

امنیت شبکه

مدرس: ندا ادیب

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.

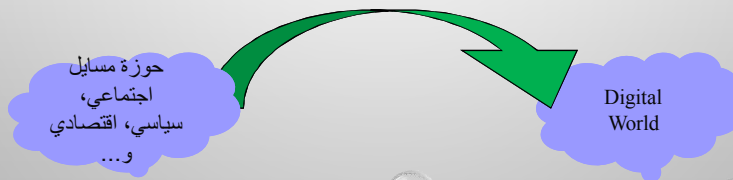
2- Cryptography And Network Security Principles And
Practice Fifth Edition By William Stallings, 2011.

ارزیابی

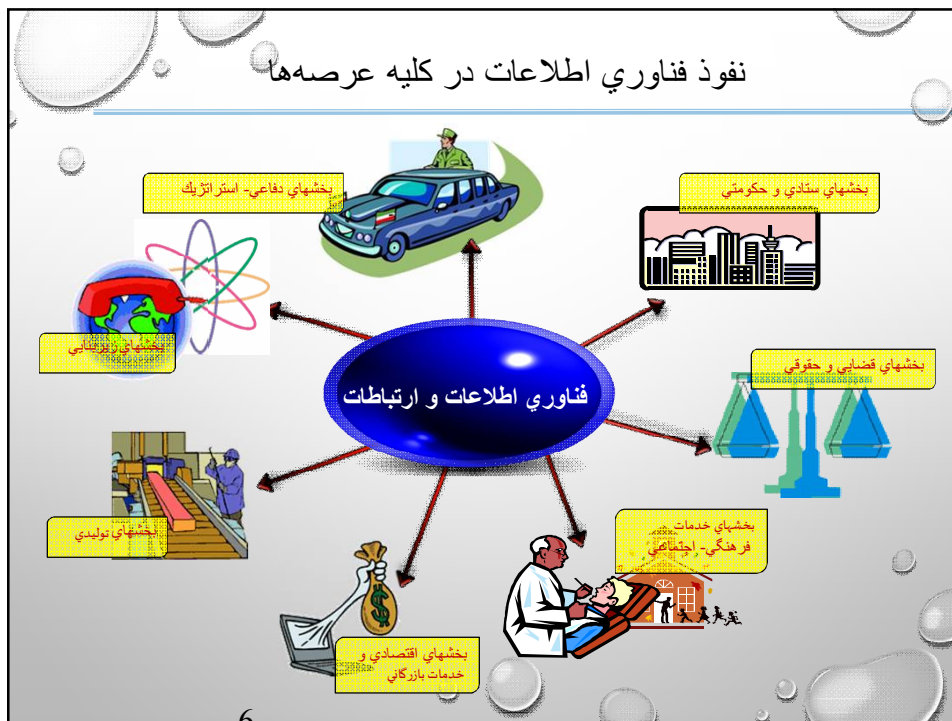
- میان ترم ۱۰٪
- پایان ترم ۶۰٪
- پروژه و سمینار ۳۰٪

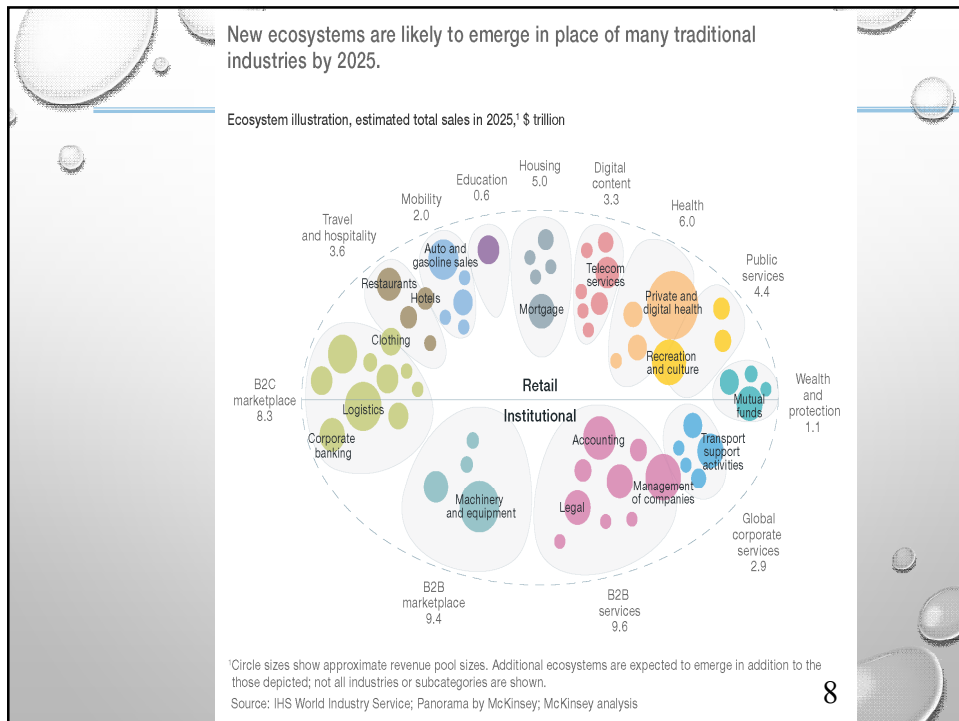
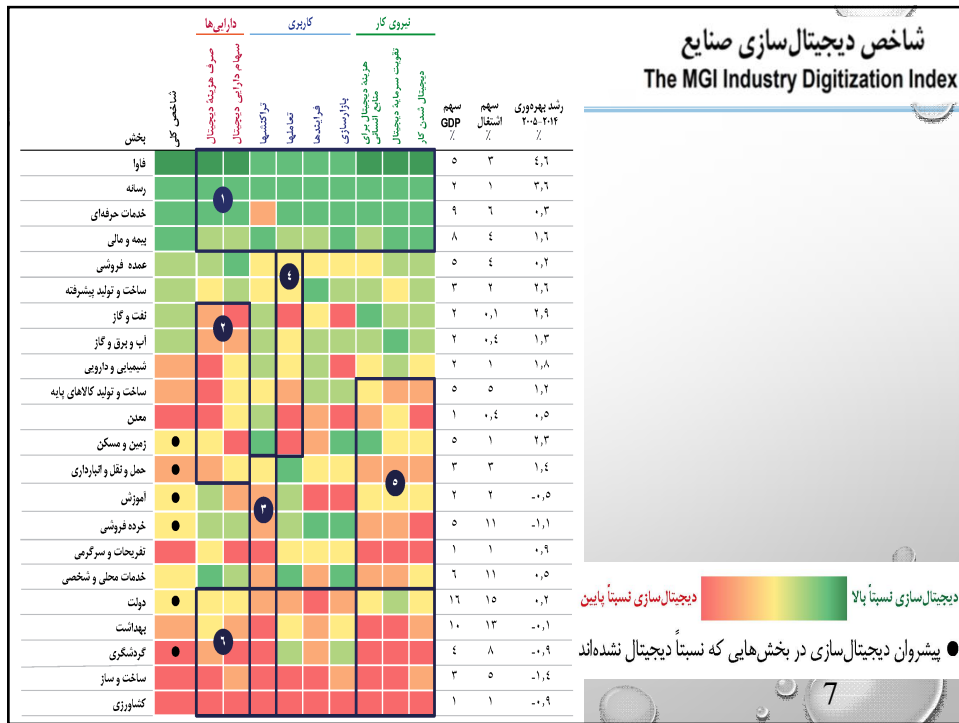
تغییرات اساسي حاصل از توسعه فناوری اطلاعات

- سریع‌تر شدن کامپیوترها
- رشد سریع شبکه
- دسترسی‌های راه دور
- تجارت الکترونیک
- و کلاً گرایش به سوی کنترل الکترونیکی هرچیز مهم و با ارزش



نفوذ فناوری اطلاعات در کلیه 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)

ماهیت جدید حملات

- پیچیدگی فراوان
- مکانیزه
- انجام عملیات از راه دور
- کانالهای ارتباطی متنوع
- انتشار روشهای موفق حمله

انگیزه‌های ایجاد نا امنی در فضای سایبر متنوع است

- انگیزه‌های سیاسی، نظامی (برتری استراتژیک)
- انگیزه‌های مالی و اقتصادی (سود بیشتر)
- انگیزه‌های علمی (پیشرفت علم)
- انگیزه‌های روانی (شهرت طلبی)
- انگیزه‌های حقوقی (بی اعتبار کردن سیستم)

تنوع دشمنان



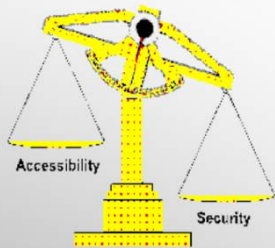
- جاسوس ها (تجاری، سیاسی، نظامی)
- تروریست‌ها
- مجرمین (عادی، سازمان یافته)
- هکرها
- نفوذی‌ها
- افراد نه چندان مطمئن

راه حل ساده امن سازی

حذف تمامی اتصالات و ارتباطات شبکه با سایرین

قراردادن سیستمها در اتاقهای محافظت شده

قراردادن یک محافظ در درب هر اتاق



حذف بسیاری از دستاوردهای شبکه ها

تعاریف

تعاریف

- مهندسی امنیت: مجموعه فعالیت‌هایی است که برای حصول و نگهداری سطوح مناسبی از
 - محرمانگی (Confidentiality)
 - صحت (Integrity)
 - قابلیت دسترسی (Availability)
 - جوابگویی (Accountability)
 - اصالت (Authenticity) و
 - قابلیت اطمینان (Reliability)به صورت سیستماتیک در یک سازمان انجام می‌شود.

تعاریف

- **محرمانگی:**
- اطلاعات برای افراد، موجودیت‌ها یا فرآیندهای غیرمجاز در دسترس قرار نگیرد یا افشا نشود.
- **صحت : صحت سیستم و صحت داده**
- صحت داده: داده‌ها به صورت غیر مجاز تغییر پیدا نکنند یا از بین نروند.
- صحت سیستم: فعالیت‌های مورد انتظار از سیستم بدون عیب و خالی از دستکاری‌های غیر مجاز (تعمدی یا تصادفی) در سیستم انجام شود.

تعاریف

• اصالت:

- هویت واقعی يك موجودیت با هویت مورد ادعا یکسان باشد.

• قابلیت دسترسی:

- در دسترس و قابل استفاده بودن منابع برای يك موجودیت احراز اصالت شده در هنگام نیاز.

• جوابگویی (حساب پذیری):

- فعالیت‌های موجودیت‌ها در سیستم اطلاعاتی قابل ردیابی و بررسی باشد.

• قابلیت اعتماد:

- سازگار بودن رفتارها و نتایج مورد انتظار، استمرار فعالیتها و سرویسهای مورد انتظار در طول زمان و در شرایط بحرانی.

تعاریف

- امنیت IT : حفاظت از سیستم های اطلاعاتی به منظور دستیابی به اهداف قابل اجرا در حفظ محرمانگی، صحت، قابلیت دسترسی، حساب پذیری، اصالت و قابلیت اعتماد.

• دارایی(asset):

- آنچه برای سازمان دارای ارزش است.

• تهدید(threat):

- پتانسیل وقوع يك رویداد ناخواسته که ممکن است به سیستم یا سازمان خسارت وارد کند.
- نقاط ضعف يك دارایی یا گروهی از دارایی‌ها که ممکن است توسط يك تهدید فعال شود.

• رخنه(flaw):

• صدمه:

- نتیجه يك رویداد ناخواسته

تعاریف

- حمله (Attack): تلاش عمدی برای رخنه در یک سیستم یا سوء استفاده از آن.
- Breach : نقض سیاست امنیتی یک سیستم
- نفوذ (Intrusion) : فرایند حمله و رخنه ناشی از آن
- آسیب پذیری (Vulnerability) : نقطه‌ای از سیستم که احتمال رخنه از آنجا وجود داشته باشد.

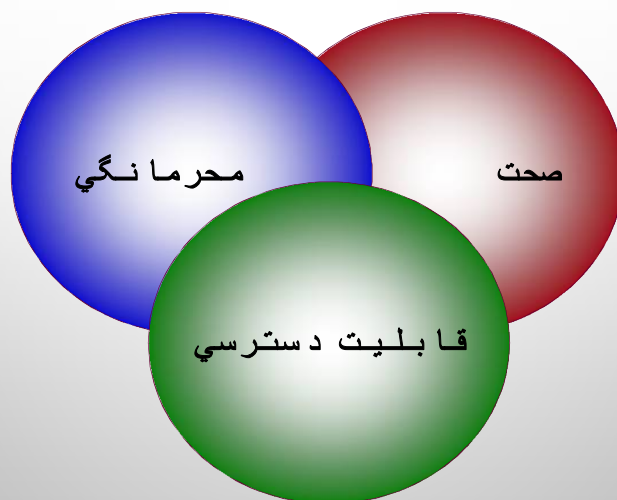
تعاریف

- روش دفاعی (safeguard): تجربه، روال، یا مکانیزم مورد استفاده جهت کاهش مخاطرات.
- کنترل‌های پایه (baseline control): مجموعه حداقلی از روشهای دفاعی برای تأمین امنیت سازمان
- مانده مخاطره (residual risk): مخاطرات باقی‌مانده پس از پیاده سازی روش های دفاعی

تعاریف

- مدیریت ریسک (risk management): فرآیند کامل شناسایی، کنترل و حذف یا کاهش رویدادهای نامطمئن که ممکن است به منابع سیستم IT خسارت وارد کند.
- خط مشی امنیتی (security policy): قوانین، دستورالعملها و تجربیاتی که بیان کننده چگونگی مدیریت، حفاظت و توزیع داراییها (شامل اطلاعات حساس) در داخل سازمان است.

مولفه های امنیت



مؤلفه‌های امنیت

■ محرمانگی (Confidentiality)

- عدم افشا محتوا
- عدم امکان تحلیل ترافیک
- عدم نشت اطلاعات
- عدم افشای نامها (Anonymity)

مؤلفه‌های امنیت

■ صحت (Integrity)

- اصالت داده‌ها (عدم حذف، اضافه و تکرار)
- اصالت مبدأ داده‌ها (Data Origin Authentication)
- اصالت و حضور موجودیتها (n-line Entity Authentication)
- انکارناپذیری (Non-Repudiation)

مؤلفه‌هاي امنيت

■ قابليت دسترسي (Availability)

● سهولت دسترس‌يهاي مجاز : حل تقابل ذاتي امنيت و تسهيل ارتباطات

● مقابله با حملات جلوگیری از ارائه سرویس (Denial of Service)

استاندارد X.800

استاندارد X.800

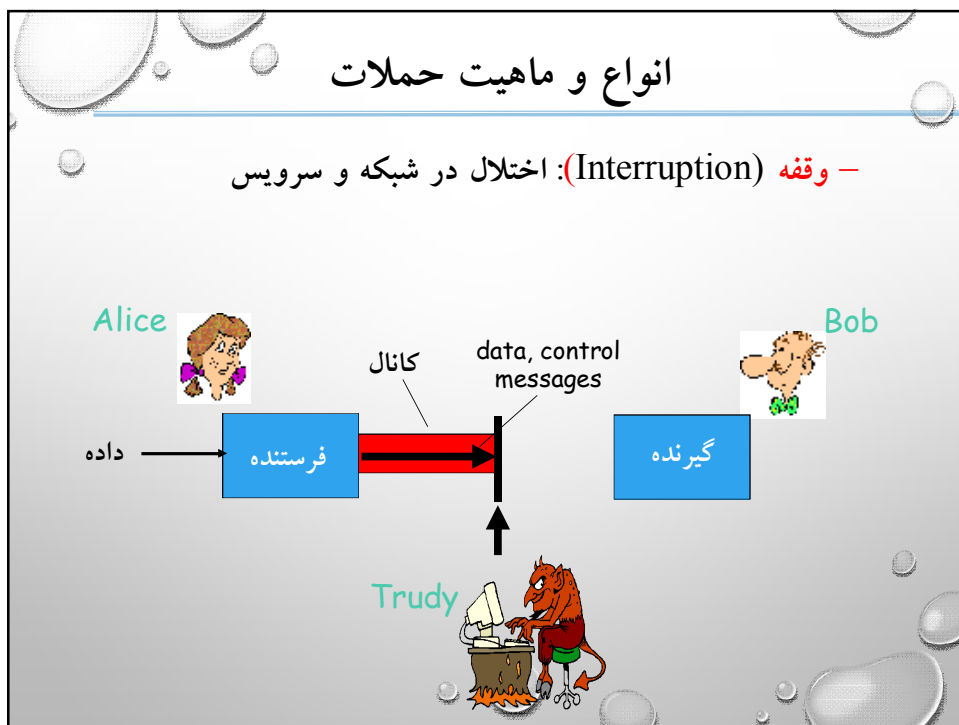
- فراهم کننده یک چارچوب سیستماتیک برای توصیف
 - حملات امنیتی
 - مکانیزم های امنیتی
 - سرویس های امنیتی

تعاریف در X.800

- حمله امنیتی (Security Attack) :
تلاش برای **رخنه** در یک سیستم
- مکانیزم امنیتی (Security Mechanism) :
روش در نظر گرفته شده برای **تشخیص**، **جلوگیری** و **بازیابی**
از حملات
- رمز نگاری، امضای دیجیتال ، پروتکل های احراز اصالت
و ...
- سرویس امنیتی (Security Service)
سرویس های تضمین کننده امنیت با استفاده از مکانیزمهای
بالا

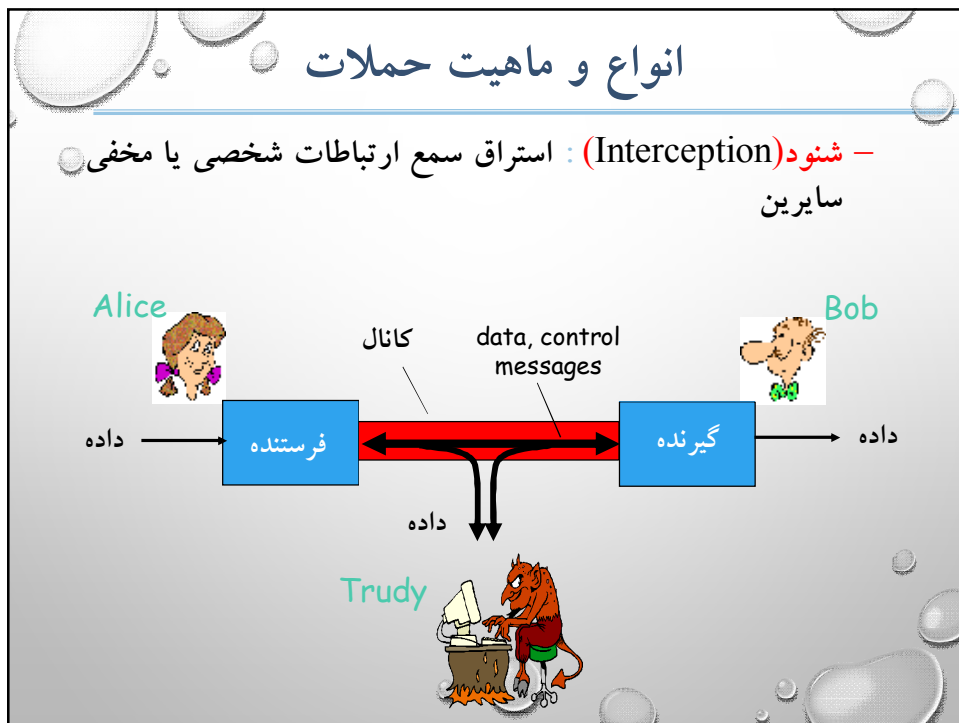
انواع و ماهیت حملات

– وقفه (Interruption): اختلال در شبکه و سرویس



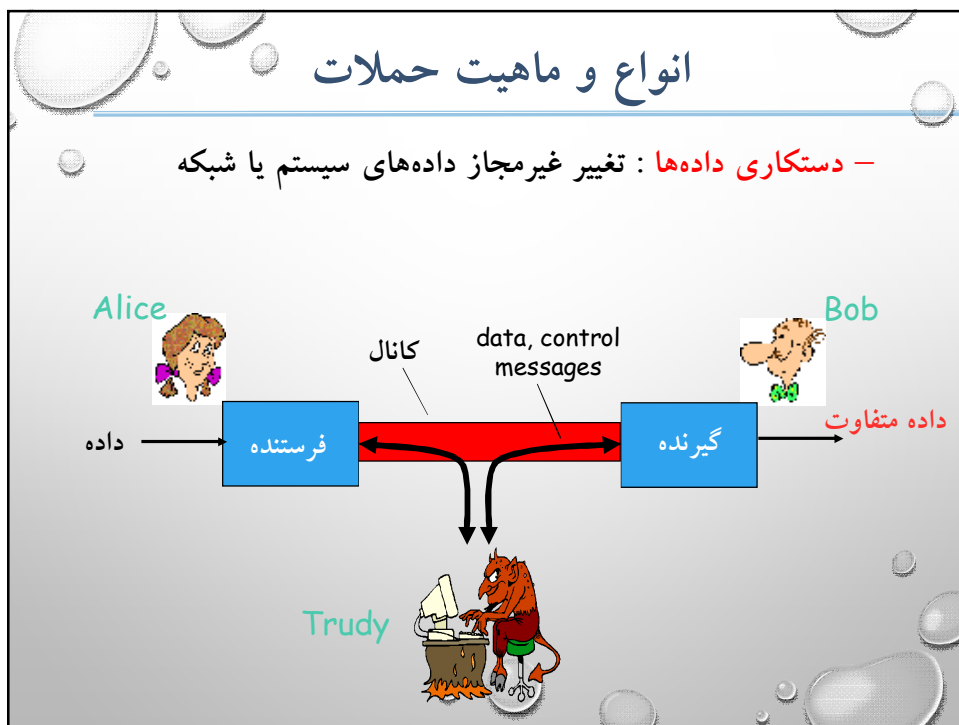
انواع و ماهیت حملات

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



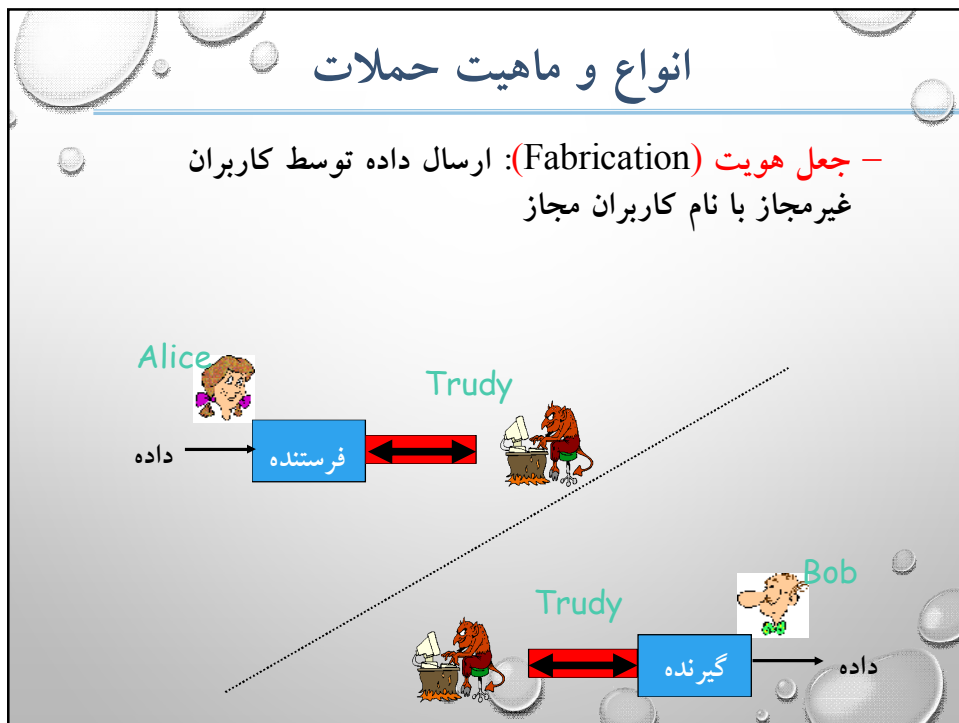
انواع و ماهیت حملات

– 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 غیر فعال (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 امنیتی (Security Attack) :

عملی که امنیت اطلاعات سازمان را نقض می کند

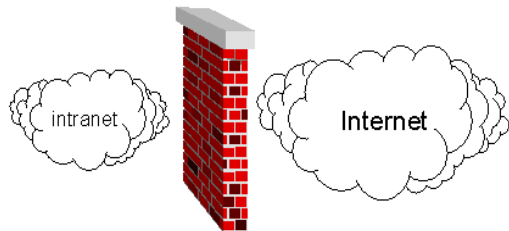
- مکانیزم امنیتی (Security Mechanism) :

روش در نظر گرفته شده برای تشخیص، جلوگیری و بازیابی از حملات

- سرویس امنیتی (Security Service)

سرویس های تضمین کننده امنیت با استفاده از مکانیزمهای بالا

دو نوع حفاظت



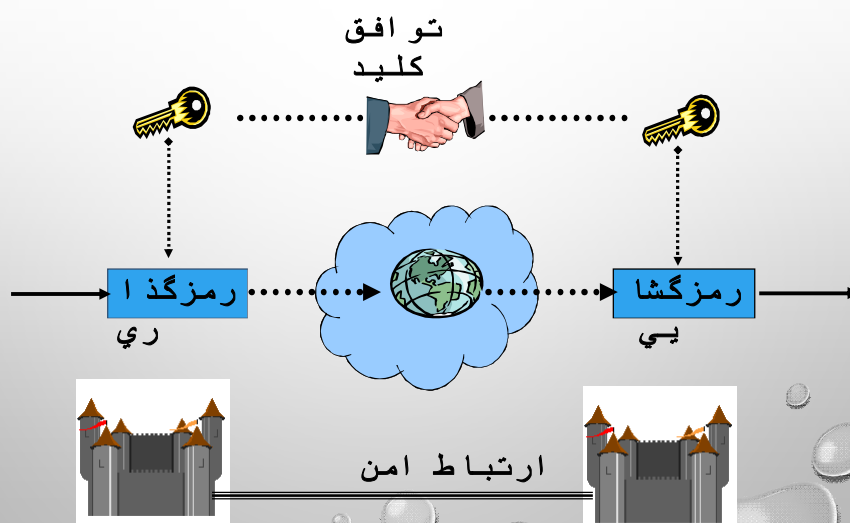
در سطح لایه شبکه (packet filtering)

تنها روی سرآیند پکتها کنترل دارد

در سطح لایه کاربرد (proxy server)

روی محتوای داده پکتها هم کنترل دارد

ارتباط امن بین شبکه ای



امن سازی در لایه دسترسی به شبکه

- + جلوگیری کامل از تحلیلهای ترافیکی
- عدم دستیابی به سرویس انتها به انتها
- تغییرات مورد نیاز باید در همه node های شبکه اعمال شود

پروتکل PPTP Point-to-Point Tunneling Protocol
(نوعی VPN ایجاد میکند)

امن سازی در لایه اینترنت

- + سرویسهای امنیتی از دید کاربردها شفاف هستند
- سرویسها وابسته به کاربر نیستند
- سرویسهای انکارناپذیری مشکل پیاده سازی می شود

Tunneling mode } IP-sec
Transport mode }

امن سازی در لایه حمل

+ سرویسهای امنیتی برای کاربردهای مورد نظر قابل اعمالند

لایه حمل

- باید در کاربردها اصلاحات مورد نیاز را اعمال نمود

-SSH (Secure Shell)

-SSL (Secure Sockets Layer)

امن سازی در لایه کاربرد

+ سرویسهای امنیتی از دید شبکه شفاف هستند

لایه کاربرد - سرویسهای امنیتی برای هر کاربرد بایستی بطور مجزا طراحی و پیاده شوند

- سیستمهای احراز اصالت و توزیع کلید (NetSP/SPX/SESAME و...)

- سیستمهای پرداخت الکترونیکی (کارت اعتبار/پول دیجیتال/چک الکترونیکی)

- WWW امن (Secure HTTP)

- پست امن (SMIME/PGP/PEM)

- دسترسی از دور امن

در بسیاری از اوقات امن سازی در چندین لایه ضرورت دارد

سرویسها

- حمله امنیتی (Security Attack) :
عملی که امنیت اطلاعات سازمان را نقض می کند
- مکانیزم امنیتی (Security Mechanism) :
روش در نظر گرفته شده برای تشخیص، جلوگیری و بازیابی از حملات
- سرویس امنیتی (Security Service)
سرویس های تضمین کننده امنیت با استفاده از مکانیزمهای بالا

سرویس های امنیتی

- سرویس امنیتی : فرایندی ارائه شده توسط یک سیستم برای محافظت از منابع
- X.800 سرویس های امنیتی را به ۵ دسته و ۱۴ 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

سرویس های 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

سرویس های امنیتی

• **انکار ناپذیری**

- Nonrepudiation, Origin
- Nonrepudiation, Destination

ISMS چیست؟

برگرفته از کلمات زیر و به معنای "سیستم مدیریت امنیت اطلاعات" است.

Information **S**ecurity **M**anagement **S**ystem



- ☐ مشخصه ای برای مدیریت امنیت اطلاعات
- ☐ دستورالعمل مدیریت امنیت اطلاعات
- ☐ پایه ای برای ارتباط قراردادی
- ☐ پایه گواهینامه شخص ثالث
- ☐ قابلیت کاربرد برای تمامی بخشهای صنعت
- ☐ تاکید بر پیش گیری

شرکتهای گواهی دهنده / اعتبار دهنده / مشاور

(IAF) نهاد اعتبار بخشی جهانی
(INTERNATIONAL ACCREDITATION FORUM)

دولتی

سازمان فناوری
اطلاعات

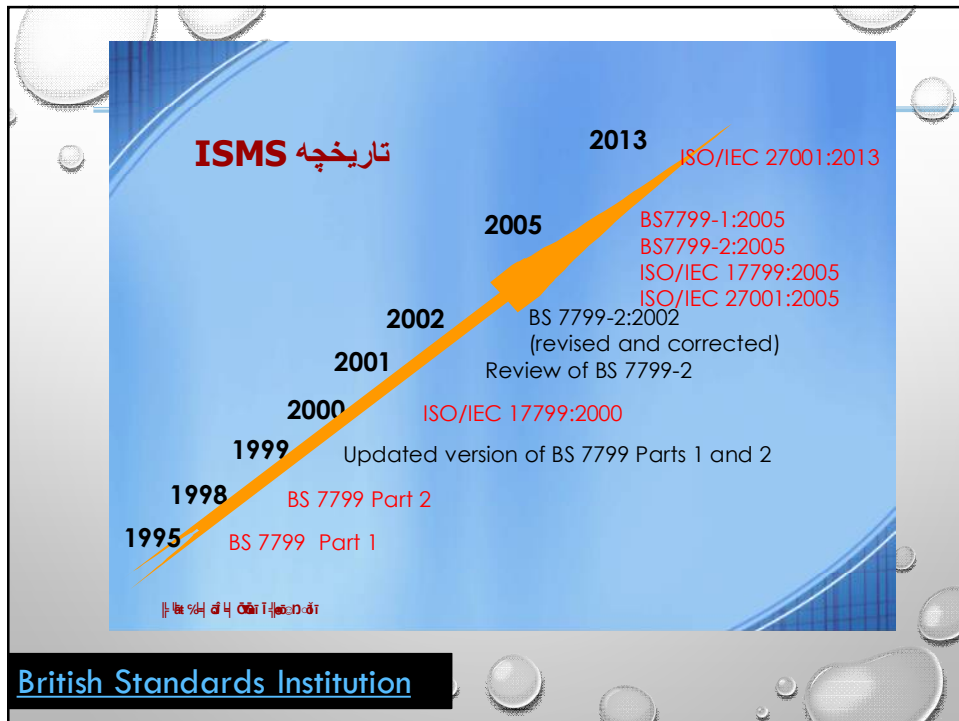
مؤسسه
استاندارد ایران

شرکتهای اعتبار دهنده
(UKAS-DAR-TGA-RAB-SCC)

شرکتهای گواهی دهنده
(TUVNORD-MIC-Aliance-SGS-IMQ-BVQI-DNV)-

خصوصی

مشاور
امن افزار، IMQ



خانواده ISO 27000	
• ISO/IEC 27000	Fundamental and Vocabulary
• ISO/IEC 27001	Information Security Management Requirements
• ISO/IEC 27002	Code of Practice
• ISO/IEC 27003	Implementation Guidance
• ISO/IEC 27004	Information security management measurements
• ISO/IEC 27005	Information security risk management
• ISO/IEC 27006	Requirements for certification bodies
• ISO/IEC 27007	Guidelines for Information security management systems auditing
• ISO/IEC 27011	Information security management guidelines for telecommunications
• ISO/IEC 27031	Business Continuity
• ISO/IEC 27032	Guidelines for cyber security
• ISO/IEC 27033	IT network security
• ISO/IEC 27034	Guidelines for application security
• ISO/IEC 27035	ISIRT Information Security Incident Response Team
• ISO/IEC 27799	Security Management in Health
• Up to ISO 27059	Reserved for future standards

مفاهیم و تشریح الزامات سیستم مدیریت امنیت اطلاعات

ISO/IEC 27001:2013

آشنایی با مفهوم استاندارد

ارائه تاریخچه ای از استاندارد های خانواده سیستم مدیریت امنیت اطلاعات

آشنایی با مفهوم بیانی سیستم مدیریت امنیت اطلاعات

تشریح دیدگاه فرآیندها و فرآیند

فرآیند مدیریت مخاطرات

آشنایی با تهیه طرح برطرف سازی مخاطرات (RTP)

نحوه تدوین بیانیه کار بست پذیری (SOA)

آشنایی با الزامات مستند سازی

تشریح اهداف کنترلی و کنترل ها

لغت نامه

Encryption	رمزگذاری
Interception	شنود
Integrity	صحت
Dos: Denial Of Service	عدم ارائه سرویس
Non Repudiation	عدم انکار
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	آسیب پذیری
Fabrication	جعل اطلاعات
Integrity	جامعیت
Masquerade	جعل هویت (ایفای نقش)
Availability	دسترسی پذیری
Tampering	دستکاری
Modification	دستکاری داده ها
Authorization	دستیابی مجاز
Circumvent	دور زدن
Audit	ثبت رویداد
Flaw, Breach	رخنه امنیتی

