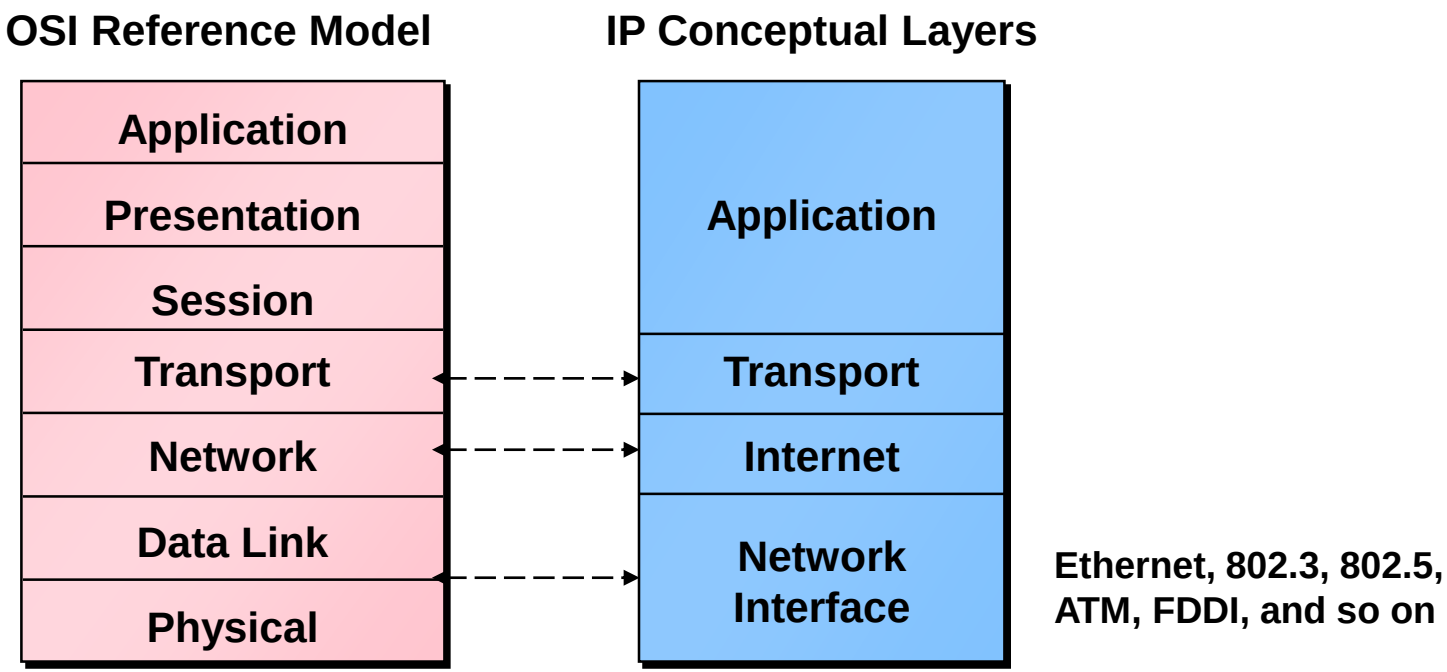
# امنیت شبکه

گردآوری: محمدعلی عظیمی

# مقدمه و معماری امنیت

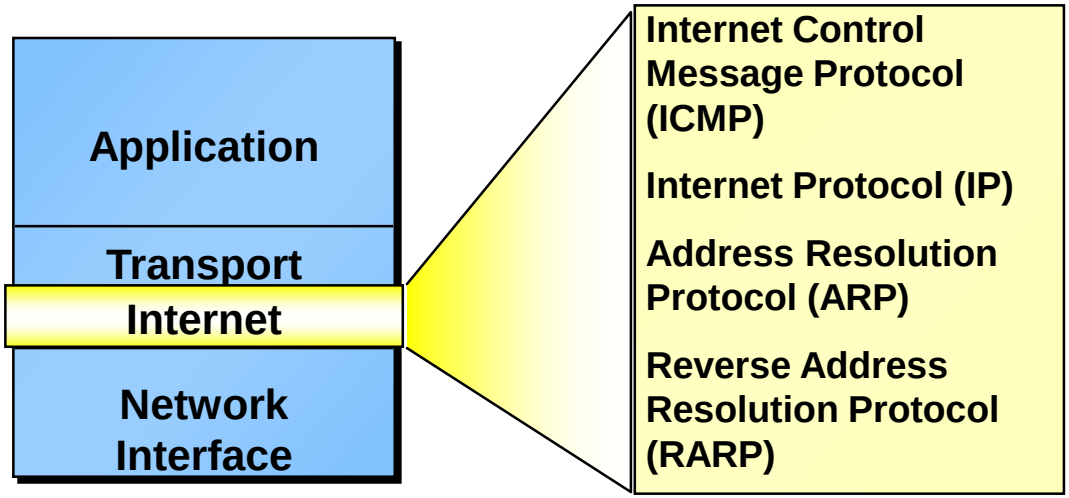
گردآوری: محمدعلی عظیمی

# نگاهی به پشته پروتکل TCP/IP



# نگاهی به لایه IP

**IP Layer**

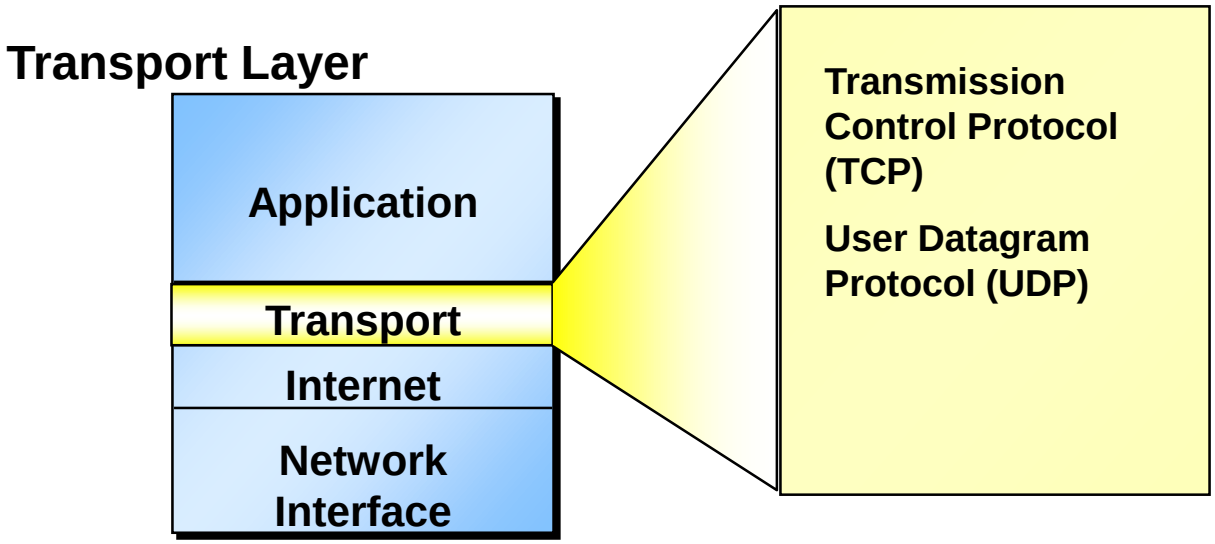



**IP Datagram**

| VERS | HLEN | Type of Service | Total Length | ID | Flags | Frag Offset | TTL |
|---|---|---|---|---|---|---|---|

| Protocol | Header Checksum | Src IP Address | Dst IP Address | IP Options | Data |
|---|---|---|---|---|---|

# نگاهی به لایه حمل



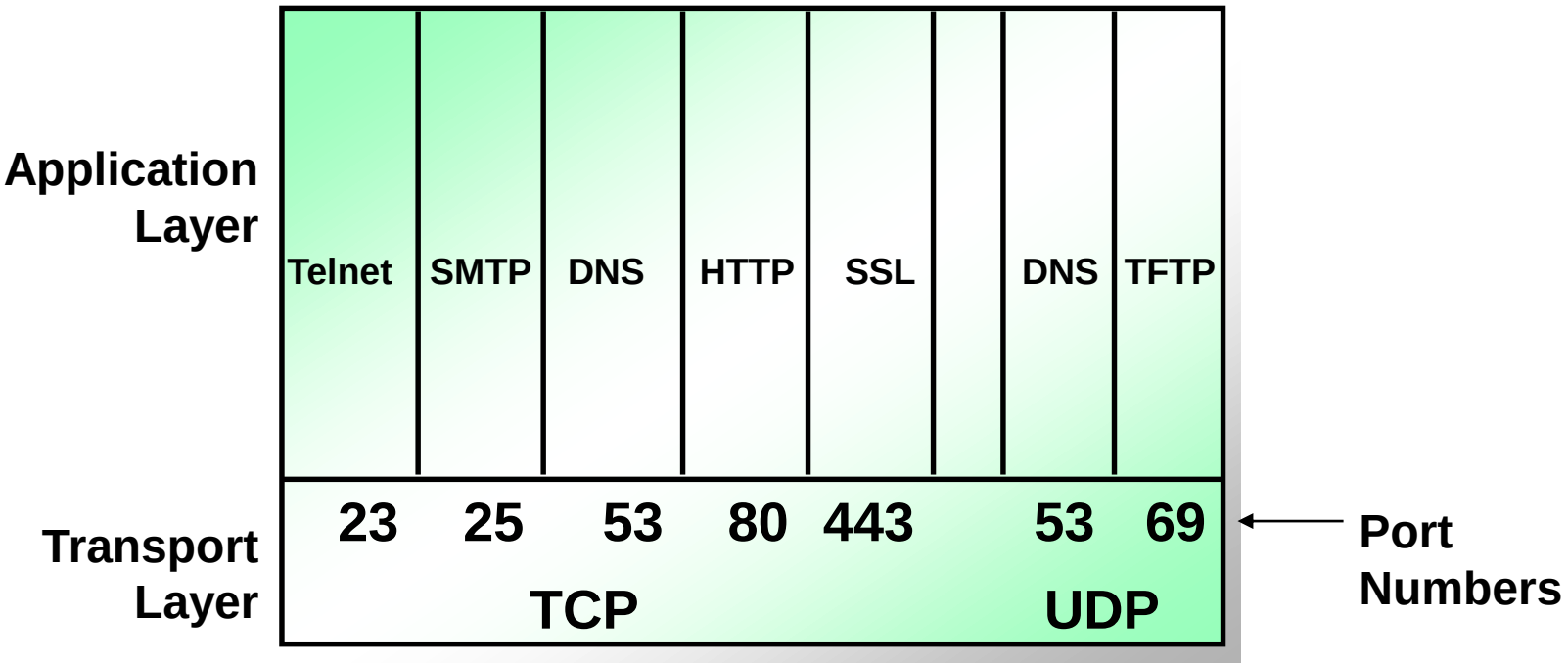

**TCP Segment Format**

| Src Port | Dst Port | Seq # | Ack # | HLEN | Reserved | Code Bits | Window | Check Sum | Urgent Ptr | Option | Data |
|---|---|---|---|---|---|---|---|---|---|---|---|

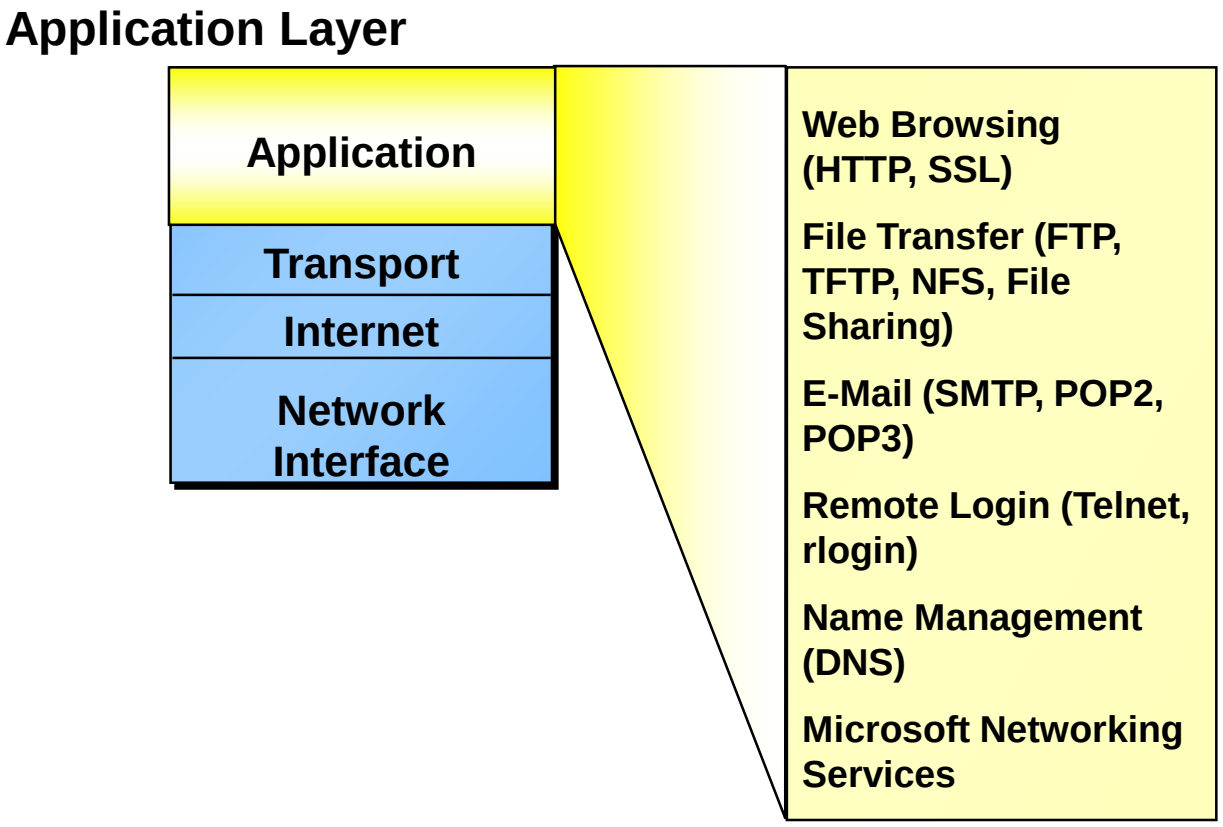
**UDP Segment Format**

| Src Port | Dst Port | Length | Check Sum | Data |
|---|---|---|---|---|

# پروتکل ها و Port Number ها



# نگاهی به لایه کاربرد



# تعریف امنیت داده

- اگر رخدادهای ناخوشایند و خطرناک را در یکی از رده های دسترسی غیرمجاز به داده ها، نشت اطلاعات محرمانه، از دسترس خارج شدن خدمات یک سرویس دهنده، تغییر مخفیانه در داده ها، سرقت داده ها، نابود شدن داده ها، جعل داده ها، اختلال در عملکرد صحیح ماشین کاربران و هر نوع تعرض به حریم داده های یک ماشین را تلقی کنیم؛ امنیت داده ها عبارت است از مجموعه تمهیدات و روشها که در یکی از بند های زیر قرار بگیرد:
- الف) تمهیداتی که اطمینان می دهد رخدادهای ناخوشایند، هرگز اتفاق نمی افتد.
- ب) تمهیداتی که احتمال وقوع رخدادهای خطرناک را کاهش می دهد.
- ج) تمهیداتی که نقاط حساس به خرابی و استراتژیک را در سطح شبکه توزیع نماید.
- د) تمهیداتی که اجازه می دهد به محض وقوع رخدادهای خطرناک، شرایط در اسرع وقت و با کمترین هزینه به شکل عادی برگردد و کمترین خسارت را به جای بگذارد. بنابراین تعریف می کنیم امنیت عبارت است از: مکانیزم های پیشگیری یا کاهش احتمال وقوع رخدادهای خطرناک و جلوگیری از تمرکز قدرت در هر نقطه از شبکه، در حین وقوع رخدادهای ناخوشایند.

# انواع تهدید

**تهدید امنیتی:**

هر عاملی که به طور بلقوه بتواند منجر به وقوع رخدادی خطرناک بشود، یک تهدید امنیتی به شمار می آید.

تهدیدهای امنیتی از عوامل زیر ناشی می شود:

۱- تهدیدهای طبیعی:

این تهدیدها از عواملی مثل: زلزله، سیل، گردباد، رعد و برق، آتشفشان، آتش سوزی و نظایر آن از قوه به فعل می رسند.

۲- تهدیدات غیر عمدی:

این تهدیدات از اشتباهات سهوی و ناخداگاه عوامل انسانی مثل: مدیر شبکه، کارکنان و کاربران ناشی می شود. این تهدید می تواند منجر به افشا یا نابودی اطلاعات و یا اختلال در خدمات معمول شبکه بشود.

بعضی از این تهدیدات غیر عمد را در زیر نام می بریم:

- طراحی ناصحیح زیرساخت شبکه یا عدم وجود افزودگی در تجهیزات شبکه
- عدم تهیه نسخه های پشتیبانی از داده های حیاتی
- سهل انگاری در وظایف روزمره مثل بررسی مستمر سیستم ها از لحاظ آلودگی به ویروس
- ناآگاهی کاربران از ماهیت عملیات خطرناک(ریسک)

۳- تهدیدات عمدی:

هرگونه اقدام برنامه ریزی شده جهت افشا، نابودی و یا تغییر در داده های حیاتی و یا ایجاد اختلال در خدمات معمول سرویس دهنده ها را تهدید عمدی می گوییم.

# چند اصطلاح

- **تهدید امنیتی:** هر عاملی که به طور بلقوه بتواند منجر به وقوع رخدادی خطرناک بشود، یک تهدید امنیتی به شمار می آید.
- حمله: هرگاه تهدیدی از قوه به فعل درآید اصطلاحاً یک حمله رخداده است؛ خواه آن حمله موجب خسارت به منابع بشود یا خواه یک تلاش نافرجام باشد.
- **تخریب یا خسارت:** حمله ای که در اثر آن منابع شبکه از بین برود یا دستکاری شود یا اطلاعات و داده های محرمانه افشا شود و یا حریم خصوصی افراد مورد تعرض قرار گیرد یا به کمک جعل هویت و فریب کاری از خدمات معمول شبکه سوءاستفاده شود، اصطلاحاً حمله به مرحله آسیب رسیده است.

# چند اصطلاح (ادامه)

- **آسیب پذیری:** هرگونه ضعف یا اشکال یک مولفه از شبکه در مقابل تهدیدات احتمالی که بتواند منجر به حمله شود، آسیب پذیری یا نقطه آسیب پذیر گفته می شود.
- **میزان خطر(ریسک):** تخمینی از احتمال وقوع یک حمله و همچنین پیش بینی خسارت هایی که متعاقب آن حمله به بار می آید را میزان خطر می گویند.
- **طرح امنیتی:** نقشه ای دقیق برای نظارت و کنترل تهدیدها، پیاده سازی عملی، استراتژی امنیتی و تحت کنترل درآوردن نقاط آسیب پذیر و به حداقل رساندن آسیب های احتمالی در صورت بروز حمله ای موفق را طرح امنیتی می گویند.
- **مکانیزم امنیتی:** هر روش یا الگوریتمی که برای تشخیص یا پیشگیری از وقوع حمله یا برگشت به وضعیت معمولی پس از وقوع حمله طراحی می شود را مکانیزم امنیتی می گویند. هیچ مکانیزم واحدی که بتواند امنیت داده ها را تضمین کند وجود ندارد.

# خدمات امنیتی:

**خدمات امنیتی:**

پیاده سازی هر نوع مکانیزم امنیتی و ارائه آن ها به کاربران به نحوی که میزان خطر را به حداقل برساند. عمده ترین خدمات امنیتی عبارتند از:

- محرمانه ماندن اطلاعات(Confidentiality):

به مجموعه مکانیزم هایی که تضمین می کند داده ها و اطلاعات مهم کاربران از دسترس افراد بیگانه و غیرمجاز دور نگه داشته شود را محرمانگی اطلاعات گویند. مهمترین روش تحقق محرمانگی استفاده از الگوریتم های رمزنگاری است.

- احراز هویت(Authentication):

مجموعه مکانیزم هایی که این امکان را فراهم می کند که بتوان مبدا واقعی یک پیام، سند یا تراکنش را بدون ذره ای تردید یا ابهام مشخص کرد را احراز هویت گویند.

# خدمات امنیتی (ادامه)

- تضمین صحت اطلاعات یا جامعیت(Integrity):

مجموعه مکانیزم هایی که از هر گونه تحریف، تکرار، دستکاری، حذف و آلوده کردن داده ها پیش گیری کند و یا حداقل باعث کشف چنین اقداماتی می شود را تضمین صحت اطلاعات می گویند.

- غیرقابل انکار ساختن پیام(Non-Repudiation):

به مجموعه مکانیزم هایی که به پیام ها و تراکنش ها پشتوانه حقوقی می بخشد و اجازه نمی دهد که فرستنده به هر طریق ارسال پیام خود را انکار کند و یا گیرنده منکر دریافت پیام شود را غیر قابل انکار ساختن پیام گویند.

- کنترل دسترسی(Access Control):

مکانیزم هایی که دسترسی به کوچکترین منابع اشتراکی شبکه را تحت کنترل در آورده و هر منبع را براساس سطح مجوز کاربران و پروسه ها در اختیار آن ها قرار می دهد.

- در دسترس بودن(Availability):

مجموعه مکانیزم هایی که این امکان را برای کاربران شبکه فراهم می کند تا در هر زمان و با توجه به کنترل ها و محدودیت های موجود در شبکه، قدرت استفاده از شبکه را داشته باشد.

# تهدیدها در شبکه به چهار دسته زیر تقسیم می شوند:

۱- استراق سمع یا شنود(Interception):

هرگاه یک شخص غیرمجاز به هر نحو بتواند نسخه ای از داده های در حال جریان بین مبدا و مقصد را به نفع خود شنود کند را حمله استراق سمع گویند.

۲- دستکاری(Manipulation):

هرگاه داده ای در حال جریان بین مبدا و مقصد توسط شخص غیرمجاز، به هر نحو دستکاری یا تحریف شود را حمله دستکاری می گویند.

۳- جعل(Fabrication):

هرگاه یک شخص غیرمجاز اقدام به تولید پیام های ساختگی کرده وآن ها را به شخص مجاز دیگری نسبت بدهد، حمله جعل و ارسال داده های ساختگی به وقوع پیوسته است.

۴- وقفه(Interruption):

هرگاه کسی بتواند سیستم یا سرویس را در شبکه از کار بیندازد، حمله وقفه رخداده است.

- استراق سمع تهدیدی علیه محرمانه ماندن اطلاعات است.
- دستکاری تهدیدی علیه صحت اطلاعات است.
- جعل تهدیدی علیه احراز هویت اطلاعات است.
- وقفه تهدیدی علیه در دسترس بودن اطلاعات است.

# تمهیدات امنیتی

**تمهیدات امنیتی در هر شبکه باید در سه مورد زیر مشخص شده باشد:**

- تمهیدات پیشگیری از وقوع حمله
- تمهیدات کشف حمله در صورت وقوع
- تمهیدات بازیابی و خروج از بحران پس از وقوع حمله

# زیرساخت امنیت اطلاعات

**زیرساخت امنیت اطلاعات:**

طبق استانداردهای جهانی، فرآیند تضمین امنیت اطلاعات در چندین فاز بدست می آید. این فازها به ترتیب عبارتند از:

۱- تعریف دامنه یا حوزه(Scope Definition):

در این مرحله، فهرست دقیقی از تمام عوامل انسانی و دست اندرکاران شبکه که به هر نحو در امنیت اطلاعات دخیل اند تهیه می شود. مطلب مهم در اینجاست که در بسیاری از سازمان ها و موسسات، اطلاعات مهمترین دارایی آن هاست و عوامل متعددی باید در حفاظت و مراقبت از دارایی آن سازمان کمک کنند.

۲- مسائل مربوط به تهدید(Threat Assessment):

در این مرحله باید تحلیل برآورد جامعی از طبیعت تهدیدهایی که علیه منابع شبکه و اطلاعات در آن وجود دارد صورت گیرد. همچنین باید منشاء این تهدیدها و موقعیت آن ها در سازمان تعیین گردد. طبیعت هر تهدید می تواند متفاوت باشد. افشای اطلاعات حساس، اشخاص غیرمجاز، تغییر مخفیانه اطلاعات و ... و منشاء تهدیدات می تواند اشتباهات عمدی یا سهوی عوامل، سوءاستفاده عوامل، اخلالگری عوامل بیرونی و ... که به هر نحو نفوذی را در سیستم بوجود آورند. موقعیت تهدید می تواند از محل فیزیکی استقرار منابع شبکه شروع شود و نیز دزدیده شدن این منابع فیزیکی را شامل شود. منابع فیزیکی، سرورها، تجهیزات مسیریابی، هارد دیسک ها و ... می باشند.

# زیرساخت امنیت اطلاعات (ادامه)

۳- تشخیص آسیب:

تهدید الزاماً به حمله و آسیب نمی انجامد. پس از تعیین تهدیدها، باید نقاط آسیب پذیر سیستم به دقت بررسی شود که منظور از نقطه آسیب پذیر، هرگونه مولفه سخت افزاری، نرم افزاری و یا سیستم عامل است که بروز یک اشکال بلقوه در آن می تواند به حمله و خسارت منتهی گردد.

۴- تشخیص ریسک:

امنیت امری نسبی است و هیچ گاه چیزی به نام امنیت ۱۰۰٪ قابل تعریف نیست و از طرفی می تواند هزینه طراحی و پیاده سازی یک الگوی امنیتی بسیار گران تر از خود شبکه شود. پس لازم است در این مرحله میزان خسارت مالی که در اثر تبدیل هر تهدید به حمله تخمین زده شود و هزینه پیشگیری و مقابله با آن تهدید ارزیابی شود. با توجه به بررسی این دو مقدار می توانید ریسک را در بهترین حالت کنترل نمایید.

# زیرساخت امنیت اطلاعات (ادامه)

۵- راهکار مدیریت ریسک:

پس از تعیین فهرست تهدیدها و تعیین ضرر ناشی از تبدیل آن ها از قوه به فعل و همچنین ارزیابی میزان بودجه موجود برای هر تهدید، استراتژی های زیر اتخاذ می گردد:

الف) استراتژی های پیشگیرانه:

شامل استفاده از تکنولوژی های برتر، ابزار های نظارت و مراقبت، آموزش عوامل انسانی، پیش بینی سخت افزار و ...

ب) استراتژی های مقابله:

شامل تعیین ابزارهای کشف حمله، تعیین روش های بازیابی داده ها، بیمه تجهیزات و ... ؛ در این مرحله باید کیله تهدیدات پیشگیرانه و راه های مقابله با تهدیدات مشخص شود و آن بخشی از تهدیدات که هیچ پیش بینی خاصی در مورد آن ها نشده به دقت مشخص گردد و به صورت دقیق و رسمی مستندسازی گردد. خروجی این مرحله به صورت یک آئین نامه و مجموعه ای از طرح و نقشه خواهد بود.

# زیرساخت امنیت اطلاعات (ادامه)

۶- پیاده سازی طرح امنیتی:

پس از تدوین طرح امنیتی، باید آن را در عمل پیاده سازی کرد. بخش بزرگی از یک نقشه امنیتی فقط در گروی اعمال سیاست ها، آموزش افراد و اطمینان از تعهد افراد است. بنابراین به مدیریت قوی و ارزیابی مستمر نیاز دارد. مدیر پروژه باید هدایت صحیح مراحل قبلی و نیز عملیات نصب و راه اندازی ابزارهای امنیتی و پیکربندی آن ها براساس استراتژی تعیین شده، داشته باشد.

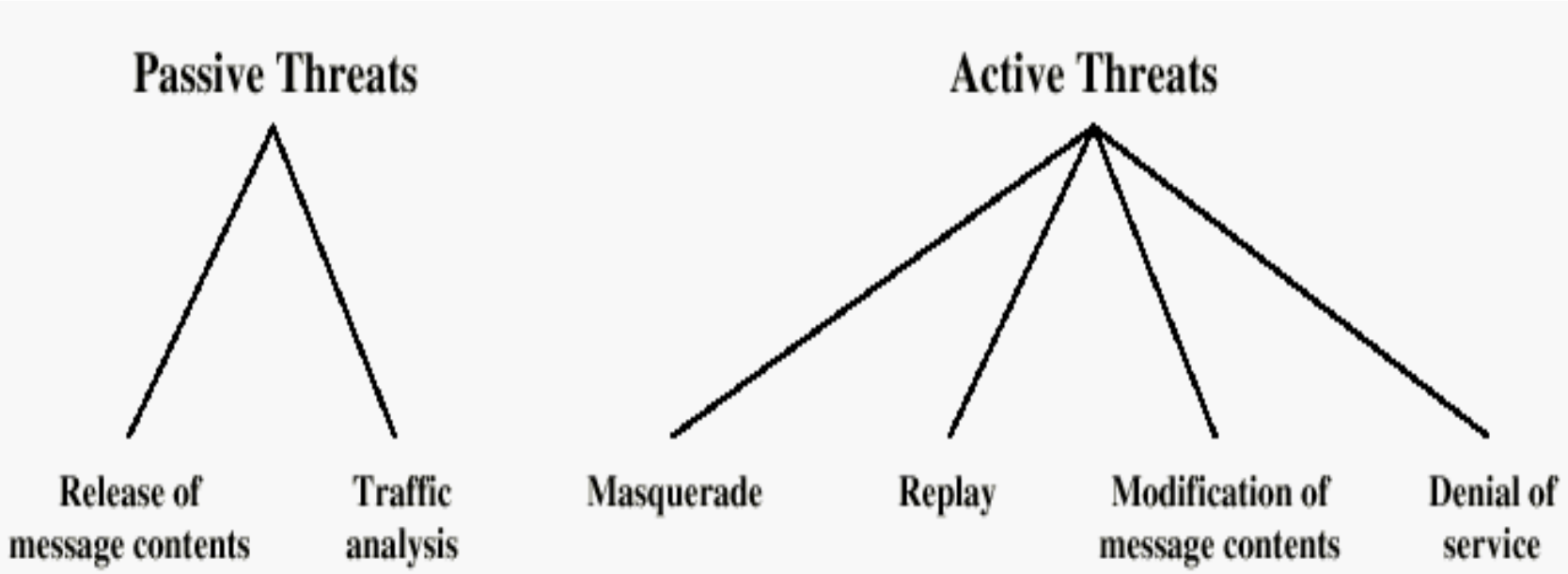
۷- بررسی امنیت:

هیچ استراتژی کامل نخواهد بود مگر آنکه به طور متناوب و در مقاطع زمانی برنامه ریزی شده مورد ارزیابی قرار بگیرد. در این صورت با توجه به تغییرات دوره ای که در جهت رفع نقایص طرح امنیتی ایجاد می کنیم، صحت از امنیت را تا حد مطلوبی افزایش می دهد.

# انواع سرویسهای امنیتی

- Confidentiality (privacy)
- Authentication (who created or sent the data)
- Integrity (has not been altered)
- Non-repudiation (the order is final)
- Access control (prevent misuse of resources)
  - Authorization
- Availability (permanence, non-erasure)
  - Denial of Service Attacks
  - Virus that deletes files

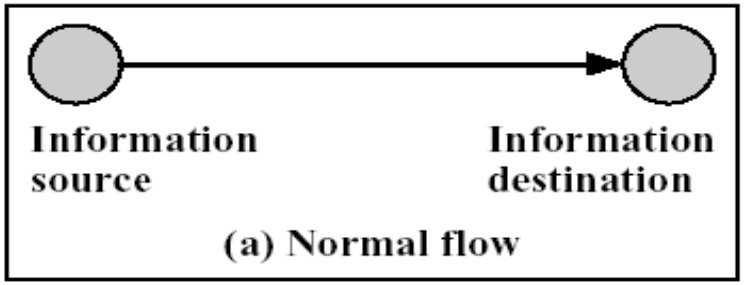
# انواع حملات فعال و غیرفعال

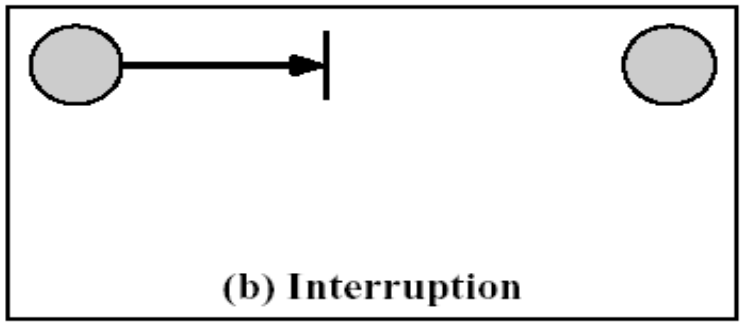


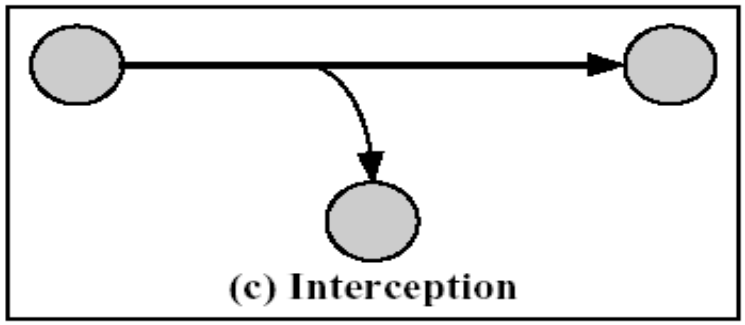

مانند حملات شناسایی Reconnaissance (Host scan, port scan) ، session hijacking, SYN attacks, Privilege escalation (ftp cwd ~root)

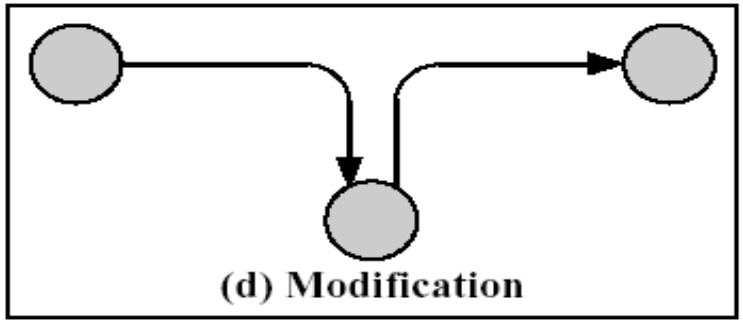
Active and Passive Security Threats

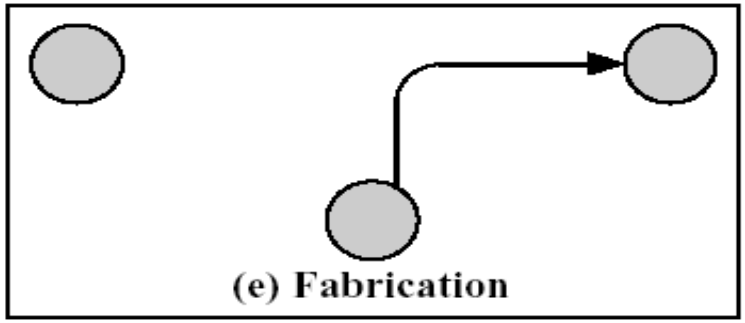
# دسته بندی روشهای انجام حملات



# دسته بندی مکانیسم های مقابله با حملات-۱

- سیاستگذاری
  - مانند تغییر متناوب password ها
- کنترل های سخت افزاری
  - مانند استفاده از gateway های سخت افزاری
- کنترل های نرم افزاری
  - مانند کنترل دسترسی در سیستم عامل
- کنترل های فیزیکی
  - مانند کنترل رفت و آمد به اتاق سرور

# دسته بندی مکانیسم های مقابله با حملات-۲

- Policies and social education
- Traffic Control
  - E.g.: Path selection, Choke Points, Filtering
- Monitoring and Inspection
  - E.g.: Event logging, Intrusion detection, CDR data retention, DPI, IP traceback
- Encryption
  - Confidentiality, user, origin and message authentication, digital signatures
- Access control
  - Physical, host-based (smartcard, data access authorization, …), network-based (Address-based, Firewalls, Ingress filtering…)

# مدل امنیت شبکه بر پایه استاندارد X.805

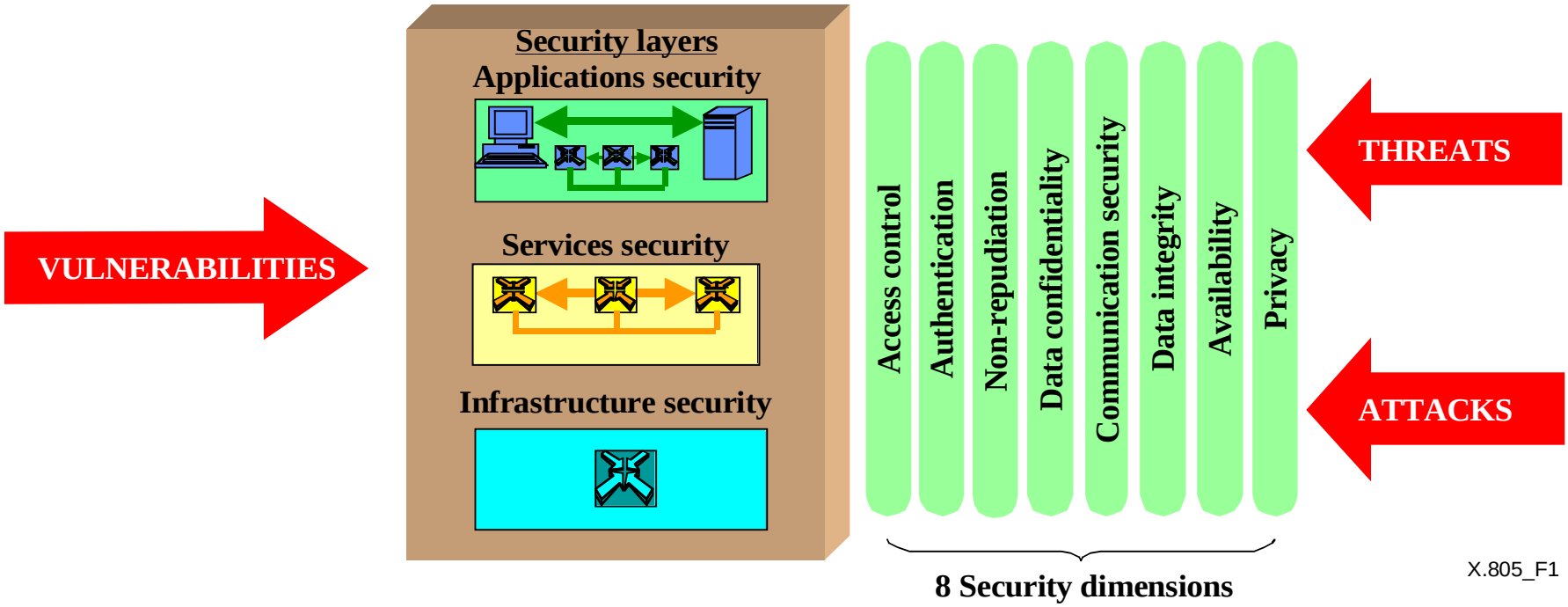
این استاندارد در سال ۲۰۰۴ توسط ITU تصویب گردیده و مدل مبنای امنیت شبکه تلقی میشود.

# اهداف/سرویسهای امنیت شبکه

- 1) Access control;
- 2) Authentication;
- 3) Non-repudiation;
- 4) Data confidentiality;
- 5) Communication security;
- 6) Data integrity;
- 7) Availability; and
- 8) Privacy.

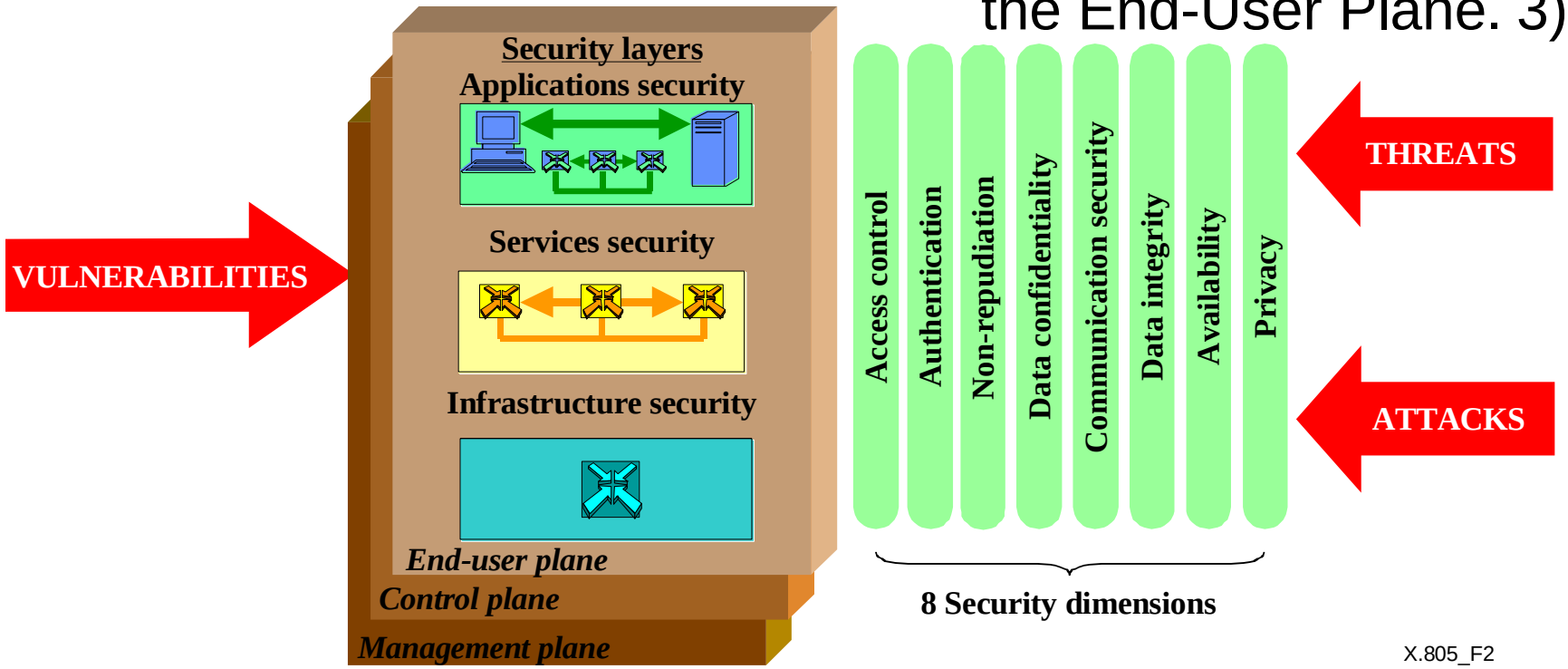
# لایه های امنیت

- the Infrastructure Security Layer –
- the (Network) Services Security Layer –
- the (User) Applications Security Layer –



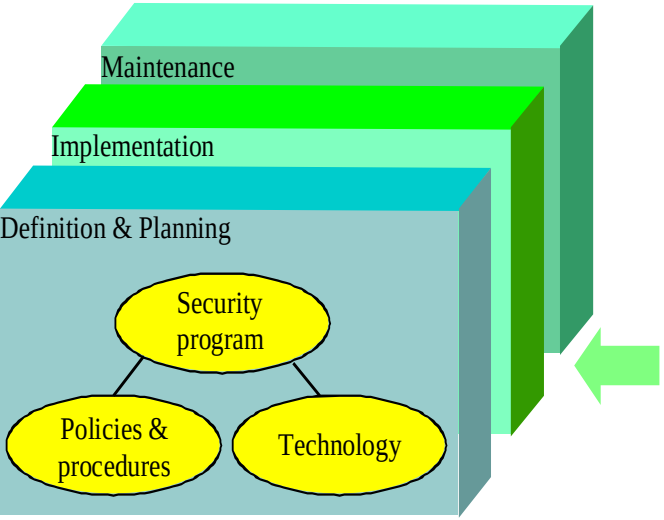
# حوزه های فعالیت شبکه

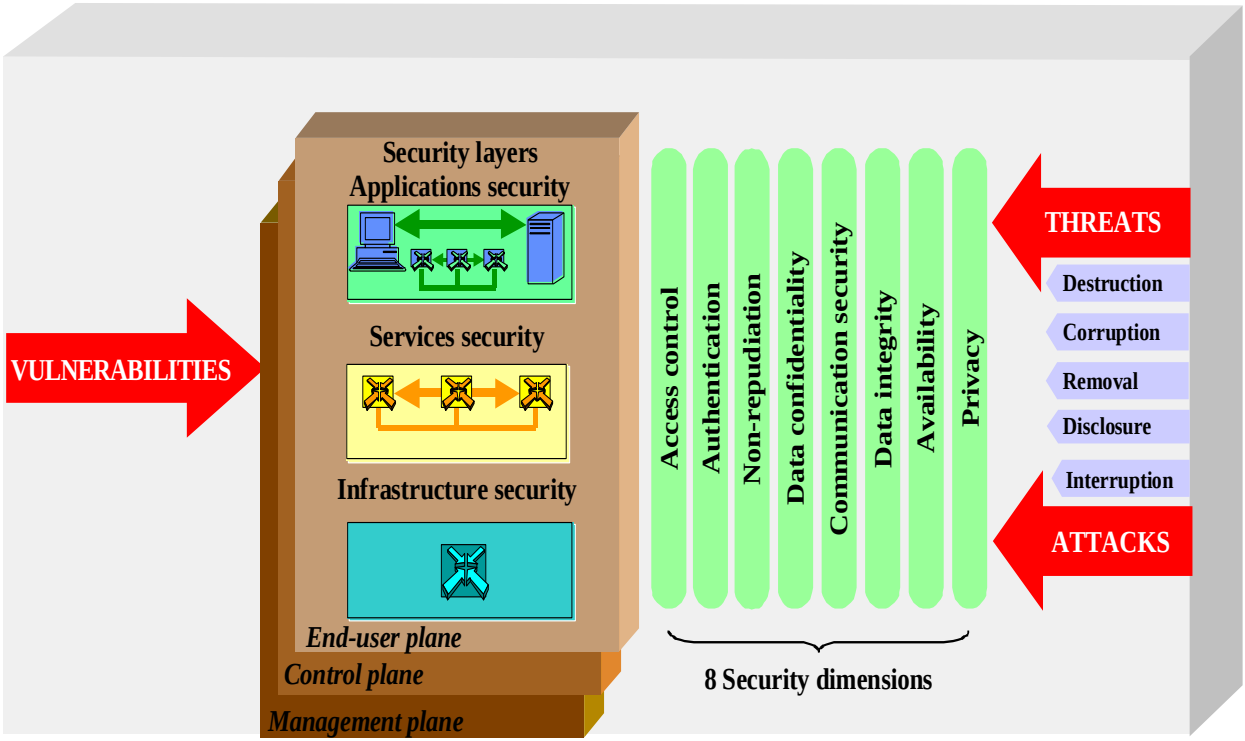
the Management Plane; 1)
the Control Plane; and 2)
the End-User Plane. 3)



# فازبندی برنامه ریزی امنیتی

the Definition and Planning phase; 1)
the Implementation phase; and 2)
the Maintenance phase. 3)



# منابع


- William Stallings, Cryptography and Network Security Principles and Practices
- Man Young Rhee, Internet Security Cryptographic Principles, Algorithms and Protocols
- William Stallings, Network Security Essentials, Fourth Edition
- علی ذاکرالحسینی و احسان ملکیان، امنیت داده ها
- احسان ملکیان، نفوذگری در شبکه و روشهای مقابله