امنیت شبکه

علی فانیان
a.fanian@cc.iut.ac.ir

فهرست مطالب

- کتاب مرجع
- ارزیابی
- مفهوم امنیت
- تعاریف
- استاندارد X.800
- مدلها و معماری امنیت شبکه

کتاب مرجع

Text Book:
1-INFORMATION SECURITY Principles and Practice, Second Edition by Mark Stamp, 2011.
2- CRYPTOGRAPHY AND NETWORK SECURITY PRINCIPLES AND PRACTICE FIFTH EDITION by William Stallings, 2011.

ارزیابی

- میان ترم ٪۳۰
- پایان ترم ٪٤٥
- پروژه و سمینار ٪۲۰
- داوری مقاله ٪۵

ارزیابی

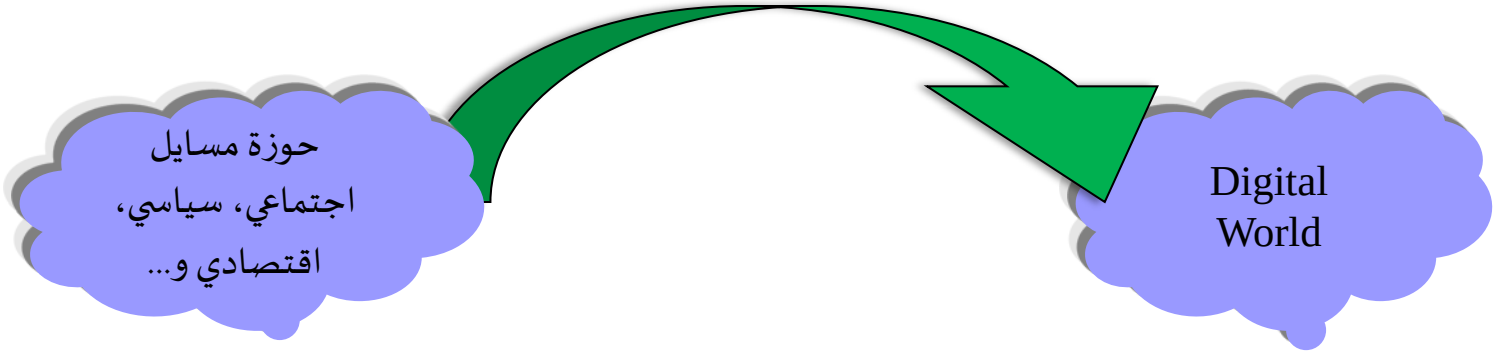
- پروژه ٪۲۰
  - تمرکز بر یک موضوع تحقیقاتی
  - تاریخ برگزاری سمینارها هفته اول و دوم خرداد
  - تاریخ تحویل گزارش ۳۱ خرداد (بدون تمدید، حتی برای یک روز)
  - ۱۵سمینار ، هر سمینار یک ساعت کامل

ارزیابی

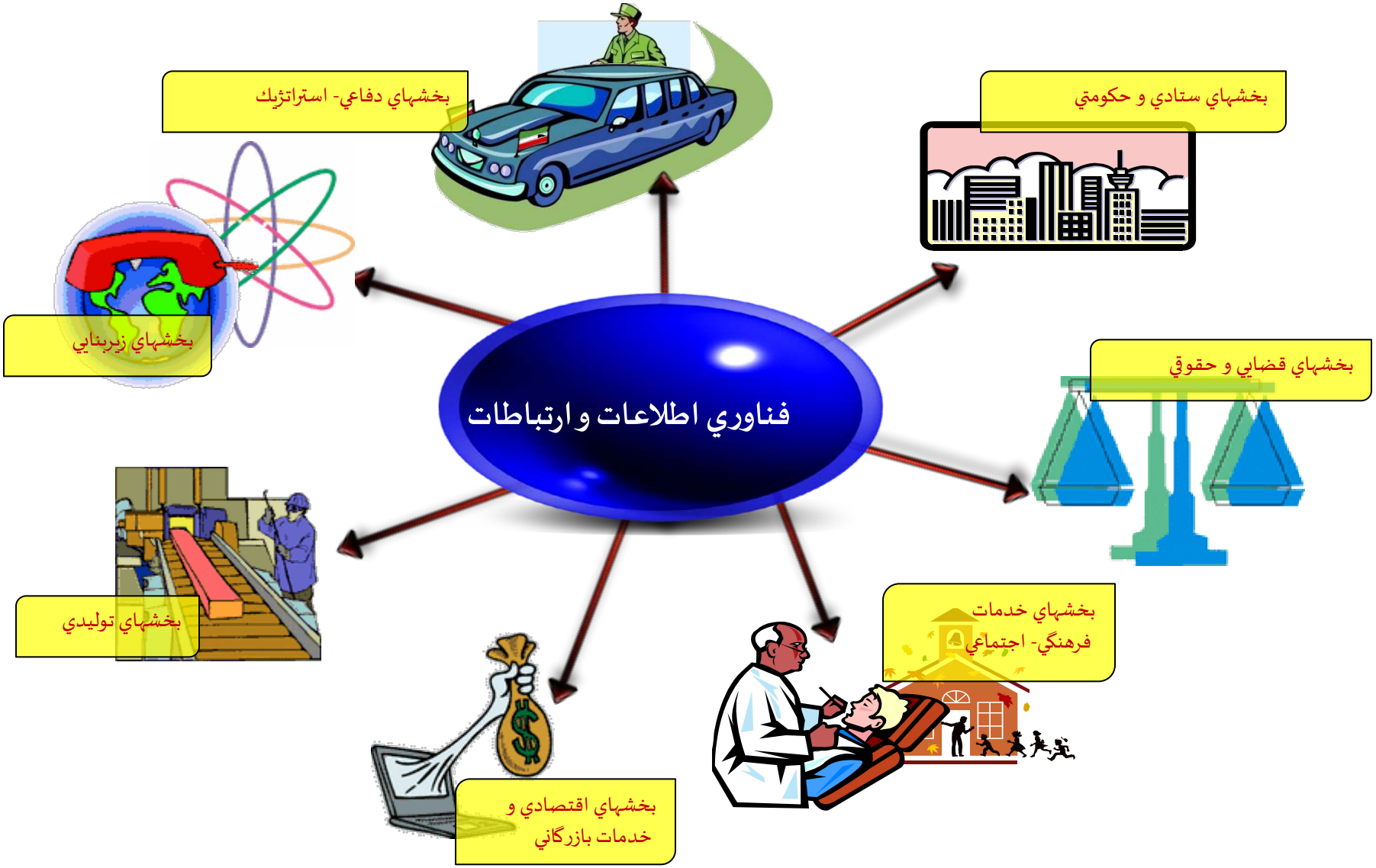
- داوری ۵٪
- داوری حداقل ٤ مقاله مرتبط با حوزه امنیت
- تاریخ شروع داوری ۱۰ تیر
- تاریخ اتمام داوری ۲۰ تیر

تغييرات اساسي حاصل از توسعه فناوري اطلاعات

- سريع‌تر شدن كامپيوترها
- رشد سريع شبكه
- دسترسي‌هاي راه دور
- تجارت الكترونيك
- و كلاً گرايش به سوي كنترل الكترونيكي هرچيز مهم و با ارزش



نفوذ فناوري اطلاعات در كليه عرصه‌ها



تنوع تهدیدات و روند رشد آنها

- حمله اینترنتی، ساده و کم خطر است و به سختی قابل ردگیری است.
- یافتن آسیب پذیری در برنامه ها و کاربردها الزاماً نیازی به دراختیار داشتن سورس کد ندارد.
- زیر ساختهای حیاتی به طور فزاینده ای به اینترنت متکی شده اند.
- نفوذگران از طریق پهنای باند وسیع و اتصالات پرحجم به تدارک حمله می پردازند (از طریق بیگاری گرفتن از حجم وسیعی از کامپیوترهای خانگی)

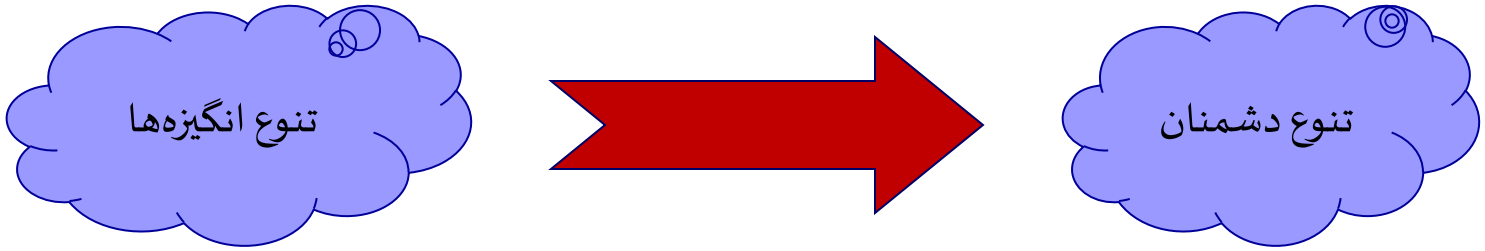
ماهيت جديد حملات

- پيچيدگي فراوان
- مكانيزه
- انجام عمليات از راه دور
- كانالهاي ارتباطي متنوع
- انتشار روشهاي موفق حمله

انگيزه‌هاي ايجاد نا امني در فضاي سايبر متنوع است

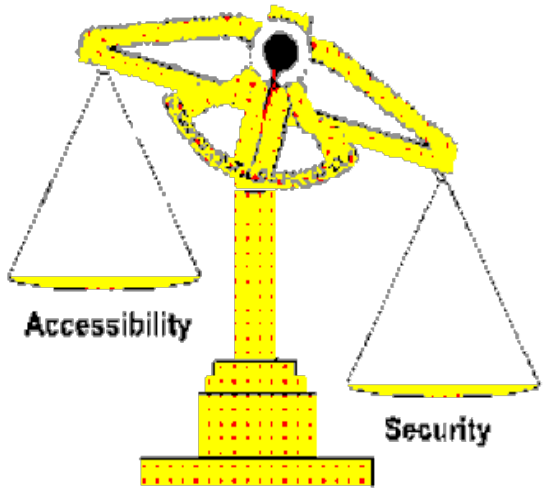
- انگيزه‌هاي سياسي، نظامي (برتري استراتژيك)
- انگيزه‌هاي مالي و اقتصادي (سود بيشتر)
- انگيزه‌هاي علمي (پيشرفت علم)
- انگيزه‌هاي رواني (شهرت طلبي)
- انگيزه‌هاي حقوقي (بي اعتبار كردن سيستم)

تنوع دشمنان



- جاسوس ها (تجاري، سياسي، نظامي)
- تروریست‌ها
- مجرمين (عادي، سازمان يافته)
- هکرها
- نفوذي‌ها
- افراد نه چندان مطمئن

راه حل سادة امن‌سازي



- حذف تمامي اتصالات و ارتباطات شبكه با سايرين
- قراردادن سيستمها در اتاقهاي محافظت شده
- قراردادن يك محافظ در درب هر اتاق

حذف بسياري از دستاوردهاي شبكه‌ها

تعاریف

تعاريف

- مهندسي امنيت: مجموعه فعاليت‌هايي است كه براي حصول و نگهداري سطوح مناسبي از
  - محرمانگي (Confidentiality)
  - صحت (Integrity)
  - قابليت دسترسي (Availability)
  - جوابگويي (Accountability)
  - اصالت (Authenticity) و
  - قابليت اطمينان (Reliability)

  به صورت سيستماتيك در يك سازمان انجام مي‌شود.

تعاريف

- محرمانگي: اطلاعات براي افراد، موجوديت‌ها يا فرآيندهاي غيرمجاز در دسترس قرار نگيرد يا افشا نشود.
- صحت : صحت سيستم و صحت داده
  - صحت داده: داده ها به صورت غير مجاز تغيير پيدا نكنند يا از بين نروند.
  - صحت سيستم: فعاليت‌هاي مورد انتظار از سيستم بدون عيب و خالي از دستكاري هاي غير مجاز (تعمدي يا تصادفي) در سيستم انجام شود.

تعاريف

- اصالت: هويت واقعي يك موجوديت با هويت مورد ادعا يكسان باشد.
- قابليت دسترسي: در دسترس و قابل استفاده بودن منابع براي يك موجوديت احراز اصالت شده در هنگام نياز.
- جوابگويي (حساب پذيري): فعاليت‌هاي موجوديت‌ها در سيستم اطلاعاتي قابل رديابي و بررسي باشد.
- قابليت اعتماد: سازگار بودن رفتارها و نتايج مورد انتظار، استمرار فعاليتها و سرويسهاي مورد انتظار در طول زمان و در شرايط بحراني.

تعاريف

- امنيت IT : حفاظت از سيستم هاي اطلاعاتي به منظور دستيابي به اهداف قابل اجرا در حفظ محرمانگي، صحت، قابليت دسترسي، حساب پذيري، اصالت و قابليت اعتماد.
- دارايي(asset): آنچه براي سازمان داراي ارزش است.
- تهديد(threat): پتانسيل وقوع يك رويداد ناخواسته كه ممكن است به سيستم يا سازمان خسارت وارد كند.
- رخنه(flaw): نقاط ضعف يك دارايي يا گروهي از داراييها كه ممكن است توسط يك تهديد فعال شود.
- صدمه: نتيجة يك رويداد ناخواسته

تعاريف

- حمله(Attack) :تلاش عمدي براي رخنه در يك سيستم يا سوء استفاده از آن.
- Breach : نقض سياست امنيتي يك سيستم
- نفوذ(Intrusion) : فرايند حمله و رخنه ناشي از آن
- آسيب‌پذيري(Vulnerability) : نقطه‌اي از سيستم كه احتمال رخنه از آنجا وجود داشته باشد.

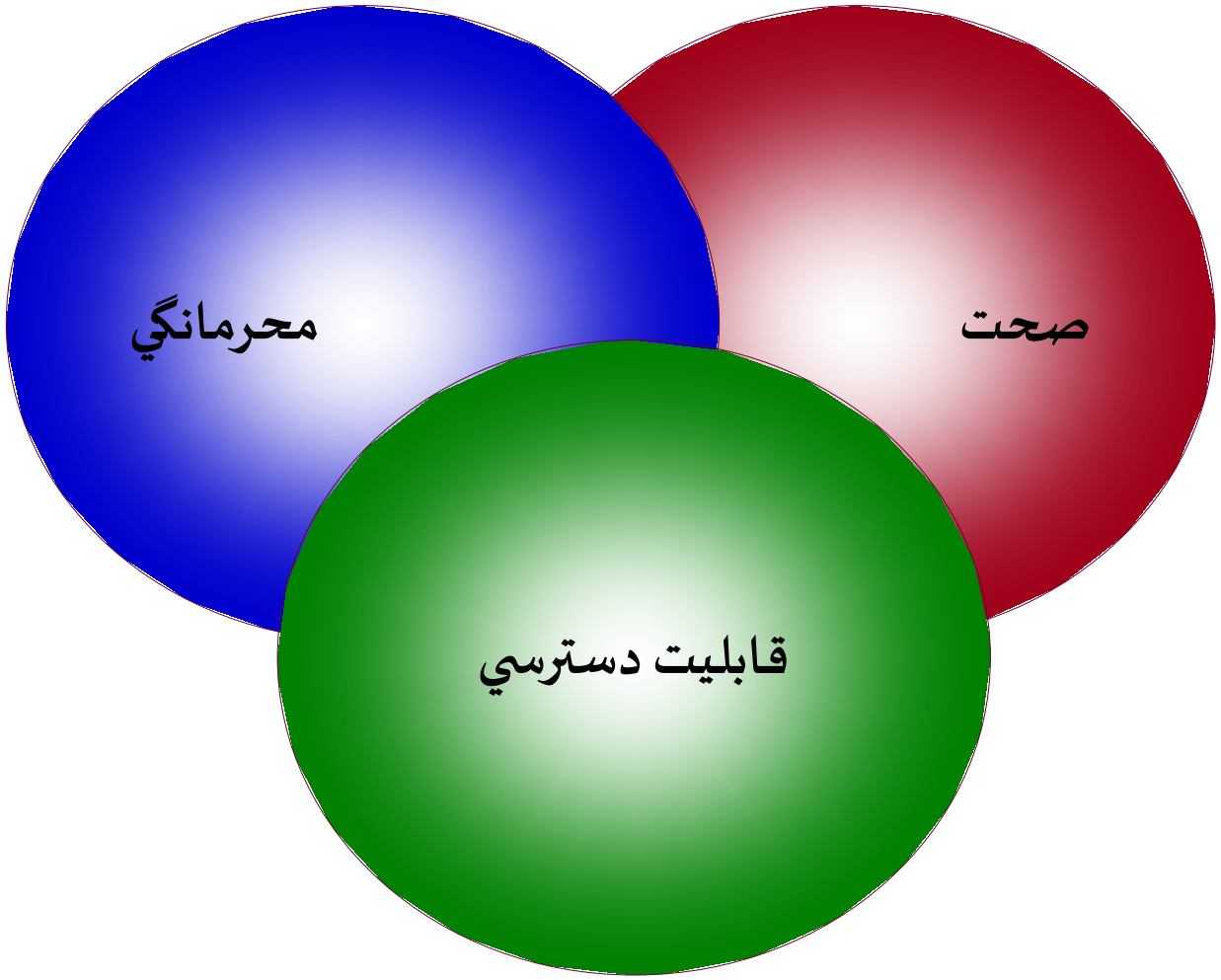
تعاريف

- روش دفاعي(safeguard): تجربه، روال، يا مكانيزم مورد استفاده جهت كاهش مخاطرات.
- كنترل‌هاي پايه(baseline control): مجموعة حداقلي از روشهاي دفاعي براي تأمين امنيت سازمان
- ماندة مخاطره(residual risk): مخاطرات باقي‌مانده پس از پياده سازي روش هاي دفاعي

تعاريف

- مديريت ريسك(risk management): فرآيند كامل شناسايي، كنترل و حذف يا كاهش رويدادهاي نامطمئني كه ممكن است به منابع سيستم IT خسارت وارد كند.
- خط مشي امنيتي (security policy): قوانين، دستورالعمل‌ها و تجربياتي كه بيان كنندة چگونگي مديريت، حفاظت و توزيع دارايي‌ها (شامل اطلاعات حساس) در داخل سازمان است.

مولفه های امنیت



مؤلفه‌هاي امنيت

- محرمانگي (Confidentiality)
  - عدم افشا محتوا
  - عدم امكان تحليل ترافيك
  - عدم نشت اطلاعات
  - عدم افشاي نامها (Anonymity)

مؤلفه‌هاي امنيت

- صحت(Integrity)
  - اصالت داده‌ها (عدم حذف, اضافه و تكرار)
  - اصالت مبدأ داده‌ها (Data Origin Authentication)
  - اصالت و حضور موجوديتها (On-line Entity Authentication)
  - انكارناپذيري (Non-Repudiation)

مؤلفه‌هاي امنيت

قابليت دسترسي(Availability)

- سهولت دسترسيهاي مجاز: حل تقابل ذاتي امنيت و تسهيل ارتباطات
- مقابله با حملات جلوگيري از ارائه سرويس (Denial of Service)

استاندارد X.800

استاندارد X.800

- فراهم کننده یک چارچوب ستماتیک برای توصیف
  - حملات امنیتی
  - مکانیزم های امنیتی
  - سرویس های امنیتی

تعاريف در X.800

- حمله امنيتي(Security Attack) :

تلاش برای رخنه در یک سیستم

- مكانيزم امنيتي(Security Mechanism) :

روش درنظرگرفته شده براي تشخيص, جلوگيري و بازيابي از حملات

-رمز نگاري، امضاي ديجيتال ، پروتكل هاي احراز اصالت و...

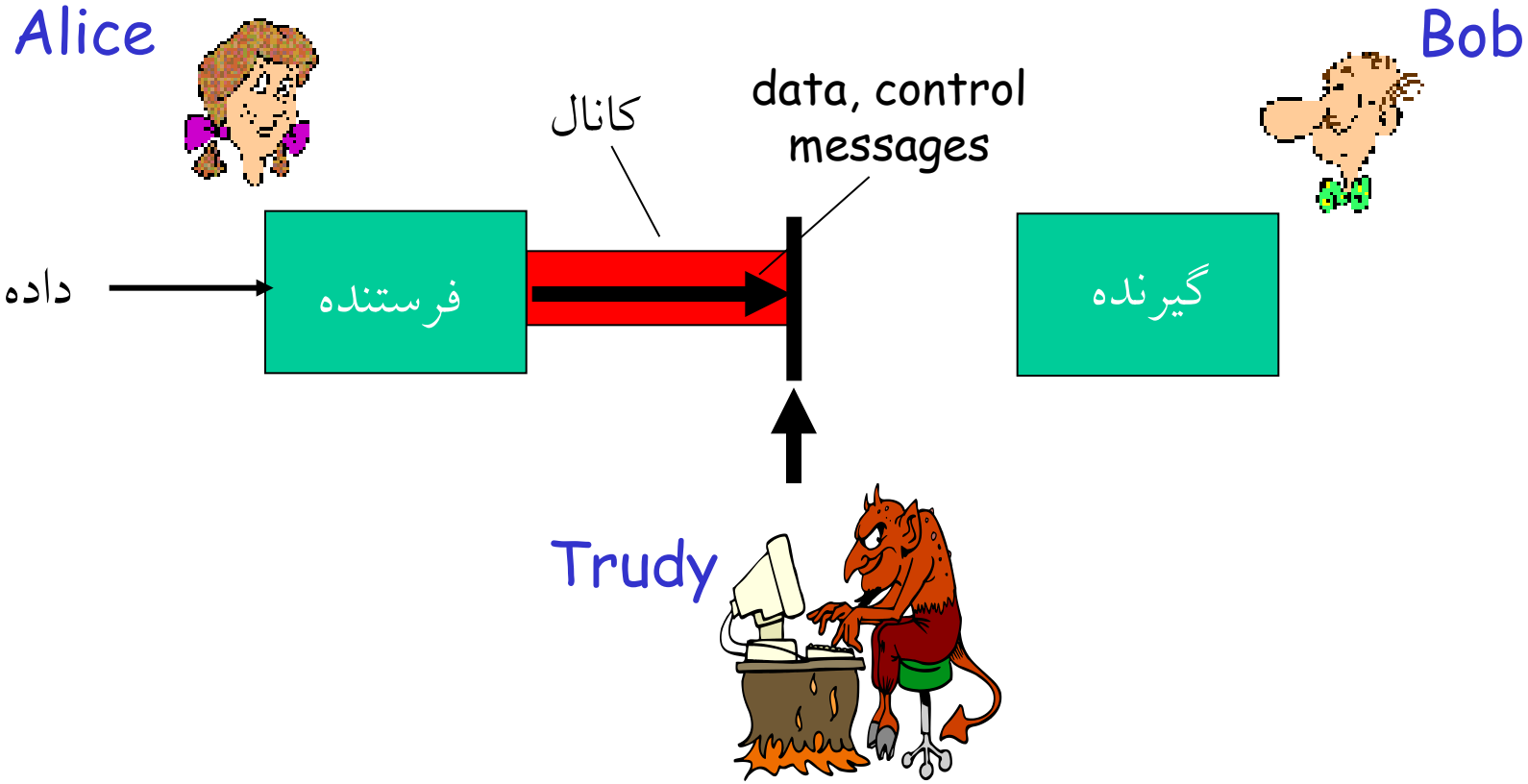
- سرويس امنيتي(Security Service)

سرويس هاي تضمين كننده امنيت با استفاده از مكانيزمهاي بالا

- محرمانگي، انكار ناپذيري، صحت و..

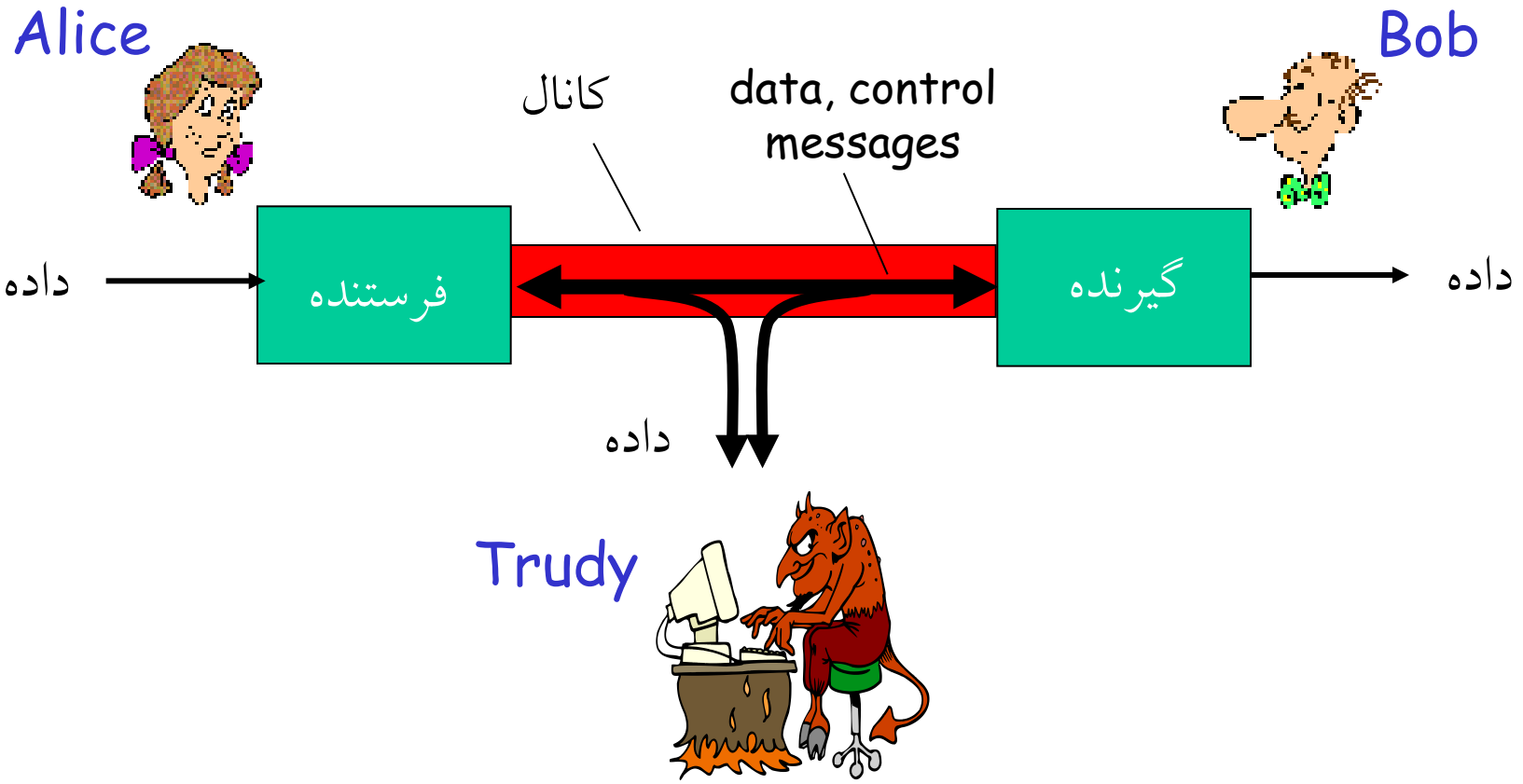
انواع و ماهیت حملات

– وقفه (Interruption): اختلال در شبکه و سرویس



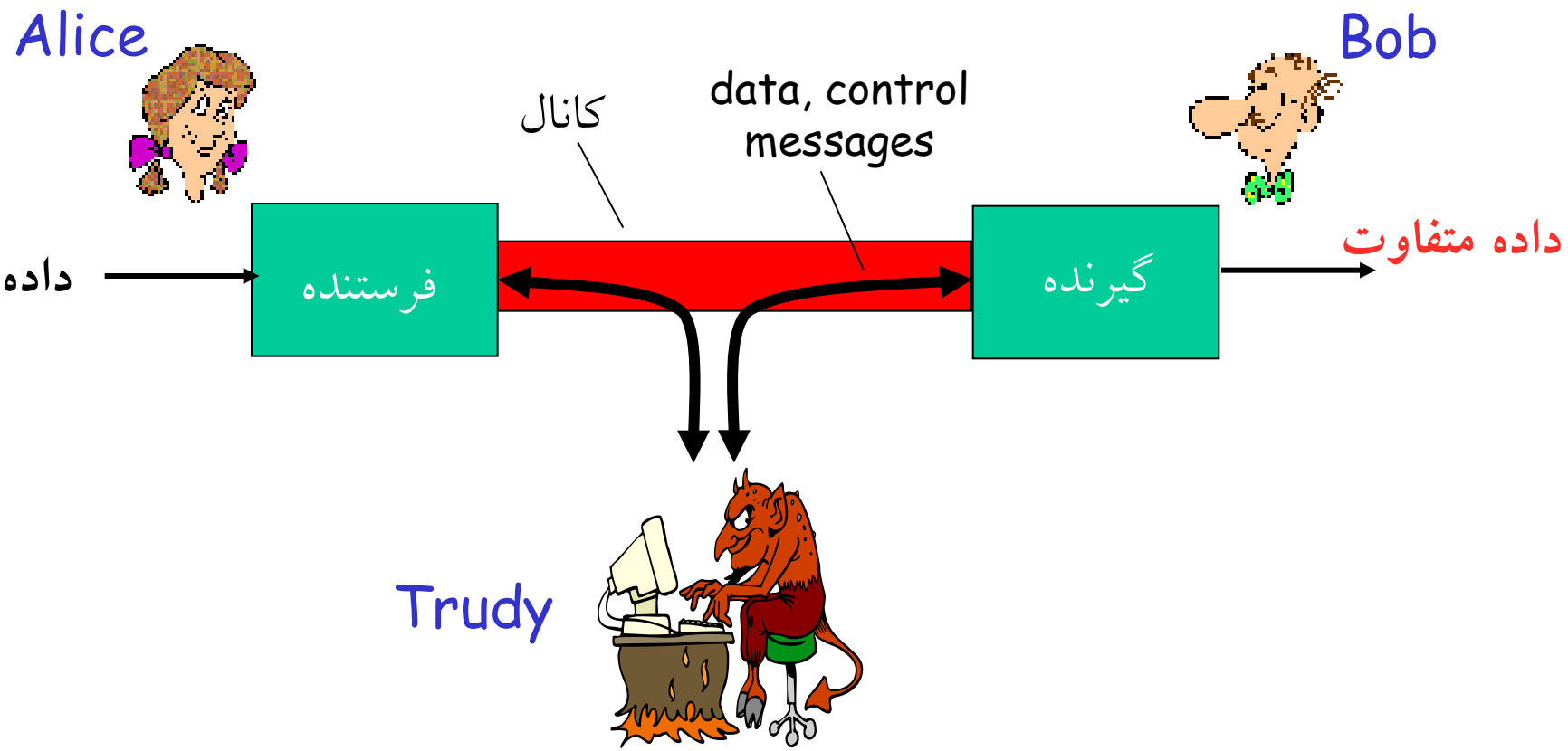
انواع و ماهیت حملات

– شنود(Interception) : استراق سمع ارتباطات شخصی یا مخفی سایرین



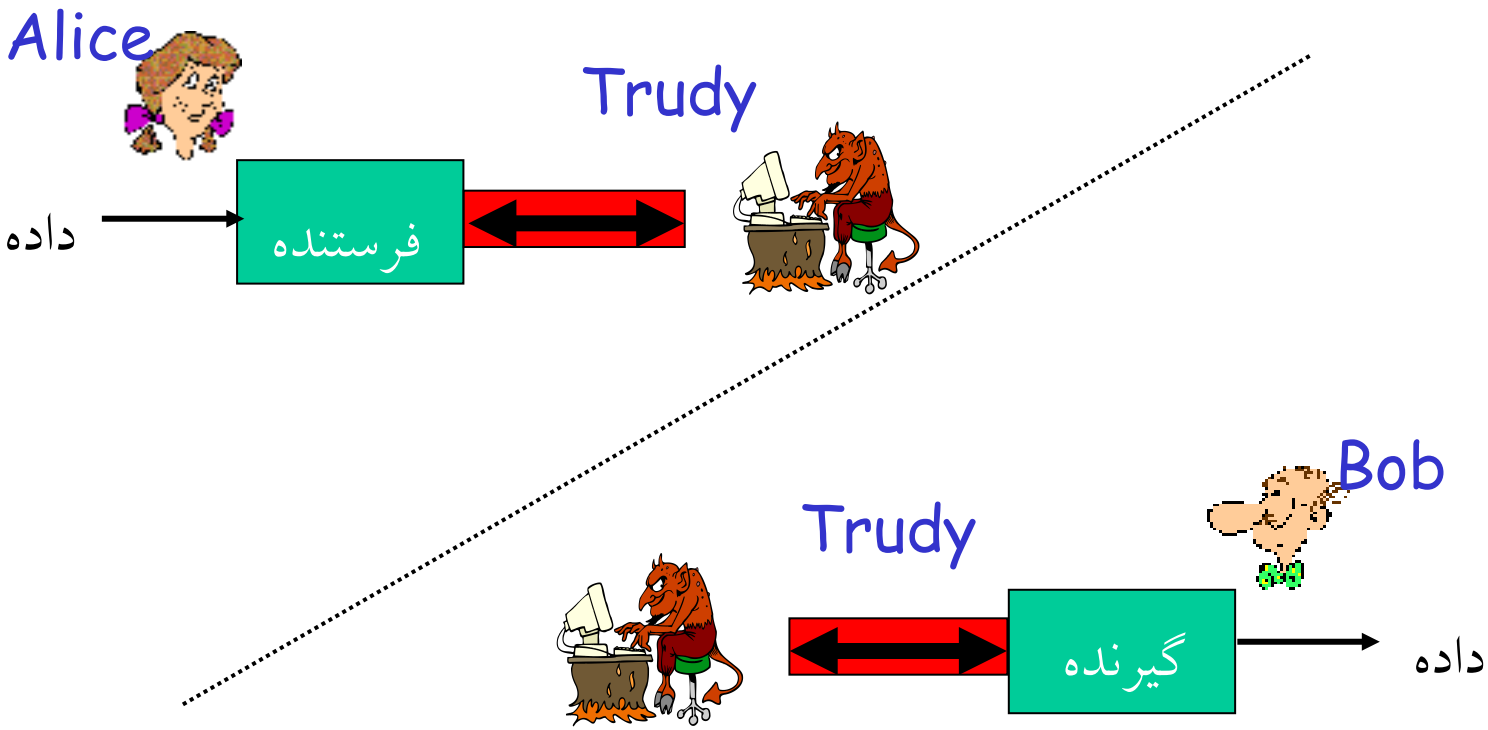
انواع و ماهیت حملات

– دستکاری داده‌ها : تغییر غیرمجاز داده‌های سیستم یا شبکه



انواع و ماهیت حملات

– جعل هویت (Fabrication): ارسال داده توسط کاربران غیرمجاز با نام کاربران مجاز



دسته بندی کلی حملات

- حملات غیرفعال (Passive attack)
  - شنود
    - افشاء پیام
    - تحلیل ترافیک
- حملات فعال (Active attack)
  - جعل هویت (Masquerade)
  - ارسال دوباره پیغام (Replay)
  - تغییر (Modification)
  - عدم ارائه سرویس (Denial of Service)

مکانیزمها

- حمله امنيتي(Security Attack) :

عملي كه امنيت اطلاعات سازمان را نقض مي كند

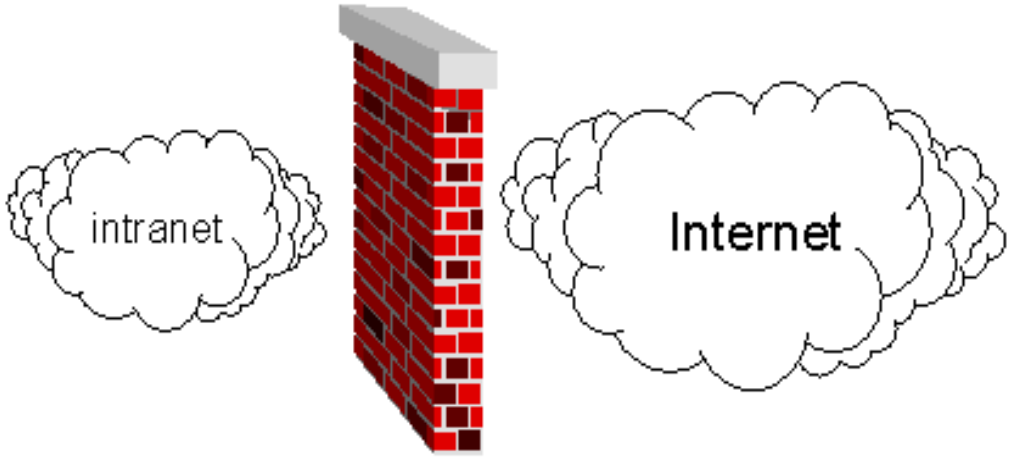
- مکانیزم امنيتي(Security Mechanism) :

روش درنظرگرفته شده براي تشخيص, جلوگيري و بازيابي از حملات

- سرویس امنيتي(Security Service)

سرويس هاي تضمين كننده امنيت با استفاده از مكانيزمهاي بالا

دو نوع حفاظت



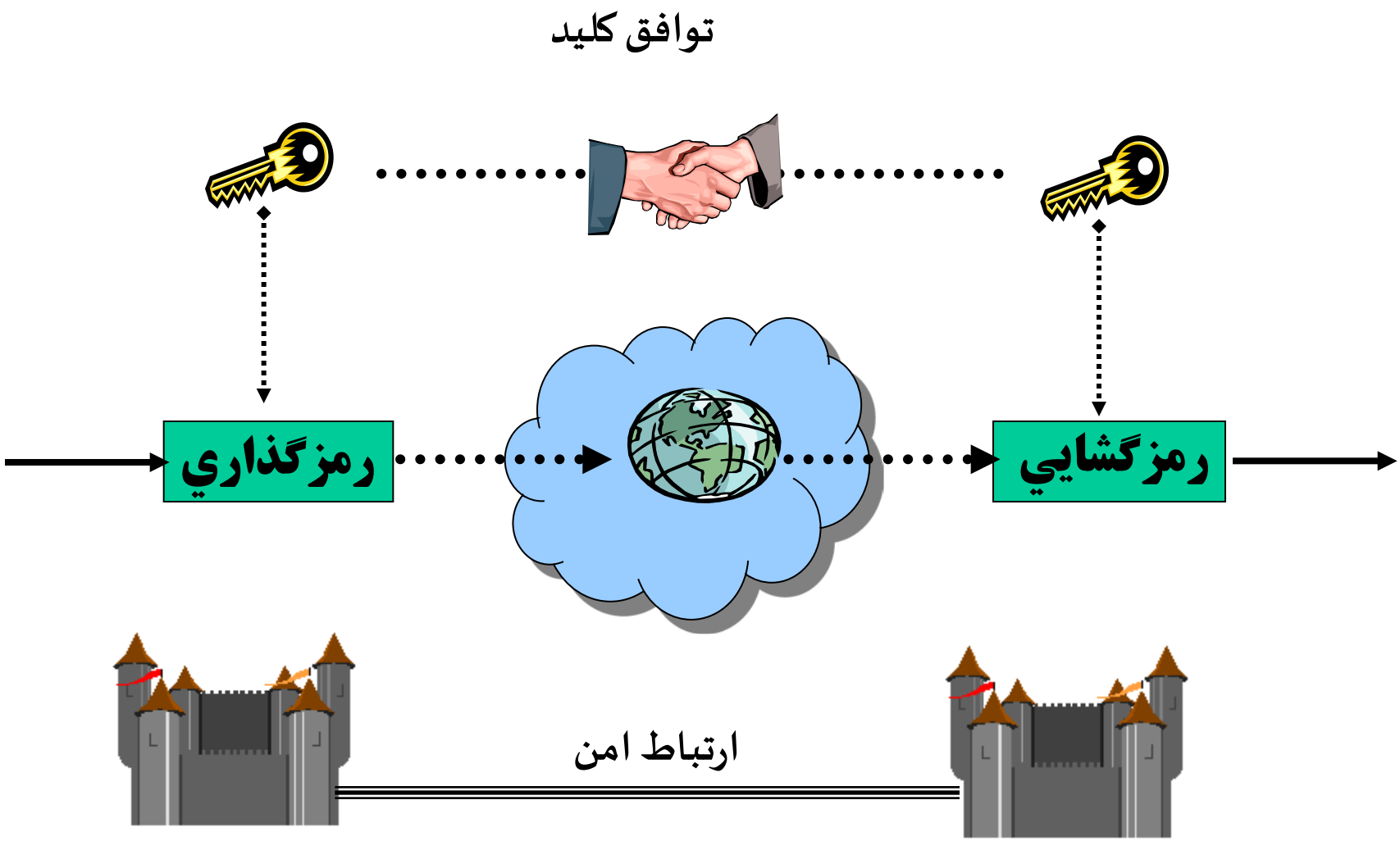
درسطح لایه شبکه(packet filtering)

تنها روي سرآيند پكتها كنترل دارد

درسطح لایه کاربرد(proxy server)

روي محتواي دادة پكتها هم كنترل دارد

ارتباط امن بين‌شبكه‌اي



امن‌سازي درلاية دسترسي به شبكه

لايه اتصال به شبكه

+ جلوگيري كامل ازتحليلهاي ترافيكي
- عدم دستيابي به سرويس انتها به انتها
- تغييرات مورد نيازبايد درهمة **node**هاي شبكه اعمال شود

پروتكل **PPTP** (نوعي **VPN** ايجاد ميكند)

امن‌سازي در لاية اينترنت

لايه شبكه

+ سرويسهاي امنيتي ازديد كاربردها شفاف هستند
- سرويسها وابسته به كاربر نيستند
- سرويسهاي انكارناپذيري مشكل پياده‌سازي مي‌شود

IP-sec

- **Tunneling mode**
- **Transport mode**

امن‌سازي در لاية حمل

لايه حمل

+ سرويسهاي امنيتي براي كاربردهاي مورد نظر قابل اعمالند
- بايد در كاربردها اصلاحات مورد نيازرا اعمال نمود

-SSH (Secure Shell)

-SSL (Secure Sockets Layer)

امن‌سازي در لاية كاربرد

لايه كاربرد

+ سرويسهاي امنيتي ازديد شبكه شفاف هستند
- سرويسهاي امنيتي براي هركاربرد بايستي بطور مجزا طراحي و پياده شوند

- سيستمهاي احراز اصالت و توزيع كليد(NetSP/SPX/SESAME و...)
- سيستمهاي پرداخت الكترونيكي (كارت اعتبار/پول ديجيتال/چك الكترونيكي)
- WWW امن (Secure HTTP)
- پست امن(SMIME/PGP/PEM)
- دسترسي ازدور امن

دربسياري ازاوقات امن‌سازي درچندين لايه ضرورت دارد

سرويسها

- حمله امنيتي(Security Attack) :

عملي كه امنيت اطلاعات سازمان را نقض مي كند

- مكانيزم امنيتي(Security Mechanism) :

روش درنظرگرفته شده براي تشخيص, جلوگيري و بازيابي از حملات

- سرويس امنيتي(Security Service)

سرويس هاي تضمين كننده امنيت با استفاده از مكانيزمهاي بالا

سرویس‌های امنیتی

- سرویس امنیتی : فرایندی ارائه شده توسط یک سیستم برای محافظت از منابع
- X.800 سرویس های امنیتی را به ۵ دسته و ۱٤ سرویس تقسیم بندی می کند
  - احراز اصالت
  - کنترل دسترسی
  - محرمانگی
  - صحت داده
  - انکار ناپذیری

سرویس‌های امنیتی

- احراز اصالت : اطمینان از ماهیت طرفین ارتباط
- Peer Entity Authentication
  - منظور از Peer دو سیستم متفاوت که یک پروتکل مشابه را پیاده سازی کرده اند
  - هویت طرفین را در شروع ارتباط و در طول آن تضمین می کند
- Data-Origin Authentication
  - تایید هویت منبع ارسال داده
  - در مقابل حمله تکرار آسیب پذیر است

سرویس‌های امنیتی

- کنترل دسترسی (Access Control): اعمال محدودیت در دسترسی به سیستم ها و منابع از طریق شبکه
- محرمانگی : اطمینان از افشای غیر مجاز
  - Connection Confidentiality : محافظت از تمامی اطلاعات کاربر در ارتباط
  - Connectionless Confidentiality : محافظت از تمامی اطلاعات کاربر در یک بلوک داده
  - Selective-Field Confidentiality : محافظت از برخی فیلدهای اطلاعاتی در طول یک ارتباط یا یک بلوک داده
  - Traffic-Flow Confidentiality : محافظت از اطلاعاتی که با مشاهده جریان اطلاعات بدست می آید

سرویس‌های امنیتی

- صحت داده : اطمینان از عدم تغییر غیر مجاز داده
  - Connection Integrity with Recovery : سرویس صحت بر روی تمامی اطلاعات کاربر و تشخیص تمامی عوامل برهم زننده صحت با تلاش برای بازیابی
  - Connection Integrity without Recovery : مشابه قبلی بدون عملیات بازیابی
  - Selective-Field Connection Integrity
  - Connectionless Integrity
  - Selective-Field Connectionless Integrity

سرویس‌های امنیتی

- انکار ناپذیری
  - Nonrepudiation, Origin
  - Nonrepudiation, Destination

لغت نامه

Encryption	رمزگذاری
Interception	شنود
Integrity	صحت
Dos: Denial Of Service	عدم ارائه سرویس
Non Repudiation	عدم‌انکار
Confidentiality	محرمانگی
Intrusion	نفوذ
Interoperable	هم ساز
Interruption	وقفه
MAC: Message authentication code	کد احراز هویت پیام
Accountability	جوابگویی
Access Control	کنترل دسترسی

Authentication	احراز اصالت
Vulnerability	آسیب‌پذیری
Fabrication	جعل اطلاعات
Integrity	جامعیت
Masquerade	جعل هویت(ایفای نقش)
Availability	دسترس‌پذیری
Tampering	دستکاری
Modification	دستکاری داده‌ها
Authorization	دستیابی مجاز
Circumvent	دور زدن
Audit	ثبت رویداد
Flaw, Breach	رخنه امنیتی