شبکه های خصوصی مجازی

تهیه کننده : سحر عزیزمحمدی

زمستان ۹۳

چکیده

در ابتدا شبکه های اینترانت مطرح گردیدند.این نوع شبکه بصورت کاملا" اختصاصی بوده و کارمندان یک سازمان با استفاده از رمز عبور تعریف شده ، قادر به ورود به شبکه و استفاده از منابع موجود می باشند. اخیرا" ، تعداد زیادی از موسسات و سازمانها با توجه به مطرح شدن خواسته های جدید (کارمندان از راه دور، ادارات از راه دور) اقدام به ایجاد شبکه های اختصاصی مجازی VPN(Virtual Private Network)نموده اند. یک VPN ، شبکه ای اختصاصی بوده که از یک شبکه عمومی (عموما" اینترنت) ، برای ارتباط با سایت های از راه دور و ارتباط کاربران بایکدیگر، استفاده می نماید. این نوع شبکه ها در عوض استفاده از خطوط واقعی نظیر : خطوط Leased ، از یک ارتباط مجازی به کمک اینترنت برای شبکه اختصاصی بمنظور ارتباط به سایت ها استفاده می کند.

فهرست مطالب

روش های برقراری ارتباط از راه دور

شبکه های wire less

امنیت در شبکه های بی سیم

کاربردها و مزایا و ابعاد شبکه های بی سیم

خطرات –حملات وملزومات امنیتی

خطوط pstn

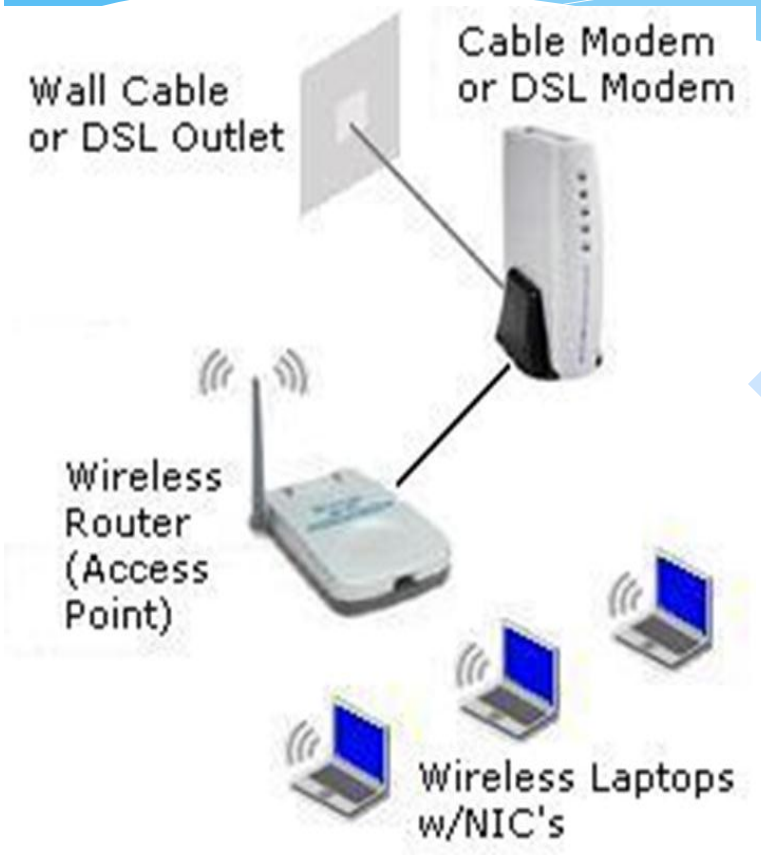
معایب و اشکالات شبکه pstn

آشنایی با voip

شبکه vpn

آموزش تصویری راه اندازی vpnدر ویندوز xp

برای برقراری ارتباط از راه دور سه روش اصلی وجود دارد که شامل:



- شبکه های wire less
- خطوط pstn
- voip
- Internet (استفاده از vpn)

شبکه های Wireless

Wireless چیست؟

* Wirelessبه تکنولوژی ارتباطی اطلاق می شود که در آن از امواج رادیویی، مادون قرمز و مایکروویو ، به جای سیم و کابل ، برای انتقال سیگنال بین دو دستگاه استفاده می شود.از میان این دستگاه ها می توان پیغامگیرها، تلفن های همراه، کامپیوتر های قابل حمل، شبکه های کامپیوتری، دستگاه های مکان یاب، سیستم های ماهواره ای و PDA ها را نام برد.تکنولوژی Wireless به سرعت در حال پیشرفت است و نقش کلیدی را در زندگی ما در سرتاسر دنیا ایفا می کند.

سیستم های WirelesS

* سیستم wire lessثابت :از امواج رادیویی استفاده میکند و خط دید مستقیم برای برقراری ارتباط لازم دارد

* سیستم wirelessقابل حمل:دستگاهی است که معمولا خارج از خانه –دفتر کار و یا در وسایل نقلیه مورد استفاده قرار میگیرد.مانند تلفن های همراه –دستگاهای پیغام گیر

* سیستم wire lessمادون قرمز:این سیستم دراموج مادون قرمز جهت انتقال سیگنالهایی محدود بهره میبرد.

امنیت در شبکه های بی سیم

* از آنجا که شبکه های بی سیم در دنیای کنونی هر چه بیشتر در حال گسترش هستند، و باتوجه به ماهیت این دسته از شبکه ها، که بر اساس سیگنالهای رادیویی اند، مهم ترین نکته در راه استفاده از این تکنولوژی، آگاهی از نقاط قوت و ضعف آن است. نظر به لزوم آگاهی از خطرات استفاده از این شبکه ها، با وجود امکانات نهفته در آن ها که به مدد پیکر بندی صحیح می توان به سطح قابل قبولی از بعد امنیتی دست یافت.

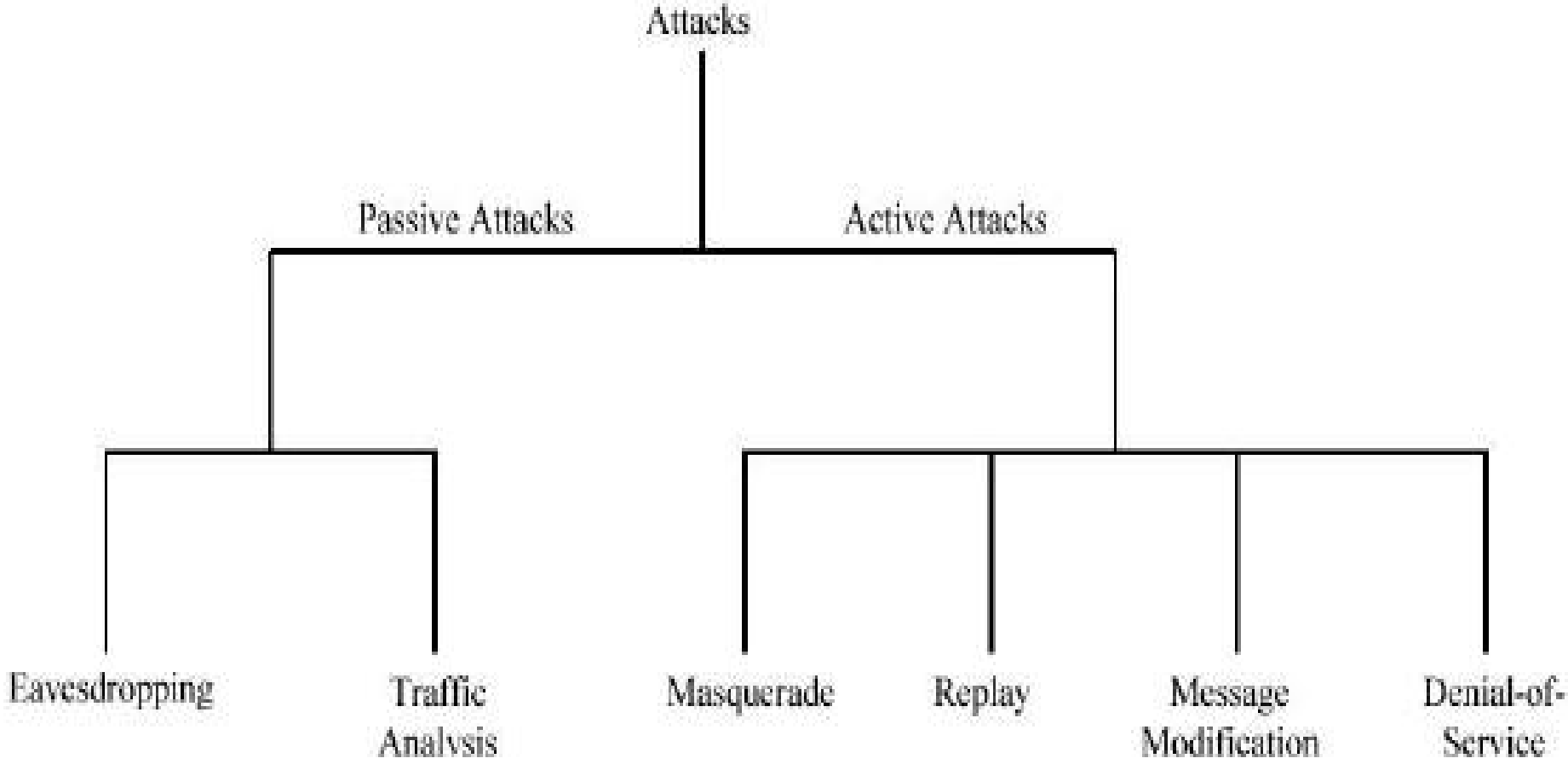
مزایا شبکه های بی سیم

کاربردهای شبکه های بی سیم

ابعاد شبکه های بی سیم

* شبکه های بی سیم بازه ی وسیعی از کاربردها، از ساختارهای پیچیده ای چون شبکه های بی سیم سلولی(که اغلب برای تلفن های همراه استفاده می شود)و شبکه های محلی بی سیم(WLAN-Wireless) گرفته تا انواع ساده یی چون هدفون های بی سیم، را شامل می شوند. از سوی دیگر با احتساب امواجی همچون مادون قرمز، تمامی تجهیزاتی که از امواج مادون قرمز نیز استفاده می کنند، مانند صفحه کلیدها، موس ها و برخی از گوشی های همراه، در این دسته بندی جای می گیرند.طبیعی ترین مزیت استفاده از این شبکه ها عدم نیاز به ساختار فیزیکی و امکان نقل و انتقال تجهیزات متصل به این گونه شبکه ها و هم چنین امکان ایجاد تغییر در ساختار مجاتزی آنهاست.از نظر ابعاد ساختاری، شبکه های بی سیم به سه دسته تقسیم می گردند:WWAN، WLAN وWPAN .

خطرهـــــا، حمـــــلات و ملزومـــــات امنیتـــــی



مطابق درخت فوق حملات امنیتی به دو دسته ی فعال و غیر فعال تقسیم می گردند

حمـــــــــــلات غیـــــــــــر فعـــــــــال

* در این قبیل حملات، نفوذگر تنها به منبعی از اطلاعات به نحوی دست می یابد ولی اقدام به تغییر محتوای اطلاعات منبع نمیکند.این نوع حمله می تواند به یکی از اشکال شنود ساده یا آنالیز ترافیک باشد.

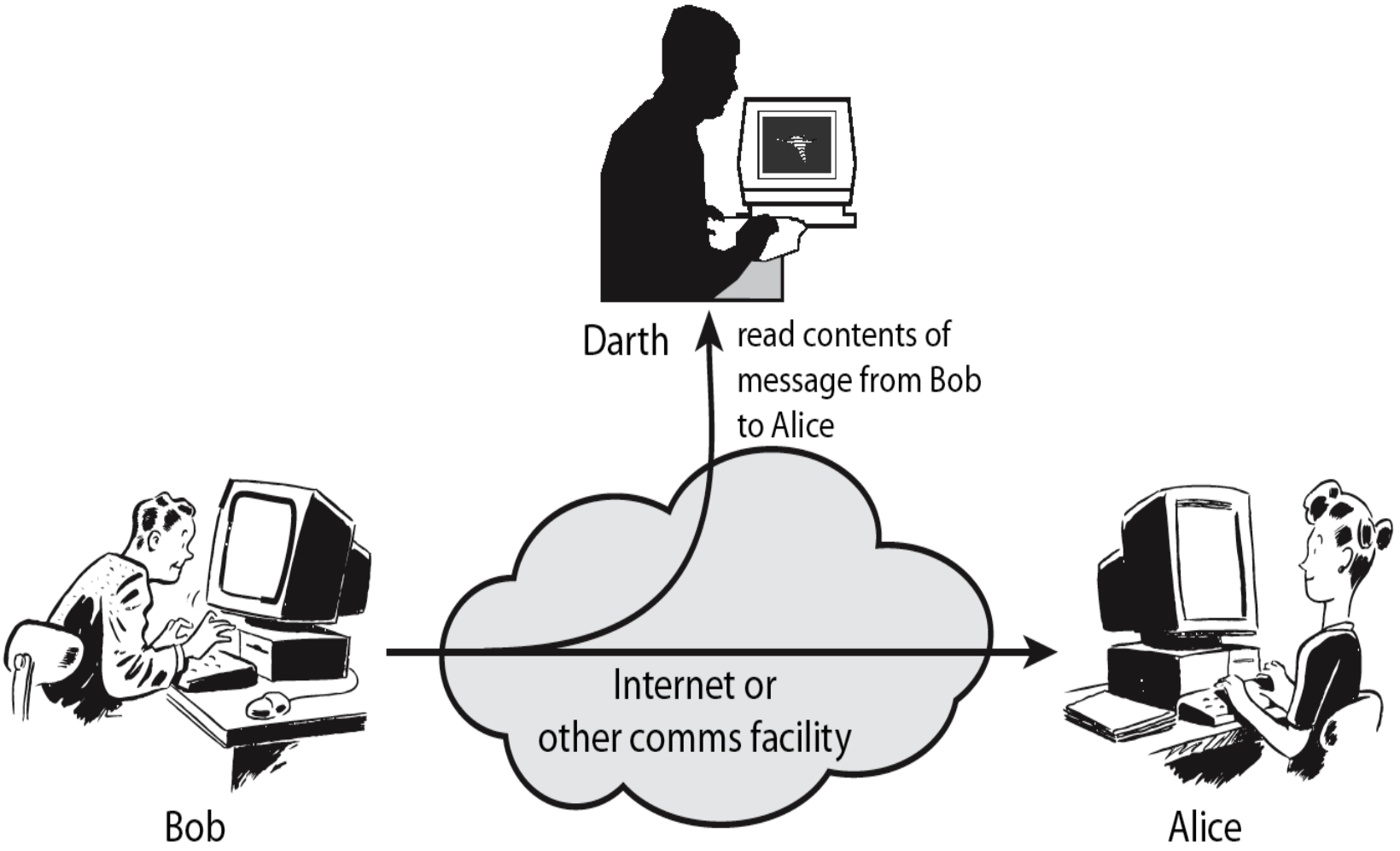
✓شنود:

* در این نوع نفوذگر تنها به پایش اطلاعات ردوبدل شده می پردازد.برای مثال شنود ترافیک روی یک شبکه محلی یا یک شبکه ی بی سیم (که مد نظر ماست) نمونه هایی از این نوع حمله به شمار می آیند.

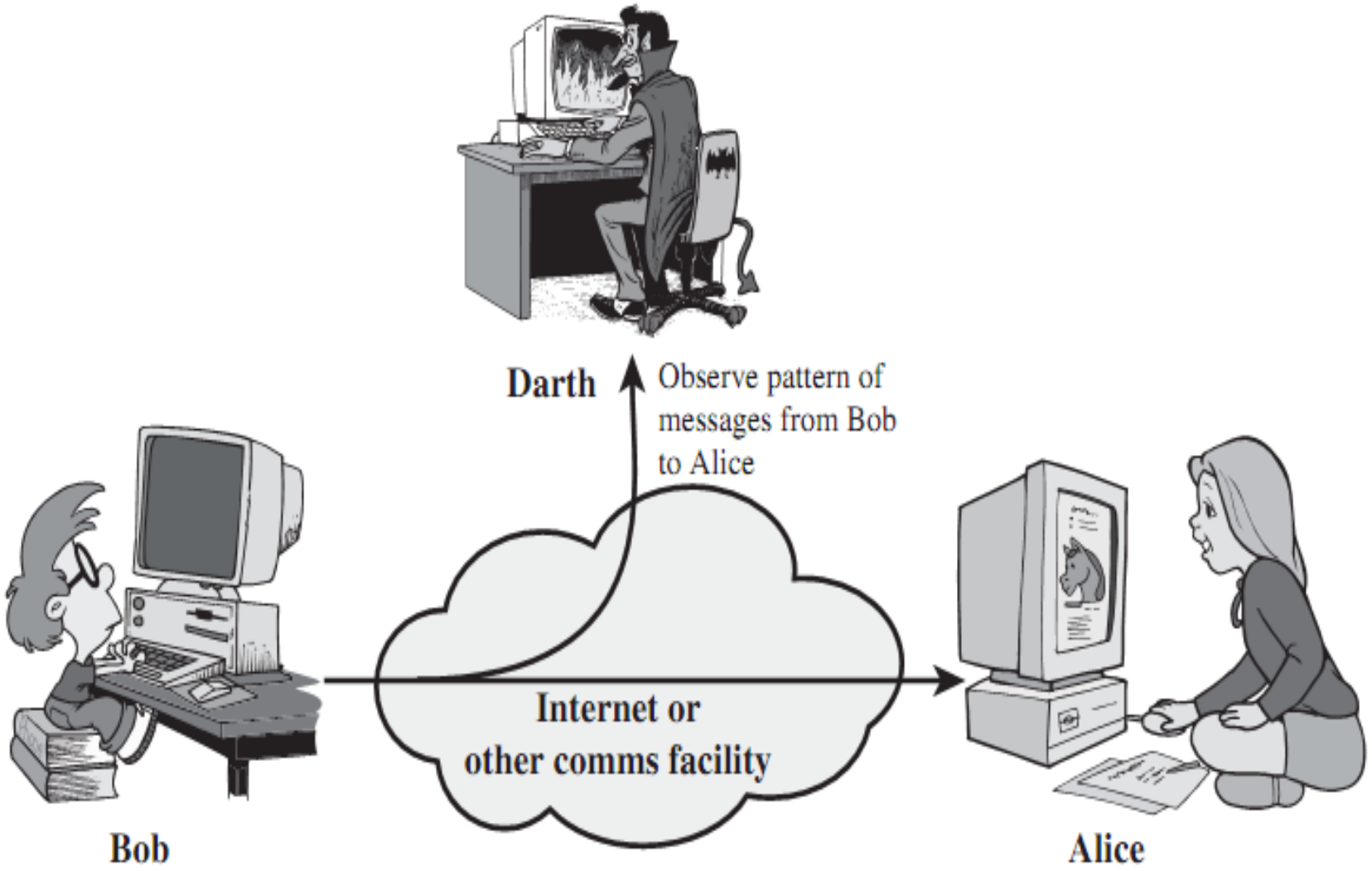
✓آنالیز ترافیک

* در این نوع حمله نفوذگر با کپی برداشتن از اطلاعات پایش شده، به تحلیل جمعی داده ها می پردازد..

آزاد سازی محتوای پیام (شنود)



آنالیز ترافیک



حمـــــــــــــــــلات فعـــــــــــــــال

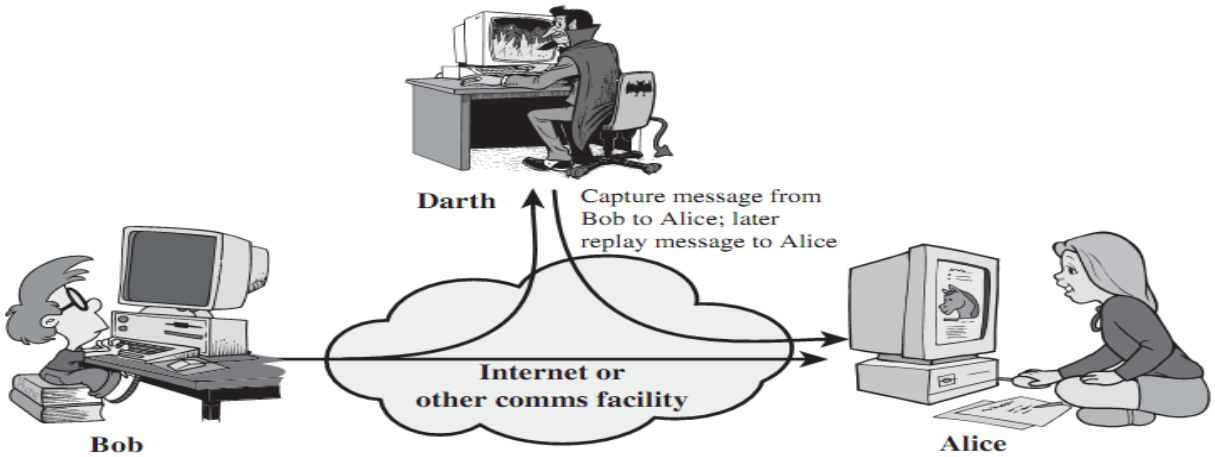
* در این نوع حملات، برخلاف حملات غیرفعال، نفوذگر اطلاعات مـوردنظر را، کـه از منابع به دست می آید، تغییر می دهد که طبیعتا انجام این تغییرات مجاز نمی باشد.از آنجایی که در این نوع حملات اطلاعات تغییر مـی کننـد، شناسـایی رخ داد حمـلات فرآیندی امکان پذیر است.این نوع حملات به چهار دسته ی مرسوم زیر تقسـیم بنـدی می شوند:

تغییر هویت

* در این نوع حمله ، نفوذگر هویت اصلی را جعل می کند.این روش شامل تغییر هویت اصلی یکی از طرف های ارتباط یا تغییر جریان واقعی فرایند پردازش اطلاعات نیز می گردد.

پاسخ های جعلی

* این نوع حمله بیشتر در مواردی کاربرد دارد که فرستنده اقدام به تغییر هویت گیرنده می کند. در این حالت بسته های پاسخی که برای فرستنده به عنوان جواب به سوالات وی ارسال می گردند به معنای پرچمی برای شناسایی گیرنده محسوب می گردند.

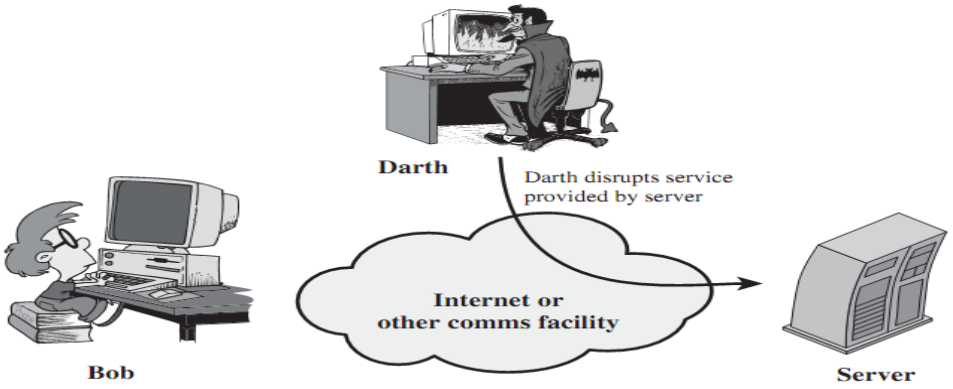


✓تغییر پیام

در برخی از موارد مرسوم ترین و متنوع ترین نوع حملات فعال،تغییر پیام است

✓حمله های Dos(Denial of Service)

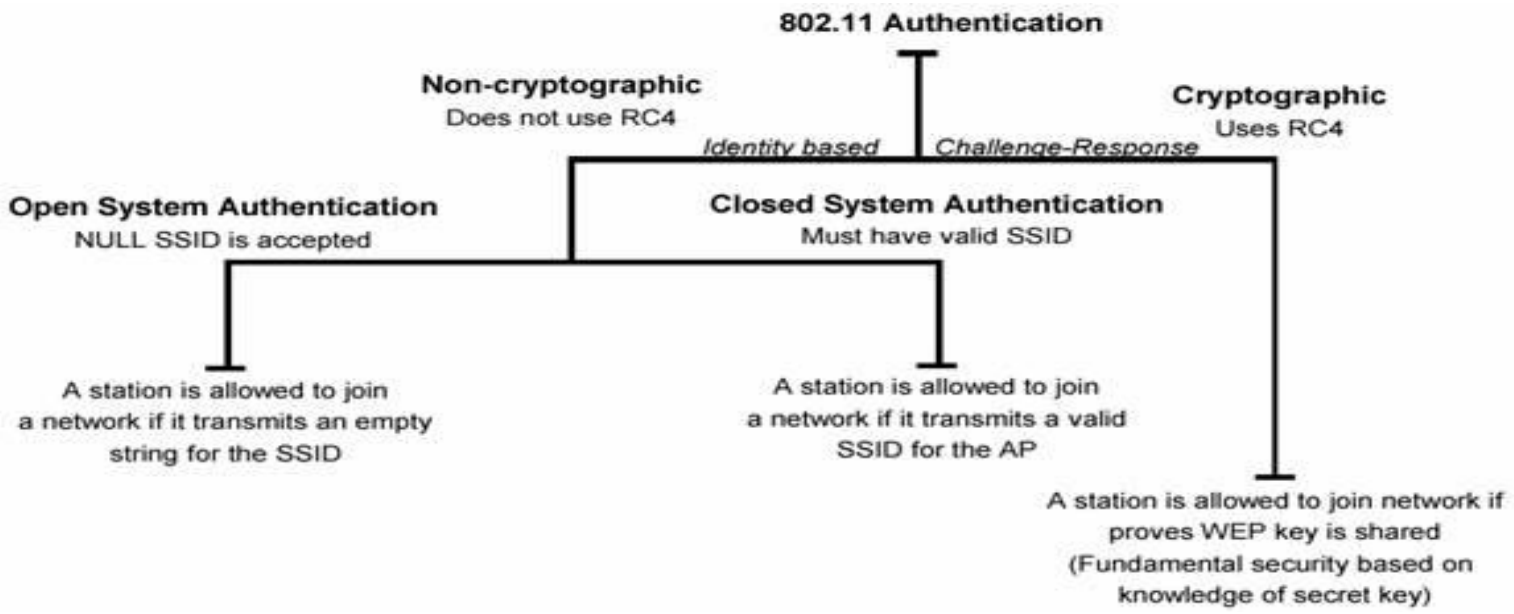
این نوع حمله در حالات معمول، مرسوم ترین حملات را شامل می شود. در این نوع حمله نفوذگر یا حمله کننده برای تغییر نحوه ی کارکرد یا مدیریت یک سامانه ی ارتباطی یا اطلاعاتی، اقدام میکند.



سه قابلیت و سرویس پایه توسط IEEE برای شبکه های محلی بی سیم تعریف می گردد

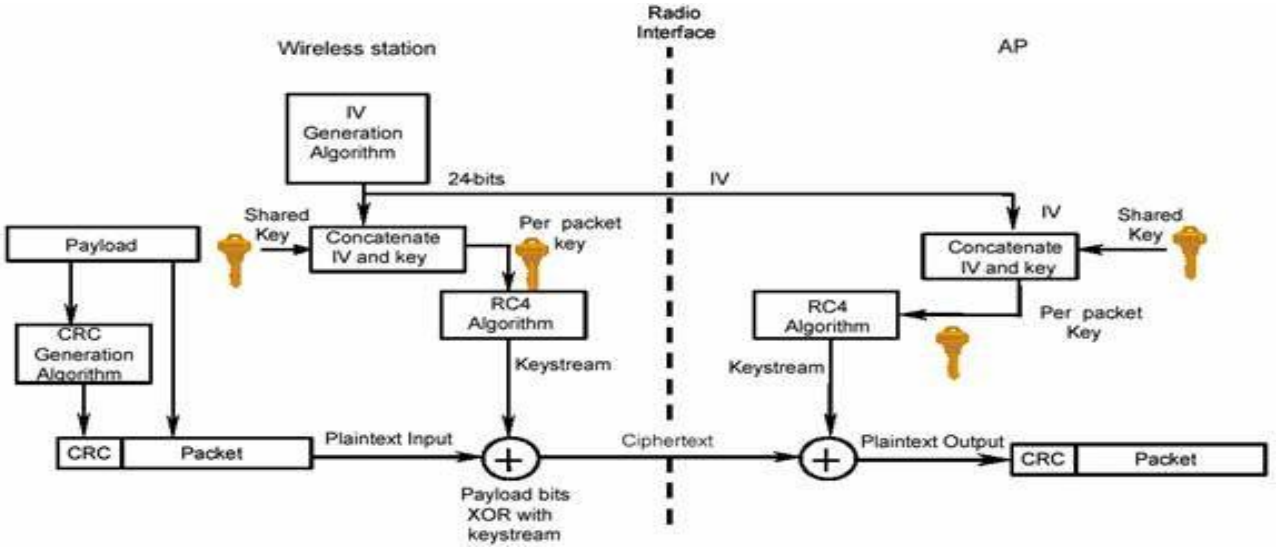
Authentication. ۱

هدف اصلی WEBایجاد امکانی برای احراز هویت مخدوم بی سیم است. این عمل در واقع کنترل دسترسی به شبکه ی بی سیم است . این مکانیزم سعی دارد که امکان اتصال مخدوم هایی را که مجاز نیستند به شبکه متصل شوند از بین ببرد.



Confidentiality.۱

محرمانگی هدف دیگر WEP است. این بعد از سرویس ها و خدمات WEP با هدف ایجاد امنیتی در حدود سطوح شبکه های سیمی طراحی شده است.سیاست این بخش از WEP جلوگیری از سرقت اطلاعات در حال انتقال بر روی شبکه ی محلی بی سیم است.

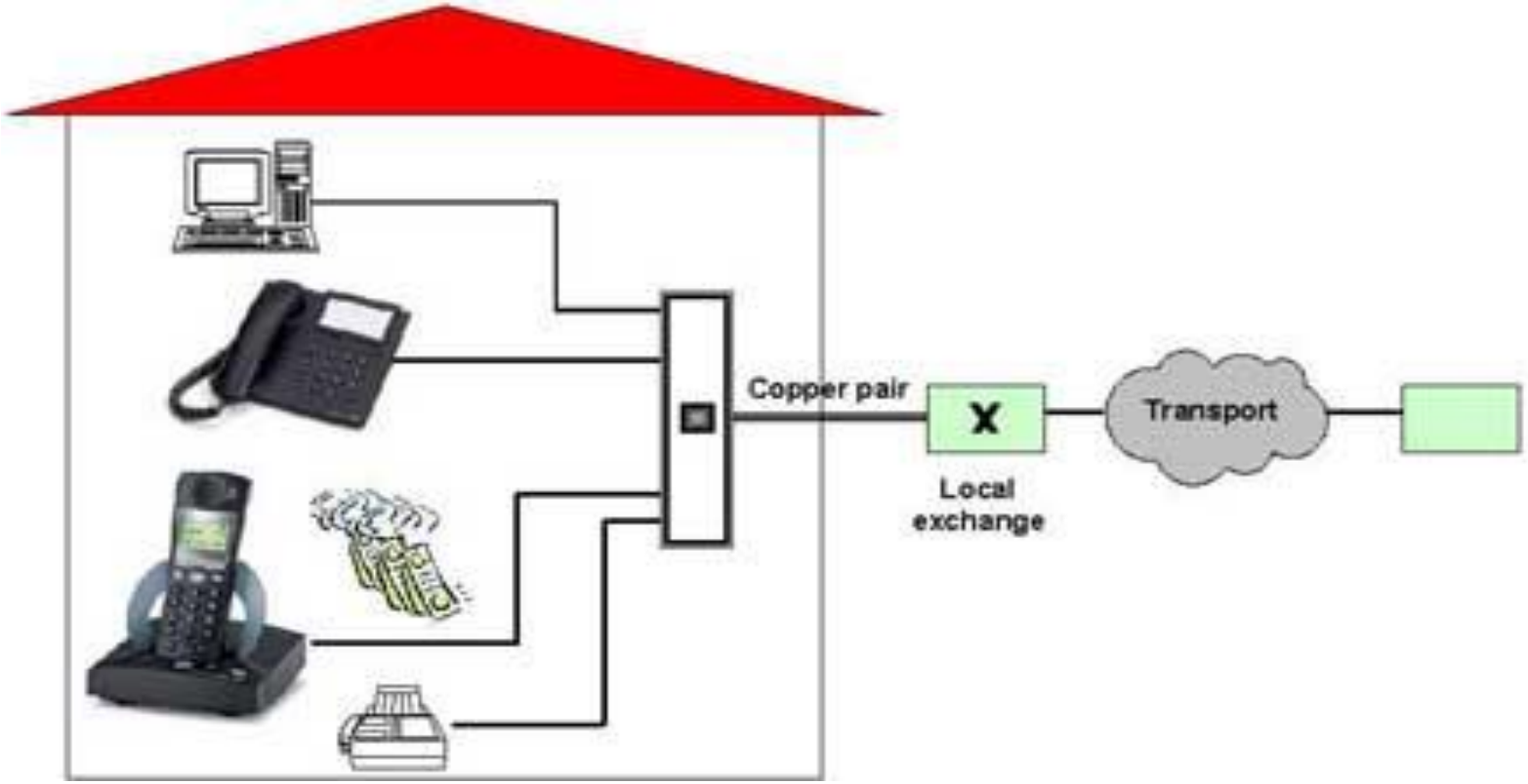


۱. Integrity

هدف سوم از سرویس ها و قابلیت های WEP طراحی سیاستی است که تضمین می کند پیام ها و اطلاعات در حال تبادل در شبکه، خصوصا میان مخدوم های بی سیم و نقاط دسترسی، در حین انتقال دچار تغییر نمی گردند. این قابلیت در تمامی استانداردها، بسترها و شبکه های ارتباطی دیگر نیز کم و بیش وجود دارد.

خطوط PSTN

* **شبکه عمومی سوئیچینگ تلفن(PSTN)**
* PSTN مخفف Public Switching Telephone Network است و عملکرد آن به صورت زیر می باشد:



* زمانی که شما در منزل یا محل کار قصد تماس گرفتن دارید ابتدا گوشی تلفن را بر می دارید و صدای بوق خاصی را می شنوید (به این معنی که شما مجاز به شماره گیری و استفاده از شبکه تلفن ثابت هستید) ارتباط شما با مرکز تلفن محلی (LOCAL) خود بوسیله دو رشته سیم مسی که از درب منزل یا محل کار شما به نزدیکترین پست (POST) (همان جعبه های کوچک سربی رنگ که در روی دیوار معابر نصب شده و به آن مقداری کابل وارد و خارج شده است)رفته است و از پست به کافو می رود(کافوها همان کمدهای سبز رنگ است که در کنار خیابانها نصب شده است) و از کافوها به چاله حوضچه که در زیر زمین توسط مخابرات حفر شده می رود و از آنجا به مرکز تلفن وارد می شود.

معایب و اشکالات شبکه PSTN

* شبکه PSTN مبتنی بر سوئیچ مداری است و برای ارائه سرویس تنگناهای زیر دارد:
* – پهنای باند غیر قابل انعطاف
* – عدم ارائه سرویس باند عریض : در این جا، اصولا به خاطر خاصیت بلادرنگ بودن خدمات (Real Time) نیاز به پهنای عرض کم است.
* – جدا نکردن لایه‌های مختلف در مراکز
* مشکلات لایه (Access) در ساختار موجود
* – جدا نشدن لایه سوئیچ از لایه‌های دیگر (Service, Access ,Control)
* – جدا نشدن لایه سرویس از لایه‌های دیگر
* – خدمات اتصال متقابل با انعطاف پایین، با توجه به مقوله افزونگی یا Redundancy
* – مشکلات ارتقاء

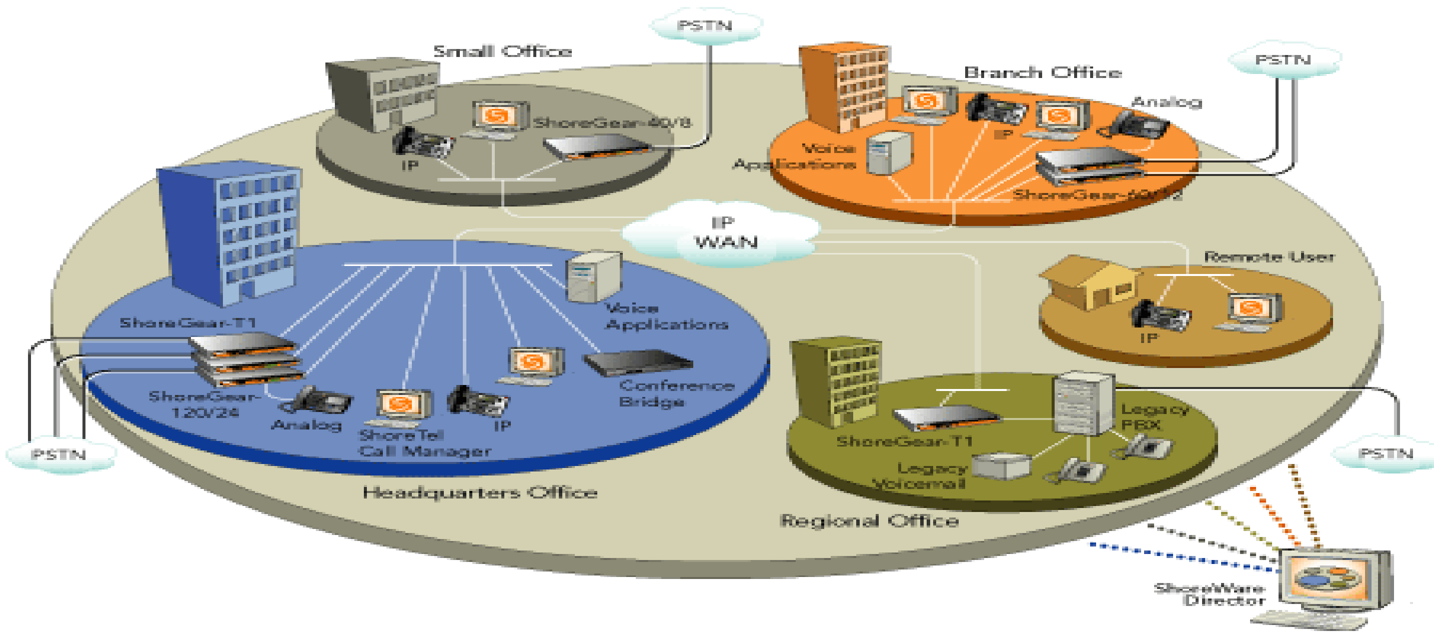
آشنائی با VoIP

- ارتباطات محاوره ای صرفا" از طریق تلفن و به کمک خطوط PSTN (برگرفته از Public Switched Telephone Network) ، انجام می گردید . در سیستم فوق ، سیگنال های صوتی آنالوگ با استفاده از کابل های مسی حمل و مبادله داده خصوصا" در مسافت های طولانی گرانقیمت و ارتباطات دوسویه ویدیوئی رویائی بیش نبود (در آن زمان صرفا" از تلویزیون استفاده می گردید که به عنوان یک رسانه دوسویه محسوب نمی گردد).

VoIP چیســــــــــــــــــــــــــــــــــت ؟

- VoIP (برگرفته از Voice over internet protocol) که با نام IP تلفنی نیز از آن یاد می شود ، امکان استفاده از اینترنت برای مکالمات تلفنی را فراهم می نماید . در مقابل استفاده از خطوط تلفن سنتی ، VoIP از فن آوری دیجیتال استفاده می نماید و نیازمند یک اتصال broadband نظیر DSL است . هم اینک شرکت های متعددی سرویس فوق را در اختیار علاقه مندان قرار می دهند .

متداولترین کاربرد VoIP برای موارد شخصی و استفاده در منازل ، سرویس های تلفنی مبتنی بر اینترنت است که با محوریت یک سوئیچ تلفن انجام می شود

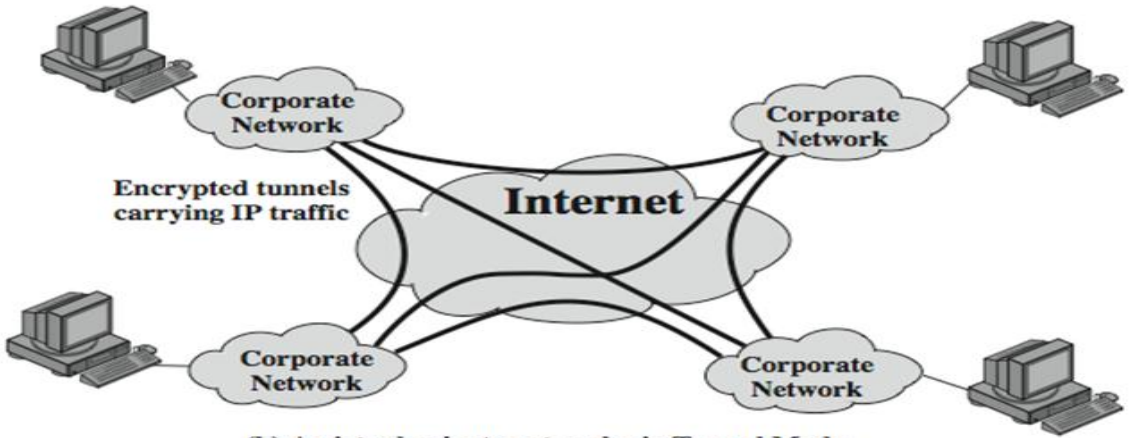


مزایای استفاده از VoIP نسبت به PSTN

- در زمان استفاده از خطوط PSTN ، کاربران عملا" هزینه زمان استفاده شده توسط شرکتی که مدیریت خط PSTN را برعهده دارد ، پرداخت می نمایند و هر اندازه که بیشتر با تلفن صحبت نمایند هزینه بیشتری را نیز می بایست پرداخت نمایند. علاوه بر این ، نمی توان بطور همزمان با بیش از یک شخص گفتگو نمود .در فن آوری VoIP می توان هر زمان و با هر شخص گفتگو نمود . کافی است که در آن مقطع زمانی سایر افرادی که شما می خواهید با آنان گفتگو نمائید نیز به اینترنت متصل شده باشند . مکالمه برقرار شده تا زمان دلخواه (مستقل از هزینه های مربوطه) می تواند ادامه یابد. علاوه بر این ، می توان در یک زمان با چندین نفر گفتگو نمود . در زمان گفتگو با سایر افراد و بطور همزمان می توان با آنان داده ئی (نظیر تصاویر ، نمودارها و تصاویر ویدیوئی) را نیز مبادله نمود

شبکه vpn

- شبکه خصوصی مجازی یا Virtual Private Network که به اختصار VPN نامیده می شود، امکانی است برای انتقال ترافیک خصوصی بر روی شبکه عمومی. معمولا از VPN برای اتصال دو شبکه خصوصی از طریق یک شبکه عمومی مانند اینترنت استفاده می شود.منظور از یک شبکه خصوصی شبکه ای است که بطور آزاد در اختیار و دسترس عموم نیست. VPN به این دلیل مجازی نامیده می شود که از نظر دو شبکه خصوصی ، ارتباط از طریق یک ارتباط و شبکه خصوصی بین آنها برقرار است اما در واقع شبکه عمومی این کار را انجام می دهد



(b) A virtual private network via Tunnel Mode

دسته بندی VPN براساس رمزنگاری

* **VPNرمزشده** : VPN های رمز شده از انواع مکانیزمهای رمزنگاری برای انتقال امن اطلاعات بر روی شبکه عمومی استفاده می کنند. یک نمونه خوب از این VPN ها ، شبکه های خصوصی مجازی اجرا شده به کمک IPSec هستند.

۱. **VPN رمزنشده** : این نوع از VPN برای اتصال دو یا چند شبکه خصوصی با هدف استفاده از منابع شبکه یکدیگر ایجاد می شود. اما امنیت اطلاعات در حال تبادل حائز اهمیت نیست یا این که این امنیت با روش دیگری غیر از رمزنگاری تامین می شود. یکی از این روشها تفکیک مسیریابی است. منظور از تفکیک مسیریابی آن است که تنها اطلاعات در حال تبادل بین دو شبکه خصوصی به هر یک از آنها مسیر دهی می شوند. (MPLS VPN) در این مواقع می توان در لایه های بالاتر از رمزنگاری مانند SSL استفاده کرد.

آمـــــوزش تصـــــویری راه انـــــدازیVPN در ویندوز XP

* **مراحل ایجاد ارتباط به VPN در محیط Windows XP**

۱. برای شروع به منوی زیر می رویم.

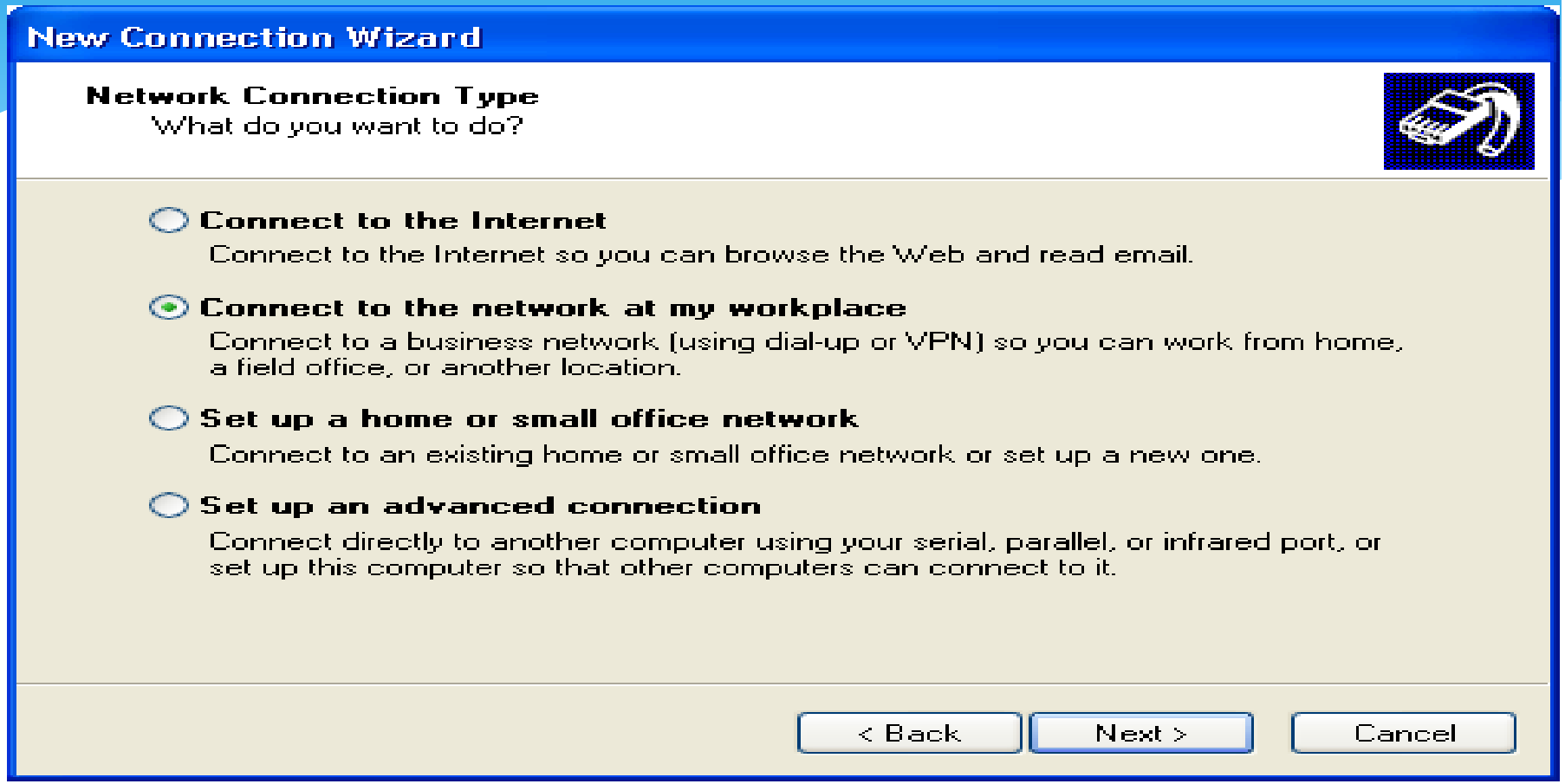
* Start→control panel→network connection→create a new connection

* را انتخاب می کنیم .

* ۲- پنجره ای باز می شود.

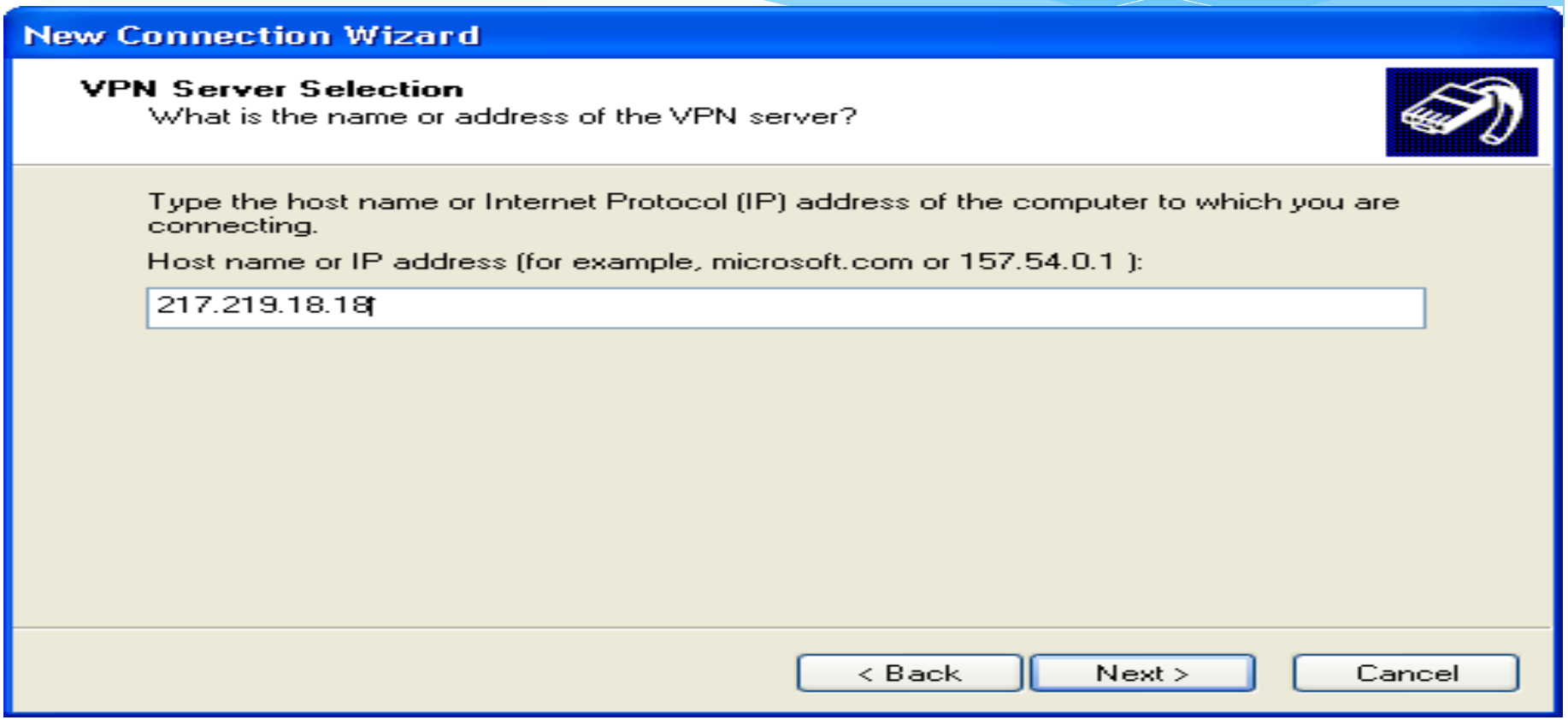

New Connection Wizard
Welcome to the New Connection Wizard
This wizard helps you:
• Connect to the Internet.
• Connect to a private network, such as your workplace network.
• Set up a home or small office network.
To continue, click Next.
< Back
Next >
Cancel

گزینه Next را کلیک می کنیم. صفحه ای مانند زیر باز می شود گزینه دوم را انتخاب می کنیم.



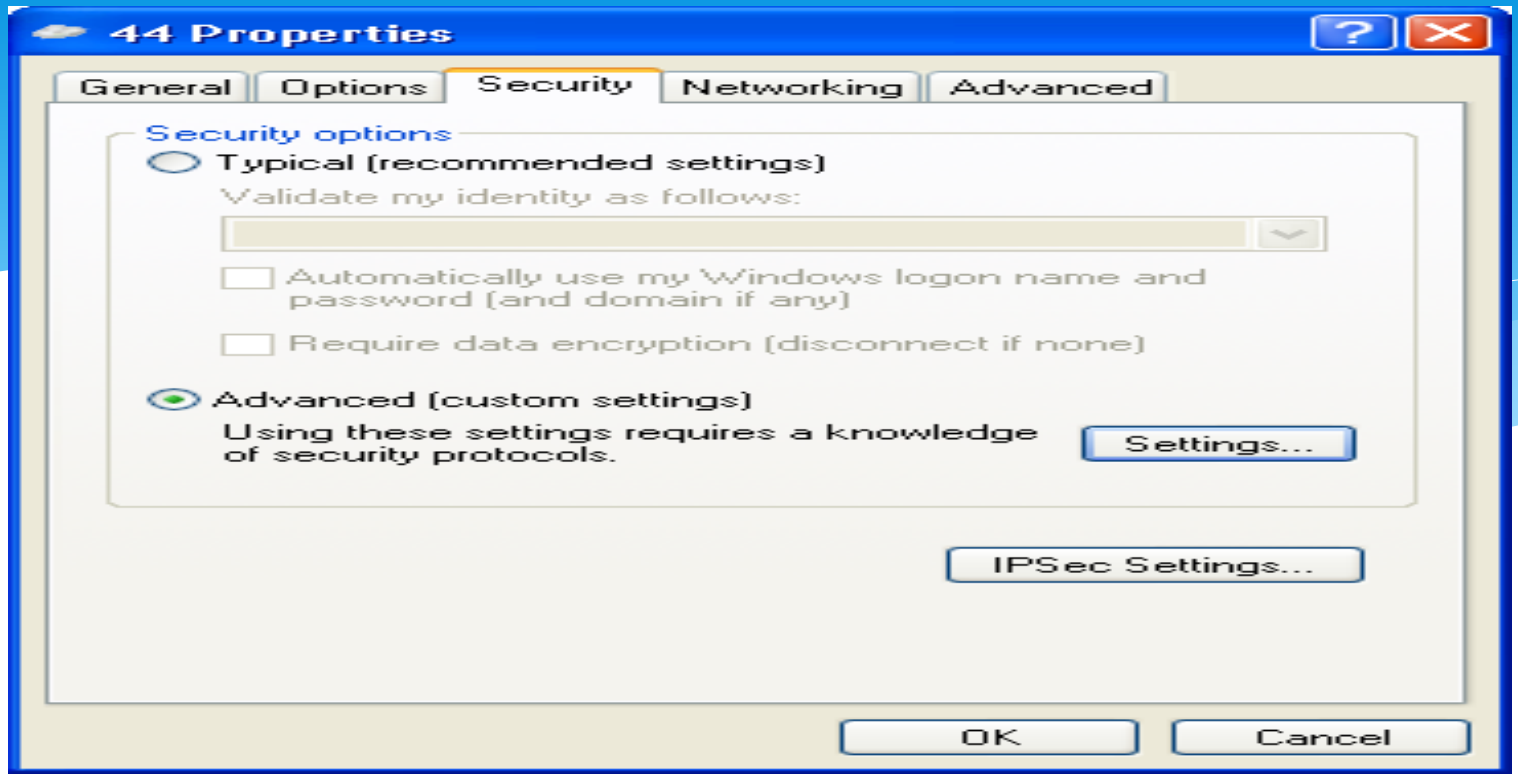
بعد از آن صفحه مانند زیر باز می شود، گزینه Virtual Private Network Connection را انتخاب می کنیم.

در پنجره ای که باز می شود یک اسم به طور دلخواه تایپ می کنیم سپس برروی Next کلیک کرده صفحه ای دیگر باز می شود در قسمت host name:vpn1.iut.ac.irرا وارد می کنیم.



سپس روی دکمه مربوطه کلیک کرده صفحه ای مانند زیر باز می شود

برروی گزینه Security می رویم . سپس گزینه Advanced(Custom Setting) را کلیک می کنیم . گزینه Setting کلیک می کنیم تا پنجره زیر باز شود.



در قسمت Data encryption گزینه no encryption را انتخاب می کنیم .
در قسمت Protocol allow these گزینهunencryption و password challeng handshake Authentication (۳و۱)


Advanced Security Settings
Data encryption:
No encryption allowed (server will disconnect if it requires encryption)
Logon security
Use Extensible Authentication Protocol (EAP)
Properties
Allow these protocols
Unencrypted password (PAP)
Shiva Password Authentication Protocol (SPAP)
Challenge Handshake Authentication Protocol (CHAP)
Microsoft CHAP (MS-CHAP)
Allow older MS-CHAP version for Windows 95 servers
Microsoft CHAP Version 2 (MS-CHAP v2)
For MS-CHAP based protocols, automatically use my Windows logon name and password (and domain if any)
OK
Cancel

منابع وماخذ

۱. Geoff Huston, Interconnection, peering and settlement

۲. Micheal.L.Katz and Carl shapio, Network Externalities, competition, and compatibility

۳. Digital Tornado, brief history of the Internet

۴. .www.isoc.org/guest/zakan/Internet/History.HIT.htmi

۵. ITRC.www.ITRC.ir

۶. نام *کتاب* : آشنایی با شبکه مجازی *VPN* . نویسنده : مینو به تابان. ناشر : سایت اموزش ایرانیان. زبان *کتاب* : فارسی.

با تشکر فراوان از توجه شما

پایان