعناوين خاصة خلف عنوان انترنت عام (حقيقي). كما يقوم بالعملية العكسية فيترجم العناوين العامة إلى عناوين خاصة لأجل الخدمات الداخلية.

يطبق الترشيح في جدران النار على ثلاث مستويات في بنية طبقات **OSI**.



توضع جدران النار على طبقات الشبكة

1. مرشحات الرزم

تعمل المرشحات على الطبقات 3 و4 من نموذج **OSI**. حيث تطبق قواعد قبول أورفض الرزم ولكل رزمة على حدى. وهي قواعد نموذجية تعتمد على عنواني الانترنت المصدر والهدف.وأرقام منافذ **TCP/UDP** للمصدر والهدف. يمكن تعريف قواعد مرور بالاتجاهين. كما يمكن توظيف جدار النار عن طريق موجه يرشح رزم **TCP/IP** حيث يختبر ترويسات **TCP/IP** لأجل كل رزمة تمر من خلاله.

من الصعب التعامل مع بعض البروتوكولات مثال:عندما يرسل الزبون طلب **ftp** إلى مخدم **ftp**، لا يستطيع جدار النار أن يربط بيانات الرزم القادمة من المخدم بالطلب المقابل لها.

يمكننا أن نعرف قواعد تغطية **blanket** لأجل كل الرزم القادمة على المنفذ **20**، أوكل الرزم المقدمة على المنفذ **20** ومن عناوين **IP** مرشحة بشكل متقدم. لكننا لا نستطيع تعريف قواعد بشكل ديناميكي. لكن هذا النوع من جدران النار لا يحدد ما إذا كانت الرزمة داخلة أوخارجة من الشبكة كما يمكن خداعه بسهولة واسطة**spoofed packets**.

2. مرشحات الرزم المعتمدة على الحالة Statefull packet filters

تتميز مرشحات الرزم المعتمدة على الحالة بأنها تفهم الطلبات **request** والاستجابات **replies**. فمثلاً، هي تعرف نموذج سلسلة **TCP** المفتوحة (**SYN،SYN-ACK، ACK**)، حيث تحدد القواعد بناءً على الرزمة الأولى وباتجاه واحد ثم تنشأ الحالة **state** بعد أول رزمة خارجة. وتعالج بقية رزم الاتصال آلياً بمعنى أنها تفحص عنواني المصدر والهدف والتطبيق المستخدم والعلاقة بين

الرزم الحالية والرزم السابقة خلال نفس الجلسة. يمكن لجدران النار المعتمدة على الحالة أن تدعم سياسات لمجال واسع من البروتوكولات أكثر من مرشحات الرزم البسيطة.
يمكن أن يتم الترشيح بواسطة الموجهات مما يعطي أداء عالي بتكلفة بسيطة. وأكثر من ذلك فمن السهل بناء هيكل آمن يقدم وظائف محدودة. أما أنظمة لينكس فتستخدم بنية جداول عناوبين الانترنت **iptables** لتعريف مجموعات قواعد ترشيح الرزم. وعادة تقيد سياسات الترشيح الإجبارية بمعاملات في ترويسات **TCP** و**IP**.

3. الوكلاء في طبقة الدارة Circuit – level proxies

تطبق وكلاء الدارات قواعد شبيهة بتلك التي تملكها مرشحات الرزم إلا أنها لا توجه الرزم . وتقرر القواعد ما هي الوصلات المسموح بها وما هي الوصلات الممنوعة . حيث تولد الوصلات المسموح بها وصلات جديدة من جدار النار إلى الهدف. نوعاً ما. يشبه هذا النوع في عمله المرشحات مرشحات الرزم المعتمدة على الحالة لكن أداؤه منخفض وهو قليل الانتشار . وبشكل عام يعتبر استخدام هذا النوع من المرشحات محدود

4. الوكيل في طبقة التطبيق

يمكن أن يكون جدار النار مخصص لأجل بروتوكول أوتطبيق معين وعندها يدعى بالوكيل **Proxy**. يقوم الوكيل بتقليد عمل كلاً من المخدّم والزبون من البروتوكول على جدار النار . فعندما يتصل الزبون إلى جدار النار، يتصرف الوكيل كمخدّم فيقيم الطلب لذلك يعتبر الوكيل مثالاً على "الاستدعاء المسيطر عليه" **controlled invocation** فوكيل البريد الالكتروني على سبيل المثال يمكنه الترشيح إلى الخارج أي فحص حركة المرور الخارجة للتأكد من خلوها من الفيروسات والدودات والحشو**spam**. إذا قبل طلب الزبون، فيتصرف الوكيل كزبون و يتصل بالمخدّم المطلوب. تعود الإجابة عبر جدار النار فتعالج وتفحص من قبل الوكيل. لا يرى العالم الخارجي من كائنات شبكتك سوى الوكيل. بينما يكون الوكيل كائن شفاف بالنسبة لمستخدمي شبكتك ما عدا في حالة الحذف مثل حذف ارتباطات البريد الالكتروني.
عادة ما يعمل وكلاء طبقة التطبيق على حواسيب مدعمة **hardened PC**. ويمكنها أن تقدم تحكم جيد على محتويات حركة المرور الداخلة والخارجة. وفي هذا المجال، فان وكيلات طبقة التطبيق تقدم مستوى عالي من الأمن عندما تهيأ بالشكل المناسب. لكن من سلبياتها أن كمية المعالجة كبيرة جداً لأجل كل اتصال وتحتاج تهيئة معقدة. وفي هذا المجال ينخفض مستوى الأمن الذي يقدمه وكلاء طبقة التطبيق، وقد سجلت العديد من نقاط الضعف في منتجات جدران

النار الموجودة حالياً. بشكل عام فان أداء وكلاء طبقة التطبيقات أقل منه لمرشحات الرزم وكلفتها أعلى. وأكثر من ذلك فانك ستحتاج إلى مخدم وكيل لأجل كل خدمة تريد حمايتها. لذلك فإن حل الوكيل لا يتناسب مع نموالطلب على الخدمات المقدمة على الانترنت.

يمكن تشبيه عمل مرشحات الرزم بعملية ترشيح مكالمات الهاتف وفقاً لرقم. بينما يمكن تمثيل عمل وكلاء طبقة التطبيق بعملية مراقبة مكالمات التلفون عن طريق الاستماع إلى المحادثة.

5. سياسات جدار النار

تقسم سياسات جدران النار إلى نوعين أساسيين:

سياسات السماح:permissive وهي تحدد لكل أنواع حركة المرور المسموحة وتغلق فقط بعض الخدمات الخطيرة مثل **telnet** أو**SNMP** أوأرقام منافذ معروف أنها تستخدم عادة لشن هجمات. وهنا من السهل الوقوع في الخطأ عندما تنسى إغلاق شيء ما كان عليك إغلاقه حيث يمكن استغلاله دون أن تدرك ذلك.

سياسات التقييد: وهي تغلق كل حركة المرور وتسمح فقط بحركة المرور المؤكد تحقيقها أهداف مفيدة، مثل **smtp،pop3،http** أو**SSH**. وهذه السياسة الأكثر أمناً فإذا نسيت فتح شيء تحتاجه وهوآمن يمكنك فتحه لاحقاً.

عادة تمثل السياسة الأمنية كقائمة **Access Control List ACL**. وتظهر مجموعة قواعد جدار النار المعيارية كما يلي:

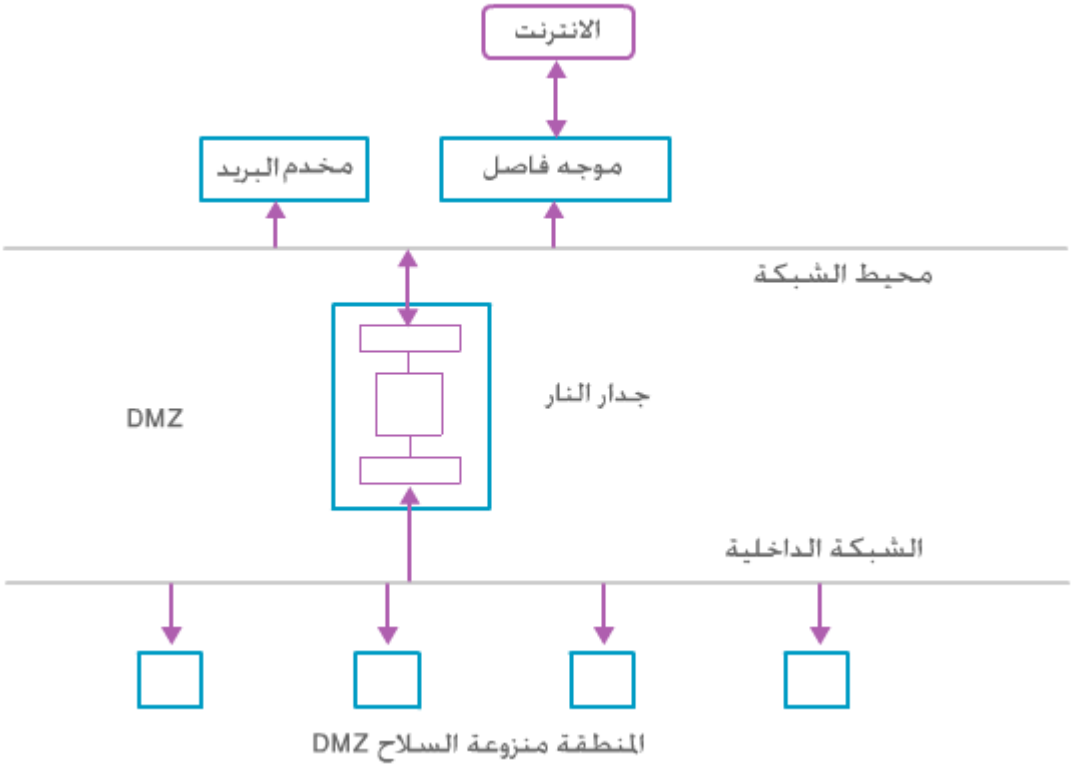
- السماح من الشبكة إلى الانترنت: **http، ftp، SSH،DNS**.
- السماح من أي مكان إلى مخدّم البريد: **SMTP،DNS**.
- السماح من مخدّم البريد إلى الانترنت: **DNS،SMTP**.
- السماح من الداخل إلى مخدّم البريد: **SMTP،pop3**.
- السماح برزم الرد (أي الرزم الناتجة كرد على اتصال سابق).
- **أغلق أي شيء آخر.**

من المهم الإشارة إلى أنه عند استخدام جدار النار في الواقع من المهم جداً تحديد وإدارة مجموعات القواعد.

6. الشبكات المحيطية Perimeter Network

يحتاج مخدّم البريد الولوج إليه من خارج الشبكة ليستلم البريد، لذلك يجب أن يتواجد على الجهة الداخلية لجدار النار. عندها فقط يمكن لجدار النار أن يحمي الدخول إلى مخدّم البريد من

الخارج. ويحتاج مخدّم البريد إلى الولوج إليه من الداخل ليستقبل البريد من الشبكة الداخلية . لذلك يجب أن يكون في الجهة الخارجية لجدار النار. كما يجب أن يتمكن جدار النار أن يوقف الديدان والفيروسات من الانتشار خارج شبكتك وكذلك منع خروج الوثائق السرية . يمكنك أن تحل هذه المسألة بإنشاء شبكة محيطية، وتسمى منطقة منزوعة السلاح **demilitarized Zone (DMZ)** تحتوي الخدمات التي تحتاج الولوج إليها من داخل وخارج جدار النار. وبالتالي يمكنك وضع مخدّم البريد في هذه المنطقة وكذلك تضع مخدّم الويب ومخدمات الأسماء.



7. قصور جدران النار ومشاكلها

- لا تستطيع جدران النار أن تحمي الشبكة من المهددات الداخلية.
- إغلاق الخدمات يمكن أن يسبب إزعاج للمستخدم.
- من الصعب دعم بعض البروتوكولات.
- جدران النار المرشحة للرزم لا تقدم ترشيح على أساس المحتوى. لذلك يمكن أن يمر بريد يحوي فيروسات.
- جدران النار غير معنية بنقاط الضعف في نظام التشغيل أوالتطبيقات.
- تستخدم اليوم العديد من الخدمات **http** على المنفذ 80 لذلك فمن الصعب تحديد حركة المرور الشرعية التي تستخدم هذا المنفذ.

- انتشار أنفاق البروتوكولات بمعنى إرسال بيانات لبروتوكول ما باستخدام بروتوكول آخر أبطل مفعول جدار النار.
- لا يمكن لجدار النار فحص حركة المرور المعماة.

7. كشف الاقتحام Intrusion detection

تستخدم آليات التعمية لمنع بعض الهجمات لكنها غير كافية. حيث يوجد أنواع جديدة من الهجمات مثل هجوم رفض الخدمة **denial-of-service**، حيث يمكن في مثل هذه الحالة أن تزيد التعمية من المشكلة. كما يمكن أن تفشل تقنيات الشبكات المحيطية وجدران النار ربما بسبب سوء في التهيئة والإعداد مما قد يسبب خرقاً أمنياً. عندها لا تملك أي من الآليات السابقة القدرة على كشف الهجمات أثناء حدوثها. لذلك وجد ما يسمى نظام كشف الاقتحام **Intrusion detection system (IDS)**.

يتألف نظام كشف الاقتحام **IDS** من مجموعة من الحساسات موجودة إما على الحواسب أو على الشبكة مهمتها جمع البيانات. تدار هذه الحساسات من قبل إدارة مركزية تحلل البيانات وتبلغ عن الاقتحامات وممكن أن تحفز ردود فعل معينة.

يوجد نوعان من طرق كشف الاقتحامات، ***كشف سوء الاستخدام*** **misuse detection** و***كشف الشذوذ*** **anomaly detection**.

يجب حماية الاتصالات بين الحساسات والإدارة، كما يجب حماية مخزن قاعدة بيانات التوقيع وسجلات الأداء. ويجب أيضا وضع خطة أوبرنامج للحصول على تحديثات التوقيع من مصنع كاشف الاقتحام الـ **IDS**. وإلا يمكن أن تتم مهاجمة والتلاعب بالكاشف نفسه. علماً انه يوجد نقاط ضعف في نظم الكشف يمكن استغلالها وخرق نظامك.

يوجد عدة أنواع لنظم كشف الاقتحام منها:

1. تقييم نقاط الضعف vulnerability assessment

حيث تم تقييم حالة الأمن في الشبكة وتجمع معلومات حول المنافذ المفتوحة وحزم البرمجيات المستخدمة وطبولوجيا الشبكة. ثم تحدد قائمة بنقاط الضعف مرتبة وفقاً لأولويتها. ويجب إجراء هذا الفحص دورياً لمعرفة ما يستجد من تهديدات لشبكتك.

2. كشف سوء الاستخدام misuse detection

يبحث كشف سوء الاستخدام عن أثر هجوم أوتوقيعه **attack signature**. فهذا الهجوم هونموذج من حركة المرور أوالفعاليات المشبوهة في سجلات الأداء. فمثلاً يمكن أن يحتوي التوقيع على عدد مرات آخر محاولات دخول فاشلة إلى حاسب حساس، أوعلى نموذج بتات في رزمة **IP** تدل على هجوم الفيضان **overflow attack** أوأنواع محددة من رزم **TCP SYN** وذلك يدل على هجوم طوفان **SYN**.

يمكن للكاشف أيضا أن يستشير السياسة الأمنية و قاعدة بيانات لنقاط الضعف المعروفة والهجمات لأنظمة المراقبة.

يجب التأكيد على أن هذه الأنظمة تعتبر جيدة بقدر ما تكون المعلومات في قاعدة بيانات التوقيع جيدة. فدوماً تكتشف نقاط ضعف جديدة وتستغل. لذلك يجب أن يحافظ المطورون على قاعدة بيانات الهجمات محدّثة دوماً كي يستطيع الزبائن تحديث قواعد بياناتهم ولتتمكن أنظمة الكشف **IDS** التي يستخدمونها من اكتشاف كافة أنواع الخروقات.

3. كاشفات الخرق المعتمدة على الشبكة Network-based- IDS

يبحث هذا النوع من الكاشفات عن تواقيع الهجوم في حركة مرور الشبكة. وعادة ما تعمل بطاقة الشبكة في النمط المختلط حيث تراقب وتحلل كل حركة المرور في الوقت الحقيقي و خلال انتقالها عبر الشبكة. حيث يستخدم مقياس لتحديد رزم الشبكة كمصدر للبيانات . يوجد ثلاث تقنيات شائعة لالتقط تواقيع هجوم:

- تطابق النموذج أوالتعبير أو**bytecode**.
- عتبة التردد أوالعبور (مثال. لتحديد محاولات مسح المنفذ).
- ارتباط الأحداث الأصغر (لم يطرح بعد كمنتج تجاري).

من المنتجات الشائعة لهذا النوع منتج **Snort** المطور في نطاق البرمجيات المفتوحة المصدر.

4. الكاشفات المبنية على أساس الحاسب المضيف\المخدم Host-based IDS

تبحث هذه الكاشفات عن تواقيع الهجوم في سجلات الدخول إلى الحواسب. وهوأيضا يتحقق من مجاميع الاختبار **checksums** لملفات مفاتيح النظام المنفذة في فترات دورية.

5. جرار العسل Honypots

هي مصادر تستخدم لخداع المهاجم ولجمع المعلومات والأدلة عن نشاطات المخترقين . فهي مصممة بحيث تحاكي النظم الحقيقية ولا تحتوى أي معلومات حقيقية. ومن المهم مراقبة كل النشاطات في هذه المنطقة وبالتعريف فان كل نشاط في هذه المنطقة هو هجوم.

أسئلة وتمارين

1. يربط بروتوكول **ARP** العناوين العتادية بعناوين الانترنت. ويمكن أن يتغير هذا الربط مع الوقت. تحتفظ كل عقدة شبكة بذاكرة **cash** تحوي بيانات**ARP** الرابطة بين عناوين الانترنت وعناوين العتاد. لكن تنتهي صلاحية محتويات هذه الذاكرة بعد عدة دقائق . وعندما تحاول العقدة إيجاد عنوان العتاد لعنوان انترنت، تبحث أولا في ذاكرتها فان لم تجده. تقوم ببث طلب **ARP** ويحتوي على عنوان انترنت وعنوان عتاد العقدة نفسها بالإضافة إلى عنوان انترنت العقدة المطلوب إيجاد عنوان عتادها. ترد العقدة صاحبة عنوان الانترنت بعنوان العتاد الخاص بها. وتهمل بقية العقد طلب **ARP**. كيف يمكن أن تتم عملية تزوير طلب **ARP**، وما هي الإجراءات الدفاعية التي يمكن اتخاذها ضده.
2. الزبون **A** (**a.example.org**) يريد الوصول إلى المخدم **B** المعروف باسم ال **DNS** **b.example.org**. يطلب الزبون عنوان الانترنت ل **B** من مخدم **DNS** المحلي. إذا لم يكن المخدم المحلي يحتفظ بهذه المعلومات فهو يستعلم من مخدم **DNS** المخول لأجل **B**. يحتوي الاستعلام على رقم تسلسلي طوله 16 بت. يقوم مخدم **DNS** المحلي بتحديث ذاكرته **cache** إذا استقبل جواب مع الرقم التسلسلي الصحيح. و تهمل بقية الردود . افترض أن مهاجم يرسل بنفس الوقت إلى مخدم **DNS** الخاص ب **A** استعلامات كاذبة عن عنوان انترنت **B** وردود كاذبة من مخدم **DNS** الخاص ب **B** وتحمل عنوان انترنت خاطئ ل **B**. كيف بسرعة سينجح هذا الهجوم في خداع مخدم **DNS** الخاص ب **A** ليقبل عنوان انترنت **B** الكاذب؟ (يمكن لمخدمات **DNS** أن تتعامل مع عدة عمليات بحث على التوازي).
3. يفترض أن تكون العقد التي تشغل بروتوكولي **IPsec** و**SSL** عقد آمنة. ما هي آليات الأمن الإضافية التي تحتاج إعدادها على هذه العقد لجعل هذا الافتراض صحيح
4. ما هي الميزات الأمنية التي تتوقعها من نظام البريد الالكتروني الآمن، ومن الحواسيب التي تشغل نظام بريد الكتروني آمن؟ ما هي طبقة البروتوكول الأكثر مناسبة لمثل هذه الخدمة الأمنية؟ في جوابك ميز بين الخدمات التي تريد تقديم إمكانية تخبئة المصدر **anonymity** وتلك التي لا تقدم هذه الإمكانية.
5. اختبر تضمين نفق **IP** ضمن **IP** في تصميم جدار النار المرشح للرزم.
6. تعتبر الانترنت مصدر الإصابة بالفيروسات. بالمقابل تقوم جدران النار بحماية الشبكة الداخلية من التهديدات الخارجية. هل تستطيع جدران النار الحماية ضد الإصابة بالفيروسات. عند الإجابة خذ بالحسبان مختلف أنواع جدران النار.كيف يمكن للحماية بالتعمية في طبقة **TCP/IP** أوفي طبقة التطبيقات أن تؤثر في قدرة جدران النار على الحماية ضد الفيروسات.
7. تسمح شركة لموظفيها باستخدام الحواسيب المحمولة في البيت وخلال السفر. اقترح بنية أمنية لحماية الحواسيب المحمولة، وشبكة الشركة الداخلية.

الفصل الثالث: أمن النقال

1. مقدمة

في الأجيال الأولى لخدمة الهاتف النقّال عانت هذه الخدمة من مشاكل كثيرة في نوعية الخدمة وأيضاً في المستوى المتدني للأمن من حيث الاستيقان وسرية المكالمة.

2. نظام الهاتف النقال GSM

في مواجهة تدني المستوى الأمني لخدمة الهاتف النقّال في أجيالها الأولى . تكونت مجموعة دراسة تدعى **Group Special Mobile GSM** أو **Global System for Mobile Communications** لتوصيف الجيل الثاني شبكة الهاتف المحمول.

ومن الأهداف الأمنية لهذه الشبكة الرقمية نذكر:

1. منع الاستخدام غير الشرعي لخدمة الهاتف النقّال.
2. حماية حركة المرور الصوتية.
3. حماية بيانات الإشارة على قناة الراديو.
4. دعم للأمن الفيزيائي حيث يجب أن يكون ممكناً ملاحقة تجهيزات الهاتف النقّال المسروقة.

مع ملاحظة أنه حالما تكون حركة المرور على الشبكة الثابتة لا تقدم أي حماية بالتعمية.

1. مكونات

يوجد لكل مستخدم لخدمة الهاتف النقال **GSM** اشتراك في شبكته الرئيسية وفيما يلي أهم المفاهيم المستخدمة في هذه الخدمة:

- **الشبكة المزارة visited network:** وهي الشبكة التي تُطلب منها الخدمة.
- **محطة الهاتف النقّال Mobile Station MS.**
- **جهاز الهاتف النقّال Mobile Equipment ME.**
- **بطاقة هوية المشترك Subscriber Identity Module SIM:** وهي بطاقة ذكية تنجز عمليات التعمية وتخزن المفاتيح ذات العلاقة، كما يمكن أن تحتوي بعض المعلومات الشخصية للمشترك مثل دفتر العناوين الشخصي.

أما على جهة الشبكة فيوجد:

- **المحطة الأساسية Base Station BS.**
- **مركز التحويل الهاتف النقّال Mobile Switching Center MSC.**

- **سجل أماكن الموقع الرئيسي للمشترك Home Location Register HLR:** يقوم كل من سجل أماكن الموقع الرئيسي للمشترك **HLR** وسجل موقع الزائر **VLR** بإدارة معلومات توجيه وتطواف المكالمة **Call Rooming** بين الخلايا.
- **مركز الاستيقان Authentication Center AuC:** يدير مركز الاستيقان **AuC** المعلومات المرتبطة بأمن المشترك.
- **سجل موقع الزائر Visitor Location Register VLR:** يقوم كل من سجل أماكن الموقع الرئيسي للمشترك **HLR** وسجل موقع الزائر **VLR** بإدارة معلومات توجيه وتطواف المكالمة **Call Rooming** بين الخلايا.

وتدار العلاقة بين مختلف مقاسم الشبكة بواسطة اتفاقات مستوى الخدمة **Service Level SLAs Agreements**.

هوية المشترك الدائمة **GSM** هي **International Mobile Subscribe Identity IMSI**. ويتشارك المشترك وكل من سجل أماكن الموقع الرئيسي للمشترك **HLR** ومركز الاستيقان **AuC** بمفتاح استيقان طوله **128** بت يرمز له بـ K_i. ويخزن هذا المفتاح على بطاقة المشترك **SIM** المفتاح K_i, وكذلك على الـ **TMSI** (سنشرحه لاحقاً) وهوية المشترك الدائمة **IMSI** ومفتاح التعمية الحالي K_c طوله **64** بت. كما توظف في هوية المشترك **SIM** خوارزميات A_3 وA_8 (سنشرحه لاحقاً)، يتم التحكم بالدخول إلى **SIM** باستخدام معرف شخصي **PIN(personal identification number)** حيث تقفل الـ **SIM** بعد ثلاثة محاولات دخول فاشلة. ويمكن أن يفك قفلها باستخدام مفتاح فك قفل شخصي **PUK(personal unblocking key)**.

2. الهوية المؤقتة لمشترك الهاتف النقّال Temporary Mobile Subscriber Identity TMSI

- عندما تتصل محطة الهاتف النقّال **MS** بالشبكة يجب أن تعرف عن نفسها بطريقة ما . فإذا استخدمت هوية ثابتة في كل مكالمة فسيكون ممكناً ملاحقة مكان المشترك حتى لوعميت حركة مروره. لذلك وكخطوة باتجاه سرية أفضل للمشترك ترسل هوية المشترك الدائمة **IMSI** غير معماة فقط عندما تقوم محطة الهاتف النقّال **MS** باتصال مبدئي بشبكة الـ **GSM**.
- بعد ذلك تحدد هوية المشترك المؤقتة **TMSI** وتستخدم في كل مراكز التبديل **MSC**. وهكذا فمن الطبيعي أن لا تستخدم هوية المشترك الدائمة **IMSI** للعنونة في مسير موجات الراديو.
- يحافظ سجل موقع الزائر **VLR** على علاقة من هوية المستخدم المؤقتة **TMSI** و معرف موقع المجال إلى هوية المستخدم الدائمة **IMSI**، وبالتالي عندما يتحرك المشترك من مجال مركز تبديل **MSC** إلى آخر تحدد هوية مستخدم مؤقتة **TMSI** جديدة . وتحتفظ سجلات موقع الزائر على مطابقة دائماً بين الهوية الدائمة **IMSI** والهوية المؤقتة **TMSI**.
- وبالخلاصة فإن حماية معلومات موقع مشترك الهاتف النقال هو موضوع أمني يخص خدمات النقال. حيث يسبب استخدام المعرفات الشخصية الثابتة لكشف موقع المستخدم.

3. خوارزميات التعمية

يستخدم نظام الهاتف الجوال **GSM** التعمية التناظرية للتعمية والاستيقان من المشترك. و يعتمد ثلاثة خوارزميات تعمية هي:

1. خوارزمية الاستيقان **A3**.
2. خوارزمية التعمية **A5** وتستخدم لتعمية إشارات التحكم وبيانات المستخدم.
3. خوارزمية توليد المفاتيح **A8**.

لم تنشر هذه الخوارزميات لكنها تسربت أوأستنتجت.

- تكون خوارزميتا **A3** و**A8** متشاركتان بين المشترك والشبكة الرئيسية، لذلك تستطيع كل شبكة أن تختار خوارزمياتها **A3** و**A8** الخاصة. فقط يجب أن يتحدد شكل دخلها وخرجها.
- تحسب الخوارزميات **A3** و**A8** إجابة **RES** ومفتاح تعمية **Kc** من قيمة عشوائية **RAND** والمفتاح **Ki**.

- يجب أن تبقى مدة المعالجة تحت قيمة محددة مثال: **500 msec** لأجل الخوارزمية **A8**.
- إحدى الخيارات لأجل **A3/A8** هي الخوارزمية **COMP128**. هذه الخوارزمية ضعيفة وقابلة لهجمات تسترد المفتاح **Ki** من البطاقة **SIM**، يمكن باستخدام هذا المفتاح نسخ بطاقة **SIM**.
- كما يجب أن تكون الخوارزمية **A5** متشاركة بين كل مقاسم الشبكة. و يجب أن تكون معيارية. ويوجد نسختان منها الأولى **A5/1** وأخرى أقل أمناً هي **A5/2**.

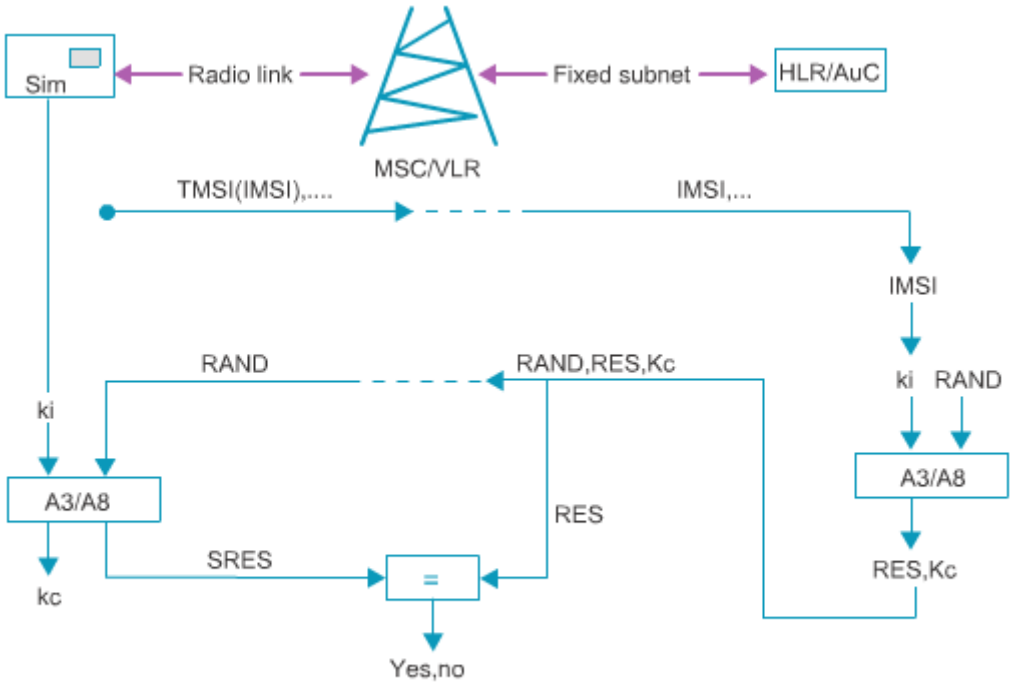
وبالرغم من عدم نشر مواصفات هذه الخوارزميات إلا انه سجل اختراقات لها.

4. الاستيقان من هوية المشترك

تبدأ عملية استيقان المشترك من قبل الشبكة في الحالات التالية:

1. تسجيل أول دخول له إلى الشبكة.
2. بعد إعادة تشغيل مركز التحويل الهاتف النقّال وسجل موقع الزائر.
3. عندما يدخل المشترك إلى خدمة ما مثل بدء أوإنهاء مكالمة.
4. عندما يريد المشترك أن يغير المعلومات المتعلقة به في سجل موقع الزائر **VLR** أوسجل أماكن الموقع الرئيسي للمشترك **HLR**، مثل تحديث الموقع بما يغير في سجل موقع الزائر**VLR** .
5. في حالة حدوث عدم تطابق بالرقم التسلسلي المستخدم في عملية التعمية.

يصف الشكل التالي حركة الرسالة خلال الاستيقان.



GSM

تحتوي الرسالة الابتدائية من جهاز الهاتف النقّال **ME** إلى سجل موقع الزائر **VLR** على بطاقة هوية المشترك **SIM** وهوية المشترك المؤقتة **TMSI** وهوية المشترك الدائمة **IMSI**. يربط سجل موقع الزائر **VLR** هوية المشترك المؤقتة **TMSI** إلى هوية المشترك الدائمة **IMSI** وتمرر هوية المشترك الدائمة **IMSI** إلى سجل أماكن الموقع الرئيسي للمشترك **HLR** ومركز الاستيقان **AuC** عبر الشبكة الثابتة.

1. يولد مركز الاستيقان **AuC** قيمة عشوائية طولها **128** بت .
2. يحسب الإجابة **RES=A3(Ki, RAND)**، و مفتاح تعمية طوله **64** بت **Kc=A8(Ki,RAND)**.
3. ترسل الثلاثية **(RAND,RES,Kc)** إلى سجل موقع الزائر **VLR**.
4. يقوم سجل موقع الزائر **VLR** بتخزين القيمة العشوائية **RAND** و المفتاح **Kc** وتمرر القيمة العشوائية **RAND** إلى محطة الهاتف النقّال **MS**. يعتبر المفتاح **Kc** ذو قيمة في مجال مكاني واحد.
5. في محطة الهاتف النقّال **MS**، تحسب النتيجة **SRES=A3(Ki, RAND)**، في بطاقة هوية المشترك **SIM** .

6. ترسل **SRES** بواسطة محطة الهاتف النقّال **MS** ثانية إلى سجل موقع الزائر.
7. يقوم سجل موقع الزائر بمقارنة القيمتان **SRES** و**RES**. ويعتبر الاستيقان ناجحاً إذا تطابقت القيمتان.

لتسريع عمليات الاستيقان المتلاحقة في الشبكة المزارة، يرسل مركز الاستيقان **AuC** عدة ثلاثيات **(RAND,RES,Kc)** إلى سجل موقع الزائر، ثم تستخدم تباعاً لاستيقان المشترك.

5. التعمية

بشكل عادي تكون كل حركة المرور (صوتية، أوغير صوتية) عبر شبكة الراديومعماة. و تقوم البنية التحتية بتحديد خوارزمية التعمية التي ستستخدم، أوإذا كنا سنوقف التعمية و بالتالي عدم تقديم حماية للسرية. وعند الضرورة، ترسل محطة الهاتف النقّال **MS** إلى الشبكة بخوارزميات التعمية التي تدعمها، وعندها تقوم الشبكة باختيار إحداها بالاعتماد على ترتيب الأولويات المسبق لديها، وبحيث تكون قادرة على دعمها، ثم ترسل اختيارها إلى محطة الهاتف النقّال **MS**.

تسمح ميزة مؤشر التعمية **ciphering indicator** لجهاز الهاتف النقّال **ME** بتحديد فيما إذا كانت التعمية غير مفعلة وإعلام المستخدم بذلك. يمكن عدم تفعيل هذه الميزة من قبل مقسم الشبكة الرئيسي عن طريق إعداد حقل البيانات الإداري **EFAD** في بطاقة هوية المشترك **SIM** بالشكل المناسب، فإذا لم يلغى تفعيلها في بطاقة هوية المشترك **SIM** سترسل إلى المستخدم تنبيه كلما حدث اتصال غير معمى.

معمية A5:

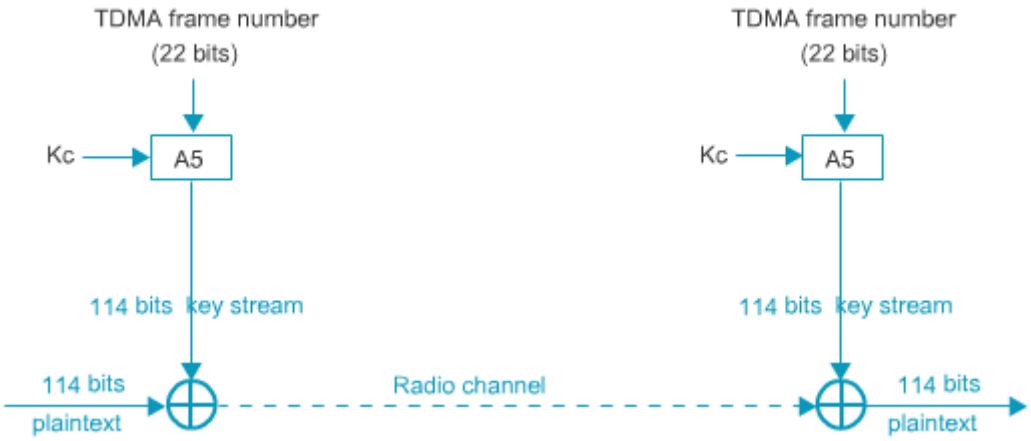
هي معمية جدولية تطبق على إطارات البيانات **frames** من الطول **114** بت.

يحسب المفتاح لأجل كل إطار من المفتاح السري **Kc(64 bit)** ورقم الإطار الذي طوله **22** بت.

بما أن وصلات الراديو يصاحبها ضجيج يفضل استخدام المعميات الجدولية وذلك لأن:

- في حالة المعميات الكتلية فإن وجود بت واحد خاطئ في الإطار المعمى يؤثر على مجمل الإطار البسيط.
- بينما في المعميات الجدولية البت الخاطئ في الإطار المعمى يؤثر على فقط على بت واحد من الإطار البسيط.

لكن وفق معايير اليوم يعتبر الطول **64** بت للمفتاح قصير نوعاً ما.



6. دروس مستفادة

يمكن أن تتعلق مميزات الطبقة الفيزيائية باختيار خوارزميات التعمية.

7. الخدمات المعتمدة على الموقع location-based Service

يسجل نظام **GSM** مواقع تجهيزات الهاتف النقّال.

لذلك يمكن لهذه المعلومات أن تقدم خدمة مبنية على الموقع **LBS** مثل:

- معلومات حركة المرور لسائقي السيارات.
- خدمات مواقع طارئة حيث تقوم الخدمة بتحديد موقع جهاز الهاتف النقّال **ME** الذي يتصل برقم الطوارئ. هذه الخدمة إجبارية في بعض البلاد. فمثلاً قوانين الولايات المتحدة تشدد في خدمة موقع الجوال على مجال دقة **125m**.

8. ميزات ومساوئ GSM

ميزات تقنية GSM:

تتميز تقنية **GSM** بالميزات التالية:

1. لا يرسل الاستيقان **challenge-response** أي معلومات سرية بشكل غير واضح. لذلك فقد أزيلت إحدى أهم نقاط الضعف في شبكات الجيل الأول.
2. تعمى حركة المرور الصوتية على شبكة الراديو لكن المكالمات ترسل بشكل واضح (غير معمى) بعد المحطة الأساسية **BS**.
3. توجد تعمية اختيارية لبيانات الإشارة **SIGNALING DATD** لكن يمكن لجهاز الهاتف النقّال **ME** أن يطلب عدم تفعيل هذه التعمية.

4. يوجد بعض الحماية لخصوصية الموقع باستخدام مفهوم **TMSI** لكن يمكن للمهاجمين أن يستخدموا ما يدعى لاقطات **IMSI** التي تطلب من **MS** أن تعود إلى الاستيقان الابتدائي باستخدام **IMSI**.
5. توجد حقوق دخول للوكالات القانونية إلى سجلات بيانات حركة المشتركين.
6. يوجد تمايز بين هوية المشترك **IMSI** وهوية الأداة **IMEI** لذلك يمكن تتبع الأدوات المسروقة.

مساوئ تقنية GSM:

يوجد عدد من الانتقادات الموجهة إلى **GSM** أهمها:

1. عدم نشر المعميات وبالتالي فحصها واختبارها من قبل الجمهور.
2. تقديم استيقان أحادي الجانب من المشترك إلى الشبكة، ولا يوجد استيقان للشبكة المزارة إلى المشترك.

9. دروس مستفادة

لا تضيع جانب هجمات مستوى التطبيق عندما تحلل الخدمات الأمنية المقدمة إلى المستخدم.

3. نظام الاتصالات النقّالة العالمي UMTS Universal Mobile Telecommunication System

بدأ العمل في الجيل الثالث من نظم اتصالات الجوال في بداية التسعينات. إحدى هذه النظم هو نظام الاتصالات النقّالة العالمي **UMTS Universal Mobile Telecommunication System**.

تشبه بنية الأمن في **UMTS** بنية الأمن في **GMS**، حيث يمتلك المشترك **UMTS** معيار على جزء تعريف عالمي للمشترك وهو جزء من أداة المستخدم **UE** ومفتاح سري متشارك مع الـ **AuC** في الشبكة الرئيسية.

تقوم أداة المستخدم **UE** بطلب الخدمات من الشبكة المزارة.

1. هجمات المحطة الرئيسية المزيفة False Base Station Attacks

المشكلة: في نظام **GSM** لا يقوم جهاز الهاتف النقّال **ME** بالاستيقان من الشبكة . لذلك لا يستطيع جهاز الهاتف النقّال **ME** أن يعرف فيما إذا كان المحطة الأساسية **BS** مزيفة . هو من

يطلب من أن يجري الاستيقان باستخدام هوية المشترك الدائمة **IMSI** أوأن يلغي تفعيل التعمية أوأن المحطة الأساسية **BS** حقيقية (أصيلة)..

الحل: للتعامل مع هذه المشكلة، يمكن أن نقترح عملية استيقان متبادلة بين جهاز الهاتف النقّال **ME** والشبكة.

لكن يوجد عدة أسباب تمنع هذا الحل الساذج:

1. سبق وقام جهاز الهاتف النقّال **ME** بتأسيس علاقة مباشرة مع الشبكة الرئيسية فقط لذلك فالاستيقان من الشبكة المزارة ليس عملي.
2. تعميم بروتوكول **challenge-response** ليقدم استيقان متبادل لن يمنع هجوم **BS** المزيف. فالمهاجم يحتاج فقط إلى الانتظار حتى يتم **BS** الأصلي عملية الاستيقان ثم يستخدم معلومات هذا الاتصال والخاصة بعملية الاستيقان وذلك بإرسال إشارة أقوى من إشارة **BS** الحقيقي.
3. إن آليات الاستيقان بالتعمية محدودة الإمكانيات عند استخدامها في القنوات مرتفعة الضجيج (مثل شبكات الراديو). فأي بت خاطئ في الرسالة سيفشل عملية الاستيقان.

2. خوارزميات التعمية

- يمكن أن تكون دوال الاستيقان f_1 وf_2، ودوال توليد المفتاح f_3 وf_4 وf_5 خاصة بمزود الخدمة.
- كما يوصى باستخدام معمية كتلية طول كتلتها **128** بت ومفتاحها **128** بت في نواته.
- مع التنويه لضرورة أن تكون خوارزمية التعمية لوصلة الراديو و خوارزمية اختبار السلامة لبيانات الإشارة على شبكة الراديو معياريتين.
- وقد تبنت معايير **UMTS** خوارزمية **KASUMI**. وهي معمية **feistel** بثمانية دورات طول كتلتها **64** بت وطول مفتاحها **128** بت. تستخدم هذه الخوارزمية في نمط **OFB** للتعمية، بينما تستخدم في نمط **CBC-MAC** لحماية سلامة المعلومات . علماً أن كل الخوارزميات التي تستخدمها **UMTC** منشورة.

3. الاستيقان والاتفاق على المفاتيح في UMTS Authentication and Key Agreement AKA

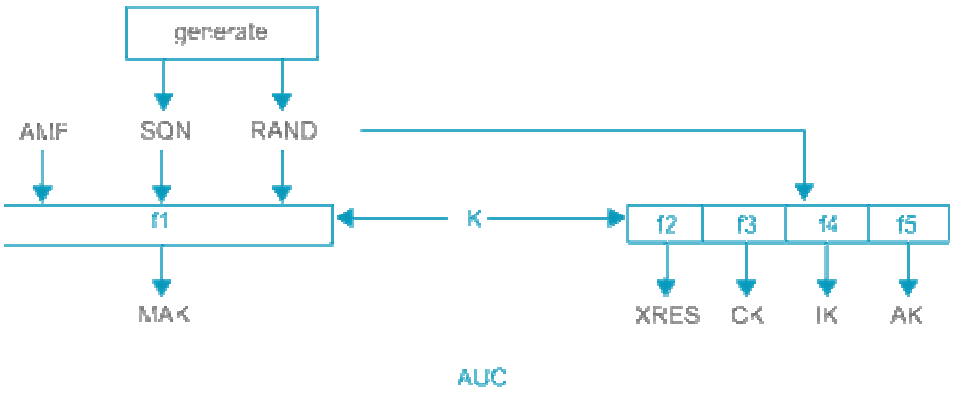
يتشارك المركز الرئيسي **AuC** والمشترك **USIM** بمفتاح سري **K** طوله **128** بت مع المحافظة على رقم تسلسلي للتزامن **SQN**.

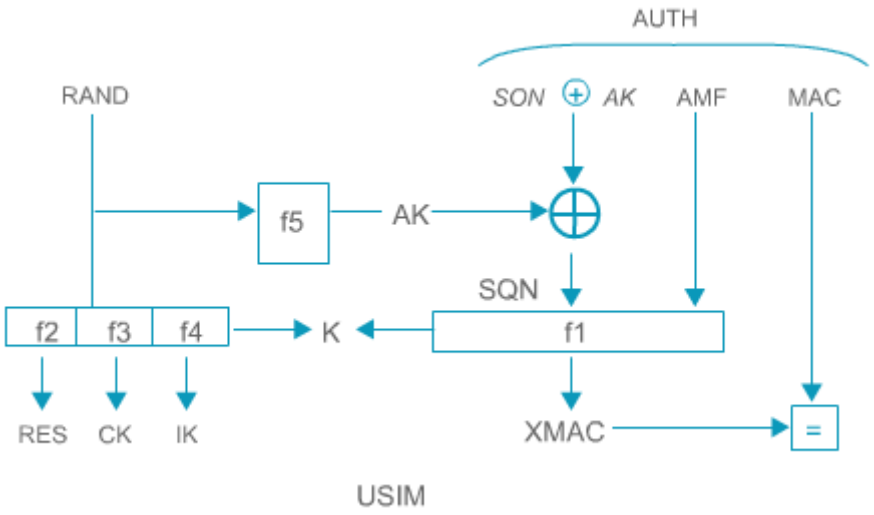
عند الإجابة على طلب استيقان. يولد مركز الاستيقان **AuC** الأرقام التالية:

- رقم عشوائي **RAND**.
- إجابة متوقعة **XRES=f2(RAND,K)**.
- مفتاح تعمية **CK=f3(RAND,K)**، طوله 128 بت.
- مفتاح سلامة **IK=f4(RAND,K)**، طوله **128** بت.
- مفتاح **ANONYMITY AK=f5(RAND,K)**، طوله **48** بت.
- رسالة الاستيقان المرمزة **Message Authentication Code MAC** للرقم العشوائي **RAND**، والرقم التسلسلي **SEQ**، وحقل إدارة الاستيقان**AMF** (والذي يمكن أن يحتوي زمن حياة المفتاح).
- القيمة **AUTN = (SQN ⊕ AK, MAC)** .

يرسل مركز الاستيقان **AuC** شعاع الاستيقان المكون من **(RAND,AUTN,XRES,CK,IK)** إلى **VLR/SGSN**.

يخزن **VLR/SGSN** القيم **RAND,AUTN,XRES,CK,IK)** لأجل المشترك **IMSI** و يمرر قيمة **RAND** و **AUTN** إلى أداة المستخدم **UE**.





بناءً على قيم **RAND** و**UTN**، يقوم **USIM** أولاً بحساب قيم **K)،AK=*f*5(RAND** و $SQN = (SQN \oplus AK) \oplus AK$. ثم يحسب رسالة الاستيقان المرمزة **XMAC** باستخدام **RAND**، **SQN** و**AMF**. وتقارن هذه القيمة مع قيمة رسالة الاستيقان المرمزة **MAC** المستقبلة. وفي حال التطابق فإن هذا يؤكد على أن **RAND** و**AUTN** مولدين من قبل **AuC** الرئيسي. وفي حال عدم التطابق يقوم المشترك **USIM** بإيقاف عمل البروتوكول. ولا تستعمل هذه العمليات عملية استيقان من شبكة الخدمة.

وبالعودة إلى حالة المطابقة فان **USIM** يتابع البروتوكول ويختبر شرعية القيمة **SQN** لاكتشاف هجمات من نوع **REPLAY**، وفي حال فشل هذا الاختبار، يبلغ إلى سجل موقع الزائر **VLR** خطأ تزامن. وبذلك يكون هجوم المحطة الأساسية **BS** المزيف قد مِنع باستخدام عمليتين الأولى هي عبارة عن عملية تحديث **FRESHNESS** لمفتاح والثانية هي عملية حماية سلامة بيانات التحكم، وليس بالاستيقان من شبكة الخدمة.

أخيراً. يقوم **USIM** بحساب الإجابة **RES** والمفاتيح **CK** و**IK** من **RAND** و مفتاحه السري **K**، ويعيد الإجابة **RES** إلى سجل موقع الزائر **VLR**. فيقوم سجل موقع الزائر **VLR** بمقارنة **RES** مع **XRES** لضمان عملية الاستيقان من **USIM**.

4. أمن الهاتف النقّال المبني وفق IPv6

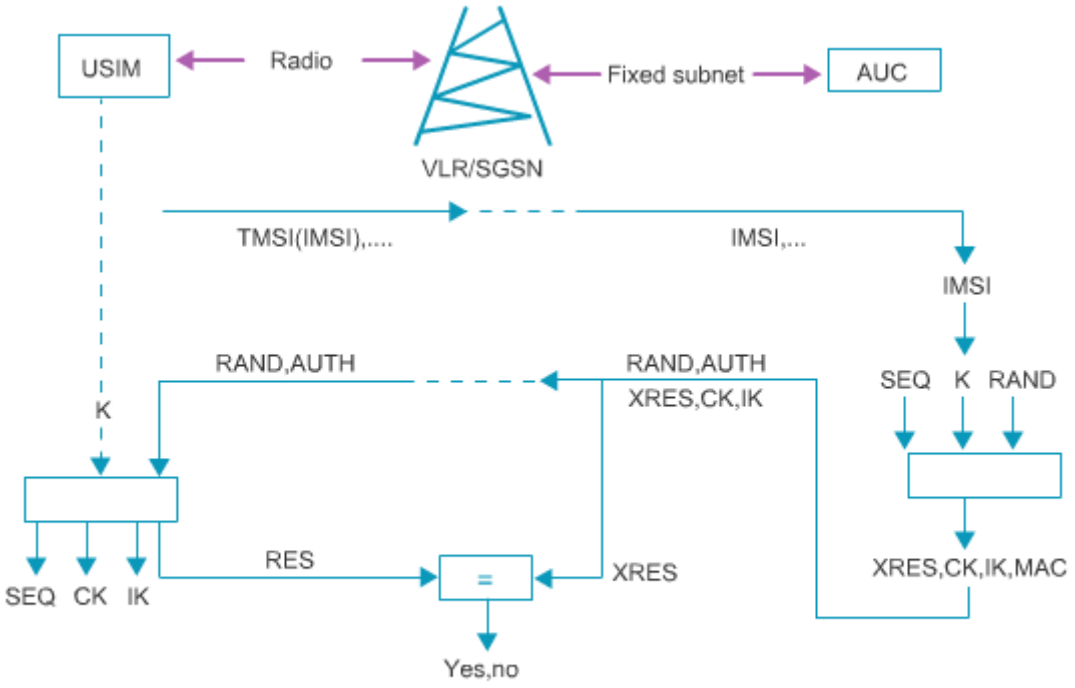
كانت المشكلة الأمنية بالنسبة إلى **GSM** و**UMTS** هي التحكم بالدخول إلى الخدمات عندما يكون المستخدم هونقّال ولم يؤسس اتصال آمن مع مقسم **operator** الشبكة حيث تقدم الخدمة . سنستخدم في هذه الفقرة مفهوم نقّال **IPv6** لشرح نوع آخر من مشاكل الهاتف النقّال.

عندما يتغير موقع أداة نقّال كيف يمكن لبقية العقد أن تتأكد من صحة المعلومات الجديدة حول الموقع الجديد. الحل المعياري لهذه الحالة هواستخدام عملية الاستيقان. لكنك ستواجه مشكلتان.

الأولى أنه للاستيقان من رسالة، علينا معرفة هوية المرسل، لكن في رزم **IP** فان هوية المرسل هي عنوان **IP**. وللتحقق بأدوات التعمية من صحة العنوان، عليك أن تربط هذا العنوان بمفتاح تعمية، وضوحاً سيكون هذا المفتاح هو**PKI**، لكن حالياً لا تستخدم التعمية بالمفتاح العام في الهاتف النقّال وهذا الأمر لن يتغير في المدى المنظور.

الثانية، إن الاستيقان من مصدر البيانات لا يحل المشكلة. في حالة الشبكات السلكية كان يمكن للعقدة أن تكذب بشأن هويتها.مثلاً يمكن لـ **A** أن يدعي انه **B** لكي يستقبل الرسائل الموجهة إلى **B**. بينما يمكن لعقدة الهاتف النقّال أن تكذب بشأن هويتها وموقعها. حيث يمكن لـ **A** أن يدعي أن **B** في موقعه (موقع **A**) لذلك فحركة المرور الموجهة إلى **B** سيستقبلها **A**. أويمكن لـ **A** أن يدعي أن **B** في موقع ليس موجود فعلياً وبالتالي تضيع حركة المرور الموجهة إلى **B**. يمكن لكلا الهجومين أن يتوقفا بالتحقق من أن **B** هومن يعطي المعلومات عن موقعه.

يوجد نوع آخر من هجمات حجب الخدمة **deneal-of-sevice**. حيث يمكن لـ **A** أن يدعي انه في موقع **B**، لذلك فحركة المرور الموجهة إلى **A** ستذهب فعلياً إلى **B**. وعندها يمكن لـ **A** أن ينفّذ هجوم القنبلة **bombing attack**، حيث يقوم **A** بطلب كم كبير من حركة المرور سيوجه فعلياً إلى **B**. في هذه الحالة لن يكون كافياً التحقق من أن **A** هوفعلاً من يعطي المعلومات عن موقعه.



UMTS

تعد هجمات القنبلة جزءاً من مفهوم التحكم بالتدفق. ففي هذا النوع من الهجوم ترسل البيانات إلى الضحية التي لم تطلبها أصلاً. وهنا لا يكفي التحقق من مصدر البيانات وإنما يجب أيضا التحقق من أن المستقبل يرغب فعلاً باستقبال البيانات. وبالتالي سنحتاج هنا إلى التخويل **Authorization** من الهدف الذي سنرسل البيانات إليه بدل من الاستيقان من مصدر الطلب.

يعتبر موضوع التحكم بالتدفق من اختصاص طبقة الإرسال **transport layer** لكن كان القرار بمعالجة هذا المفهوم في طبقة **IP** حتى لا يتم تغيير بروتوكولات طبقة الإرسال.

1. دروس مستفادة:

لقد غيرت قابلية التنقل **mobility** قواعد الأمن. ففي الشبكات الثابتة يمكن للعقد أن تستخدم هويات مختلفة في الجلسات المختلفة (مثل **NAT** في **IPv4**). لكن في كل جلسة تكون الهوية الحالية هي الموقع الذي ترسل إليه الرسائل. بينما في العقد الهاتف النقّالة فانه علينا التعامل مع الهوية والموقع كمفهومين منفصلين.

2. نقّال

يحدد عنوان **IPv6** عقدة أوموقع **IPv6**. أما عنوان **IPv6** الهاتف النقّال **MIPv6** فيتألف من **128** بت، تحدد البتات الـ **14** الأولى منها بادئة الشبكة الفرعية (الموقع) وأما البتات الباقية فتحدد معرف الواجهة **interface ID** (هوية ضمن الموقع المحدد بالجزء الأول). لا تختلف عناوين **IPv6** للعقد المتنقّلة عنها للعقد الثابتة. يمكن للعقدة المتنقّلة أن تعنون دائماً بعنوان مقرها الرئيسي **home address HoA** سواء كانت مرتبطة بمقرها الرئيسي حالياً أوأنها بعيدة عنه.

ويعتبر عنوان المقر الرئيسي هوعنوان **IP** للعقدة المتنقلة المعطى لها خلال ارتباطها بشبكتها الرئيسية. وتتمتع العقدة المتنقلة وأداة شبكتها الرئيسية بإعداد مسبق لأمن **IP** وذلك بتشكيل نفق آمن. فمعايير تصميم **IPv6** حددت استخدام بروتوكول **ESP** لحماية معلومات التحكم **MIPv6** بين الهاتف النقّال وأداة الشبكة الرئيسية. ولأن عقدة الهاتف النقّال متصلة ببعض الوصلات الغريبة والمختلفة عن شبكتها الرئيسية. فهي أيضا قابلة للعنونة بعنوان **CoA** **care-of-address**. **CoA** هوعنوان **IP** حيث بادئة الشبكة فيه من الشبكة الغريبة المزارة.

5. الشبكات اللاسلكية WLAN

الشبكة المحلية اللاسلكية **WLAN** هي تقنية للشبكات المحلية اللاسلكية المعرفة بالمعايير **IEEE802.11**.

يهدف الأمن في هذا النوع من الاتصالات إلى حماية سلامة وسرية البيانات المرسلة لا سلكياً . لذلك يجب اختيار خوارزميات التعمية المناسبة وتعريف إجراءات إدارة المفاتيح المتوافقة. كما يجب التحكم بالدخول إلى الشبكة المحلية والدخول إلى تجهيزات الهاتف النقّال. ذلك أن الشبكات المحلية اللاسلكية **WLAN** الغير محمية ستعطي المهاجم الفرصة لاستخدام خدمة الشبكة **bandwidth** دون دفع أجورها. أوأن يستخدم النظام المستهدف كقاعدة مرحلية للقيام بهجمات على طرف ثالث.

يمكن أن تعمل الشبكات المحلية اللاسلكية **WLAN** في احد نمطين: الأول هونمط البنية التحتية **infrastructure** حيث تتصل التجهيزات الهاتف النقّالة بالشبكة المحلية عن طريق نقاط عبور**access points**. أما النمط الثاني فهونمط **ad hoc** وفيه تتخاطب التجهيزات النقّالة بشكل مباشر.

سنركز على أمن **WLAN** من النوع الأول وعلى التحكم بالدخول إلى تجهيزات نقاط العبور.

تملك كل نقطة عبور معرف تهيئة خدمة يرمز له بـ **Service Set Identifier SSID**.

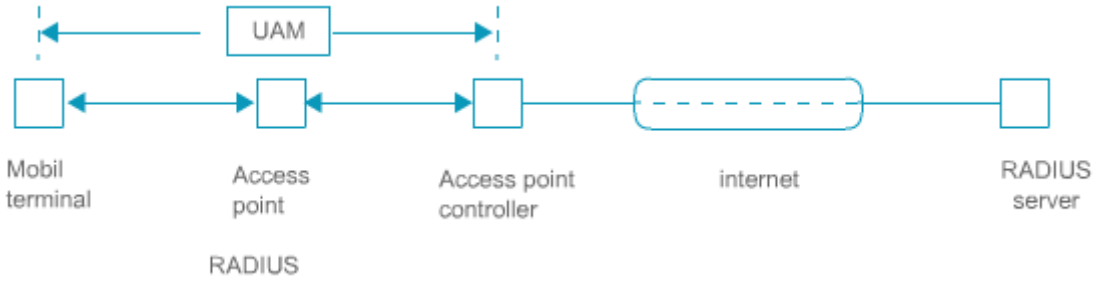
إن الشبكة المحلية اللاسلكية **WLAN** المفتوحة **open WLAN** لا تفرض قيود على الاتصال بنقطة العبور ولكن ذلك لا يعني بالضرورة أنها ليست محمية حيث من الممكن أن تقدم الأمن على مستويات أخرى من الشبكة.

تدعى نقاط العبور المهيئة للعموم بالبقع الساخنة **hot spot**.

ولضمان التحكم بالدخول إلى الشبكة المحلية اللاسلكية **WLAN**. يمكن أن تهيئ نقاط العبور بحيث لا تقوم ببث **Broadcast** معرف تهيئة الخدمة **SSID** الخاص بها، وإنما أن تشترط على الزبائن معرفة معرف تهيئة الخدمة **SSID** الخاص بها ليتمكنوا من الاتصال معها . و بالتالي يصبح هذا المعرف **SSID** هوالسر اللازم لتمكن الزبائن من الاتصال. لكن هذا الخيار لا يعمل دائماً بشكل جيد. لأن المعرف **SSID** متضمن في العديد من رسائل الإشارة التي من الممكن اعتراضها من قبل المهاجم. لذلك يجب أن لا تعامل هذه المعلومة كسر. من ناحية أخرى فإن ، تجهيزات نقاط العبور وهي مزودة بـ **SSID** افتراضية. فإذا لم يتم تغييرها عند تركيب نقطة العبور يمكن للمهاجم معرفتها. يمكن أن تعد تجهيزات نقطة العبور بحيث لا تسمح باتصال إلا لعناوين **MAC** محددة. لكن هذا الإجراء ليس فعالاً حيث من الممكن أن يتصنت المهاجم على اتصال شرعي ويلتقط عنوان **MAC** للزبون ويستخدمه لاحقاً للدخول إلى الشبكة اللاسلكية **WLAN**.

بشكل عام من الخطأ أن تبني التحكم بالدخول على أساس معلومات تستخدم لإدارة الاتصالات ، مثل عنواني **SSID** و**MAC**. لان هذه المعلومات يتم إرسالها أثناء إعداد الاتصال أي قبل أن تبدأ آليات الأمن. لذلك ربما تكون الاستراتيجية الأفضل هوترك الزبون ليؤسس اتصال مع تجهيزة نقطة العبور ثم تجري عملية الاستيقان منه قبل أن يعطى حق الدخول إلى أي خدمة محمية.

آلية الدخول العام **Universal Access Mechanism UAM** الممثلة في الشكل التالي تشرح هذه الاستراتيجية. بافتراض أن الزبون قد نصب على جهازه مستعرض انترنت. يأخذ الزبون الذي يتصل بنقطة العبور عنوان **IP** متغير من مخدم **DHCP**. عندما يبدأ مستعرض الانترنت الموجود على جهاز الزبون. يتم اعتراض أول طلب منه موجه إلى مخدم **DNS** أو طلب **HTTP** و يتم توجيه الزبون عبر جلسة **HTTPS** إلى صفحة خاصة للسؤال عن اسم المستخدم وكلمة المرور. ويقوم مخدم الويب في متحكم تجهيزة نقطة العبور بإحالة التحقق من اسم المستخدم وكلمة المرور إلى مخدم **RADIUS**. وحالما يتم الاستيقان من الزبون، يمكن لتجهيزة نقطة العبور أن تطبق آلية التحكم بالدخول على طلبات الزبون بناء على هويته بالطريقة المعتادة.



1. بروتوكول WEP

كان بروتوكول **Wireless Equivalent Privacy WEP** يهدف إلى حماية سرية وسلامة البيانات العابرة بين تجهيزة الهاتف النقّال وتجهيزة نقطة العبور، وذلك لتوثيق طرفيات تجهيزات النقّال بالنسبة للشبكة. ويبنى الاستيقان على سر متشارك. لذلك يجري إعداد يدوي لما يدعى أسرار مسبقة التشارك **preshared secrets** على كل الطرفيات التي يجب أن تأخذ حق عبور، و على كل تجهيزات نقاط العبور في الشبكة. يعتبر هذا الحل مناسباً للشبكات الصغيرة نسبياً . و عادة يستخدم نفس المفتاح لكل الطرفيات.

يستخدم بروتوكول **WEP** المعميات الجدولية للتعمية. في هذا النوع من المعميات، يجب أن لا تكرر مفاتيح التعمية، لأن نتيجة تطبيق عملية **XOR** بين نصين معميين بنفس مفتاح التعمية تطابق نتيجة تطبيق عملية **XOR** بين النصين قبل التعمية. لذلك يمكن استغلال هذه الخصائص الإحصائية لاستنتاج النصوص البسيطة (الغير معماة) وحساب جدول مفاتيح التعمية . لذلك يستخدم شعاع ابتدائي **Initial Vector IV** طوله **24** بت ليدخل عنصر العشوائية إلى عملية التعمية.

يتشارك المرسل والمستقبل بمفتاح سري طوله **40** بت أو**104** بتات. لإرسال رسالة **m** يقوم. المرسل بحساب مجموع اختباري **checksum** طوله **32** بت **CRC-32(m)**، ويأخذ الشعاع الابتدائي **IV** ويولد باستخدام المعمية الجدولية **RC4** والمفتاح $K' = IV \,||\, K$ جدول مفاتيح.

وبالتالي فالنص المعمى **c** هو: $c = (m \,||\, CRC-32(m)) \oplus RC4(K')$

ثم يرسل النص المعمى و الشعاع الابتدائي **IV** إلى المستقبل الذي يحسب قيمة $c \oplus RC4(K') = (m \,||\, CRC-32(m))$ ويتحقق من المجموع الاختباري.

للاستيقان من زبون ما. ترسل تجهيزة نقطة العبور تحدي **challenge** غير معمى إلى الزبون . يستخدم الزبون المفتاح المتشارك والخوارزمية السابقة لتعمية التحدي. ثم تقوم تجهيزة نقطة العبور بالتحقق من الجواب.

تعاني آليات التعمية المستخدمة في بروتوكول **WEP** من خللين رئيسيين في التصميم.

الأول، تعتبر بالدالة الخطية **CRC-32** التي تعتبر جيدة لتحديد الأخطاء العشوائية لكنها لا تقدم أي دفاع ضد التغييرات المقصودة. وبالتالي فعندما تستخدم بالترابط مع عملية التعمية الخطية (**XOR**) للمعمية الجدولية فإنها لا تقدم حماية حقيقية للسلامة.

المشكلة الثانية تكمن في حجم الشعاع الابتدائي **IV**. فهوالجزء الوحيد المتغير الطول في المفتاح K'.

وبالتالي يمكن للمهاجم أن يراقب حركة المرور لفترة طويلة حتى يتكرر الشعاع الابتدائي **IV** ثم يحاول إعادة بناء جداول المفاتيح مع الشعاع الابتدائي **IV** المقابلة لها.

بالإضافة إلى المشاكل السابقة في بروتوكول **WEP**. يوجد نقطة أخرى تتعلق بالخوارزمية **RC4** حيث حصل تقدم ملموس في محاولات كسر هذه الخوارزمية والوصول إلى مفتاحها.

2. بروتوكول WiFi للدخول المحمي WPA WiFi Protected Access

لقد فشل بروتوكول **WEP** في تحقيق أهدافه الأمنية بشكل تام. لذلك فقد صمم بروتوكول **WPA** كحل سريع مبدئي يزيل نقاط الضعف الرئيسية في بروتوكول **WEP** إلى أن يتم إتمام بناء بنية الأمن لشبكة **WLAN**. وقد صمم **WPA** ليعمل على العتاد الحالي لشبكة **WLAN**. وطور أيضا اجرائيات لاستيقان الزبون للشبكة ولتأسيس مفاتيح تعمية بشكل ديناميكي.

لحماية السلامة تم استبدال **CRC-32** بترميز سلامة الر سالة **Message Integrity Code (MIC)** يدعى **Michael**. وقد تمت مضاعفة طول الشعاع الابتدائي **IV** إلى **48** بت.

ينشئ بروتوكول **Temporal Key Integrity Protocol TKIP** بنية هرمية مفتاحية . يحتاج الزبون وتجهيزة نقطة العبور إلى زوج مفاتيح رئيسية طويل الأمد **Pairwise Master Key (PMK)**. يستخدم **PMK** لتوليد أزواج مفاتيح مؤقتة **Pairwise Transient Keys PTKs** لأجل كل اتصال وتستخدم هذه المفاتيح لحماية حركة المرور بين طرفية الهاتف النقّال و تجهيزة نقطة العبور. ويستخدم بروتوكول **WPA** بمفاتيح رئيسية متشاركة مسبقاً **(WPA-PSK)**، حيث يحسب **PMK** بواسطة دالة توليد المفتاح **PBKDF2** كما يلي:

PMK=PBKDF2(passphrase، SSID، SSID length، 4096، 256)

الدخل هو: **passphrase** طوله **20** محرف كحد أدنى.

SSID هومعرف لنقطة العبور.

طول **SSID**.

يضغط هذا الدخل **4069** مرة لينتج مفتاح طوله **256** بت. تأخذ الخوارزمية التي تحسب **PTK** المفتاح الرئيسي **PMK** وعنوان **MAC** لكلا الأداتين، وقيم التحدي المولد من الأداتين. يرسل قيمة تحدي بشكل علني غير مشفر.

يعتبر **WPA-PSK** نقطة ضعف أمام هجمات تخمين كلمة المرور. حيث يقوم المهاجم بتسجيل الرسائل المتبادلة بين الضحية والشبكات اللاسلكية **WLAN** عند الاتصال بها. حيث يقوم بتخمين قيمة لعبارة المرور **passphrase** وحساب المفتاح الرئيسي **PMK**، بالاعتماد على عبارة المرور المخمن وقيمة **SSID** المعروفة وطول **SSID**، والمفتاح المؤقت **PTK** من المفتاح **PMK** وعناوين **MAC** المعترضة وقيم التحدي. ثم يقوم بفك تعمية الرسائل المعماة التي كان قد سجلها باستخدام المفتاح **PTK**. فإذا كانت النتيجة هي نص ذي معنى. عندها فعبارة العبور المخمنة صحيحة باحتمال عالي.

لا تعتبر آليات الأمن في **WPA** قوية كما يتمنى المرء من منظور التعمية. لكن يبقى بروتوكول **WPA** أكثر تطوراً وبشكل واضح عن **WEP**.

3. IEEE 802.11i – WPA2

تمت إعادة صياغة آليات امن **WLAN** في المعايير **IEEE 802.11i**، المنشورة عام **2004**. تعرف هذه المعايير أيضا باسم **WPA2**. حيث استبدلت المعمية الجدولية **RC6** بالمعمية **AES** في النمط **CCMB**، بمعنى نمط العداد مع نمط **CBC-MAC**. لكن يحتاج **WPA2** إلى تغيير التجهيزات لضمان التوافقية.

6. BLUETOOTHE

هي تقنية للشبكات اللاسلكية في نمط **ad hoc**، وتستخدم للاتصالات ذات المدى القصير (حتى **10** متر) بين الأدوات الشخصية مثل الحاسب الشخصي، لوحة المفاتيح، الفأرة، الطابعة، سماعة الرأس، أوأي أجهزة محيطية أخرى، تشكل منطقة الشبكة الشخصية. مثل هذه الشبكة لا تحتاج إلى بنية معقدة لإدارة المفاتيح. وبالتالي يمكن لأداتين أن تؤسسا جلسة آمنة بينهما يدوياً باستخدام عملية الازدواجية **pairing**، بمعنى أن يدخل المستخدم نفس الرمز **PIN** في كلا الأداتين.

لأجل حماية حركة المرور بين الأداتين بالتعمية، يولد مفتاح اتصال طوله **128** بت من الرمز **PIN**. يستخدم مفتاح الاتصال لعمليات الاستيقان اللاحقة بين الأداتين. حيث تتم عمليات الاستيقان باستخدام بروتوكول **challenge-response**. وبشكل مشابه للاستيقان في **GSM**. باستخدام **PIN** المتشارك، طول هذا الرمز **PIN**، قيمة عشوائية يولدها المرسل و أيضا باستخدام عنوان المستقبل، تولد مفاتيح اتصالات مؤقتة لتعمية الرسائل.

لقد صممت بنية أمن **BLUETOOTHE** لأجل الشبكات الشخصية . فإذا تغير مدى تقنية **BLUETOOTHE** فيجب أن تطور بنية الأمن.

أسئلة وتمارين

1. يجب على مزودي خدمة الهاتف أن تتعامل مع شكاوي الزبائن الذين يدعون أنهم لم يجروا المكالمات التي يبدوا أنها أجريت من هاتفهم. ما نوع إجراءات الحماية الممكن توفيرها للتعامل مع مثل هذه المشكلة؟

2. ناقش المسائل التي ستظهر عند ترخيص التصنت في أنظمة المحمول ذات التجوال العالمي.

3. لنفرض MAC طوله 128 بت يستخدم لاستيقان الرسالة على قناة معدل أخطائها 1:1000. ما هواحتمال رفض الرسالة بسبب خطأ في الإرسال عندما يكون طول الرسالة 1K بت، 2K بت و1K بايت؟ ما هي الاحتمالات عندما يرتفع معدل الخطأ إلى 1:100؟ لأجل كلا معدلي الأخطاء، ما هي الاحتمالات إذا استخدم MAC طوله 32 بت؟

4. تقوم العقد التي أسست جلسة على طبقة النقل بتغيير عنوان الانترنت لها خلال الجلسة . كيف يمكن حماية الجلسة على مستوى طبقة الانترنت في مثل هذه الحالة. أعطي تحليلاً للمسائل العامة المتعلقة بالسرية لهذه الحالة، وللحل المناسب لهذه المسائل . و للحل المقترح حالياً للمناقشة في ITEF.

5. ما الجهود التي يجب بذلها من مالك العنوان لإنشاء CGA صحيحة (شرعية) بالمقارنة مع جهود مهاجم لأجل القيم Sec = 1، 2،3 عندما تحتاج حساب قيم الاختزال hash إلى 1msec.

6. لنفرض نقطة وصول ترسل 1500 بايت رزمة في IEEE 802.11b بمعدل بيانات 11ميغابت. كم يجب على المهاجم أن ينتظر ليبدأ إعادة IV؟ إذا ولدت IV بشكل عشوائي، فقدر وسطياً كم يجب على المهاجم أن ينتظر ليحدث أول تضارب (أي أن تعمى رزمتان بنفس IV).

7. يقوم بروتوكول WEP "تحدي الإجابة" WEP challenge-response بإرسال تحديات بشكل غير معمى بينما يعمي الإجابة. هل يحدث تعمية التحديات وترك الإجابة غير معماة أي فرق.

8. صف هجوم تتم بواسطته إعادة توجيه رزم IP لـ WEP المعمى إلى هدف يختاره المهاجم.

9. قارن بين الخدمات الأمنية المقدمة بواسطة UAM و802.1X والخدمات الأمنية في EAP.

الفصل الرابع: أمن قواعد البيانات

1. مقدمة

قاعدة البيانات هي مجموعة بيانات منظمة بطريقة ذات معنى.

ينظم نظام إدارة قاعدة البيانات **DBMS a data base system** طريقة تخزين البيانات و يؤمن للمستخدمين طرق استرداد هذه المعلومات. فإذا لم يوجد تحكم بالوصول إلى قاعدة البيانات ستضعف الخدمات التي تقدمها قاعدة البيانات لأنك ستحجم عن وضع البيانات المهمة فيها .

فقواعد البيانات تقدم معلومات انفرادية، مثل: سجلات الموظفين في شركة، سجلات الطلاب في جامعة. وقد سنت العديد من الدول تشريعات تفرض على الشركات حماية البيانات الشخصية .

لذلك يأخذ أمن قواعد البيانات أهمية خاصة. وهو يختلف عن أمن نظم التشغيل.

فنظام التشغيل يدير البيانات. فالمستخدم يستخدم دوال نظام التشغيل لينشئ ملف أويحذفه أوليفتحه للقراءة أوللكتابة. وأي من هذه العمليات لا يهتم بمحتويات الملف.

بينما يجري مستخدم قاعدة البيانات عمليات تتعلق بمعلومات قاعدة البيانات. وتعتبر عملية البحث في قاعدة البيانات الاستخدام الأكثر تكراراً في قاعدة البيانات. لذلك فمن لوازم قرارات التحكم بالوصول التي يتخذها **DBMS** أن تهتم أيضا بمحتويات قاعدة البيانات. والمثال الشائع هو قاعدة بيانات الرواتب حيث يجب الحفاظ على سرية الرواتب التي تتجاوز عتبة معينة.

وبالتالي يمكننا القول أن أمن قاعدة البيانات يتوضع في كفة المستخدم من ميزان مستخدم - آلة.

من جهة أولى: تبدوحماية المعلومات الحساسة أمراً سهلاً. ففي قاعدة بيانات الرواتب، يمكنك ببساطة إضافة شرط إلى عبارة الاستعلام يفحص مبلغ الراتب. هذا الاحتياط عملي عندما تعرف ما هي البيانات التي تريد حمايتها، حيث يمكن أن يهتم المتطفل بأجزاء مختلفة من المعلومات منها:

- بيانات محددة: القيم المخزنة في قاعدة البيانات.
- حدود: الحدود الدنيا والعليا لقيم عددية مثل الرواتب يمكن أيضا أن تكون مفيدة.
- النتائج السلبية: مثال: إذا حوت قاعدة بيانات على الإدانات الجرمية ستكون معلومة أن شخص ما له سجل خالي من الإدانات الجرمية هي معلومة حساسة.
- قيم احتمالية: القدرة على تخمين بعض النتائج من استعلامات أخرى.

في نهاية المطاف فإن عليك أن تدافع عن نفسك ضد كل الاحتمالات. وتصبح حماية البيانات أكثر صعوبة عندما تسمح قاعدة البيانات بالاستعلامات الإحصائية. لأن دمج نتائج الإحصائيات بطريقة ذكية يمكن أن يسرب معلومات حساسة تحاول أن تحرص على حمايتها.

إذاً يجب أن تأخذ كل المخاطر السابقة بالحسبان بشكل جدي.

لكن من جهة أخرى: يجب أيضا أن لا تهمل حقيقة أن قاعدة بياناتك يجب أن تحقق الأهداف التي بنيت من اجلها وهي الوصول السريع والسهل إلى المعلومة.

تحمل محتويات قاعدة البيانات المعلومات حول الكائنات الخارجية بالنسبة لنظام الحاسب. مثل : مستويات المخزون في المستودع، نتائج امتحانات الطلاب، أرصدة الحسابات البنكية، أوالمقاعد المتوفرة في رحلة، ويجب أن تعكس محتويات قاعدة البيانات هذه الحقائق بشكل صحيح. لذلك يتعاون أمن قاعدة البيانات مع تطبيقات حماية السلامة لتحقق الأهداف التالية:

- **توافق داخلي internal consistency**: بمعنى أن تتبع المحتويات في قاعدة البيانات قواعد محددة مسبقاً. مثل مستويات التخزين يجب أن لا تنخفض تحت الصفر.
- **توافق خارجي external consistency**: تعني أن تكون محتويات قاعدة البيانات صحيحة، مثل أن مستويات التخزين المدخلة في قاعدة البيانات تطابق مستويات التخزين في المستودع. يمكن لنظام **DBMS** أن يساعد في منع حدوث أخطاء عند تحديث قاعدة البيانات، لكنك لا تستطيع الاعتماد كلياً عليه لتحقيق حالة توافق.

2. قواعد البيانات العلائقية Relational Databases

تعتبر قواعد البيانات العلائقية هي النمط الأوسع انتشاراً اليوم. وسنعرض بشكل سريع إلى المفاهيم الأساسية لهذا النمط من قواعد البيانات.

قواعد البيانات العلائقية **Relational Database**: هي قاعدة بيانات تظهر لمستخدميها كمجموعة جداول (وجداول فقط).

هذا التعريف هومن وجهة نظر مستخدمي قاعدة البيانات. وهولا يتطرق إلى بنيتها الفيزيائية.

تعرف العلاقة R على أنها مجموعة جزيئة من الجداء الديكارتي $D1\times....\times D_n$ حيث **$D_1,...,D_n$** حيث **Di** هومجموعة قيم الخاصية (الحقل) **i**. يعبر عن عنصر من العلاقة **R** بالشكل $(v_1,....,v_n)$:$v_i \in D_i$ بمعنى أن قيمة الخاصية ذات الترتيب **i** يجب أن تكون عنصر في **D_i** ، تدعى العناصر في **tuple** بالحقول. عندما لا يحتوي الحقل على أي قيمة نعتبر انه يحوي القيمة **null** وهي هنا تعني انه "لا يوجد قيمة" وليس المعنى أن "القيمة غير معروفة".

يمكن أن تكون العلاقة الموضحة في الشكل التالي جزء من قاعدة بيانات وكيل رحلات.

Name	Day	Flight	Status
A	Mon	GR123	private
B	Mon	YL011	business
B	Wed	BX201	
C	Tue	BX201	business
A	Thu	FL9700	business

Flight	Destination	Departs	Days
GR123	THU	7:55	1-4-
YL011	ATL	8:10	12345-7
BX201	SLA	9:20	1-3-5-
FL9700	SLA	14:00	-2-4-6-
GR127	THU	14:55	-2-5-

جدولي Diary وFlights

يوجد لعلاقة **Diary** أربع خصائص: الاسم، اليوم، الرحلة والوضع مجالاتها هي:

- الاسم: كل أسماء الزبائن الممكنة.
- اليوم: أيام الأسبوع، **sat, sun ,mon ,tue ,wed ,thu ,fri**.....
- رقم الرحلة: مؤلف من رقمين إلى أربعة.
- الوضع: عمل أوخاص.

تدعى اللغة المعيارية المستخدمة لوصف البيانات التي نريد استردادها من قاعدة بيانات علائقية بلغة الاستعلام الهيكلية **Structured Query Language SQL**. وفيما يلي أهم عمليات إدارة البيانات فيها:

SELECT: تسترد البيانات من العلاقة.

```
SELECT name, status
        FROM diary
        WHERE day ='mon'
```

وعندها ستظهر النتائج التالية

name	status
A	Private
B	business

UPDATE: تحدث قيم الحقول في العلاقة،

```
UPDATE Dairy
        SET Status = private
        WHERE Day = ‘sun’;
```

بمعنى جعل كل الرحلات يوم الأحد رحلات خاصة.

DELETE: لحذف **tuples** من العلاقة.

```
DELETE FROM Diary
        WHERE name = ‘Alice’;
```

يحذف كل رحلات **Alice** من **Diary**.

INSERT: تضيف **tuples** إلى العلاقة:

```
INSERT INTO Flights (Flight, Destination, Days)
            VALUES (‘GR005’, ‘GOH’, ’12-45-’)
```

الأمر السابق يدخل بيانات يدخل **tuples** إلى **Flights** ويبقي الحقل **Departs** غير محدد.

عادة، ترى العلاقات كجداول، والخصائص تقابل الأعمدة في الجداول، حيث تستخدم أسماء الخصائص كترويسات للأعمدة. تقابل الأسطر أوالسجلات في الجدول إلى **tuples**.

في نمط العلاقة، لا يمكن أن يحتوي الجدول على مؤشرات أووصلات إلى جداول أخرى .

ويوجد في قواعد البيانات العلائقية عدة أنواع من العلاقات.

- علاقات أساسية (جداول): أوتدعى علاقات حقيقية، وهي علاقات مستقلة و هي غير مشتقة من علاقات أخرى، ولها بياناتها المستقلة.
- المشهد **View**: هي علاقات مشتقة من علاقات أخرى، وتعرف بالاعتماد على علاقات أخرى، وهي لا تملك بياناتها المستقلة والمخزنة فيها.
- نتائج الاستعلام **Query**: يمكن لنتائج استعلام أن تملك اسم أولا تملك اسم. وهي لا تملك تصميم موجود في قاعدة البيانات.

1. مفاتيح قاعدة البيانات

يجب أن توجد في كل قاعدة بيانات طريقة لتعريف كل السجلات بطريقة واحدة و واحدة فقط ، أحيانا يمكن أن يكون حقل واحد هوالمعرف المطلوب، أوربما أكثر من واحد.

تعريف: المفتاح الرئيسي **A primary key** لعلاقة ما هوالمعرف الأصغر للعلاقة . يجب أن يحقق المفتاح العام **K** الشروط التالية:

- الوحدانية **Uniqueness**: أي لا يوجد أي سجلات في الجدول لها نفس القيمة لـ **K**.

- الأصغر **Minimality**: بمعنى إذا كان **K** مفتاح أساسي مركب . فلا يمكن حذف أي مكون من مكونات **k** بدون تدمير الوحدانية.

مثلا في علاقة **Diary** يمكن لمركّب حقلي الاسم واليوم أن يكون مفتاح أولي وذلك بفرض أن الزبون سيذهب في رحلة واحدة في اليوم. بينما في علاقة **Flight** يمكن أن يكون رقم الرحلة لوحده مفتاح أساسي.

يجب أن تحتوي كل علاقة على مفتاح أساسي وإلا فان العلاقة يمكن أن تحتوي على **tuples** مكررة. إذا كان الحقل الذي يمثل المفتاح الأساسي في جدول ما هوحقل في جدول ثاني ندعوه في الجدول الثاني مفتاح مساعد (ثانوي) **Foreign Key**.

في مثالنا نجد حقل رقم الرحلة هوالمفتاح الأساسي في جدول **Flight** وهومفتاح ثانوي في جدول **Diary**.

2. وظائف السلامة Integrity Roles

يمكنك أن تعرف في قاعدة البيانات قواعد تفرض التوافق الداخلي وتساعد في التوافق الخارجي (الدقة). عادة تكون معظم هذه القواعد خاصة بالتطبيق، لكن يوجد قاعدتين ملازمتين لنمط قاعدة البيانات العلائقي.

- قاعدة سلامة الوجود **Entity Integrity Rule**: وتعني عدم السماح لأي مكون للمفتاح الأساسي في علاقة أساسية أن تكون له القيمة **null**.
- تسمح لنا هذه القاعدة بإيجاد كل السجلات في العلاقة الأساسية.
- قاعدة سلامة المرجعية **Referential Integrity Rule** يجب أن لا تحتوي قاعدة البيانات على قيم للمفتاح الثانوي غير متطابقة.

تمثل قيم المفتاح الثانوي مرجع إلى بيانات أخرى في جداول أخرى. وبالتالي عدم التطابق في قيم المفتاح الثانوي تعني وجود قيمة في حقل مفتاح ثانوي ليست موجودة في حقل المفتاح الأساسي المرجع له.

بالإضافة إلى هاتين القاعدتين. يوجد قواعد سلامة أخرى خاصة بالتطبيقات يمكن توصيفها . حيث يمكنك أن تستخدم هذه القواعد لتحقق ما يلي:

- اختبارات الحقل: لمنع الأخطاء في البيانات المدخلة. في مثالنا يمكننا أن نحرص على عدم إدخال قيم عشوائية في حقل الوضع وذلك من خلال فحص القيمة لتكون إحدى القيمتين عمل أوخاص.

- مجال الاختبارات: عندما تتعامل مع قواعد البيانات الإحصائية وربما تحتاج إلى قواعد لاختبار فيما إذا كانت نتائج الاستعلامات قد حسبت بالنسبة إلى عينة كافية.
- اختبارات توافق **consistency checks**: يمكن أن تشير البيانات في قاعدة البيانات إلى مظاهر في العالم الخارجي وبالتالي يجب أن تتوافق مع هذه المظاهر. في مثالنا يمكننا أن نجري اختبار ليوم رحلات زبون بالمقارنة مع قائمة أيام مغادرة الرحلات . فمثلاً الزبون **A** غادر يوم الاثنين على الرحلة **GR123** يتوافق مع حقيقة أن هذه الرحلة تغادر يومي الاثنين والخميس من كل أسبوع.

يتوضع عادة هذا النوع من قواعد التوافق في طبقة التطبيق. ويقدم نظام إدارة قواعد المعطيات **DBMS** البنية اللازمة لتحديد وتطبيق مثل هذه القواعد. مثال على ذلك هو زناد السلامة **Integrity Trigger** وهوبرنامج يربط إلى غرض في قاعدة البيانات ليختبر صفات توافق محددة لهذا الغرض. بحيث ينفذ هذا البرنامج عندما تحاول العمليات **INSERT، UPDATE، DELETE** تعديل محتويات هذا الغرض.

3. التحكم بالوصول Access Control

يجب على نظام **DBMS** أن يتحكم بطرق وصول المستخدمين إلى قاعدة البيانات لكي يستطيع حماية المعلومات الحساسة. ولكي ترى كيف يمكن توظيف المتحكمات فيجب أن تتذكر انه يمكن توفير الوصول إلى قاعدة البيانات على مستويين هما:

- عمليات التعامل مع البيانات من خلال العلاقات الأساسية.
- عمليات التعامل مع الأغراض المختلطة مثل المشاهد **Views** أو اللقطات **SNAPSHOTS**.

كما يمكنك أن تنظر إلى التحكم بالوصول من خلال استخدام قواعد تقوم بما يلي:

- تقييد العمليات المتاحة للمستخدم.
- تعريف متطلبات الحماية لأجل كل عنصر بيانات بشكل مستقل.

يؤثر قرارك بشأن نوع التحكم بالوصول الذي ستتبناه على السياسة الأمنية التي ستفرضها . والعكس بالعكس. لكن مهما كان خيارك فيجب أن تسعى لتحقيق الهدفين التاليين:

- الكمال **Completeness**: أي ضمان حماية كل حقول قاعدة البيانات.
- التوافق **Consistency**: بمعنى عدم تضارب قواعد الوصول إلى عنصر بيانات ما.

ونقول إن السياسة الأمنية متوافقة إذا لم يوجد أي عنصر في قاعدة البيانات يمكن الوصول إليه بطرق مختلفة ناتجة عن قواعد تحكم بالوصول مختلفة. ومن المهم عدم منع طلبات الوصول الشرعية، كما يجب أن لا تتوفر إمكانية التحايل على سياسة وصول معينة.

1. نمط أمن SQL SQL security mode

يتبع نمط أمن **SQL** تحكم بالوصول مبني على ثلاث كائنات.

- المستخدمين: يتم الاستيقان من هوية المستخدم أثناء عملية تسجيل الوصول ، و يمكن لنظام إدارة قواعد المعطيات **DBMS** أن يجري عملية الاستيقان أو أن يقبل هويات المستخدم التي تم الاستيقان منها بواسطة نظام التشغيل.
- الأحداث **ACTIONS**: وتتضمن **SELECT**، **UPDATE**، **DELETE**، و**INSERT**.
- الأغراض: جداول **TABLE**، مشاهد **VIEWS**، وأعمدة للجداول والمشاهد، كما توجد أيضا أنواع بيانات تعرف من قبل المستخدم.

يقوم المستخدم بطلب إجراء حدث على غرض ويقرر نظام إدارة قواعد لبيانات **DBMS** فيما إذا كان مسموح لهذا المستخدم إجراء هذا الحدث.

بشكل عام عند إنشاء غرض من قبل مستخدم ما، يصبح هذا المستخدم هو مالك لهذا الغرض ومبدئياً مالك الغرض هوفقط من يحق له الوصول إلى الغرض. بينما بالنسبة لبقية المستخدمين فيجب أن يمنحوا امتيازات **privileges** تحدد إمكانيات وصولهم لأي غرض.

ويتكون الامتياز من

مانح **grantor**: هوالمستخدم الذي سيمنح المستخدمين الآخرين الامتياز وغالباً ما يكون هومالك الغرض.

منحة **grantee**: هي العمليات التي سيسمح للمستخدم الممنوح إجراءها.

غرض **object**: هوالغرض الذي ستنفذ عليه العمليات.

حدث **action**: هونوع العمليات الممنوحة.

الممنوح **grantable**: هوالشخص الذي سيمنح الامتياز.

تعتبر الامتيازات والمشاهد **view** الدعامات الأساسية لنمط أمن **SQL**. فهي تقدم إطار عمل لسياسات أمن موجهة توظف في التطبيقات.

2. منح وسحب الامتيازات

تدار الامتيازات في **SQL** بالعمليتين منح **GRANT** وسحب **REVOKE**. تشير الامتيازات إلى أحداث معينة ويمكن أن تقيد بخاصيات محددة (حقول) في الجدول. ففي مثالنا نسمح فقط لعاملين **A** و**Z** بفحص وتعديل أجزاء من جدول **Diary**.

```
GRANT SELECT, UPDATE (Day, Flight)
        ON TABLE Dairy
        TO A , Z
```

كما يمكن سحب الامتيازات بشكل انتقائي.

```
REVOKE UPDATE
          ON TABLE Diary
          FROM A
```

يوجد ميزة إضافية وهي إمكانية منح حق المنح، وقد وظف في **SQL** عن طريق الخيار **GRANT**.

```
GRANT SELECT
        ON TABLE Diary
        TO A
        WITH GRANT OPTION
```

وبالتالي يمكن للعامل **A** أن يمنح بدوره امتيازات عل الجدول **Diary** للعامل **Z**.

```
GRANT SELECT
        ON TABLE Diary
        TO Z
        WITH GRANT OPTION
```

عندما يقوم مالك الجدول **Diary** بسحب الامتيازات من **A** على الجدول **Diary**، يجب أن تسحب كل الامتيازات التي منحها **A** إلى غيره، أي أن تملك عملية سحب الامتياز خاصية التعدي **cascade**، والمعلومات اللازمة لتحقيق هذه الخاصية يجب أن يوفرها نظام قاعدة البيانات.

يجب أن تلاحظ أيضا انه بمجرد أن أخذ مستخدم آخر امتيازات على بيانات ما (غرض)، لا يستطيع مالك البيانات\الغرض أن يتحكم بكيفية استخدام البيانات المأخوذة من هذا الغرض، حيث يمكن القراءة من هذا الغرض ونسخ بياناته إلى غرض آخر بدون الحاجة إلى امتيازات كتابة على الغرض الأول.

3. التحكم بالوصول من خلال المَشاهد

تعتبر المشاهد **VIEWS** علاقات مشتقة ويأخذ أمر بناءها الشكل التالي.

```
CREATE VIEW view_name [(column [,column ] .... )]
        AS subquery
        [ WITH CHECK OPTION];
```

يمكنك أن توظف التحكم بالوصول في العلاقات الأساسية (جداول) بمنح الامتيازات على بيانات العلاقات الأساسية مباشرة. لكن يمكن التعبير عن العديد من السياسات الأمنية بشكل أفضل عن طريق المشاهد. فالاستعلام الجزئي **subquery** الموجود في بناء المشهد يمكن أن يوصف شروط معقدة جداً للوصول. فمثلاً. يمكننا بناء مشهد يحتوي كل رحلات العمل في مثال جدول **Diary** كما يلي:

```
CREATE VIEW business_trips AS
        SELECT * FROM Diary
        WHERE Status = 'business'
        WITH CHECK OPTION;
```

يمكن أن يوضع التحكم بالوصول عبر المشاهد في طبقة التطبيق. وتعتبر المشاهد جيدة لعدة أسباب:

- المرونة حيث تسمح بتعريف السياسات الأمنية للتحكم بالوصول في مستوى التوصيف الذي يحتاجه التطبيق.
- يمكن للمشاهد أن تفرض سياسات أمنية مستقلة عن البيانات.
- يمكن للمشاهد أن توظف استدعاءات مسيطر عليها.
- يمكن إعادة تصنيف البيانات بسهولة.

يمكن التعبير من خلال المشاهد عن تطبيقات التحكم بالوصول الموجه كما يلي:

```
CREATE  VIEW Top_of_the_Class AS
        SELECT * FROM  Students WHERE Grade <
        (SELECT Grade FROM Students WHERE Name = current_user());
```

وذلك لعرض الطلاب الذين حصلوا على معدل علامات أقل من معدل علامات المستخدم الذي يستخدم المشهد.

يمكن توظيف التحكم بالوصول بإضافة جدول تحكم بالوصول إلى قاعدة البيانات. وعندها يمكن للمشاهد أن تشير إلى هذه الجداول. وبذلك يمكنك أيضا أن تعبر عن التحكم بالوصول المبني على أساس عضوية مجموعة بالإضافة إلى السياسات الأمنية التي تنظيم حقوق المستخدمين في منح وسحب حقوق الوصول.

وأكثر من ذلك. يمكن للمشاهد أن تعرف أوتشير إلى تصنيفات أمنية **Security Labels**. ففي مثالنا يمكن أن نصنف رحلات العمل إلى **thule** كبيانات سرية وذلك بإنشاء المشهد:

```
CONFIDENTIAL AS ≥ CREATE VIEW Flights
        SELECT * FROM Diary
        WHERE Destination = 'THU' AND Status = 'business';
```

إذا أحكمت بناء سياستك الأمنية يمكن للمشاهد أن تقدم تحكم بالدخول في حالة القراءة بدون مشاكل تقنية لكن ذلك لا ينطبق على استخدام المشاهد من قبل عمليتي التحديث والإدخال للكتابة في قاعدة البيانات. وذلك للأسباب التالية:

- يوجد مشاهد غير قابلة للتحديث لأنها لا تحتوي المعلومات التي تحتاجها للمحافظة على توافق العلاقة الأساسية المقابلة. مثلاً، لا يمكن تحديث المشهد الذي لا يحتوي على المفتاح الأساسي للجدول الذي اشتق منه هذا المشهد.
- حتى لوكان المشهد قابل للتحديث تبقى هناك مسائل أمنية مثيرة للاهتمام. ففي مثالنا يرى عامل الرحلات الذي يملك حق وصول إلى قاعدة بيانات **Diary** فقط عن طريق المشهد **business_trips** ما يلي:

Name	Day	Flight	Status
B	Mon	YL011	business
C	Tue	BX201	business
A	Thu	FL9700	business

فهل يجب أن يسمح لهذا العامل بتحديث المشهد بالعملية التالية؟

```
UPDATE business_trips
        SET Status = 'private'
        WHERE Name = 'A' AND Day = 'Thu'
```

عند تنفيذ هذا التحديث سيختفي سجل **A** من المشهد. لكن وفقا لتعريف المشهد **business_trips** لن يكون بالإمكان تنفيذ هذا التحديث بسبب وجود الخيار **check** الذي يسمح بعمليات التحديث والإدخال المتوافقة مع بنية المشهد، فإذا حذف خيار **check**، ستكون الكتابة العمياء مسموحة **blind writes**.

4. مساوئ المشاهد

لقد عرضنا الميزات التي تجعل المشاهد آلية أمنية مفيدة لكن بالمقابل يوجد للمشاهد مساوئ منها:

- يمكن أن يصبح اختبار الوصول معقداً وبطيئاً.
- يجب أن تختبر صحة تعريفات المشهد، من حيث تحقيقها فعلا للسياسة الأمنية المطلوبة.
- لا يتحقق التوافق والتمام بشكل آلي، حيث يمكن أن تتداخل المشاهد أوتفشل في التقاط كل قاعدة البيانات.

4. أمن قاعدة البيانات الإحصائية

من أهم ما يميز قاعدة البيانات الإحصائية هواسترداد المعلومات باستخدام استعلامات إحصائية (تجميعة **aggregate**) على أعمدة في الجدول. من أهم هذه الاستعلامات:

- **COUNT**: تعطي عدد القيم في عمود.
- **SUM**:مجموع القيم في عمود.
- **AVG**:معدل القيم في عمود.
- **MAX**: القيمة الكبرى في عمود.
- **MIN**: القيمة الدنيا في عمود.

يوصف صدر الاستعلام **query predicate** الخاص بالاستعلام الإحصائي مجموعة السجلات التي ستستخدم لحساب الاستعلامات الإحصائية.

أما مجموعة الاستعلام **query set** فهومجموعة السجلات التي تتطابق مع صدر الاستعلام **query predicate**.

يمكن اختصار المشاكل الأمنية لقاعدة البيانات الإحصائية بما يلي:

- تحتوي قاعدة البيانات عناصر بيانات مستقلة الحساسية. وبالتالي فليس مسموح الوصول المباشر إلى عناصر البيانات.
- يسمح للاستعلامات الإحصائية الوصول إلى قاعدة البيانات. وبسبب طبيعتها الخاصة تقرأ هذه الاستعلامات عناصر البيانات المستقلة.

كما قد أسلفنا في فقرة نماذج الأمن من الوحدة الأولى. فان نماذج الأمن تحاول ما بوسعها لمنع تدفق المعلومات باتجاهات مختلفة. لكن في قاعدة البيانات الإحصائية. يجب أن يوجد بعض التدفق للمعلومات من عناصر البيانات إلى الاستعلامات التجميعية **aggregate**. وجل ما نستطيع عمله هوتقليص هذا التدفق إلى مستوى مقبول.

Nam	Sex	Program	Units	Grade Ave
A	F	MBA	8	63
B	M	CS	15	58
C	F	CS	16	70
D	M	MIS	22	75
E	M	CS	8	66
F	F	MIS	16	81
G	F	MBA	23	68
H	M	CS	7	50
L	M	MIS	21	70

جدول الطلاب

سنأخذ أمثلتنا في هذه الفقرة من قاعدة بيانات الطلاب الموضحة في الجدول السابق.

يسمح بالاستعلامات الإحصائية على كل الأعمدة لكن لا يسمح بالقراءة المباشرة للبيانات مفردة من الأعمدة **Units** و**Grade Ave**.

ويفرض الاستعلام الإحصائي التالي:

```
Q1 : SELECT AVG(Grade Ave.)
        FROM Students
        WHERE Programme = 'MBA'
```

حيث يقوم بحساب معدل العلامات لكل طلاب **MBA**. و بالتالي **query predicate** *صدر* الاستعلام هو**Program = 'MBA'**.

التجميع والاستنتاج Aggregation and Inference

يعتبر مفهومي التجميع والاستنتاج **Aggregation and Inference** من أهم المفاهيم في أمن قواعد البيانات الإحصائية.

يشير مفهوم التجميع إلى أن مستوى الحساسية للتجميعات المحسوبة من مجموعة قيم في قاعدة بيانات يمكن أن تختلف عن مستوى الحساسية للعناصر المستقلة المكونة لهذه البيانات. فغالباً ما ستجد حالات حيث مستوى حساسية التجميع أقل من مستويات حساسية العناصر المستقلة. كما يمكن أن يكون التجميع هومعلومات تنفيذية حساسة مشتقة من مجموعة بيانات عمل اقل حساسية.

يمكن اعتبار التجميع علاقة في قاعدة البيانات وبالتالي يمكن استخدام آليات التحكم بالدخول التي سبق الحديث عنها في هذه الوحدة. على كل حال . يمكن للمهاجم أن يستغل الفروقات في الحساسية ليصل إلى البيانات الأكثر حساسية.

تشير مسألة الاستنتاج إلى اشتقاق معلومات حساسة من بيانات غير حساسة. وبالتالي يجب أن نأخذ أنواع الهجمات التالية بالحسبان:

- الهجوم المباشر: حيث يحسب التجميع على عينة صغيرة لذلك تتسرب المعلومات حول عناصر البيانات المستقلة.
- الهجوم غير المباشر: ويدمج هذا الهجوم المعلومات المتعلقة بعدة تجميعات.
- هجوم المتتبع **tracker**: وهونوع فعال من أنواع الهجمات غير المباشرة.

- نظم خطية غير حصينة: وهي هجمات متتبع، تليها خطوة أخرى باستخدام العلاقات الجبرية بين مجموعات الاستعلام لبناء معادلات تنتج المعلومات المطلوبة.

هجمات التتبع tracker

سنشرح الآن كيف يمكن أن نوظف استعلامات إحصائية لاستنتاج معلومات حساسة من جدول الطلاب مثالنا السابق. لنفرض أننا نعلم أن **C** هي أنثى في صف **CS**. بدمج الاستعلامين المشروعين التاليين:

```
Q1 : SELECT COUNT(*)
        FROM Students
        WHERE Sex = 'F' AND Programme = 'CS'

Q2 : SELECT AVG(Grade Ave.)
        FROM Students
        WHERE  Sex = 'F' AND Programme = 'CS'
```

والنتائج هي: **Q1**: **1**، **Q2**: **70**.

علمنا من الاستعلام **Q1** انه يوجد أنثى واحدة في الصف **CS**. وبالتالي فالقيمة **70** التي أنتجها الاستعلام **Q2** هي معدل علاماتها. المشكلة هنا هي أن معيار الاختيار يعرف مجموعة تحتوي عنصر واحد فقط. وبالتالي يجب أن تسمح بالاستعلامات الإحصائية فقط إذا كانت تغطي مجموعة كبيرة كافية. على كل حال، إذا كنا مهتمين بالفعل باستعلام سينتج مجموعة صغيرة، يمكننا ببساطة أن نستعلم على متمم هذه المجموعة من خلال عكس الشرط الأصلي ثم من خلال حساب الفرق بين نتيجة الاستعلام المتمم والاستعلام عن كامل قاعدة البيانات.

لكن لسوء الحظ فحتى هذا وحده لا يعتبر جيد بالحد الكافي. فلو افترضنا أن كل مجموعة استعلام **query set** ومتممتها تحتوي على الأقل ثلاث عناصر . عندئذ فان سلسلة الاستعلامات التالية:

```
Q3 : SELECT COUNT (*)
        FROM Students
        WHERE Programme = 'CS'

Q4 : SELECT COUNT(*)
        FROM Students
        WHERE Programme = 'CS' AND Sex = 'M'

Q5 : SELECT AVG(Grade Ave.)
        FROM Students
        WHERE Programme =  'CS'

Q6 : SELECT  AVG(Grade Ave.)
        FROM Students
```

WHERE Programme = ‘CS’ AND Sex = ‘M’

والتي تعيد القيم التالية **Q3**: **4**، **Q4**: **3**، **Q5**: **61**، **Q6**: **58**.

نلاحظ أن كل الاستعلامات أخذت بالحسبان عدد سجلات كبير بشكل كافي لذلك فهي ليست ممنوعة. لكن. إذا ربطت النتائج الأربعة تستطيع حساب معدل علامات **C** كما يلي $(4\times61)-(3\times58)=70$.

ربما تظن أن الصدفة (كون الطالبة **C** هي الأنثى الوحيدة في الصف **CS**) هي التي مكنت من الحصول على هذه النتائج. لكننا سنقدم الآن طريقة نظامية لإعداد هجوم.

نحتاج أولا إلى متتبع **tracker**.

يدعى صدر الاستعلام **T** الذي يسمح بتتبع المعلومات الخاصة بسجل مفرد **بمتتبع إفرادي** **individual tracker** لهذا السجل. أما المتتبع العام **general tracker** فهو تصريح يمكن أن يستخدم لإيجاد جواب أي استعلام غير مسموح به.

ليكن **T** متتبع عام، وليكن **R** تصريح يعرف بشكل وحيد السجل المفرد **r** الذي نريد سبره.

في مثالنا فإن التصريح هو**‘C’ = Name**. نبني استعلامين لقاعدة البيانات باستخدام التصريحان $R\vee T$ و $R\vee NOT\,(T)$. ولنتأكد أن كلا الاستعلامين شرعيين، نختار **T** بحيث تكون مجموعة الاستعلام **query set** ومتممتها كبيرتين بشكل كافي للسماح بالاستعلامين. ثم نجري استعلام أخير على كل قاعدة البيانات لتعطينا كل البيانات التي تسمح بإكمال هجومنا. في مثالنا يعتبر التصريح **‘CS’ = programme AND ‘F’ = Sex** هو متتبع مفرد للطالبة **C** و التصريح **‘MIS’ = programme** هومتتبع عام (**T**) من بين العديد من المتتبعات العامة الأخرى. و بالتالي أصبح لدينا الاستعلامات الثلاث التالية:

Q7 : SELECT SUM(Units)
FROM Students
WHERE Name = ‘C’ OR programme = ‘MIS’

Q8 : SELECT SUM(Units)
FROM Students
WHERE Name = ‘C’ OR NOT (programme = ‘MIS’)

Q9 : SELECT SUM(Units)
FROM Students

فإذا كانت النتائج كما يلي: **Q7**:**75**، **Q8**: **77** و**Q9**: **136**.

فان الطالبة **C** يجب أن تتجاوز **16 = 136-(77+75)** وحدة.

احتياطات

في بداية دراسة امن قواعد البيانات اعتبر تحليل هجمات الاستنتاج الإحصائي مجالاً لبحث مطول. وقد تم التوصل إلى العديد من الاحتياطات التي يمكنك اتخاذها حيال مسألة الاستنتاج؟

أولاً: يجب أن تخبئ المعلومات الحساسة وهذا يعني أن تعلم ما هي المعلومات الحساسة. وكيف يمكن أن تستنتج هذه المعلومات. على الأقل عليك أن تختبر حجم مجموعة الاستعلام **query set** قبل أن تسمح بإعطاء نتائج الاستعلامات الإحصائية.

ثانياً: يمكنك أن تقنّع البيانات، حيث يمكنك أن تبدل مدخلات قاعدة البيانات بشكل عشوائي عندئذ تعطي الاستعلامات المفردة نتائج خاطئة بينما تظل نتائج الإحصائيات صحيحة. بالإضافة لذلك، يمكنك إضافة بعض التشويش العشوائي إلى نتائج الاستعلام بحيث تكون النتائج تحتوي الإجابة الصحيحة لكنها ليست صحيحة تماماً. تعتبر هذه التقنيات دقيقة وسهلة الاستعمال ولكن لا ينصح باستخدام التبديل العشوائي في بعض قواعد البيانات كتلك المتعلقة بالبيانات الطبية.

يمكن تلافي بعض مشاكل التجميع **aggregation** بأخذ الحذر أثناء تصميم قاعدة البيانات. يمكن لتحليل بنية قاعدة البيانات أن يبوح معلومات حساسة حول العلاقات بين حقول الجداول ، مثل هذه الحقول يجب وضعها في جداول منفصلة. وبالتالي فالمستخدم الذي يملك حق الوصول إلى احد هذه الجداول لن يستطيع الربط بين هذه الحقول لكن المستخدم الذي يملك حق الوصول إلى كل الجداول يستطيع الربط بينها. لذلك عليك كمدير لقاعدة البيانات أن تكون حذراً عند توزيع الامتيازات.

في مثالنا التالي تعتبر العلاقة بين الأسماء والأداء الأكاديمي علاقة حساسة. لذلك سنستبدل جدول **students** بجدولين، يرتبطان مع بعضهما البعض برقم معرف الطالب.

ID	Sex	Program	Units	Grade Ave
B13	F	MBA	8	63
C25	M	CS	15	58
C23	F	CS	16	70
M38	M	MIS	22	75
C12	M	CS	8	66
M22	F	MIS	16	81
B36	F	MBA	23	68
C10	M	CS	7	50
M20	M	MIS	21	70

Nam	ID
A	B13
B	C25
C	C23
D	M38
E	C12
F	M22
G	B36
H	C10
L	M20

فصل جدول الطلاب إلى جدولين

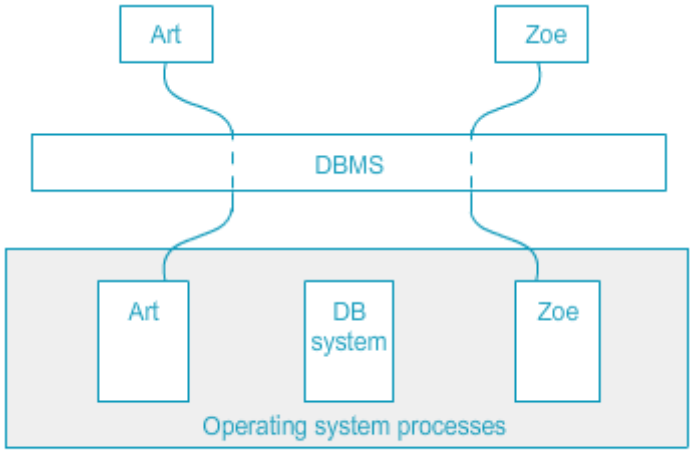
ويمكن الآن تصنيف الجدول الأول في مستوى عالي الحساسية وبالتالي لا يستطيع سوى المستخدمين المخولين الربط بين الأسماء والأداء الأكاديمي.

أخيرا. لاحظ أن مشاكل الاستنتاج ليست بسبب استعلامات مفردة وإنما بالربط الذكي بين عدة استعلامات. لذلك عليك مراقبة حركات مستخدمي قاعدة بياناتك من خلال سجلات الأداء.

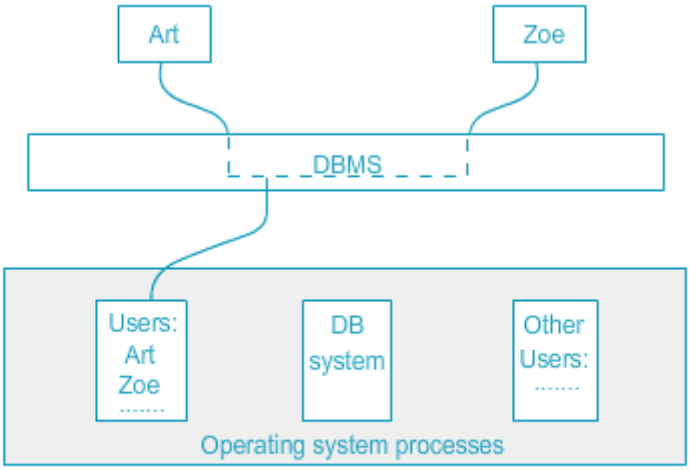
5. التكامل مع نظام التشغيل

عندما تنظر إلى قاعدة البيانات من موقع نظام التشغيل، سترى عدد من معالجات نظام التشغيل ومصادر الذاكرة التي تحتفظ بمدخلات البيانات. عملياً فان لنظام إدارة قواعد البيانات **DBMS** نفس مهام نظام التشغيل. كما أن عليه أن يمنع تداخل المستخدمين مع بعضهم البعض ومع نظام إدارة قواعد البيانات **DBMS**.

فإذا لم ترغب في مضاعفة المجهود، يمكنك أن تعطي هذه المهام إلى نظام التشغيل. في هذه الحالة، يعمل نظام إدارة قواعد البيانات **DBMS** كمجموعة من معالجات نظام التشغيل. وبالتالي سيوجد معالجات نظام للمهام العامة لإدارة قاعدة البيانات ويربط كل مستخدم لقاعدة البيانات إلى معالج نظام تشغيل منفصل. يمكن الآن لنظام التشغيل أن يميز بين المستخدمين وإذا تم تخزين كل غرض لقاعدة البيانات في ملف مستقل، يمكن لنظام التشغيل أن يقوم بكل عمليات التحكم بالدخول. وبالتالي على نظام إدارة قواعد البيانات **DBMS** فقط أن يترجم استعلامات المستخدم إلى عمليات يفهمها نظام التشغيل.



عزل مستخدمي قاعدة البيانات بواسطة نظام التشغيل



عزل مستخدمي قاعدة البيانات بواسطة نظام إدارة قواعد البيانات DBMS

6. السرية Privacy

تخزن العديد من الشركات المعلومات الشخصية لعملائها، مثل الاسم والعنوان و العمر و رقم بطاقة الاعتماد. وهي بيانات محمية قانونياً. لذلك من المهم إدارة مثل هذه البيانات.

لقد وضعت معايير **OECD** والتي هي عبارة عن إرشادات لحماية سرية البيانات الشخصية وتنقلها خارج الحدود الآمنة. وتعتمد على ثمانية مبادئ حماية:

1. مبدأ محدودية التجميع: يجب أن يوجد حدود للبيانات الشخصية المجمعة.كما يجب أن تجمع البيانات بطرق قانونية واضحة، وبمعرفة أوموافقة صاحب العلاقة.

2. مبدأ نوعية البيانات: يجب أن تتلاءم نوعية البيانات مع الأهداف التي ستستخدم لها. كما يجب أن تكون دقيقة وكاملة وحديثة.

3. مبدأ تحديد الهدف: يجب أن تحدد الأهداف التي جمعت لأجلها البيانات.

4. مبدأ محدودية الاستخدام: يجب أن لا تكشف البيانات أوأن تستخدم لغير الأهداف التي حددت بغير موافقة صاخب العلاقة أوتخويل قانوني.
5. مبدأ الحماية الأمنية: يجب أن تحمى البيانات الشخصية بإجراءات أمنية مقبولة.

6. مبدأ الانفتاح: يجب أن توجد سياسة عامة للانفتاح على التطورات ، التطبيقات ، والسياسات فيما يتعلق بالبيانات الشخصية.

7. مبدأ المشاركة الفردية: يجب أن يحصل الفرد على تأكيدات فيما إذا كان متحكم البيانات يمتلك أولا يمتلك بيانات خاصة به أوبها.

8. مبدأ المحاسبة: يجب أن يكون متحكم البيانات مسئول عن الامتثال للمبادئ الموضحة في النقط السابقة.

أسئلة

1. لنأخذ قاعدة بيانات محاسبة تتكون سجلاتها من الحقول (اسم الزبون، رقم الحساب ، رصيد، تصنيف الدائنية) وفيها الأنواع التالية من المستخدمين ، الزبون ، المحاسب ، المدير، عرف بنية الدخول من خلال المشاهد، بحيث:
   - يمكن للزبائن أن يقرأوا حسابهم فقط،
   - يمكن للمحاسبين أن يقرأوا كل الحقول ما عدا حقل تصنيف الدائنية وتعديل الرصيد لكل الحسابات.
   - يمكن للمدراء إنشاء سجلات جديدة، وقراءة كل الحقول وتعديل تصنيف الدائنية لكل الحسابات.

2. لنفرض قاعدة بيانات طلاب تحتوي أسماء طلاب وعلاماتهم في كل مقرراتهم . يزود المحاضرين بمشهد يظهر كل الطلاب في مقررهم والذين لم توضع علامة على أوراقهم بعد. هل يجب تعريف هذا المشهد مع خيار **WITH CHECK OPTION** ؟ اقترح معيار عام لقرار استخدام **CHECK OPTION** أم لا.

3. كل الاستعلامات الإحصائية على جدول الطلاب (الفقرة **4**) يجب أن تحوي على الأقل ثلاثة **tuples** في مجموعة استعلامها. استعلامات **AVG** على الحقل **Grad Ave** هي فقط المسموح بها. أوجد متتبع عام وأنشأ هجوم تتبع على معدل علامات **Grad Ave** الطالب **H**.

4. لقد رأيت أمثلة عن متحكمات الأمن متوضعة في طبقة التطبيق في أمن قاعدة البيانات . ما هي مساوئ هذا الأسلوب.

5. لنفرض قاعدة بيانات حيث تتوضع التجميعات في مستوى حساسية أعلى من عناصر البيانات التي اشتقت منها. وبالتالي يستطيع المستخدم المخول الوصول إلى هذه العناصر أن يحسب هذه التجميعات. كيف تستطيع الدفاع ضد مثل هذا الهجوم؟.

6. أعطيت قاعدة بيانات بحيث يمكن تعريف حقوق الوصول بشكل منفصل إلى كل سطر في الجدول. سوف يستخدم تحكم الوصول آليات أمنية لنظام التشغيل. ما متتالية قرارات التصميم بالنسبة إلى طريقة تخزين أغراض قاعدة البيانات في ملفات نظام التشغيل؟ (كمعيار، لنفرض نظام تشغيل يستخدم **100** بايت من بيانات الإدارة لأجل كل ملف وقاعدة بيانات بـ **10** مليون سجل.) هل هذا قرار تصميم ممكن.

الفصل الخامس: الكود الخبيث Malicious

1. مقدمة

يتضمن موضوع الكود الخبيث مجالاً واسعاً من البرمجيات المهددة لأمن الحواسيب و التي تستغل مختلف نقاط الضعف في الشبكات ونظم التشغيل والبرمجيات والأمن الفيزيائي لنشر الشحنات الخبيثة إلى أنظمة الحاسب.

في بعض الحالات، كما في حالة الفيروسات **viruses** وحصان طروادة **Trojan Horses**، يعتمد انتشار أغراض الكود الخبيث من نظام إلى آخر على الاستخدام غير المسؤول من قبل المستثمرين.

في حين يعتمد انتشار أغراض أخرى مثل الدودة بين النظم الضعيفة على قوتها الذاتية.

2. مصدر البرامج الخبيثة

في الأيام الأولى لأمن الحاسب، كان مصممو البرمجيات الخبيثة عبارة عن مبرمجون حاذقون يتباهون بابتكار تقنيات البرمجيات الخبيثة. عملياً قدم هؤلاء المبرمجين خدمات لشركات البرمجة بعرضهم للفجوات الأمنية في رزم برمجياتها الشائعة ونظم التشغيل.

ظهر حديثاً من يسمون بالقراصنة **hacker** أو**crackers**، عملياً لا يفهم هؤلاء التقنيات المؤدية إلى نقاط الضعف الأمنية غير أنهم يأخذون من الانترنت برمجيات جاهزة للاستخدام يستخدمونها لبدء هجوم ضد الأنظمة البعيدة.

ولدت هذه النزعة جيلاً جديداً من الفيروسات تسمح لأي شخص بخبرات قليلة أن يولد فيروساً ويطلقه عبر الانترنت. وينعكس هذا في العدد الكبير للفيروسات المسجلة من قبل مرجعيات مضادة الفيروسات.

3. الفيروسات

تعتبر فيروسات الحاسب الشكل الأقدم من البرمجيات الخبيثة التي تزعج مدراء الأمن.
وكما هي الفيروسات البيولوجية، فإن لفيروسات الكومبيوتر وظيفتان أساسيتان:

1. التكاثر.
2. التدمير.

وبالتالي سيحاول مصمم الفيروس تطبيق هاتين الوظيفتين بطرق جديدة ومبتكرة آملاً الهروب من تقنية مضاد الفيروسات.
تعرف وظيفة التكاثر كيف سينتشر الفيروس من نظام لآخر. بينما تقدم شحنة الفيروس القوة التدميرية التي أرادها مصمم الفيروس.

1. تقنيات تكاثر الفيروس

بالتعريف يجب أن يحتوي الفيروس على تقنية تمكنه من الانتشار من نظام لآخر. و قد يساعد هذه المهمة:

- الاستخدام المستهتر للمصادر المشتركة على الشبكة.
- تبادل الأقراص.
- تراسل البريد الالكتروني.
- أوبعض الطرق الأخرى.

حالما تستشعر الفيروسات نظام جديد، تستخدم إحدى تقنيات التكاثر لتصيب الضحية الجديدة بالعدوى.
توجد ثلاث تقنيات شائعة للتكاثر:

1. إصابة سجل الإقلاع الرئيسي **Master Boot Record MBR** .
2. إصابة الملفات.
3. إصابة الماكرو**macro**.

1. فيروسات سجل الإقلاع الرئيسي Master Boot Record:

يعتبر هذا النوع من أقدم أنواع الفيروسات، وهو يهاجم سجل الإقلاع الرئيسي **MBR** جزء القرص الصلب أوالقرص المرن المخصص لتحميل نظام التشغيل أثناء عملية الإقلاع.

ولكن بسبب كون حجم سجل الإقلاع الرئيسي **MBR** صغير (عادة **512** بايت)، لا يمكنه أن يحتوى كامل كود الفيروس اللازم لتطبيق وظيفتي التكاثر والتدمير، لذلك يخزن معظم كود الفيروس في مكان تخزين آخر. وعندما يقرأ النظام سجل الإقلاع الرئيسي **MBR** المصاب. يقوم الفيروس بإصدار تعليمات للنظام بتنفيذ الكود المخزن في مكان التخزين الإضافي، وبالتالي يتم تحميل كامل الفيروس في الذاكرة وتنفيذ شحنته.

2. فيروسات تصيب الملفات:

تصيب العديد من الفيروسات أنواع من الملفات التنفيذية حيث ينطلق الفيروس عندما يحاول نظام التشغيل تنفيذ هذه الملفات. لأجل نظم **windows** تنتهي هذه الملفات باللاحقات **.EXE** و**.COM**.

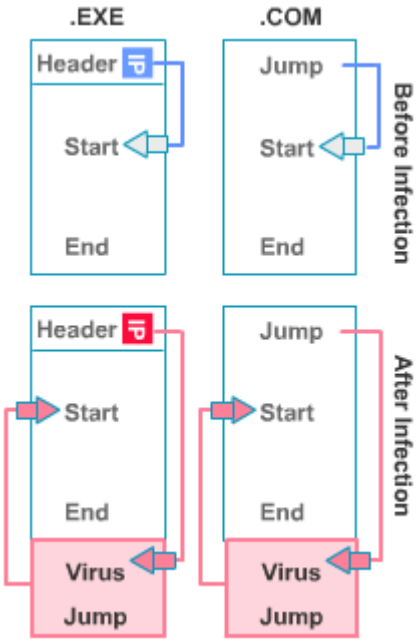
أحياناً تؤدي إجراءات تكاثر الفيروس الذي أصاب الملف إلى تعديل طفيف لكود البرنامج التنفيذي. بحيث يطبق التقنيات التي يحتاجها الفيروس ليكرر نفسه ويدمر النظام. و في بعض الحالات قد يستبدل الفيروس نسخة الملف كاملة بأخرى مصابة.

بالنسبة إلى الفيروسات التي لا تستخدم تقنيات التستر مثل الخفية **stealth** و التعمية فإنه من السهل كشفها بمقارنة مميزاتها (مثل الحجم وتاريخ التعديل) قبل وبعد الإصابة أو بمقارنة قيم المزج **hash values**.

ويوجد نوع آخر مختلف من الفيروسات التي تصيب الملف هي الفيروس المرافق **companion virus**. هذه الفيروسات مكتفية ذاتياً من ناحية الملفات التنفيذية، بمعنى أنها لا تستخدم ملف تنفيذي موجود مسبقاً وإنما تولد ملفاتها التنفيذية الخاصة بها وهي تتهرب من الكشف بأن تستخدم أسماء مشابهة لأسماء ملفات شرعية لنظام التشغيل مع تغيير طفيف في الاسم.

تعتمد هذه الفيروسات على اللاحقات الافتراضية التي تضيفها نظم تشغيل المبنية على **DOS** إلى الأوامر عند تنفيذ ملفات البرامج (**.COM**،**.EXE**، و**.BAT** بهذا الترتيب).

فمثلاً إذا كان لديك برنامج على قرصك الصلب يدعى **GAME.EXE**. فإنه يمكن لفيروس مرافق أن يستخدم الاسم **GAME.COM**. فإذا فتحت نافذة **DOS** وكتبت **GAME** فقط سينفذ نظام التشغيل ملف الفيروس **GAME.COM** بدل من الملف الذي تريده فعلياً. وهذا سبب جيد جداً لعدم استخدام الأوامر المختصرة في نظام **DOS**.



3. فيروسات الماكروmacro viruses:

تنفذ العديد من البرمجيات الشائعة خطاطات وظائفية **Macro** وذلك لتساعد في أتمتة المهام المتكررة. تستخدم هذه الوظائف **functionalities** لغة برمجة سهلة لكن قوية، مثل:

Visual Basic–based VBScript.

بالرغم من أن الماكرو يقدم إلى مستخدمي الكومبيوتر إنتاجية عالية. إلا أنها تعرض الأنظمة للإصابة بفيروسات الماكرو **macro viruses.**

ظهر هذا النوع من الفيروسات في منتصف التسعينات ، و استخدم تقنيات خشنة لإصابة المستندات المنشأة باستخدام برنامج **Microsoft Word**. وبرغم أنها بسيطة نسبياً إلا أنها انتشرت بسرعة لأن مجتمع مضادة الفيروسات لم يكن يدرك وجودها، لذلك لم يقدم أي دفاعات ضدها . لكن أصبحت فيروسات الماكرو وبسرعة مبتذلة واعتيادية وتزاحم منتجو مضادات الفيروس لإنتاج برمجيات مضادة فيروسات لفحص المستندات بحثاً عن ماكروخبيث.

من أشهر فيروسات الماكرو فيروس **Melissa** الذي ظهر عام **1999** وانتشر من خلال استخدام مستندات **word**، حيث استغل نقطة ضعف أمنية في برنامج **Microsoft Outlook.**

وتبعه مباشرة فيروس **I love you** الذي اعتمد أيضاً على استغلال نقاط ضعف مشابهة.

بالرغم من أن معظم فيروسات الماكروتصيب المستندات المنشأة باستخدام برمجيات مجموعة **Microsoft Office**، إلا أن ذلك لا يعني أن مستخدمي التطبيقات الأخرى منيعين ضد مثل هذه الفيروسات.

2. آليات مكافحة الفيروسات Antivirus Mechanisms

تشغل معظم الحواسيب الموجودة في الخدمة اليوم إحدى رزم برمجيات مضادة الفيروسات . وتتنوع هذه البرمجيات من حماية الأنظمة الفردية إلى مشروع كامل **entire enterprise**. بالإضافة إلى الرزم المصممة للحماية ضد تهديدات الفيروسات لتطبيق محدد مثل البريد الالكتروني.

تستخدم الغالبية العظمى من هذه الرزم طريقة تدعى كشف التوقيع **signature detection** لتحدد إصابة النظام بالفيروس. عملياً، هي تحافظ على قاعدة بيانات ضخمة جداً تحتوي مميزات دلالية لكل أنواع الفيروسات. بالاعتماد على رزمة مكافحة الفيروس وإعدادات تركيبها. تقوم بفحص وسائط التخزين دورياً باحثةً عن ملفات تحتوي بيانات تطابق هذه المعايير.

فإذا وجدت أي منها، تقوم رزمة مكافحة الفيروس بإحدى الإجراءات التالية:

- إذا حددت الرزمة الفيروس لكنها لا تعرف كيف تطّهر الملفات، عندها يمكنها أن تحجر الملفات ريثما يستطيع المستخدم أومدير النظام فحصها يدوياً.
- إذا كانت الإعدادات الأمنية أوالسياسة الأمنية لا تسمح بالحجر ، أو أن الملفات تجاوزت في خطورتها عتبة الخطورة المسبقة التعريف ، يمكن لرزمة مضاد الفيروسات أن يحذف الملفات المصابة في محاولة للحفاظ على سلامة النظام.

عند استخدام رزم مكافحة الفيروسات التي تعتمد على التوقيع، من المهم أن تتذكر أن فعالية الرزمة تتوقف على مدى احتوائها على توقيعات الفيروسات وبالتالي إذا لم تحافظ عليها محدثة دوماً، لن تكون رزمة مضاد الفيروسات قادرة على كشف الفيروسات الحديثة. ومع ظهور آلاف الفيروسات سنوياً لن تقدم رزم مضاد الفيروس غير المحدثة أي دفاع ضد الفيروسات.

هناك رزم أمنية أخرى ، مثل رزمة **the popular Tripwire data integrity assurance package**. والتي تقدم وظيفة مضادة الفيروسات بشكل ثانوي. صممت هذه الرزمة لتنبه مدراء النظام عن التعديلات غير المخولة للملفات. وغالباً تستخدم لكشف هجمات تخريب مخدم الويب **defacements** والهجمات المشابهة. وإذا حدث تعديل مفاجئ لملفات نظام تنفيذية خطيرة مثل **COMMAND.COM** يمكن لهذه الرزم أن تقدم تحذير للاشتباه بالإصابة بفيروس. تعمل هذه النظم عن طريق المحافظة على قاعدة بيانات لقيم المزج لكل الملفات المخزنة في النظام. حيث تقارن هذه القيم المحفوظة بالقيم المحسوبة الحالية لكشف أي ملفات معدلة.

3. تقنيات الفيروس

ظهرت تقنية كشف واستئصال الفيروس لمواجهة الجديد من التهديدات المبرمجة من قبل المطورين "الخبثاء" ستشرح في هذه الفقرة أربعة أنواع من الفيروسات والتي تستخدم تقنيات "جبانة" لمحاولة التهرب من الكشف. وهي:

1. الفيروسات متعددة الأجزاء **multipartite viruses**.
2. الفيروسات الخفية **stealth viruses**.
3. الفيروسات المتعددة الأشكال **polymorphic viruses**.
4. الفيروسات المعماة **encrypted viruses**.
5. الخدعة **Hoaxes**.
6. القنابل المنطقية **Logic Bombs**.

1. الفيروسات متعددة الأجزاء multipartite viruses

يستخدم هذا النوع من الفيروسات أكثر من تقنية للتكاثر والانتشار في محاولة منه لاختراق الأنظمة التي أعدت للدفاع ضد نوع من الفيروسات.

فمثلاً، فيروس **Maizia** المكتشف عام **1993** والذي يصيب ملفات **COM.** و**EXE.** الهامة، و على الأغلب ملف النظام **COMMAND.COM**، حيث يضيف إلى كل ملف **2.048** بايت من الكود الخبيث، وهذه الميزة تصنفه كفيروس عدوى ملف **file infector virus**. بالإضافة لذلك ، فإنه وبعد ساعتين من إصابته للنظام، يقوم بكتابة كود خبيث في **MBR**، وبذلك يتحول إلى فيروس سجل الإقلاع الرئيسي.

2. الفيروسات الخفية Stealth Viruses

يخبئ هذا النوع من الفيروسات نفسه بالتأثير على نظام التشغيل ليقوم نظام التشغيل بالتلاعب ببرزم مضادة الفيروسات لتعتقد أن كل شيء يجرى بشكل طبيعي.

مثلاً، يمكن لفيروس قطاع الإقلاع المخفي أن يكتب على سجل الإقلاع الرئيسي للنظام **MBR** كود خبيث لكنه عندئذ سيعدل أيضاً وظائف نظام التشغيل الخاصة بالوصول إلى الملفات ليغطي أثره.

عندما تطلب رزمة مضاد الفيروس نسخة عن **MBR**، يقوم كود نظام التشغيل المعدل (المصاب) بإعطاء رزمة مضاد الفيروس ما تتوقع أن تراه، أي يعطيها نسخة **MBR** نظيفة من أي توقيع فيروس.

ومن جهة أخرى عندما يقلع النظام، يقرأ **MBR** المصاب ويحمل الفيروس إلى الذاكرة.

3. الفيروسات المتعددة الأشكال Polymorphic Viruses

هي فيروسات تغير كودها أثناء انتقالها من نظام لآخر. عملياً تبقى تقنيات التكاثر والتدمير في الفيروس على حالها، لكن يتغير توقيع الفيروس بشكل ما في كل مرة يصيب نظام جديد. حيث يأمل مطورو هذا النوع من الفيروسات أن التغيير الثابت في توقيع الفيروس سيجعل رزم مضاد الفيروسات المبنية على قاعدة بيانات عديمة الفائدة.

على كل حال، فقد استطاع منتجو مضادالفيروسات أن يكتشفوا أسرار العديد من تقنيات تعدد الأشكال وبالتالي فالنسخ الحالية لمضاد الفيروسات قادرة على كشف الفير وسات المتعددة الأشكال المعروفة.

ويبقى القلق الوحيد هوأنه يلزم لمنتجي مضاد الفيروسات وقت طويل لتوليد ملفات التوقيع الضرورية لإيقاف الفيروسات المتعددة الأشكال، مما ينتج طول المدة التي يمكن لهذه الفيروسات أن تطوف في الانترنت حرة.

4. الفيروسات المعماة Encrypted Viruses

تستخدم الفيروسات المعماة تقنيات تعمية لتفادي الكشف. وهي مشابهة جداً للفيروسات متعددة الأشكال في مظهرها الخارجي، حيث يختلف توقيع الفيروس من نظام مصاب لآخر لكنها لا تولد هذه التواقيع المتغيرة بتغيير كودها وإنما عبر تغيير طريقة تخزينها على القرص.

تستخدم الفيروسات المعماة جزء صغير من كود **segment**، تدعى إجراء فك تعمية الفيروس ، وهي تحتوي على معلومات التعمية الضرورية لتحميل وفك تعمية الكود الرئيسي للفيروس المخزن في مكان آخر من القرص. يستخدم مفتاح مختلف لأجل كل عملية عدوى جديدة. مما يجعل الكود الرئيسي يظهر وكأنه يختلف من نظام لآخر. على كل حال، فإن إجرائيات فك التعمية تحتوي غالباً تواقيع دلالية تجعلها غير حصينة أمام رزم مضاد الفيروسات المحدثة.

5. الخدعة Hoaxes

لا يمكن استكمال أي مناقشة حول الفيروسات بدون ذكر الإزعاج واستهلاك الموارد و الذي يتسبب به فيروس الخدعة **Hoaxes**.

تقريباً كل مستخدم للبريد الالكتروني يستقبل من وقت لآخر، رسالة تحذيرية من صديق حول تهديد من قبل فيروس جديد يطوف الانترنت، له قدرات تدميرية كبيرة ولا توجد أي رزم مضادة فيروسات تكشفه أوتستأصله. أحد أهم وأشهر الأمثلة عن هذه الفيروسات هو فيروس **Good Times** الذي ظهر عام **1994** ولا يزال يطوف في الانترنت حتى يومنا هذا.

6. القنابل المنطقية Logic Bombs

هي أجزاء برمجية خبيثة تصيب النظام وترقد في حالة سبات حتى تنطلق عند تحقق شرط أو أكثر.

تبرمج الغالبية العظمى من القنابل المنطقية لتصيب التطبيقات المبنية بشكل مخصص للزبون ، حيث يبنيها مطوروالتطبيقات في محاولة منهم لتأكيد أن العمل سينهار إذا تركوا العمل في الشركة بشكل مفاجئ.

تعمل العديد من القنابل المنطقية ببطء بالاعتماد على تاريخ النظام أوتوقيته. مثلاً، يمكن أن يضع الموظف الذي أنهيت خدمته قنبلة منطقية تنطلق في الذكرى السنوية لتركه العمل لتدمر بيانات عمل خطيرة.

يوجد أنواع أخرى من القنابل المنطقية تستخدم معايير أكثر تعقيداً. مثلاً. قد يقوم المبرمج الـذي يخاف من إنهاء خدمته في شركة بزرع قنبلة منطقية في نظام الشركة تقوم بتعديل الرواتب حالما يقفل حساب المبرمج.

4. الديدان Worms

تعتبر الديدان من أنواع الكود الخبيث المثيرة للاهتمام والتي تشابه الفيروسات بشكل كبير. مع اختلاف واحد أساسي. فهي تنتشر كالفيروسات من نظام إلى آخر، حاملة نوع ما من الحمولات الخبيثة فبينما تحتاج الفيروسات إلى المشاركة كي تتكاثر وتنتشر، تعمد الدودة على نفسها للتكاثر، حيث تبقى في سبات في الذاكرة ثم تستغل نقطة ضعف أو اثنتين في الشبكة لتنتشر من نظام لآخر باستخدام قوتها الخاصة. تسمح هذه الميزة بانتشار أضخم ويمكن أن تنتج هجوم إنكار الخدمة ضد كامل الشبكة.

سوف ندرس في هذا الفصل:

1. دودة الانترنت.
2. دودة **Code Red**.

1. دودة الانترنت

أطلقت دودة الانترنت عام **1988** وعطلت الانترنت لعدة أيام. وقد ولدها طالب في علوم الحاسب لأهداف تدريبية. لكنها خرجت عن السيطرة وانتشرت بسرعة كبيرة مخربة عدد كبير من الأنظمة. ولعل انتشار هذه الدودة يعود لاستغلالها أربعة فجوات أمنية في أنظمة تشغيل **Unix** آنذاك هي:

1. **نمط كشف وتحديد أخطاء إرسال البريد Send mail debug mode:**

كانت نسخ رزم برمجيات البريد الالكتروني الشائعة آنذاك المستخدمة لتوجيه رسائل البريد الالكتروني عبر الانترنت تحتوي على نقاط ضعف أمنية. نقاط الضعف هذه سمحت للدودة بنشر نفسها بإرسال رسالة بريد الكتروني تحتوي على كود الدودة إلى برنامج البريد على الحاسب البعيد. الذي يصاب بالعدوى بمجرد استلامه هذه الرسالة.

2. **هجوم كلمة المرور:**

استخدمت الدودة هجوم القاموس **dictionary attack** لمحاولة كسب وصول إلى الأنظمة البعيدة باستخدام اسم مستخدم وكلمة مرور لمستخدم شرعي.

3. **Finger vulnerability:**

تسمح تقنية **finger** للمستخدمين أن يحددوا من سجل دخولهم إلى الحاسب البعيد. آنذاك كانت نسخ برمجيات **finger** تحتوي نقطة ضعف **buffer overflow** التي تسمح للدودة بالانتشار. لذلك منذ ذلك الوقت أزيل برنامج **finger** من معظم الأنظمة المتصلة بالانترنت.

4. علاقات الثقة Trust relationships:

بعد أن تصيب الدودة النظام، تحلل أي علاقة ثقة مع الأنظمة الأخرى على الشبكة وتحاول نشر نفسها إلى هذه الأنظمة من خلال طرق الثقة. هذه الميزة جعلت دودة الانترنت خطيرة جداً.

2. دودة Code Red

كانت دودة الانترنت هي الحادث الأمني الرئيسي الأول على الانترنت. ومنذ ذلك الوقت أطلقت العديد من الدودات عبر الانترنت تفاوتت في قدرتها على الانتشار والتدمير، لكن في صيف 2001 أطلقت دودة **Code Red** التي انتشرت بسرعة كبيرة بين مخدمات الويب التي تشغل نسخ غير معدلة من **Microsoft's Internet Information Server (IIS)**.

تجري هذه الدودة ثلاث نشاطات تخريبية في الأنظمة التي تخترقها:

1. تختار عشوائياً مئات عناوين الانترنت ثم تفحص فيما إذا كانت هذه الحواسب تشغل نسخة **IIS** غير حصينة. عندما تجد إحداها تقوم بنقل نفسها إلى المخدم الجديد وتقوم مباشرة بإجراء عملية بحث أخرى مما يسرع في عملية الانتشار.

2. تشوه صفحات الانترنت على مخدم الويب المحلي، حيث تستبدل المحتوى الأصلي بالنص التالي:

Welcome to http://www.worm.com!
Hacked By Chinese!

3. تزرع قنبلة منطقية تقوم ببدء هجوم رفض الخدمة **denial of service attack** ضد عنوان الانترنت **198.137.240.91**. والذي كان في ذلك الوقت ينتمي إلى مخدم الويب الذي يخدم الصفحة الرئيسية للبيت الأبيض. لذلك فقد قام مدراء النظام الحكومي بسرعة بتغيير عنوان انترنت البيت الأبيض قبل أن يبدأ الهجوم فعلياً.

5. حصان طروادة Trojan Horses

هو كود خبيث يظهر كبرنامج طبيعي (غير مؤذي) مثل لعبة أو أداة بسيطة، و عند تشغيل التطبيق يؤدي حصان طروادة الوظائف المفترض من برنامج الخدعة أن يؤديها، لكنه أيضاً ينفذ كود آخر له نشاطات خبيثة مختلفة.

وبالتالي عندما يكون المستخدم يستخدم التطبيق الجديد يكون حصان طروادة ينفذ أيضاً نشاطات خبيثة، مثل فتح ثغرة أمنية في النظام ليقوم المهاجمين باستغلالها والتلاعب بالبيانات أو تنصيب برنامج مراقبة لوحة المفاتيح.

تختلف أحصنة طروادة من الناحية الوظيفية بشكل واسع فبعضها تدمر كل البيانات المخزنة في النظام في محاولة لإحداث أكبر ضرر ممكن في وقت قصير. وبعضها الآخر ضار نوعاً ما.

مثال:

ظهرت سلسلة من أحصنة طروادة على الانترنت في منتصف عام **2002**، دعي أنها تقدم لمستخدمي الحواسب القدرة على تشغيل الألعاب المصممة لنظام **Microsoft Xbox gaming** على حواسبهم الشخصية.

عندما يشغل المستخدمون البرنامج (حصان طروادة). فهو ببساطة لا يعمل. وهويدرج قيم في **Windows Registry** تسبب فتح صفحات انترنت معينة في كل مرة يقلع فيها الحاسب. وقد أمل مصممو حصان طروادة هذا أن يكسبوا من ريع الإعلانات التي ستظهر في الكم الكبير من صفحات الانترنت التي يظهرها برنامجهم.

تعابير وكلمات دليلية

الفصل الأول: أساسيات أمن الحاسب	
confidentiality	الخصوصية
integrity	السلامة
availability	الإتاحة
vulnerabilities	نقاط الضعف
authorized	مخولين
logic bombs	قنابل منطقية
unauthorized access	دخول غير مرخص
Trojan horse	تشغيل برامج خبيثة
denial of service	هجمات حجب الخدمة
physical security	الأمن الفيزيائي
encryption	التعمية
plain text	النص الصريح
cipher text	النص المعمى
decryption	فك التعمية
Cipher	المعمية
Nonrepudiation	التبرأ
authentication	الاستيقان
Symmetric Key Algorithms	خوارزميات المفتاح المتماثل
Asymmetric Key Algorithms	خوارزميات المفتاح غير المتماثل
key management algorithm	خوارزميات تبادل المفاتيح
hashing algorithm	خوارزميات الاختصار
access control	التحكم بالدخول
authorization	التخويل
accounting and auditing	المحاسبة و التدوين
identification	التعريف

password	كلمات السر
access control matrix	مصفوفة التحكم بالدخول
Access Control List ACL	قائمة التحكم بالدخول
Privileges	الامتيازات
Role-based access control RBAC	أدوار التحكم بالدخول
security model	نموذج الأمن
state	الوضع

تعابير وكلمات دليلية

الفصل الثاني: أمن الشبكات	
Threat Models	نماذج المهددات
FireWall	جدار النار
Active Attacker	مهاجم تفاعلي
Passive Attacker	مهاجم غير تفاعلي
Traffic analysis	محلل حركة المرور
eavesdropping	بمسترق السمع
wiretapping	المتنصت
sniffing	الشمام
spoofing attacks	هجمات الرسائل المزيفة
flooding	هجمات الطوفان
squatting	هجمات الاحتلال
invoking facilities	مسهلات
Header	ترويسة
Trailer	تذييل
Payload	الحمولة
Application Layer	طبقة التطبيق
Transport Layer	طبقة النقل
Internet Layer	طبقة الانترنت
Link Layer	طبقة الربط
Ports	البوابات
ICMP	بروتوكول الإدارة
IP Security	أمن بروتوكول **IP**
stateless	عديم الحالة
Authentication Header	ترويسة الاستيقان **AH**
Encapsulating Security Payload	الحمولة الأمنية المغلفة **(ESP)**
replay protection	عملية إعادة الاستخدام

Security Parameter Index	فهرس معاملات الأمن **(SPI)**
security association SA	الرابط الأمن
Padding	البطانة
integrity check value (IVC)	قيمة اختبار السلامة
transport mode	نمط النقل
frame	الإطار
Host	عقد
Tunnel mode	نمط النفق
router	موجه
firewall	جدار نار
Initial Vector	أشعة ابتدائية **IVs**
anti-replay window	نافذة منع الإعادة
Security Association Data base	قاعدة بيانات تدعى **SAD**
Internet Key Exchange	تبادل مفاتيح الانترنت **IKE**
Message Authentication code	رمز استيقان الرسائل **MAC**
Hashing Algorithm	خوارزمية الاختزال
aggressive mode	النمط الهجومي
Security Policy Data base	قاعدة بيانات سياسة أمنية **SPD**
secure socket layer SSL / Transport Layer Security TLS connection-oriented	بروتوكول الأمن على طبقة النقل \ الأمن على طبقة المقابس
encryption	متابعة الرزم و تحسس لضياع الرزم التعمية
reliable delivery	التسليم الموثوق
Certification	الشهادات
Shared Secret Keys	المفاتيح السرية المتشاركة
Handshake Protocol	بروتوكول مصافحة **SSL**
subject alternative name	توسيعات الاسم الإضافي للموضوع
PreMasterSecet	السر الأساسي
checksums	مجاميع الاختبار
Honypots	جرار العسل

reflection attack	هجوم الانعكاس
ChangeCipherSpec	مواصفات المعمية
DNS (Domain name system)	أسماء النطاقات
DNS lookup	خدمة البحث
reverse lookup	خدمة البحث العكسي
spoofing prevention	منع التزييف
dial- in	شبكات الدخول الهاتفية
Virtual Private Network (VPN)	شبكة خاصة افتراضية
state	الحالة
iptables	جداول عناوبين الانترنت
Filter	الترشيح
Circuit – level proxies	الوكلاء في طبقة الدارة
Proxy	الوكيل
spam	الحشو
hardened PC	حواسيب مدعمة
permissive Polices	سياسات السماح
Restrictive Polices	سياسات التقييد
Access Control List	قائمة السياسة الأمنية **ACL**
Perimeter Network	الشبكات المحيطية
demilitarized Zone (DMZ)	منطقة منزوعة السلاح
Intrusion detection	كشف الاقتحام
denial-of-service	هجوم رفض الخدمة
Intrusion detection system	نظام كشف الاقتحام **(IDS)**
misuse detection	كشف سوء الاستخدام
anomaly detection	كشف الشذوذ
vulnerability assessment	تقييم نقاط الضعف
attack signature	أثر هجوم أو توقيعه
overflow attack	هجوم الفيضان
Network-based- ID	كاشفات الخرق المعتمدة على الشبكة
Host-based IDS	الكاشفات المبنية على أساس الحاسب المضيف\المخدم

تعابير وكلمات دليلية

الفصل الثالث: أمن النقال	
Mobile Station	الهاتف النقّال بـ MS
Mobile Equipment	جهاز الهاتف النقّال بـ ME
Subscriber Identity Module	بطاقة هوية المشترك SIM
Base Station	المحطة الأساسية BS
Mobile Switching Center	مركز التحويل الهاتف النقّال MSC
Home Location Register	سجل أماكن الموقع الرئيسي للمشترك HLR
Authentication Center	مركز الاستيقان AuC
Visitor Location Register	سجل موقع الزائر VLR
International Mobile Subscribe Identity IMSI	هوية المشترك الدائمة
TMSI	هوية المشترك المؤقتة
visited	الشبكة المزارة
ciphering indicator	ميزة مؤشر التعمية
PIN(personal identification number)	معرف شخصي
PUK(personal unblocking key)	مفتاح فك قفل شخصي
frames	إطارات البيانات
location-based Service	الخدمات المعتمدة على الموقع
Signaling Data	لبيانات الإشارة
Universal Mobile Telecommunication System	نظام الاتصالات النقّالة العالمي UMTS
UE	أداة المستخدم
False Base Station Attacks	هجمات المحطة الرئيسية المزيفة
SQN	رقم تسلسلي للتزامن
RAND	رقم عشوائي
Message Authentication Code	رسالة الاستيقان المرمزة MAC
operator	مقسم
deneal-of-sevice	هجمات حجب الخدمة
interface ID	معرف الواجهة

home address HoA	عنوان المقر الرئيسي
access points	نقاط عبور
Service Set Identifier SSID	معرف تهيئة خدمة
hot spot	بالبقع الساخنة
Universal Access Mechanism UAM	آلية الدخول العام
preshared secrets	أسرار مسبقة التشارك
Initial Vector	شعاع ابتدائي IV
checksum	مجموع اختباري
Pairwise Master Key	زوج مفاتيح رئيسية طويل الأمد (PMK)
Pairwise Transient Keys PTKs	أزواج مفاتيح مؤقتة

تعابير وكلمات دليلية

الفصل الرابع: أمن قواعد البيانات	
a data base system	نظام إدارة قاعدة البيانات DBMS
internal consistency	توافق داخلي
external consistency	توافق خارجي
tuple Relational Database	قواعد البيانات العلائقية
Structured Query Language SQL	بلغة الاستعلام الهيكلية
View	المَشهد
Query	الاستعلام
primary key	المفتاح الرئيسي
Uniqueness	الوحدانية
Minimality	الأصغر
Foreign Key	مفتاح مساعد (ثانوي)
Integrity Roles	وظائف السلامة
Entity Integrity Rule	قاعدة سلامة الوجود
Referential Integrity Rule	قاعدة سلامة المرجعية
Integrity Trigger	زناد السلامة
SNAPSHOTS	اللقطات
Completeness	الكمال
consistency	التوافق
SQL security mod	نمط أمن SQL
Actions	أحداث
TABLE	جداول
privileges	امتيازات
grantor	مانح
grantee	منحة
object	غرض
grantable	الممنوح

GRANT	منح
cascade	خاصية
subquery	فالاستعلام الجزئي
aggregate	تجميعة
query predicate	صدر الاستعلام
query set	مجموعة الاستعلام
Aggregation	التجميع
Inference	الاستنتاج
tracker	هجوم المتتبع
individual tracker	بمتتبع إفرادي
general tracker	المتتبع العام
Privacy	السرية
cascade	التعدي

تعابير وكلمات دليلية

الفصل الخامس: الكود الخبيث Malicious	
Malicious	الكود الخبيث
viruses	فيروسات
Trojan Horses	حصان طروادة
hacker	القراصنة
Master Boot Record	سجل الإقلاع الرئيسي MBR
macro	الماكرو
hash values	قيم المزج
companion virus	الفيروس المرافق
Macro	خطاطات وظائفية
macro viruses	فيروسات الماكرو
Antivirus Mechanisms	آليات مكافحة الفيروسات
signature detection	كشف التوقيع
multipartite viruses	الفيروسات متعددة الأجزاء
stealth viruses	الفيروسات الخفية
polymorphic viruses	الفيروسات المتعددة الأشكال
encrypted viruses	الفيروسات المعماة
Hoaxes	فيروس الخدعة
Logic Bombs	القنابل المنطقية
Worms	الديدان
Sendmail debug mode	نمط كشف و تحديد أخطاء إرسال البريد
dictionary attack	هجوم القاموس
Trust relationships	علاقات الثقة
denial of service attack	هجوم رفض الخدمة