الموضوع الاول :خصائص الشبكة اللاسلكية

الموضوع الثاني :امنية الشبكة

خصائص الشبكة اللاسلكية

- يتم توصيل الأجهزة المعروفة باسم نقاط الوصول (APs) بالشبكة السلكية في مواقع ثابتة ،ونظرًا للنطاق المحدود، فإن معظم شبكات WLANالتجارية (على سبيل المثال في الحرم الجامعي أو في المطار) تحتاج إلى عدة نقاط وصول للسماح باتصالات لاسلكية غير منقطعة. تستخدم نقاط الوصول إما تقنية **الطيف المنتشر** (وهي تردد لاسلكي عريض النطاق يتراوح مداه بين حوالي 30 إلى 50 مترًا) أو **الأشعة تحت الحمراء** ولكن هذا له نطاق قصير جدًا (أي حوالي 1 إلى 2 متر) ويمكن حظره بسهولة، وبالتالي فهو محدود الاستخدام.

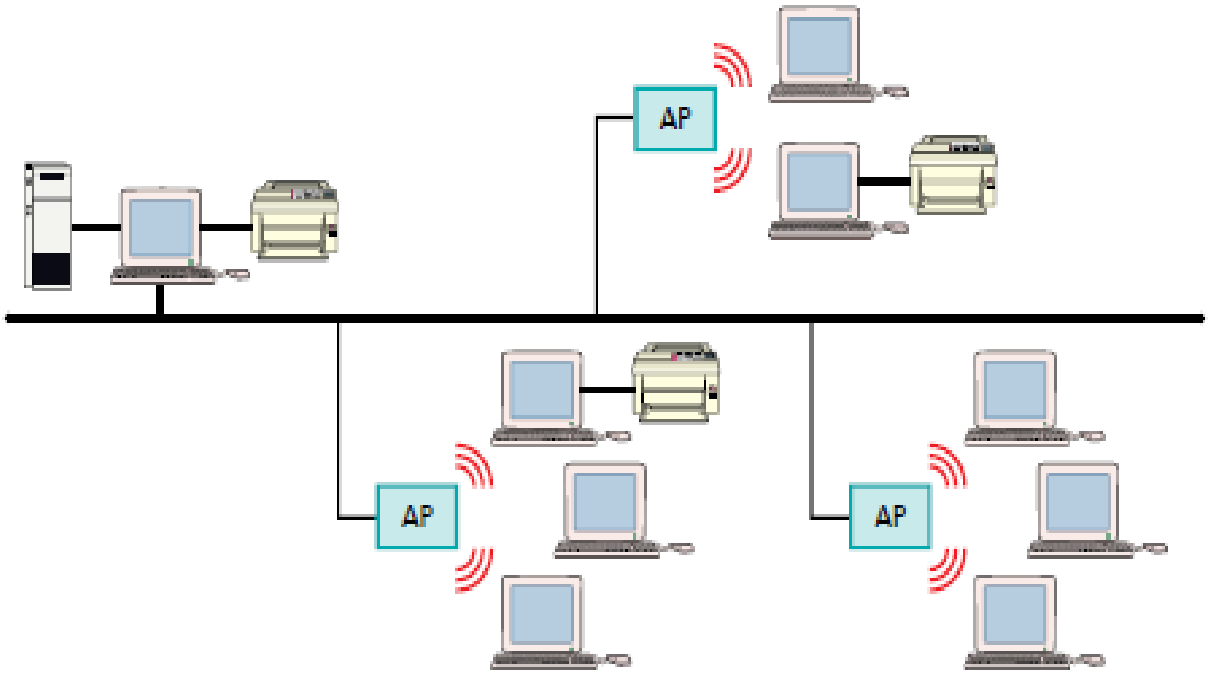

Figure 4.5 A network connecting WLANs

- تستقبل نقطة الوصول البيانات وتنقلها بين شبكة WLANوبنية **الشبكة السلكية**. ويستطيع المستخدمون الوصول إلى شبكة WLANمن خلال محولات شبكة WLAN، والتي تكون مدمجة في الأجهزة أو عبارة عن وحدات قابلة للتوصيل.

المزايا يمكن لجميع أجهزة الكمبيوتر الوصول إلى نفس الخدمات والموارد (على سبيل المثال، الطابعات، والماسحات الضوئية،وإمكانية الوصول إلى الإنترنت من أي مكان ضمن نطاق نقاط الوصول).

- لا توجد كيبلات لأجهزة الكمبيوتر والأجهزة الفردية، وبالتالي يتم تحسين السلامة.
- النظام أكثر مرونة، حيث يمكن للمستخدمين نقل أجهزة الكمبيوتر المحمولة الخاصة بهم من مكاتبهم.

عيوب الشبكة اللاسلكية

- يعد الأمان مشكلة كبيرة نظرًا لأن أي شخص لديه حاسوب محمول مزود بشبكة WLANيمكنه الوصول إلى الشبكة إذا كان بإمكانه التقاط إشارة. لذلك من الضروري تبني تقنيات تشفير البيانات المعقدة.
- قد تكون هناك مشاكل تداخل يمكن أن تؤثر على الإشارة.
- معدل نقل البيانات أبطأ من معدل نقل البيانات في شبكة LANالسلكية.

wifi

- يشير مصطلح WiFiإلى أي نظام يمكن من خلاله الاتصال بشبكة أو بجهاز كمبيوتر واحد من خلال الاتصالات اللاسلكية
- تعتمد أنظمة WiFiعلى شكل ما من أشكال نقاط الوصول، والتي تستخدم تقنية التردد اللاسلكي لتمكين الجهاز من استقبال وإرسال الإشارات.لاحظ أن WiFiليس اختصارًا لـ wireless fidelityمفهوم خاطئ شائع! .بل هو اسم العلامة التجارية لأي منتج يعتمد على معيار .IEEE802.11

البلوتوث

- هو مثال على تقنية **الشبكات الشخصية اللاسلكية** (WPAN) يتم استخدام نقل الطيف المنتشر (الموجات الراديوية) لتوفير روابط لاسلكية بين الهواتف المحمولة وأجهزة الكمبيوتر وغيرها من الأجهزة المحمولة والسماح بالاتصال بالإنترنت.باستخدام هذا النظام، من الممكن إنشاء شبكة منزلية صغيرة، على سبيل المثال، للسماح بالاتصال بين أي جهاز مساعد رقمي شخصي (PDA)وهاتف محمول وجهاز كمبيوتر ومشغل وسائطوطابعة. ومع ذلك، فإن النطاق صغير جدًا (حوالي 10 أمتار). تشمل أمثلة استخدامهنقل الصور من الكاميرا الرقمية إلى الهاتف المحمول أونقل تفاصيل الهاتف إلى الكمبيوتر. إنه يتصرف مثل شبكة LANصغيرة.

أمن الشبكات

- هناك العديد من المشاكل الأمنية الموثقة تنشأ عند استخدام شبكات مثل الإنترنت. فهناك العديد من التهديدات الأمنية التي تتعرض لها الشبكات وهناك العديد من الطرق المتنوعة لمكافحة هذه التهديدات. سيتم التركيز على أربعة مجالات:

1. معرف المستخدم(user ID)
2. كلمة المرور Password
3. التشفيرEncryption
4. تقنيات المصادقة Authentication techniques.

معرفات المستخدم(User IDs)

- عند تسجيل الدخول إلى أي نظام شبكة، سيُطلب من المستخدم كتابة معرف مستخدم.يؤدي هذا إلى تعيين **امتيازات المستخدم** بمجرد نجاح إجراء تسجيل الدخول على سبيل المثال،على الشبكة، يكون الامتياز الأعلى مستوى للمسؤول، الذي يمكنه تعيينكلمات المرور، وحذف الملفات من الخادم، وما إلى ذلك، بينما قد يسمح امتياز المستخدم فقطبالوصول إلى منطقة عمله الخاصة.

كلمات المرور

- بعد إدخال معرف المستخدم، سيُطلب من المستخدم كتابةكلمة المرور الخاصة به. يجب أن تكون هذه عبارة عن مزيج من الأحرف والأرقام التي قد يكون من الصعب على أي شخص آخر تخمينها. عند كتابة كلمة المرور، غالبًا ما تظهر على الشاشة على هيئة ******** حتى لا يتمكن أي شخص من رؤية ما كتبه المستخدم. إذا لم تتطابق كلمة مرور المستخدم مع معرف المستخدم، فسيتم رفض الوصول. تطلب العديد من الأنظمة كتابة كلمة المرور مرتين للتحققمن أخطاء الإدخال. للمساعدة في حماية النظام، يُسمح للمستخدمين فقط بإدخال كلمة المرور الخاصة بهم عددًا محدودًا من المرات - عادةً ما يكون الحد الأقصى لعدد المحاولات المسموح بها قبل أن يقفل النظام المستخدم. بعد ذلك، لن يتمكن المستخدم من تسجيل الدخول حتى يعيد مسؤول النظام تعيين كلمة المرور الخاصة به.عند استخدام بعض مواقع الإنترنت، إذا نسي المستخدم كلمة المرور الخاصة به، فيمكنهطلب إرسال كلمة المرور إلى عنوان بريده الإلكتروني

التشفير

- التشفير هو تحويل البيانات إلى رمز عن طريق خلطها أو ترميزها.يتم ذلك باستخدام برنامج تشفير (أو مفتاح تشفير). نظرًا لأن البيانات كلها متداخلة، فإنها تبدو بلا معنى بالنسبة للمخترق أو أي شخص يصل إلى البيانات بشكل غير قانوني. يجب التأكيد على أن هذه التقنية لا تمنع الوصول غير القانوني، بل إنها تجعل البيانات عديمة الفائدة لشخص ما إذا لم يكن لديه برنامج فك التشفير الضروري (أو مفتاح فك التشفير). يتم استخدامه لحماية البيانات المهمة (مثل التفاصيل المصرفية للشخص).

يعمل النظام على النحو التالي:يكتب المستخدم رسالة ويستخدم الكمبيوتر الذي يرسل هذه الرسالة مفتاح تشفير لتشفير البيانات. على سبيل المثال، يتم تشفير الرسالة "هذا مثال" (المرسلة في 15 أبريل) إلى "Kr Kr T7 43 W04887W".في الطرف الآخر، يمتلك الكمبيوتر المتلقي مفتاح فك تشفير يستخدمه لفك تشفير الرسالة. لاحظ أن تاريخ إرسال الرسالة مهم لأنه يشكل جزءًا من خوارزمية التشفير.مفاتيح التشفير أكثر تعقيدًا بكثير من المفتاح أعلاه، وذلك لمنع استخدام أجهزة الكمبيوتر لكسر الشفرة. يتم استخدام خوارزميات متطورة للغاية مما يجعل الشفرات غير قابلة للكسر تقريبًا

تقنيات المصادقة

- كما هو موضح أعلاه، هناك العديد من الطرق التي يمكن لمستخدم الكمبيوتر من خلالها إثبات هويته.ويُطلق على ذلك المصادقة، ويُستخدم نوع من المصادقة في المثال المصرفي الذي يلي. تتبنى معظم الأنظمة منطق المصادقة التالي:شيء تعرفه - على سبيل المثال رقم التعريف الشخصي/كلمة المرورشيء يخصك - على سبيل المثال بطاقة البنك الخاصة بك شيء فريد لك - على سبيل المثال بصمات أصابعك.هناك حاجة إلى اثنين على الأقل من هذه في اللحظة التي يتعين على المستخدم فيها إثبات هويته. على سبيل المثال، يستخدم المثال المصرفي التالي:شيء تعرفه - اللقب، رقم المرجع، رقم التعريف الشخصي، تاريخ آخر تسجيل دخول شيء يخصك - يتم إدخال البطاقة في قارئ البطاقات لإنتاج الرمز المكون من 8 أرقام. وفي المستقبل، سيتم تقديم الميزة الثالثة (مثل ماسح بصمات الأصابع المرفق بالكمبيوتر لتحديد هوية المستخدم بشكل فريد).