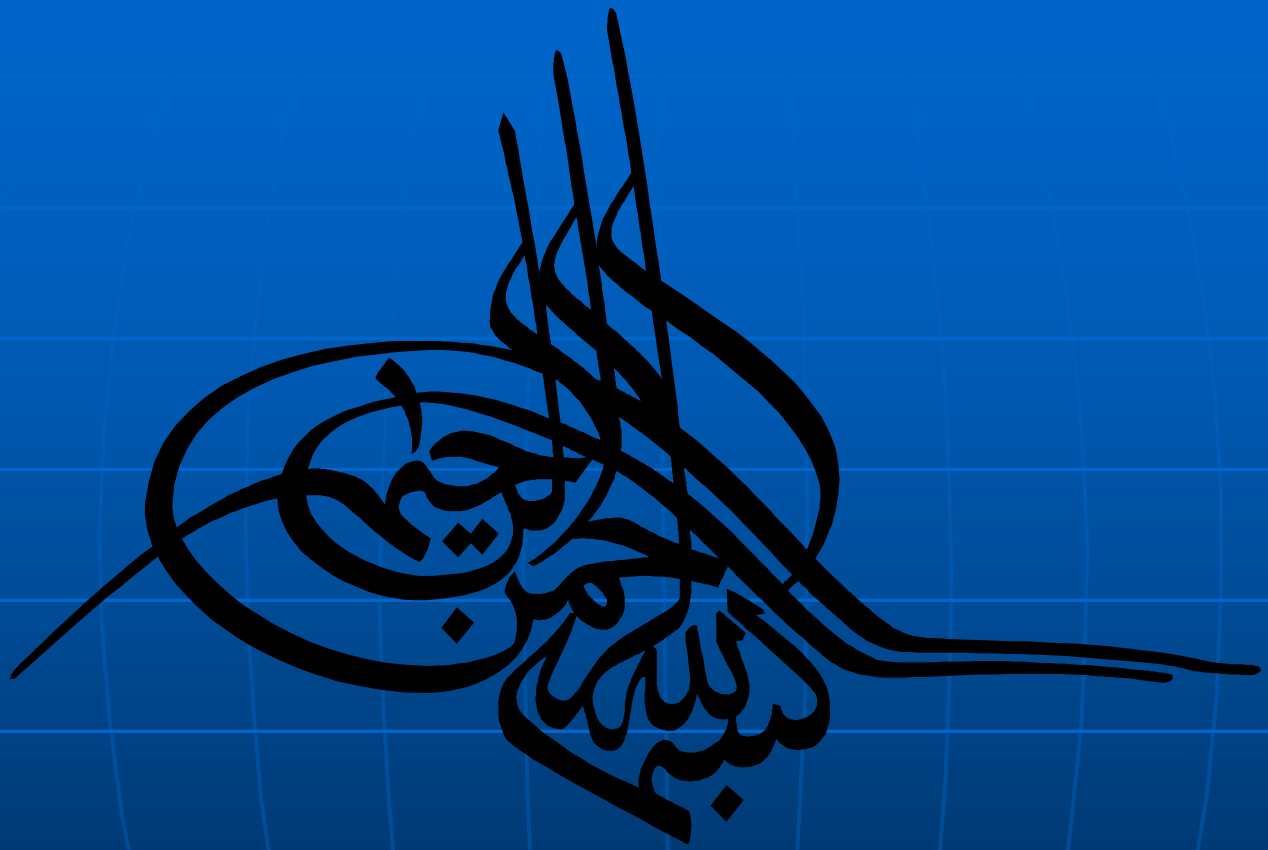

بسم الله الرحمن الرحيم

امنیت اطلاعات و هکر ها

مقدمه

امنیت به معنی حفاظت از داده‌ها در مقابل کاربران غیر مجاز است.
حصول اطمینان کاربران از مجاز بودن در رابطه با انجام کاری که برای آن تلاش می‌کنند.

حفاظت از داده‌ها در مقابل افشای غیرمجاز، تغییر یا تخریب.
سیستم نیازمند آگاهی از قیود معینی است که کاربران نباید آنها را نقض کنند.

امنیت پایگاه داده و اطلاعات (Data Security)چیست؟

امنیت پایگاه داده فرآیند حفاظت از داده های سازمان در برابر دسترسی و استفاده غیر مجاز، افشاگری، تخریب و یا تغییر می باشد .

مدیریت امنیت داده زیر مجموعه ای از مدیریت تکنولوژی اطلاعات می باشد که خود نیزشامل زمینه های مختلفی می باشد.

پایگاه های داده و به طبع امنیت داده های سازمان در واقع اصلی ترین چالش مدیران عامل و مسئولان IT سازمان می باشد .امروزه

گسترش استفاده از سیستم های کامپیوتری، سایت های اینترنتی و برنامه های کاربردی موجب گردیده که مباحث مربوط به امنیت

پایگاه داده دارای اهمیت بسیار بالایی باشد و در نتیجه با توجه به نقش اطلاعات به عنوان کالای با ارزش در تجارت امروز، لزوم

حفاظت صحیح ازآن ضروری تر به نظر می رسد. برای رسیدن به این هدف هر سازمان بسته به ارزش داده های خود، نیازمند پیاده

سازی یک سیاست کلی جهت مدیریت امنیت داده ها می باشد.

امنیت اطلاعات تهدیدی بزرگ برای سازمانها

به عنوان یک مدیرعامل، مدیر فناوری اطلاعات و یا راهبر پایگاه داده ، به چه میزان از امنیت

اطلاعات سازمان خود اطمینان دارید ؟ - آیا منابع اطلاعاتی (پایگاه های داده) سازمان خود را

به خوبی می شناسید ؟ آیا دسترسی و استفاده از این اطلاعات به خوبی کنترل می شود؟ آیا تا به

حال به این موضوع اندیشیده اید که در صورت افشای اطلاعات حساس موجود در پایگاه های

داده شرکت شما چه اتفاقی رخ می دهد؟

امنیت اطلاعات تهدیدی بزرگ برای سازمانها

باید به این نکته توجه داشته باشید که در بسیاری از موارد هزینه افشای اطلاعات و داده ها جبران ناپذیر است و در بسیاری

موارد دیگر سازمان را متحمل ضرر های بسیاری می کند.

از آنجایی که مسائل امنیتی اغلب به سادگی دیگر بخشهای فن آوری اطلاعات، توجیه اقتصادی قابل لمس ندارند، بنابراین این امر

در بسیاری از موارد (به طور عام در کشور ما) مورد توجه مدیران ارشد سازمان قرار گرفته نمی شود.

بحث امنیت اطلاعات و به طور خاص مدیریت امنیت پایگاه های داده نیازمند مهارتهای خاص همچون راهبری امنیت پایگاه داده

می باشد. متاسفانه به دلیل گستردگی دانش های فوق و عدم اولویت امنیت در سایر فعالیتهای فناوری، این بحث از نظر مدیران

فناوری اطلاعات و راهبران پایگاه داده به میزان لازم مورد توجه قرار گرفته نمی شود.

این موضوع، کلیه فعالیتهای تجاری سازمان را همیشه با یک ریسک بزرگ روبرو می سازد.

مفاهیم اصلی امنیت اطلاعات

امنیت داده ها به چهار مفهوم کلی قابل تقسیم است :

- محرمانگی (Confidentially)
- تمامیت (Integrity)
- اعتبار و سندیت (Authenticity)
- دسترس پذیری (Availability)

مفاهیم اصلی امنیت اطلاعات

- **محرمانگی (Confidentially):**
محرمانگی اطلاعات یعنی حفاظت از اطلاعات در مقابل دسترسی و استفاده غیر مجاز . داده های محرمانه

تنها توسط افراد مجاز قابل دسترسی می باشند.

- **تمامیت (Integrity):**

در بحث امنیت اطلاعات، تمامیت به این معناست که داده ها نمی توانند توسط افراد غیر مجاز ساخته، تغییر

و یا حذف گردند. تمامیت ، همچنین یکپارچگی داده ها که در بخشهای مختلف پایگاه داده ذخیره شده اند را

تحت الشعاع قرار می دهد.

مفاهیم اصلی امنیت اطلاعات

- **اعتبار و سندیت (Authenticity)**

اعتبار و سندیت دلالت بر موثق بودن داده ها و نیز اصل بودن آنها دارد. به طریقی که اطمینان حاصل شود

داده ها کپی یا جعلی نیستند.

- **دسترس پذیری (Availability)**

دسترس پذیری به این معنی می باشد که داده ها، پایگاه های داده و سیستمهای حفاظت امنیت، در زمان

نیاز به اطلاعات در دسترس باشند.

حفره امنیتی

پیامدهای منفی یک حفره امنیتی چیست؟

- کاهش درآمدوافزایش هزینه
- خدشه به اعتبار و شهرت یک سازمان
- ازدست دادن اطلاعات مهم پیامدهای قانونی
- سلب اعتماد مشتریان و سرمایه گذاران

مزایای سرمایه گذاری در امنیت اطلاعات

- کاهش احتمال غیر فعال شدن سیستم ها و برنامه ها
- استفاده موثر از منابع انسانی و غیر انسانی در یک سازمان
- کاهش هزینه از دست دادن داده
- افزایش حفاظت از مالکیت معنوی

مدیریت خطرات امنیتی

رویکرد پیشگیرانه چیست؟

- شناسایی تهدیدات موجود در یک سازمان
- اولویت بندی خطرات
- نحوه مدیریت در یک سطح قابل قبول
- کاهش خطر آسیب پذیری

مدیریت خطرات امنیتی

دستاوردهای پیاده سازی فرایند مدیریت خطرات امنیتی

- زمان پاسخ به تهدیدات
- مدیریت قانونمند
- هزینه های مدیریت زیر ساخت
- مدیریت و اولویت بندی خطرات

هکرها

روش‌های حمله

و

راه‌های مقابله با آنها

هکرها چه کسانی هستند؟

هکر به معنای نفوذگر ، به شخصی اطلاق می‌شود که هدف اصلی او نشان دادن قدرت خود به کامپیوتر و سایر ماشین‌ها می‌باشد. هکر یک برنامه‌نویس کنجکاو است که صدمه‌ای وارد نمی‌کند ، حتی باعث تحکیم انتقالات می‌شود. در واقع این افراد محافظان شبکه هستند که با بررسی ضعف‌های شبکه سعی در تصحیح و تقویت خطوط ارتباطی می‌کنند.

خصوصیات هکرها:

1) وارد شدن به سیستم
2) شکست دادن محاسبات
3) کنجکاوی در اطلاعات محرمانه

دسته‌بندی هکرها:

1-**(White Hat Hackers Group)**گروه نفوذگران کلاه سفید
2-**(Black Hat Hackers Group)**گروه نفوذگران کلاه سیاه
3-**(Gray Hat Hackers Group)** گروه نفوذگران کلاه خاکستری
4-**(Pink Hat Hackers Group)**گروه نفوذگران کلاه صورتی

انواع حملات هکرها:

* حمله از نوع دستکاری اطلاعات (Modification):

* حمله از نوع افزودن اطلاعات (Fabrication):

* حمله از طریق استراق سمع (Sniffation):

* حمله از نوع وقفه (Interruption):

انگیزه‌های حمله هکرها:

1) بدست آوردن ثروت از طریق جابجا کردن داده‌ها و یا پیدا کردن کارت اعتباری
2) جاسوسی و کسب اطلاعات از سایر سازمان‌ها
3) آزار رسانی و کسب شهرت در میان مردم (بیشتر جنبه‌ی روانی دارد)
4) فاش کردن اطلاعات محرمانه
5) قطع ارتباط و یا اختلال در ارتباط
6) اهداف تروریستی و خرابکارانه
7) تفریح و امتحان کردن دیواره‌های امنیتی
8) انتقام و ضربه زدن

تعدادی از حملات معروف که توسط هکرها انجام می‌شوند:

1) حمله از طریق **IP**

2) حمله از طریق **TCP**

3) حمله از طریق **Applet**

4) حمله از طریق **Fire Wall**

5) حمله از طریق جعل کردن وب

6) حمله به کلمات عبور

7) حمله از طریق استراق سمع

8) حمله از طریق مودم ها

1) حمله از طریق IP (Internet Protocol):

این نوع حمله ساده‌ترین حمله هکرها است. این روش حمله در دو مرحله انجام می‌گیرد:

1- جستجو 2- نفوذ و انجام عملیات

هکر اول تمام تلاش خود را برای بدست آوردن **IP** صرف می‌کند ؛ این کار با بررسی ، پردازش دستی و فکری داده‌های در حال تبادل امکان‌پذیر است. همچنین می‌توان آنها را از ترتیبی که در اتصال به شبکه انجام شده ، پیدا کرد. پس از کشف شماره‌های سریال‌های آدرس **IP** ، هکر خود را در بین سرویس دهنده و کاربر قرار می‌دهد و با ارسال بسته‌های تقلبی ، اطلاعات را به سرقت می‌برد.

2) حمله از طریق TCP (Transmission Control Protocol):

این نوع حمله از متداول‌ترین نوع حمله به سرویس دهنده‌های مرتبط با اینترنت است. هدف اصلی هکر از حمله به **TCP** تحت کنترل درآوردن کامپیوترهایی است که از طریق سرویس دهنده به شبکه متصل شده‌اند. هکر در این روش کاربر را از سرویس دهنده جدا ساخته و خود را به جای کاربر به سرویس دهنده معرفی می‌کند به طوری که سرویس دهنده هکر را به عنوان یک کاربر معتبر بشناسد ؛ از این پس هرگونه تبادلات بین سرویس دهنده و هکر انجام می‌شود. حمله به **TCP** بسیار آسان‌تر و مؤثرتر از حمله به **IP** است و کار را راحت‌تر می‌کند ، چرا که در این روش هکر تنها یک بار حمله می‌کند و از مقابله با سیستم‌های امنیتی رمز عبور فرار می‌کند.

3) نفوذ به کامپیوتر از طریق Applet:

Applet توسط مرورگرها به حافظه بارگذاری می‌شوند ، **Applet**ها اغلب توسط برنامه **Java** نوشته می‌شوند. **Applet**های مخربی می‌توان نوشت و آنها را بر روی وب سایت قرار داد. این **Applet**های مخرب جاسوس هکرها هستند که اعمال خواسته شده‌ی آنان را انجام می‌دهند. **Applet**ها از متداول‌ترین و مخرب‌ترین نوع حملات هکرها به حساب می‌آیند. هکر در **Applet** به صورتی عمل می‌کند تا مرورگر به صورت پیوسته و مکرر آنها را اجرا نماید که غالباً این نوع حمله به متوقف شدن سیستم می‌انجامد.

4) حمله از طریق Fire Wall:

روشی که هکرها به وسیله آن از دیواره آتش عبور می‌کنند **Fire Wall** نام دارد. در این روش هکر پورت‌های باز در دیواره آتش را مورد بررسی قرار داده و سعی می‌کند تا دیواره آتش را کنار گذاشته و راه‌های ارتباطی را باز نماید. دانستن این که کدام پورت دیواره آتش باز است ، از اطلاعات بی‌نهایت سودمند است.

5) حمله از طریق مودم‌ها:

Modem یکی از رایج‌ترین ابزارهای ارتباطی مربوط به شبکه است ؛ مودم به کاربر امکان می‌دهد تا از طریق خط تلفن به شبکه متصل شده و به تبادل اطلاعات بپردازند. محصولات کنترل از راه دور به کاربران امکان می‌دهند تا به تمام منابع کامپیوتر خود دسترسی داشته باشند. اگر در این محصولات سیستم امنیتی تنظیم نشود ، بهترین راه نفوذ هکرها می‌شوند. هکر در اولین مرحله اقدام به تهیه فهرستی از شماره تلفن‌هایی که مودم به آنها متصل می‌شود ، می‌نماید و سپس توسط ابزار مربوطه ، شماره تلفن را کنترل می‌نماید. پس از شماره‌گیری و در صورت ارتباط ، سیگنالی ارسال می‌شود و هکر آن شماره را در لیست قرار می‌دهد.

6) حمله به کلمات عبور:

این نوع حمله یکی از پرطرفدارترین و کارآمدترین نوع حمله‌ها می‌باشد. در بسیاری از سازمان‌ها کلمات عبور بسیار معمولی ، اغلب از بسیاری اطلاعات حساس محافظت می‌کنند. متأسفانه با وجود سیستم‌های امنیتی ، این کلمات عبور ضعیف به راحتی کشف شده و هکر به این اطلاعات دسترسی پیدا می‌کند. به خاطر این گونه مشکلات است که هر کاربر یک کلمه عبور و حتی برخی چند کلمه عبور دارند. نرم‌افزارهای بسیاری جهت پیدا کردن کلمات عبور وجود دارند.

7) استراق سمع داده‌ها:

Snifferها ابزاری هستند که هکر به وسیله آنها در لایه فیزیکی شبکه اقدام به استراق سمع داده‌ها می‌کند. **Sniffer**ها فقط جهت استراق سمع داده‌ها مورد استفاده قرار می‌گیرند و در تغییر داده‌ها نقشی ندارند. اطلاعاتی که **Sniffer** به سرقت می‌برد امنیت تک تک ماشین‌های شبکه محلی را به خطر می‌اندازد.

8) جعل کردن یک وب:

یکی دیگر از شیوه‌های حمله هکرها جعل کردن یک وب می‌باشد. در این روش یک نسخه از وب سایت کپی می‌شود ؛ وب کپی شده دارای تمام ظواهر وب اصلی است ، اما در پس زمینه کلمات عبور و رمزهای وارد شده توسط بازدیدکنندگان این صفحه‌ی جعلی برای هکر ارسال می‌شوند و تمام اعمال زیر نظر وی انجام می‌گیرند.

مقابله با نفوذ از طریق مودم‌ها:

اگر شبکه دارای مودم ناامن و بدون کلمات عبور باشد ، به راحتی مورد حمله هکرها قرار می‌گیرد ؛ البته پیشگیری از این نوع حملات ساده است. استفاده از یک خط شماره‌گیری و مودم قوی اولین راه پیشگیری است. اگر به مودم احتیاج است باید آنها را تحت نظارت کلی سیستم و خط شماره‌گیری در بیاورید ، همچنین در مواقعی که به آنها احتیاجی نیست باید غیرفعال شوند. به علاوه از کلمات عبور طولانی و دشوار استفاده شود. زمانی که شما برای مودم خود یک کلمه عبور دشوار قرار دهید ، هکرها هرچه قدر که به شبکه و خطوط شما آشنا باشند ، باید برای هر کاراکتر کلمه شما وقت بسیاری را صرف کنند. به عنوان مثال اگر کلمه عبور شما دارای 20 کاراکتر و ترکیبی از حروف و اعداد باشد ، هکر جهت کشف آن با سیستمی به سرعت **2 GHz** نیاز به یک هفته زمان دارد. همچنین اگر از سیستم تغییر کلمه‌ی عبور خودکار استفاده کنید ، هکرها شانس بسیار کمی برای پیدا کردن این کلمه عبور دارند.

مقابله با جستجوی پورت‌های باز:

برای مقابله با این حمله بهترین عمل این است که تمام پورت‌های باز و بی‌مصرف را ببندید. هکر پورت‌های باز را جستجو می‌کند تا در هنگام حمله آنها را مورد استفاده قرار دهد و راه خود را به داخل شبکه باز کند. بیشترین حملات هکرها ناشی از باز بودن این پورت‌ها است.

مقابله با شناسایی از طریق وب:

برای آن که یکی از قربانیان حملات در سایت‌های وب نباشید و هکر نتواند از طریق وب به شناسایی شبکه شما اقدام کند ، در ابتدا سعی کنید که میزان حساسیت و سطح امنیت مورد نیاز شبکه را مورد بررسی قرار دهید و سپس تعیین کنید که چه اطلاعاتی باید محرمانه بمانند و چه اطلاعاتی می‌توانند در اختیار کاربران قرار گیرند.

مقابله با شکستن رمزهای عبور:

برای مقابله با این حملات ابتدا باید کلمات عبوری انتخاب کنید که در فرهنگ لغات نباشند ؛ کلمه‌هایی که از یک سری عدد و حروف درهم ریخته تشکیل می‌شوند درصد احتمال بسیار کمی برای کشف شدن دارند ؛ همچنین هر چه قدر طول کلمه عبور بیشتر باشد ، هکر باید زمان بیشتری جهت شکستن رمز عبور صرف کند.

نرم‌افزار فیلترگذار کلمات عبور ، کلیه این اعمال را انجام می‌دهد ؛ این برنامه با دریافت نام و کلمه عبور جدید ، آنها را طبق الگویی که شما برایش تعریف می‌کنید ، کنترل می‌نماید. آخرین روش دفاعی در این گونه از حمله هکرها به کارگیری سیستم کدبندی رمزهای عبور است. این برنامه کلیه رمزها و کلمات عبور را به وسیله یک کد مخصوص ، که فقط برای سیستم عامل معنی دارد ، انتقال می‌دهد.

مقابله با حمله‌های ناشی از حدس زدن شماره سریال:

ساده‌ترین و کارامدترین شیوه برای محافظت در برابر حمله های ناشی از حدس زدن شماره سریال این است که مطمئن شوید مسیریاب و هر یک از سرویس دهنده‌های موجود در سیستم شما از سیستم حفاظتی بررسی ردپا برخوردار هستند یا خیر. هرگاه یک هکر بخواهد در میان مسیریاب و دیوار آتش قرار گیرد و عملیات نفوذی خود را انجام دهد ، می‌توانید حرکات وی را مشاهده نمایید.

امنیت در کامپیوترهای شخصی (جلوگیری از نفوذ هکرها):

تا اینجا بحث درباره سیستم‌های شبکه بود. سیستم‌های خانگی نیز مورد حملات هکرها قرار می‌گیرند مخصوصاً در ایران!!!

بیشتر حملات هکرها در کامپیوترهای خانگی در اتاق‌های گفتگو **(Chat Rooms)** رخ می‌دهند. اگر بر روی سیستم قربانی اسب تراوا **(Trojan Horse)** وجود داشته باشد ، به محض اتصال به اینترنت ، یک نامه شامل آدرس ، پورت ، نام کاربر و کلمه عبور برای هکر به آدرسی که از قبل تعیین کرده است ارسال می‌گردد. شما به عنوان یک کاربر از دریافت و بازکردن نامه‌های بی‌نام و نشان ، ناآشنا و مشکوک به طور جدی خودداری کنید. استفاده از دیوار آتش بهترین روش در جلوگیری از حملات می‌باشد. اغلب هکرهای ایرانی جوانانی هستند که از برنامه‌های آماده استفاده می‌کنند ؛ این برنامه‌ها قادر به جستجوی رمز برای هر کلمه‌ی عبوری نمی‌باشند و محدودیت‌هایی در این زمینه دارند. از اجرای نرم‌افزارهای ارسالی کاربران دیگر خودداری نمایید.

آخرین نکات در مورد مقابله با حملات هکرها:

1) به هر کسی اعتماد نکنید (مهندسی اجتماعی).

2) اگر سیستم شما دچار مشکل شد ، آن را تحویل شخص غریبه‌ای ندهید.

3) از دریافت و اجرای برنامه‌های رایگان و عجیب مثل برنامه‌هایی که سرعت اینترنت را افزایش می‌دهند ، تا اطمینان کامل کسب نکرده‌اید ، خودداری کنید.

4) اگر بر روی سیستم خود فایل مهمی دارید ، آن را در حالت فقط خواندنی و پنهان قرار دهید تا هکر قادر به تغییر داده‌های آن فایل نباشد.

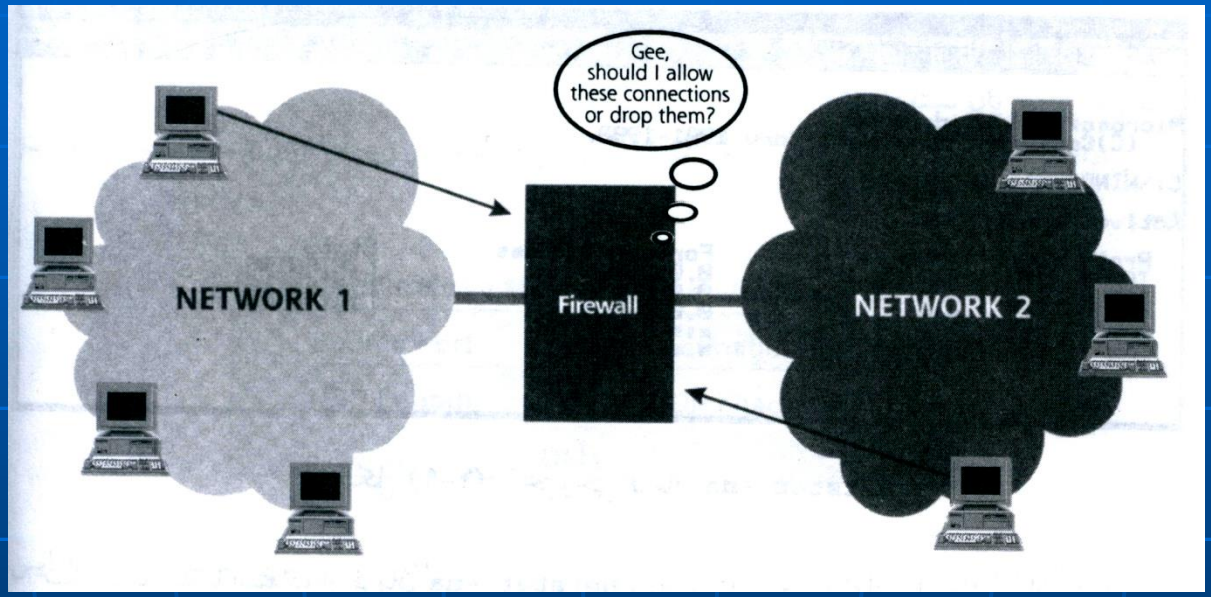
5) بر روی سیستم خود جدیدترین نسخه ضد ویروس را نصب کنید تا همیشه از وجود ویروس‌ها در امان و مطلع باشید.

6) در هنگام چَت در **Messenger**ها از نام مستعار استفاده کنید ؛ این کار باعث می‌شود تا هکر نتواند کلمه عبور شما را حدس بزند.

FIREWALL

دیوارآتش

دیوارآتش سیستمی است که در بین کاربران یک **شبکه محلی و شبکه بیرونی** قرار می گیرد و ضمن نظارت بر دسترسی ها، در تمام سطوح ورود و خروج اطلاعات را تحت نظر دارد.



قبل از ورود IP به شبکه ابتدا وارد دیوارآتش می‌TCPبسته های شوند و منتظر می مانند تا طبق معیار های حفاظتی و امنیتی پردازش شوند.

پس از پردازش و تحلیل بسته سه حالت ممکن است اتفاق بیافتد :

Accept Modeاجازه عبور بسته صادر شود.

Blocking Modeبسته حذف گردد.

Response Modeبسته حذف شود و پاسخ مناسب به آن داده شود.

به مجموعه قواعد دیوارآتش سیاست امنیتی گفته می شود.

همانطور که همه جا عملیات ایست و بازرسی وقت گیر است دیوارآتش هم بعنوان یک گلوگاه می تواند موجب تاخیر و ازدحام شود.

بن بست زمانی رخ می دهد که بسته ها آنقدر در حافظه دیوارآتش معطل شوند تا طول عمرشان تمام شود و فرستنده مجددا اقدام به ارسال می نماید؛ به همین دلیل طراحی دیوارآتش نیاز به طراحی صحیح و دقیق دارد تا از حالت گلوگاهی خارج شود.

از آنجایی که معماری شبکه بصورت لایه به لایه است، در مدل TCP/IP برای انتقال یک واحد اطلاعات از لایه چهارم بر روی شبکه ، باید تمام لایه ها را بگذراند؛ هر لایه برای انجام وظیفه خود تعدادی فیلد مشخص به ابتدای بسته اطلاعاتی اضافه کرده و آن را تحویل لایه زیرین می دهد.

قسمت اعظم کار دیوارآتش

تحلیل فیلد های اضافه شده در هر لایه و سرآیند هر بسته

می باشد.

با توجه به لایه لایه بودن معماری شبکه، طراحی دیوارآتش نیز چند لایه می باشد.

پیچیدگی پردازش در لایه سوم بسیار زیاد است

دیوارهای آتش یا فیلترهایی که قادرند مشخصات ترافیک خروجی از شبکه را برای مدتی حفظ کنند و بر اساس پردازش آنها مجوز عبور صادر نمایند، فیلتر حالت مند نامیده می شوند.

فیلتر های معمولی کار آیی لازم را برای مقابله با حملات ندارند زیرا آنها بر اساس یکسری قواعد ساده بخشی از ترافیک بسته های ورودی به شبکه را حذف می نمایند.

بسادگی قواعد دیواره آتش Firewallامروزه نرم افزارهایی مثل را کشف کرده و در اختیار نفوذ گران قرار می دهند.

نفوذگران برای آنکه داده های مخربشان حذف نشود تلاش می کنند آنها را با ظاهری TCP/IPبا تنظیم مقادیر خاص در فیلدهای بسته کاملا مجاز از میان دیوارآتش یا فیلتر به درون شبکه بفرستند.

برای مقابله با عملیاتهای کشف و شناسایی عملکرد دیوارآتش در برخورد با بسته ها، دیوارآتش باید فقط به آن گروه از بسته های قبلی ارسال SYN اجازه ورود بدهد که در پاسخ به SYN-ACK شده اند.

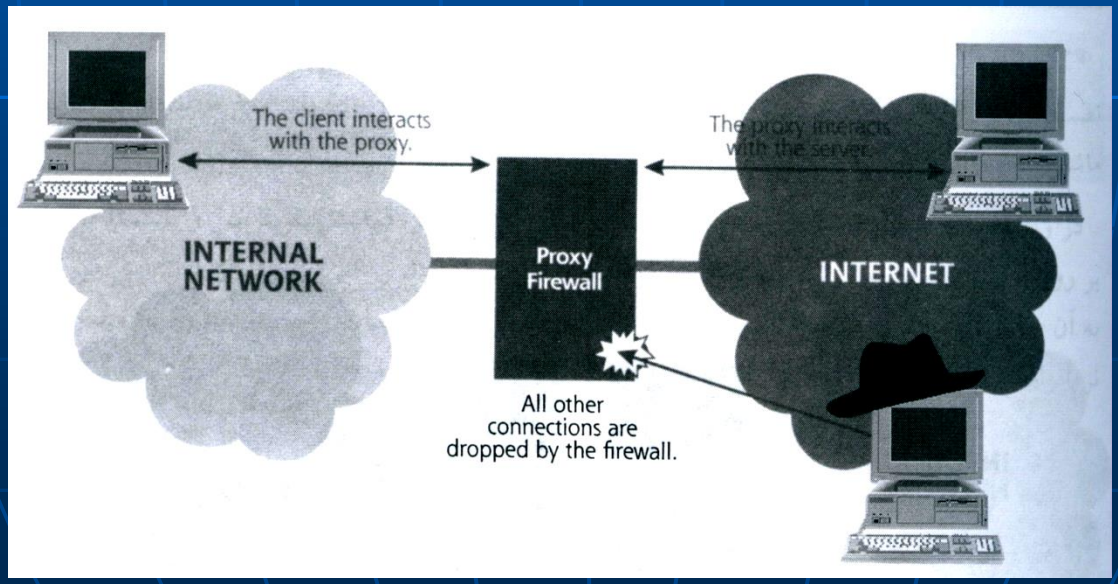
یعنی دیوارآتش باید **پیشینه بسته های قبلی** را حفظ کند تا در مواجهه با چنین بسته هایی، بدرستی تصمیم بگیرد.

بزرگترین مشکل این فیلتر ها غلبه بر **تاخیر پردازش و حجم حافظه** مورد نیاز می باشد ولی در مجموع قابلیت اعتماد بسیار بالاتری دارند و ضریب امنیت شبکه را افزایش خواهند داد.

فیلترها ی معمولی و حالت مند **فقط نقش ایست و بازرسی** را ایفا می کنند

هرگاه مجوز برقراری یک اتصال صادر شد این نشست بین دو ماشین داخلی و خارجی بصورت مستقیم برقرار خواهد شد؛ بدین معنا که بسته های ارسالی از طرفین پس از بررسی، عینا تحویل آنها خواهد شد.

وقتی ماشین مبدا تقاضای یک اتصال را برای ماشین مقصد ارسال می کند، فرآیند زیر اتفاق می افتد :



پراکسی به **نیابت از ماشین مبدا**، این اتصال را برقرار می کند. یعنی طرف نشست دیوار آتش قرار می گیرد نه ماشین اصلی!

چون دیوار آتش مبتنی بر پراکسی، باید تمام نشستهای بین ماشینهای درون و بیرون شبکه را مدیریت و اجرا کند لذا **گلوگاه** شبکه محسوب می شود و هرگونه تاخیر یا اشکال در پیکر بندی آن، کل شبکه را با بحران جدی مواجه خواهد نمود.

اگر قرار باشد از دیوارآتش مبتنی بر پراکسی در شبکه استفاده شود، اندکی از کارآیی سرویس دهنده هایی که **ترافیک بالا** مانند وب دارند کاسته خواهد شد، زیرا پراکسی یک **گلوگاه** در شبکه محسوب می شود.

اگر سرویس دهنده ای را برای **کل کاربران** اینترنت پیکر بندی کنیم بهتر است در پشت یک دیوارآتش مبتنی بر **پراکسی** قرار نگیرد.

فیلتر ها و **دیواره های آتش معمولی سریعند** ولیکن قابلیت اعتماد کمتری دارند و نمی توان بعنوان حصار یک شبکه به آنها اعتماد نمود.

بهترین پیشنهاد **استفاده همزمان** از هر دو نوع دیوارآتش است.

رمزنگاری- راه حلی برای حفظ امنیت داده ها

تعریف رمز نگاری:

رمزنگاری علم کدها و رمزهاست. عبارت است از علم شناخت و بررسی اصول و روش های تبدیل یک پیغام محرمانه خوانا برای همه به پیغامی که به صورت رمز شده درآمده و فقط برای گیرنده مجاز قابل خواندن و رمزگشایی میباشد ▪یک هنر قدیمی است و برای قرنها بمنظور محافظت از پیغامهایی که بین فرماندهان ، جاسوسان ، عشاق و دیگران ردوبدل می‌شده ، استفاده شده است تا پیغامهای آنها محرمانه بماند.

رمزنگاری دو جزء اصلی دارد: 1- الگوریتم 2- کلید.

الگوریتم یک مبدل یا فرمول ریاضی است. کلید ، یک رشته از ارقام دودویی (صفر و یک) است که بخودی‌خود بی‌معنی است ▪روش های رمز نگاری مبتنی بر کلید است که توسط الگوریتم های متقارن و یا نا متقارن قابل پیاده سازی است.

رمزنگاری- راه حلی برای حفظ امنیت داده ها

۱- معرفی و اصطلاحات

هنگامی که با امنیت دیتا سروکار داریم ، نیاز به اثبات هویت فرستنده و گیرنده پیغام داریم و در ضمن باید از عدم تغییر محتوای پیغام مطمئن شویم. این سه موضوع یعنی

1- محرمانگی

2-تصدیق هویت

3-جامعیت

در قلب امنیت ارتباطات دیتای مدرن قرار دارند و می‌توانند از رمزنگاری استفاده کنند.

اغلب این مساله باید تضمین شود که یک پیغام فقط میتواند توسط کسانی خوانده شود که پیغام برای آنها ارسال شده است و دیگران این اجازه را ندارند. روشی که تامین کننده این مساله باشد "رمزنگاری" نام دارد.

رمزنگاری- راه حلی برای حفظ امنیت داده ها

۲- الگوریتم‌ها

طراحان سیستمهایی که در آنها از رمزنگاری استفاده می‌شود ، باید از نقاط قوت و ضعف الگوریتمهای موجود مطلع باشند و برای تعیین الگوریتم مناسب قدرت تصمیم‌گیری داشته باشند. به طور كلي دو نوع الگوريتم مبتني بر كليد وجود دارد:

1- سيستم هاي كليد متقارن

2- سيستم هاي كليد نامتقارن

امنیت در شبکه‌های بی‌سیم

تکنولوژی شبکه‌های بی‌سیم، با استفاده از انتقال داده‌ها توسط امواج رادیویی، در ساده‌ترین صورت، به تجهیزات سخت‌افزاری امکان می‌دهد تا بدون‌استفاده از بسترهای فیزیکی همچون سیم و کابل، با یکدیگر ارتباط برقرار کنند. شبکه‌های بی‌سیم بازه‌ی وسیعی از کاربردها، از ساختارهای پیچیده‌یی چون شبکه‌های بی‌سیم سلولی -که اغلب برای تلفن‌های همراه استفاده می‌شود- و شبکه‌های محلی بی‌سیم (WLAN – Wireless LAN) گرفته تا انوع ساده‌یی چون هدفون‌های بی‌سیم، را شامل می‌شوند. از سوی دیگر با احتساب امواجی همچون مادون قرمز، تمامی تجهیزاتی که از امواج مادون قرمز نیز استفاده می‌کنند، مانند صفحه کلیدها، ماوس‌ها و برخی از گوشی‌های همراه، در این دسته‌بندی جای می‌گیرند.
طبیعی‌ترین مزیت استفاده از این شبکه‌ها عدم نیاز به ساختار فیزیکی و امکان نقل و انتقال تجهیزات متصل به این‌گونه شبکه‌ها و هم‌چنین امکان ایجاد تغییر در ساختار مجازی آن‌هاست. از نظر ابعاد ساختاری، شبکه‌های بی‌سیم به سه دسته تقسیم می‌گردند:

WWAN، WLAN و WPAN.

مقصود از WWAN، که مخفف Wireless WAN است، شبکه‌هایی با پوشش بی‌سیم بالاست. نمونه‌یی از این شبکه‌ها، ساختار بی‌سیم سلولی مورد استفاده در شبکه‌های تلفن همراه است. WLAN پوششی محدودتر، در حد یک ساختمان یا سازمان، و در ابعاد کوچک یک سالن یا تعدادی اتاق، را فراهم می‌کند. کاربرد شبکه‌های WPAN یا Wireless Personal Area Network برای موارد خانگی است. ارتباطاتی چون Bluetooth و مادون قرمز در این دسته قرار می‌گیرند.

منشأ ضعف امنیتی در شبکه‌های بی‌سیم و خطرات معمول

خطر معمول در کلیه‌ی شبکه‌های بی‌سیم مستقل از پروتکل و تکنولوژی مورد نظر، بر مزیت اصلی این تکنولوژی که همان پویایی ساختار، مبتنی بر استفاده از سیگنال‌های رادیویی به‌جای سیم و کابل، استوار است. با استفاده از این سیگنال‌ها و در واقع بدون مرز ساختن پوشش ساختار شبکه، نفوذگران قادرند در صورت شکستن موانع امنیتی نه‌چندان قدرت‌مند این شبکه‌ها، خود را به‌عنوان عضوی از این شبکه‌ها جازده و در صورت تحقق این امر، امکان دست‌یابی به اطلاعات حیاتی، حمله به سرویس دهنده‌گان سازمان و مجموعه، تخریب اطلاعات، ایجاد اختلال در ارتباطات گره‌های شبکه با یکدیگر، تولید داده‌های غیرواقعی و گمراه‌کننده، سوءاستفاده از پهنای‌باند مؤثر شبکه و دیگر فعالیت‌های مخرب وجود دارد.

در مجموع، در تمامی دسته‌های شبکه‌های بی‌سیم، از دید امنیتی حقایقی مشترک صادق است :

1. تمامی ضعف‌های امنیتی موجود در شبکه‌های سیمی، در مورد شبکه‌های بی‌سیم نیز صدق می‌کند. در واقع نه تنها هیچ جنبه‌یی چه از لحاظ طراحی و چه از لحاظ ساختاری، خاص شبکه‌های بی‌سیم وجود ندارد که سطح بالاتری از امنیت منطقی را ایجاد کند، بلکه همان گونه که ذکر شد مخاطرات ویژه‌یی را نیز موجب است.
2. نفوذگران، با گذر از تدابیر امنیتی موجود، می‌توانند به‌راحتی به منابع اطلاعاتی موجود بر روی سیستم‌های رایانه‌یی دست یابند.
3. اطلاعات حیاتی‌یی که یا رمز نشده‌اند و یا با روشی با امنیت پایین رمز شده‌اند، و میان دو گره در شبکه‌های بی‌سیم در حال انتقال می‌باشند
4. حمله‌های DoS به تجهیزات و سیستم‌های بی‌سیم بسیار متداول است.
5. نفوذگران با سرقت کدهای عبور و دیگر عناصر امنیتی مشابه کاربران مجاز در شبکه‌های بی‌سیم، می‌توانند به شبکه‌ی مورد نظر بدون هیچ مانعی متصل گردند.

(ادامه)

6 با سرقت عناصر امنیتی، یک نفوذگر می‌تواند رفتار یک کاربر را پایش کند. از این طریق می‌توان به اطلاعات حساس دیگری نیز دست یافت.

7 کامپیوترهای قابل حمل و جیبی، که امکان و اجازه‌ی استفاده از شبکه‌ی بی‌سیم را دارند، به‌راحتی قابل سرقت هستند. با سرقت چنین سخت افزارهایی، می‌توان اولین قدم برای نفوذ به شبکه را برداشت.

، می‌توانند توسط نفوذگران سرقت شده یا تغییر یابند.

8 یک نفوذگر می‌تواند از نقاط مشترک میان یک شبکه‌ی بی‌سیم در یک سازمان و شبکه‌ی سیمی آن (که در اغلب موارد شبکه‌ی اصلی و حساس‌تری محسوب می‌گردد) استفاده کرده و با نفوذ به شبکه‌ی بی‌سیم عملاً راهی برای دست‌یابی به منابع شبکه‌ی سیمی نیز بیابد.

9 در سطحی دیگر، با نفوذ به عناصر کنترل کننده‌ی یک شبکه‌ی بی‌سیم، امکان ایجاد اختلال در عمل‌کرد شبکه نیز وجود دارد.

عناصر فعال شبکه‌های محلی بی‌سیم

ایستگاه بی سیم

نقطه ی دسترسی

شبکه‌های محلی بی‌سیم

1 ایستگاه بی سیم

ایستگاه یا مخدوم بی‌سیم به طور معمول یک کامپیوتر کیفی یا یک ایستگاه کاری ثابت است که توسط یک کارت شبکه‌ی بی‌سیم به شبکه‌ی محلی متصل می‌شود. این ایستگاه می‌تواند از سوی دیگر یک کامپیوتر جیبی یا حتی یک پویش گر بارکد نیز باشد. در برخی از کاربردها برای این‌که استفاده از سیم در پایانه‌های رایانه‌یی برای طراح و مجری دردسرساز است، برای این پایانه‌ها که معمولاً در داخل کیوسک‌هایی به‌همین منظور تعبیه می‌شود، از امکان اتصال بی‌سیم به شبکه‌ی محلی استفاده می‌کنند. در حال حاضر اکثر کامپیوترهای کیفی موجود در بازار به این امکان به‌صورت سرخود مجهز هستند و نیازی به اضافه‌کردن یک کارت شبکه‌ی بی‌سیم نیست.

کارت‌های شبکه‌ی بی‌سیم عموماً برای استفاده در چاک‌های PCMCIA است. در صورت نیاز به استفاده از این کارت‌ها برای کامپیوترهای رومیزی و شخصی، با استفاده از رابطی این کارت‌ها را بر روی چاک‌های گسترش PCI نصب می‌کنند.

(ادامه)

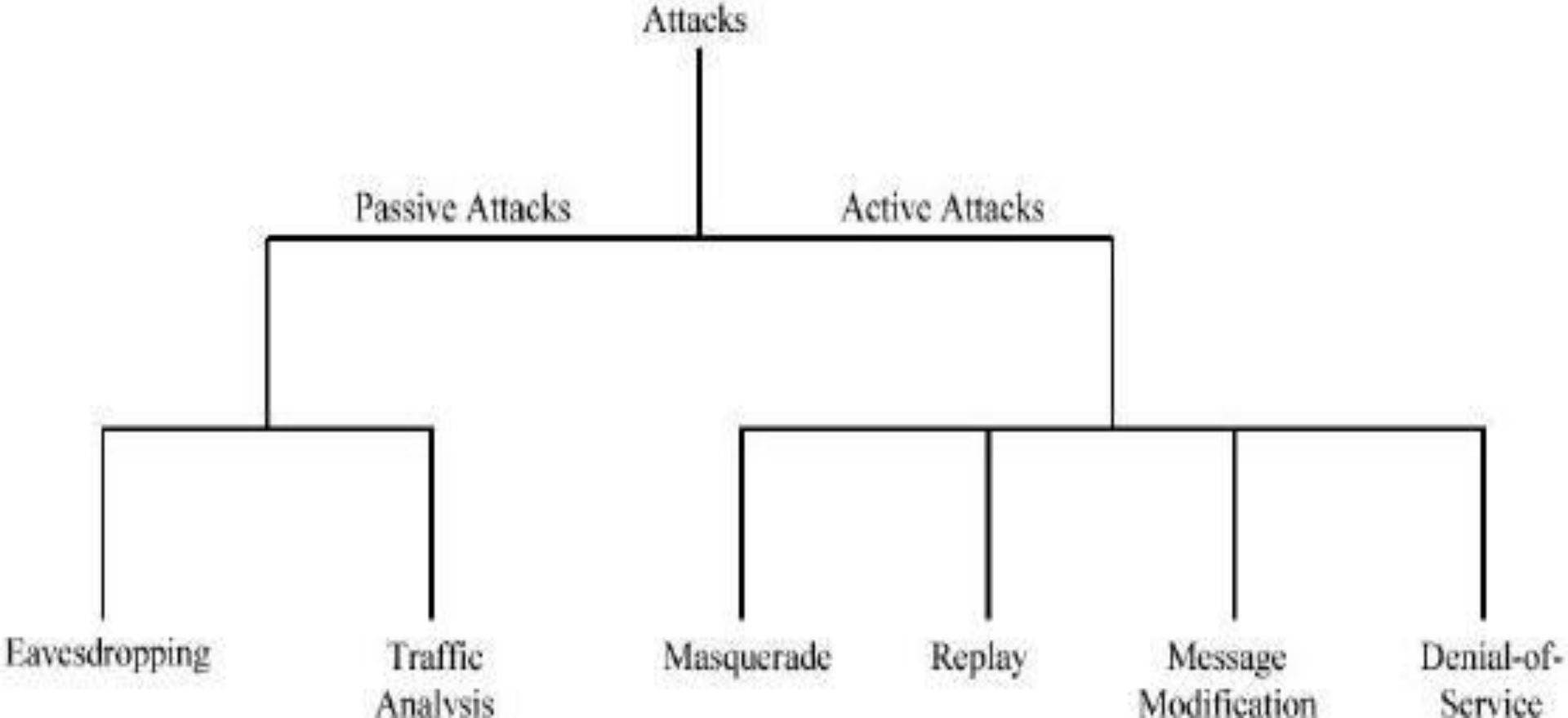
نقطه ی دسترسی

نقاط دسترسی در شبکه‌های بی‌سیم، همان‌گونه که در قسمت‌های پیش نیز در مورد آن صحبت شد، سخت افزارهای فعالی هستند که عملاً نقش سوییچ در شبکه‌های بی‌سیم را بازی‌کرده، امکان اتصال به شبکه های سیمی را نیز دارند. در عمل ساختار بستر اصلی شبکه عموماً سیمی است و توسط این نقاط دسترسی، مخدوم‌ها و ایستگاه‌های بی‌سیم به شبکه‌ی سیمی اصلی متصل می‌گردد.

خطرها، حملات و ملزومات امنیتی

همان گونه که گفته شد، با توجه به پیشرفت های اخیر، در آینده یی نه چندان دور باید منتظر گسترده گی هرچه بیش تر استفاده از شبکه های بی سیم باشیم. این گسترده گی، با توجه به مشکلاتی که از نظر امنیتی در این قبیل شبکه ها وجود دارد نگرانی هایی را نیز به همراه دارد. این نگرانی ها که نشان دهنده ی ریسک بالای استفاده از این بستر برای سازمان ها و شرکت های بزرگ است، توسعه ی این استاندارد را در ابهام فرو برده است. در این قسمت به دسته بندی و تعریف حملات، خطرها و ریسک های موجود در استفاده از شبکه های محلی بی سیم بر اساس استاندارد IEEE 802.11x می پردازیم.

شکل زیر نمایی از دسته بندی حملات مورد نظر را نشان می دهد :



مطابق درخت فوق، حملات امنیتی به دو دسته ی فعال و غیرفعال تقسیم می گردند.

حملات غیرفعال

شنود

آنالیز ترافیک

حملات فعال

تغییر هویت

پاسخ های جعلی

تغییر پیام

حمله هایDos (Denial-of-service)

هفت مشکل امنیتی مهم شبکه های بی سیم

مسأله شماره ۱: دسترسی آسان

راه حل شماره ۱ : تقویت کنترل دسترسی قوی

مسأله شماره ۲ : نقاط دسترسی نامطلوب

راه حل شماره۲ : رسیدگی های منظم به سایت

مسأله شماره ۳ : استفاده غیرمجاز از سرویس

راه حل شماره۳ : طراحی و نظارت برای تأیید هویت محکم

مسأله شماره ۴ : محدودیت های سرویس و کارایی

راه حل شماره۴ : دیدبانی شبکه

مسأله شماره ۵: جعل MAC و session

مسأله شماره ۶: تحلیل ترافیک و استراق سمع

راه حل شماره۶ : انجام تحلیل خطر

مسأله شماره ۷ : حملات سطح بالاتر

راه حل شماره ۷ : هسته را از LAN بی سیم محافظت کنید

ابعاد مختلف امنیت

* امنیت سیگنال (Signal Security)
* امنیت داده‌ها (Data Security)
* امنیت سیستم (System Security)

زواياي مختلف تحقيق در زمينة امنيت سيستم‌هاي اطلاعاتي

	سيستم‌هاي رمزنگاري	پروتكل‌هاي رمزنگاري	سيستم‌هاي عامل و زبان‌هاي برنامه‌نويسي	كاربردها	محيط‌هاي عملياتي
امنيت سيگنال					
امنيت داده‌ها					
امنيت سيستم					

زواياي مختلف تحقيق در زمينة امنيت سيستم‌هاي اطلاعاتي

	سيستم‌هاي رمزنگاري	پروتكل‌هاي رمزنگاري	سيستم‌هاي عامل و زبان‌هاي برنامه‌نويسي	كاربردها	محيط‌هاي عملياتي
امنيت سيگنال					
امنيت داده‌ها					
امنيت سيستم					

- اقدامات پشتيباني الكترونيك و ضدآن (ESM , CESM)
- اقدامات آگاهي از سيگنال و ضدآن (SIGINT , SIGSEC)
- اقدامات ضد الكترونيكي و ضدآن (ECM , ECCM)

زواياي مختلف تحقيق در زمينة امنيت سيستم‌هاي اطلاعاتي

زواياي مختلف تحقيق در زمينة امنيت سيستم‌هاي اطلاعاتي

	سيستم‌هاي رمزنگاري	پروتكل‌هاي رمزنگاري	سيستم‌هاي عامل و زبان‌هاي برنامه‌نويسي	كاربردها	محيط‌هاي عملياتي
امنيت سيگنال					
امنيت داده‌ها					
امنيت سيستم					

- پياده سازي الگوريتمها
  - الگوريتمهاي قالبي
  - الگوريتمهاي دنباله‌اي
  - الگوريتمهاي مبتني بر خم بيضوي
  - ...

زواياي مختلف تحقيق در زمينة امنيت سيستم‌هاي اطلاعاتي

	سيستم‌هاي رمزنگاري	پروتكل‌هاي رمزنگاري	سيستم‌هاي عامل و زبان‌هاي برنامه‌نويسي	كاربردها	محيط‌هاي عملياتي
امنيت سيگنال					
امنيت داده‌ها					
امنيت سيستم					

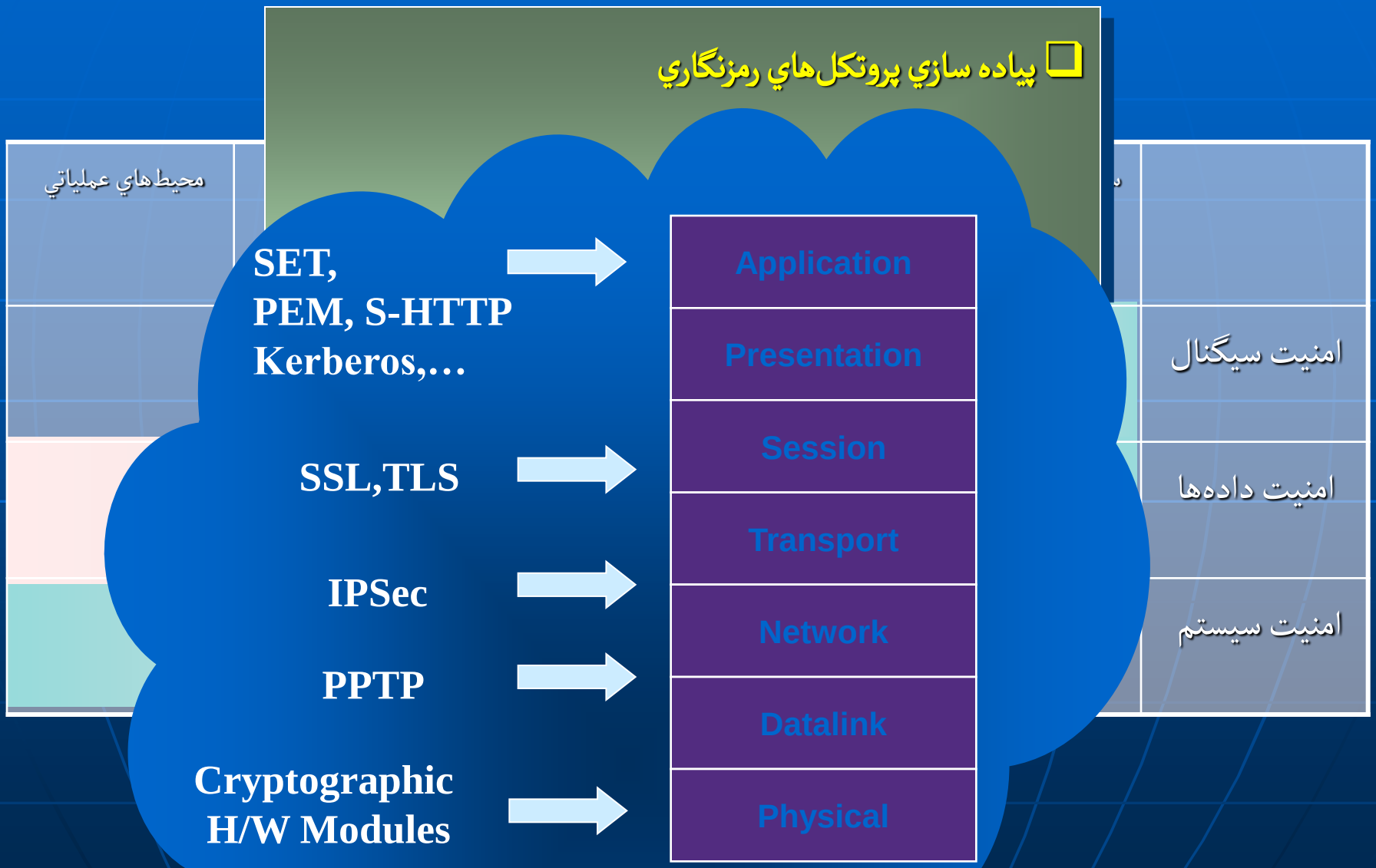
- طراحي پروتكل‌هاي رمزنگاري
  - پروتكل‌هاي احراز اصالت
  - پروتكل‌هاي توزيع كليد
  - پروتكل‌هاي ويژة امنيتي

زواياي مختلف تحقيق در زمينة امنيت سيستم‌هاي اطلاعاتي

	سيستم‌هاي رمزنگاري	پروتكل‌هاي رمزنگاري	سيستم‌هاي عامل و زبان‌هاي برنامه‌نويسي	كاربردها	محيط‌هاي عملياتي
امنيت سيگنال					
امنيت داده‌ها					
امنيت سيستم					

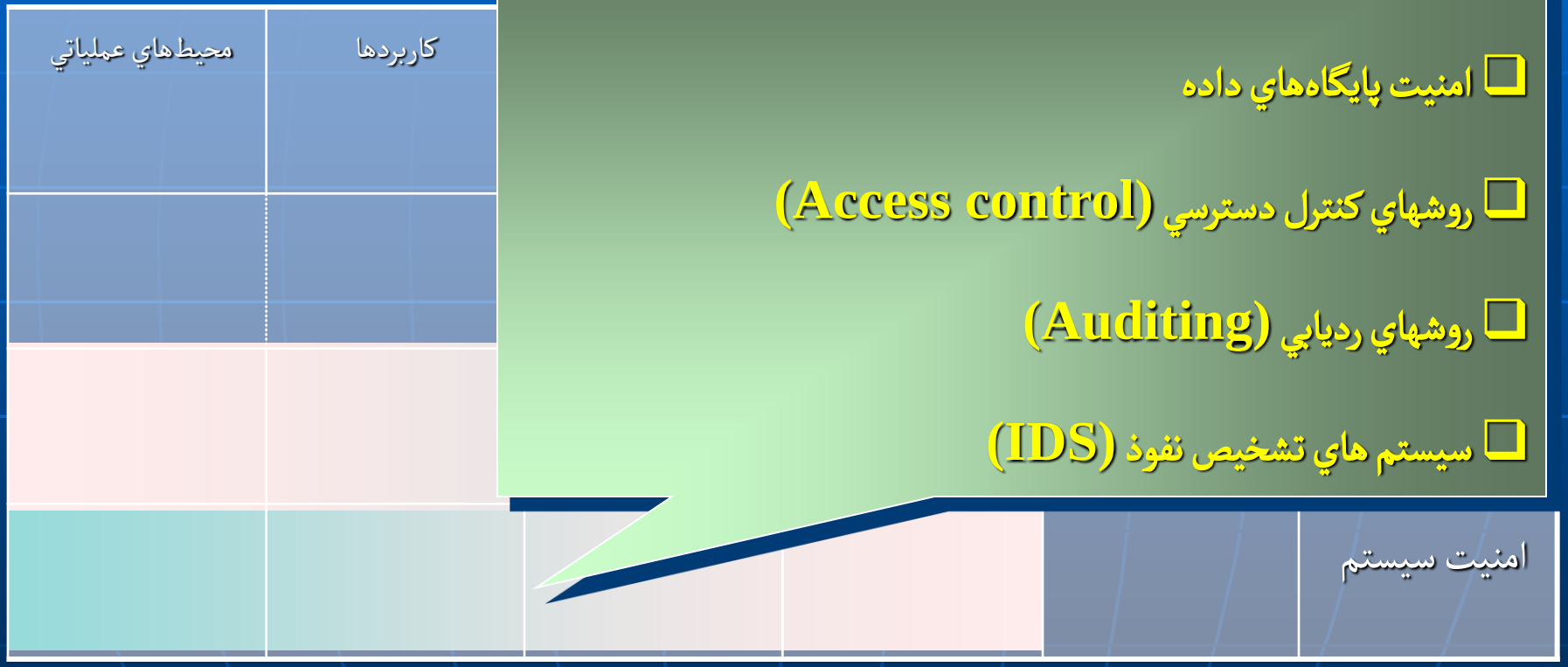
- تحليل پروتكل‌هاي رمزنگاري
  - روش‌هاي شهودي
  - روش‌هاي صوري

زواياي مختلف تحقيق در زمينة امنيت سيستم‌هاي اطلاعاتي



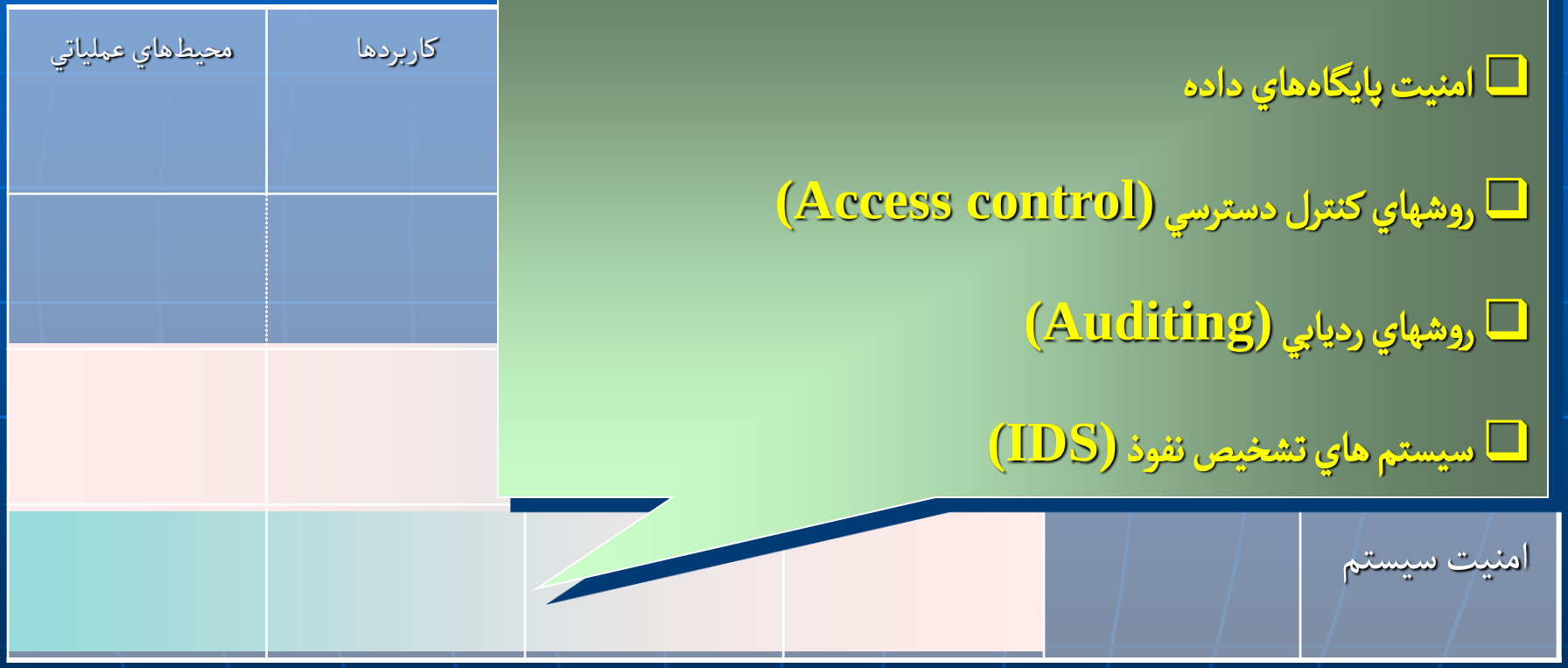
زواياي مختلف تحقيق در زمينة امنيت سيستم‌هاي اطلاعاتي

- امنيت سيستم‌هاي عامل
- امنيت پايگاه‌هاي داده
- روشهاي كنترل دسترسي (Access control)
- روشهاي رديابي (Auditing)
- سيستم هاي تشخيص نفوذ (IDS)

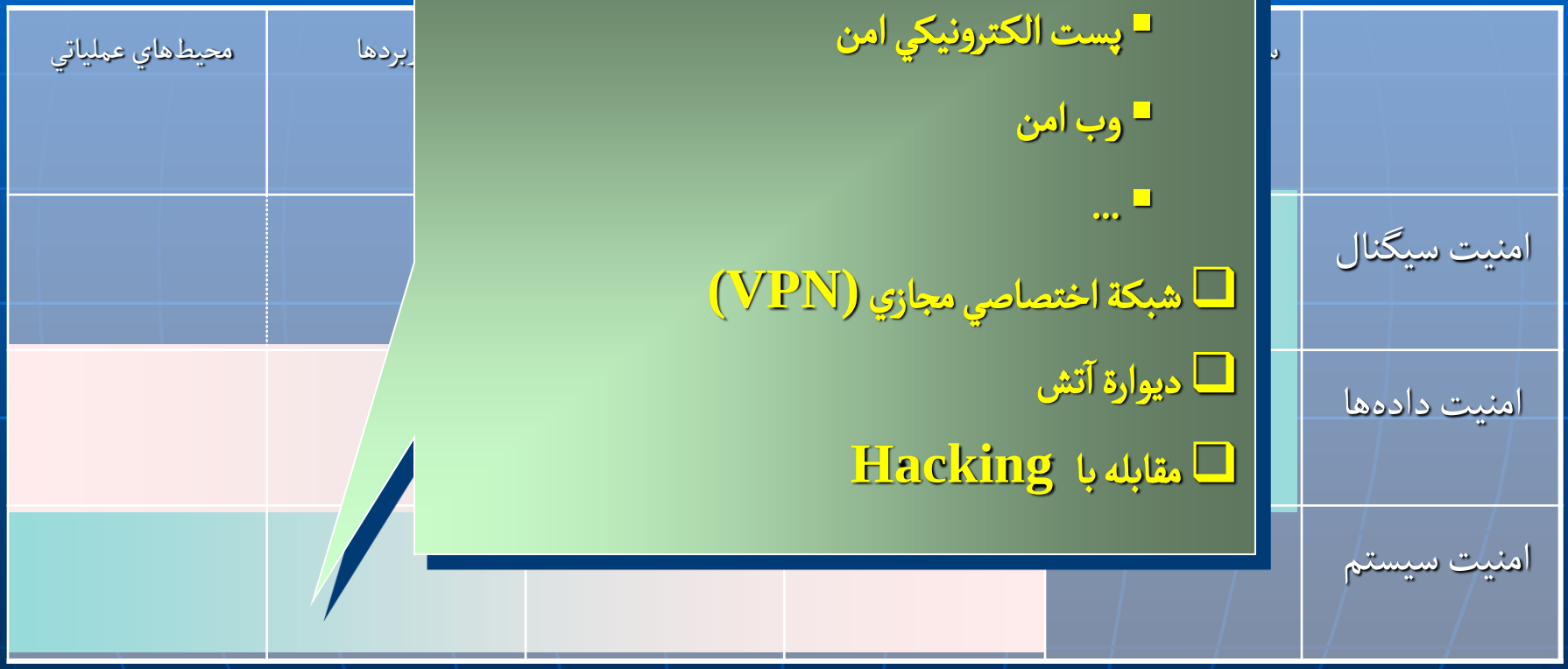


زواياي مختلف تحقيق در زمينة امنيت سيستم‌هاي اطلاعاتي

- امنيت سيستم‌هاي عامل
- امنيت پايگاه‌هاي داده
- روشهاي كنترل دسترسي (Access control)
- روشهاي رديابي (Auditing)
- سيستم هاي تشخيص نفوذ (IDS)



زواياي مختلف تحقيق در زمينة امنيت سيستم‌هاي اطلاعاتي



زواياي مختلف تحقيق در زمينة امنيت سيستم‌هاي اطلاعاتي

زواياي مختلف تحقيق در زمينة امنيت سيستم‌هاي اطلاعاتي