



فصل اول: مفاهیم پایه‌ای امنیت

توسط: حمید رضا شهریاری

دانشگاه صنعتی امیرکبیر

دانشکده مهندسی کامپیوتر و فناوری اطلاعات

<http://ceit.aut.ac.ir/~shahriari>



The art of war teaches us not on the likelihood of the enemy's not coming, but on our own readiness to receive him; not on the chance of his not attacking, but rather on the fact that we have made our position unassailable.

--The art of War, Sun Tzu

امنیت چیست؟

□ امنیت به (طور غیر رسمی) عبارتست از حفاظت از آنچه برای ما ارزشمند است.

■ در برابر حملات عمدی

■ در برابر رخدادهای غیر عمدی



امنیت چیست؟

□ NIST* امنیت را به صورت زیر تعریف نموده است:

■ حفاظت از سیستم های اطلاعاتی به منظور حفظ صحت (integrity)، دسترس پذیری (availability) و محرمانگی (confidentiality) مربوط به منابع سیستم. (شامل سخت افزار، نرم افزار، firmware، داده ها و اطلاعات و ارتباطات)

*National Institute of Standards and Technology

امنیت اطلاعات: گذشته و حال

امنیت اطلاعات در دنیای نوین

- نگهداری اطلاعات در کامپیوترها
- برقراری ارتباط شبکه ای بین کامپیوترها
- برقراری امنیت در کامپیوترها و شبکه ها

امنیت اطلاعات سنتی

- نگهداری اطلاعات در قفسه های قفل دار
- نگهداری قفسه ها در مکانهای امن
- استفاده از نگهبان
- استفاده از سیستمهای الکترونیکی نظارت
- به طور کلی: روشهای فیزیکی و مدیریتی

نیازهای امنیتی

□ بنابراین :

در گذشته، امنیت با حضور فیزیکی و نظارتی تامین
میشد

ولی

امروزه از ابزارهای خودکار و مکانیسم های هوشمند
برای حفاظت از داده ها استفاده می شود

نیازهای امنیتی : گذشته و حال

- تعداد حملات علیه امنیت اطلاعات به طور قابل ملاحظه‌ای افزایش یافته است.
- امروزه تدارک حمله با در اختیار بودن ابزارهای فراوان در دسترس به دانش زیادی احتیاج ندارد (بر خلاف گذشته)

برخی چالشها

- آسیب پذیریهای نرم افزارها
- روشهای روانشناختی و مهندسی اجتماعی بسیار موثر هستند.
- منافع مالی حاصل از نفوذ به سیستمها

۱. بازارهای خرید و فروش آسیب پذیری

۲. بازارهای خرید و فروش سیستمهای تحت کنترل

۳. روشهای متعدد سوءاستفاده از سیستمهای تحت کنترل

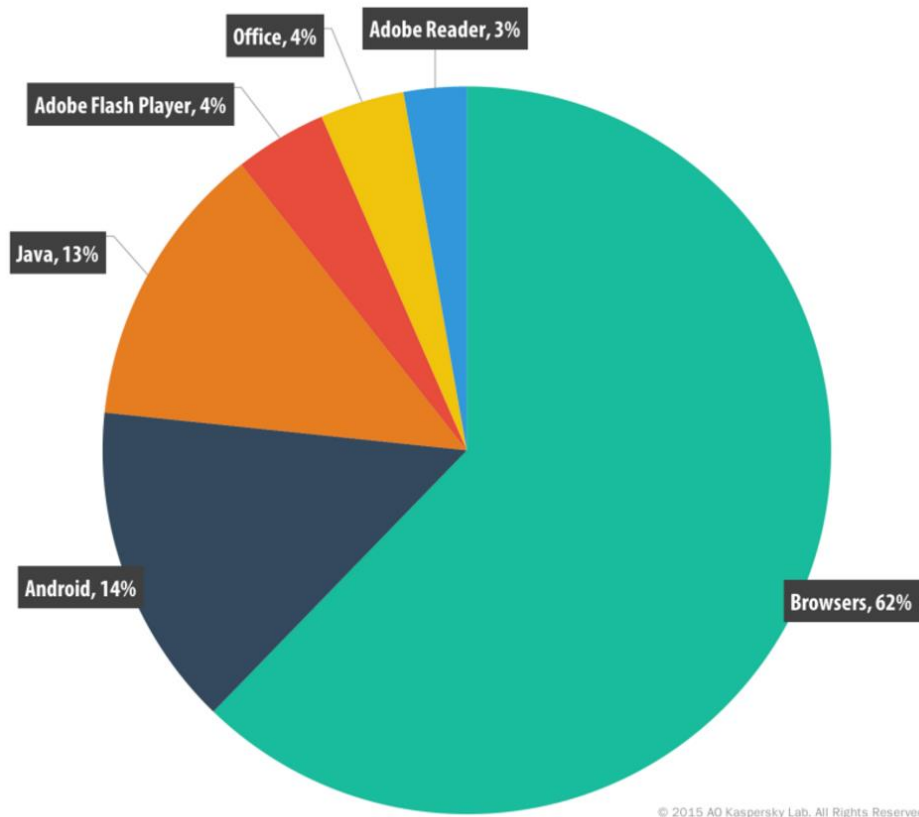
Lots of vulnerability disclosures (2015)

	Product Name	Vendor Name	Product Type	Number of Vulnerabilities
1	Mac Os X	Apple	OS	385
2	Iphone Os	Apple	OS	376
3	Flash Player	Adobe	Application	313
4	Air Sdk	Adobe	Application	246
5	AIR	Adobe	Application	246
6	Air Sdk & Compiler	Adobe	Application	246
7	Internet Explorer	Microsoft	Application	231
8	Chrome	Google	Application	187
9	Firefox	Mozilla	Application	178
10	Windows Server 2012	Microsoft	OS	155
11	Ubuntu Linux	Canonical	OS	152
12	Windows 8.1	Microsoft	OS	151

source: www.cvedetails.com/top-50-products.php?year=2015

<http://ceit.aut.acir/~shahriari>

Vulnerable applications being exploited



Source: Kaspersky Security Bulletin 2015



مقدمه

برخی حملات نمونه

چرا تسخیر سیستمها؟

۱- سرقت آدرس IP و پهنای باند

- هدف مهاجم: مشابه یک کاربر تصادفی اینترنت به نظر برسد.
- استفاده از IP ماشین آلوده یا تلفن برای:

- **Spam** (e.g. the storm botnet)

Spamalytics: 1:12M pharma spams leads to purchase
1:260K greeting card spams leads to infection

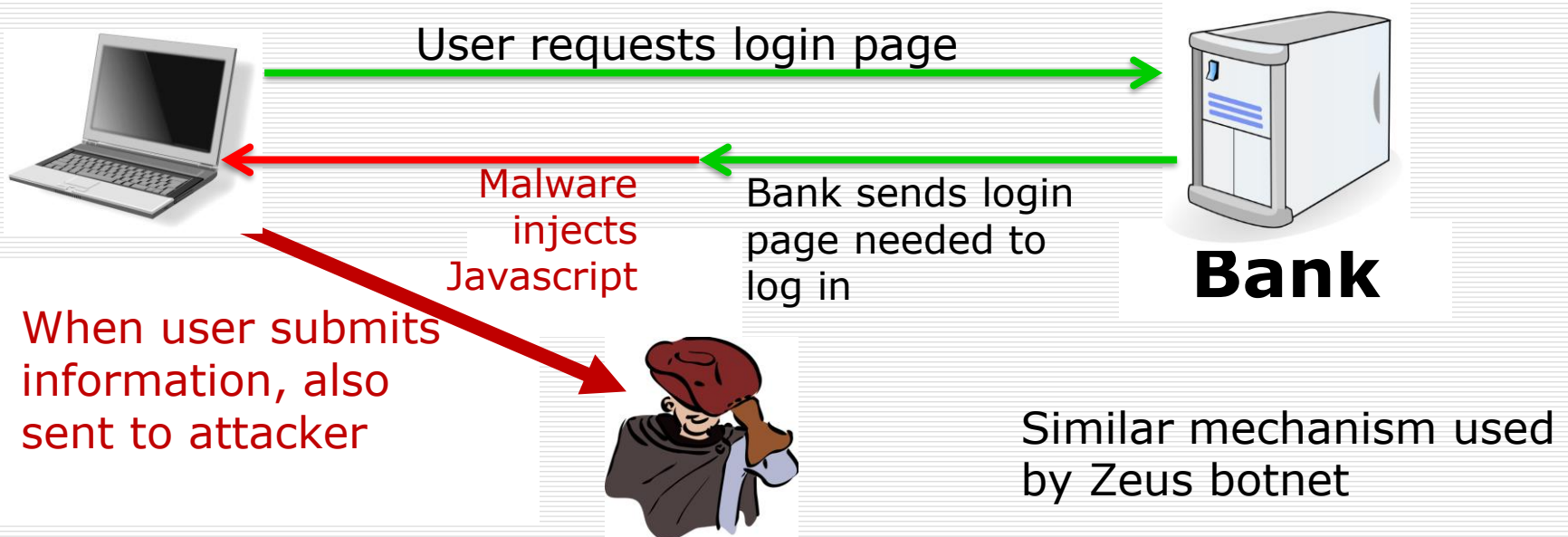
- **Denial of Service:** Services: 1 hour (20\$), 24 hours (100\$)
- **Click fraud** (e.g. Clickbot.a)

چرا تسخیر سیستمها؟

۲- سرقت اطلاعات مهم کاربر

استفاده از keylogger برای سرقت گذرواژه‌ها

مانند SilentBanker (و بسیاری نمونه های مشابه)



Man-in-the-Browser (MITB)

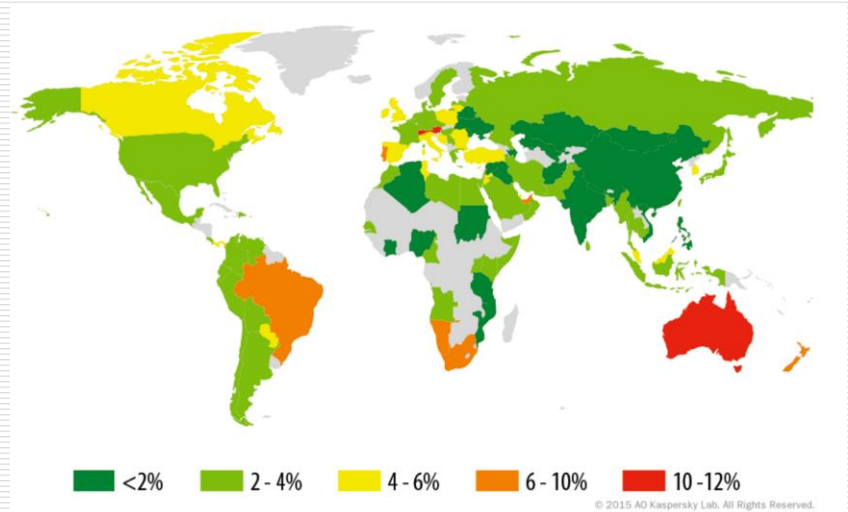
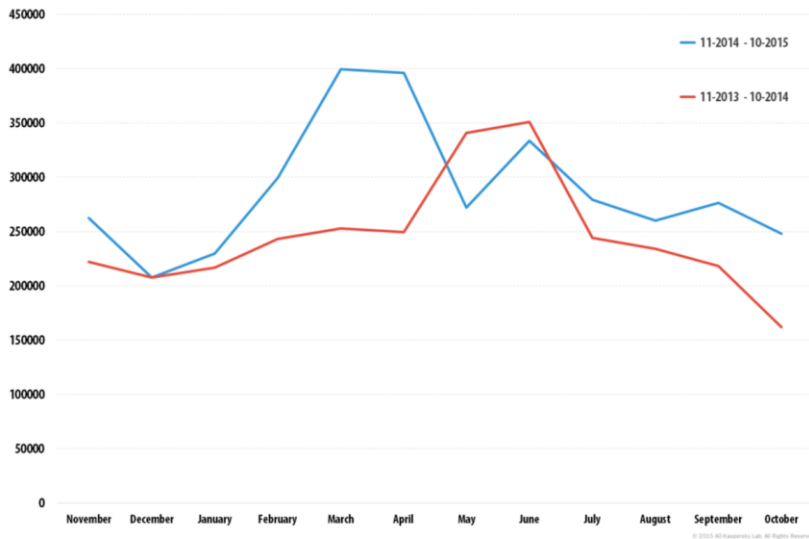
وجود تعداد زیادی بدافزار مالی

1	Trojan-Downloader.Win32.Upatre
2	Trojan-Spy.Win32.Zbot
3	Trojan-Banker.Win32.ChePro
4	Trojan-Banker.Win32.Shiotob
5	Trojan-Banker.Win32.Banbra
6	Trojan-Banker.Win32.Caphaw
7	Trojan-Banker.AndroidOS.Faketoken
8	Trojan-Banker.AndroidOS.Marcher
9	Trojan-Banker.Win32.Tinba
10	Trojan-Banker.JS.Agent

- size: 3.5 KB
- spread via email attachments
- also found on home routers

Source: Kaspersky Security Bulletin 2015

Users attacked: stats



≈ 300,000 users worldwide

A worldwide problem

Source: Kaspersky Security Bulletin 2015

چرا تسخیر سیستمها؟

۳- باج گیر افزارها Ransomware

1	Trojan-Ransom.HTML.Agent
2	Trojan-Ransom.JS.Blocker
3	Trojan-Ransom.JS.InstallExtension
4	Trojan-Ransom.NSIS.Onion
5	Trojan-Ransom.Win32.Cryakl
6	Trojan-Ransom.Win32.Cryptodef
7	Trojan-Ransom.Win32.Snocry
8	Trojan-Ransom.BAT.Scatter
9	Trojan-Ransom.Win32.Crypmod
10	Trojan-Ransom.Win32.Shade

CryptoWall (2014-)

- targets Windows
- spread by spam emails

≈ 200,000 machines in 2015

A worldwide problem.

چرا تسخیر سیستمها؟

۴- انتشار به سیستمهای ایزوله شده

مثال: Stuxnet

Windows infection ⇒

Siemens PCS 7 SCADA control software on Windows ⇒

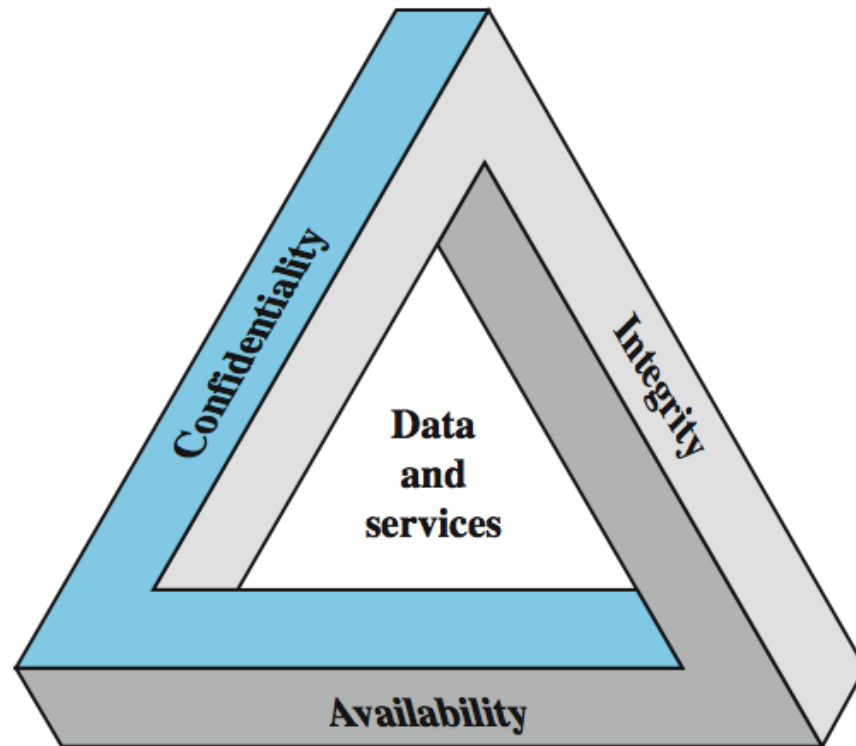
Siemens device controller on isolated network



مقدمه

نیازمندی‌های امنیت

ابعاد امنیت



ابعاد امنیت

□ **محرمانگی (Confidentiality):** عدم افشای داده‌ها و

اطلاعات به افراد غیر مجاز

□ **صحت (Integrity):** عدم تغییر غیرمجاز

■ Origin Integrity یا اصالت داده

■ Data Integrity یا صحت داده

□ **دسترسی‌پذیری (Availability):** منابع در دسترس افراد به

ویژه افراد مجاز باشند.

ابعاد امنیت

□ عدم انکار (Non-Repudiation): جلوگیری از انکار انجام کار توسط هر یک از طرفین ارتباط یا کاربران

■ مثال:

□ عدم انکار ارسال دستور خرید سهام

□ عدم انکار دریافت دستور خرید سهام

□ عدم انکار ارسال ایمیل

□ نیازمندی عدم انکار تا حدی توسط ویژگی صحت قابل برآورده کردن است.

مثال‌هایی از نیازمندی‌های امنیتی

- محرمانگی: محرمانه بودن نمرات دانشجویان
- صحت: صحت اطلاعات بیماران و عدم خدشه
- دسترس‌پذیری: در دسترس بودن سایت بانکداری اینترنتی

دشواری برقراری امنیت

- ❑ تعامل پروتکلها پیچیدگی را افزایش داده و امنیت را تهدید می کند.
- ❑ امنیت معمولاً قربانی افزایش کارایی و مقیاس پذیری می شود.
- ❑ امنیت بالا هزینه بر است.
- ❑ کاربران عادی امنیت را به عنوان مانع در برابر انجام شدن کارها تلقی می کنند و از خط مشی های امنیتی پیروی نمی کنند.

دشواری برقراری امنیت

- ❑ اطلاعات و نرم افزارهای **دور زدن** امنیت به طور گسترده در اختیار می باشند.
- ❑ برخی دور زدن امنیت را به عنوان یک مبارزه در نظر می گیرند و از انجام آن لذت می برند.
- ❑ ملاحظات امنیتی در هنگام **طراحی های اولیه** سیستم ها و شبکه ها در نظر گرفته نشده است.

چالش‌های برقراری امنیت

۱. ساده نیست.
۲. حملات بالقوه باید در نظر گرفته شود.
۳. فرایندها حالت مقابله‌ای دارند و با معلوم بودن تهدید مفهوم پیدا می‌کنند.
۴. شامل الگوریتم‌ها و اطلاعات محرمانه می‌شود.
۵. باید در رابطه با محل قرار دادن مکانیزم‌ها تصمیم‌گیری کرد.
۶. نبردی دائم میان مهاجم و مدیر سیستم وجود دارد.
۷. تا زمانی که سیستم دچار نقص امنیتی نشود، به عنوان یک مزیت محسوب نمی‌شود.
۸. نیاز به کنترل منظم دارد.
۹. اغلب پس از طراحی اعمال می‌شود.
۱۰. مانعی برای استفاده از سیستم محسوب می‌شود.

معماری امنیتی OSI

ITU-T X.800 ☐

روشی سیستماتیک جهت تعریف و فراهم نمودن نیازمندی‌های امنیتی مشخص می‌کند. (مناسب برای مدیران) ☐

کاربرد مدل برای این درس: ☐

یک دید کلی از مفاهیمی که مورد بررسی قرار خواهند گرفت را به دست می‌آوریم. ■

جنبه های امنیت

□ سه جنبه امنیت که OSI روی آن متمرکز است عبارتند از:

- **حمله امنیتی** : تلاش برای نقض امنیت
- **مکانیزم امنیتی یا کنترل امنیتی** : روش، ابزار یا فرآیندی برای مقابله با حملات امنیتی (با تشخیص، جلوگیری یا بازسازی)
- **سرویس امنیتی** : سرویس‌های فراهم کننده امنیت با استفاده از مکانیزم‌های امنیتی

□ واژگان مهم:

- **تهدید (Threat)**: یک عامل بالقوه برای نقض امنیت

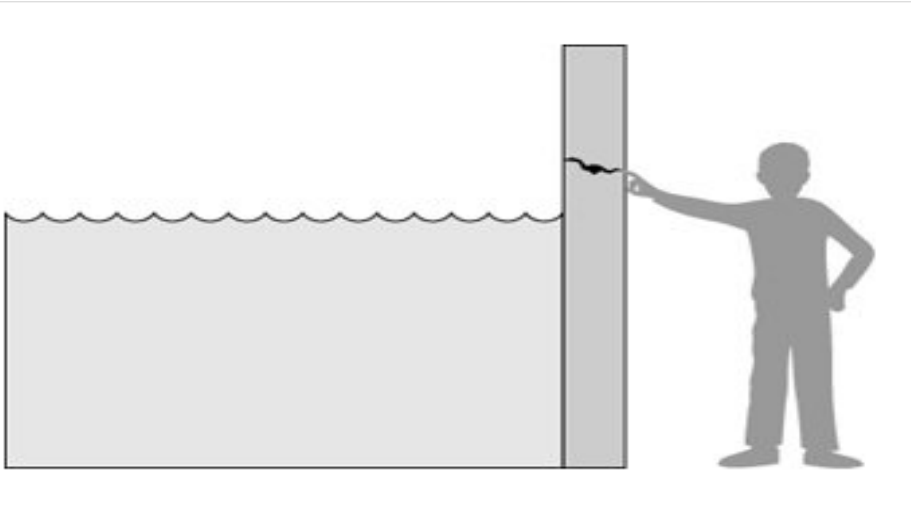
آسیب پذیری و تهدید

□ تفاوت میان تهدید و آسیب

پذیری:

■ آب موجود پشت سد به علت امکان شکستن سد، یک **تهدید** برای شخص است.

■ ترک موجود در سد به عنوان یک **آسیب پذیری** شناخته می شود.



مکانیزم امنیتی

□ انواع مکانیزمهای امنیتی (کنترل‌های امنیتی)

- بازدارنده یا Prevention: از نقض امنیت جلوگیری می‌کند.
- تشخیص یا Detection: در صورت وقوع حمله یا نقض امنیت آن را تشخیص و اعلام می‌کند.
- پاسخ یا Response: پاسخگویی به حمله برای جلوگیری از گسترش یا اقدام متقابل
- بازیابی یا Recovery: پس از تشخیص نقض امنیت، سیستم را به حالت درست قبل از حمله برمی‌گردانند.

انواع حملات

انواع حملات از نظر تاثیر در منابع سیستم یا ارتباط:
□ حملات غیرفعال (Passive attack):

- حملاتی که در آن اطلاعاتی از سیستم جمع آوری می شود. مثال:
 - انواع حملات شنود و افشای پیام (release of message content)
 - تحلیل ترافیک

□ حملات فعال (Active attack)

- حملاتی که در آن سعی می شود منابع یا رفتار سیستم تغییر کند. مثال:
 - جعل هویت (Masquerade)
 - ارسال دوباره پیغام (Replay)
 - تغییر (Modification of message)
 - منع سرویس (Denial of Service – DoS)

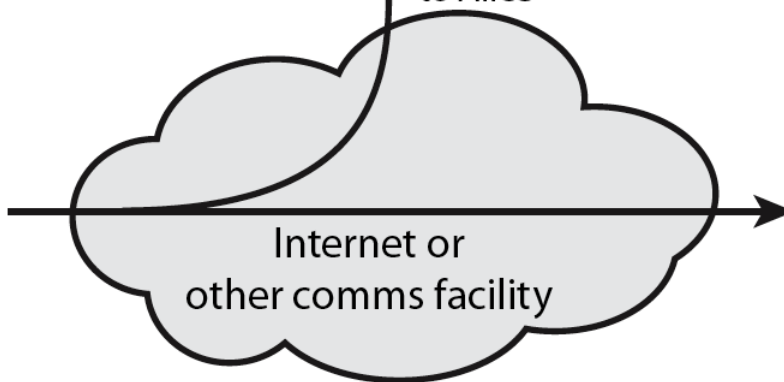
حملات غير فعال



DARTH
↑ read contents of
message from Bob
to Alice

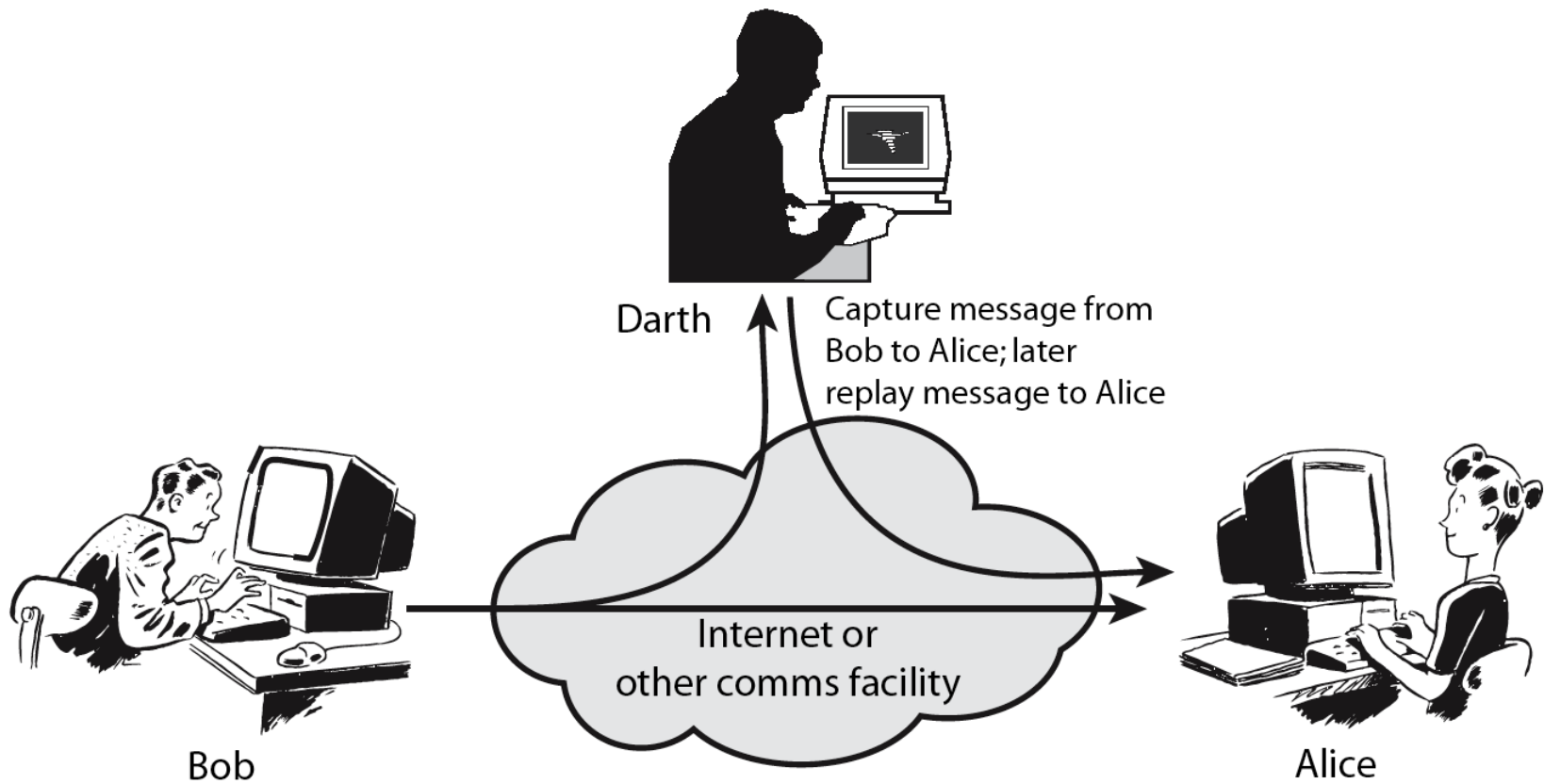


Bob



Alice

حملات فعال





انواع حملات فعال

- هنگامی که یک کاربر به جای یک کاربر دیگر خود را جا می زند.
- معمولاً شامل یک یا دو نوع از حملات فعال می شود.

Masquerade جعل

- شنود داده ها و ارسال مجدد آنها به منظور کسب نتایج غیرمجاز

ارسال مجدد Replay

- تغییر در بخشی از پیام مجاز، یا ترتیب پیامها یا زمان ارسال (به منظور کسب نتایج غیرمجاز)

دستکاری

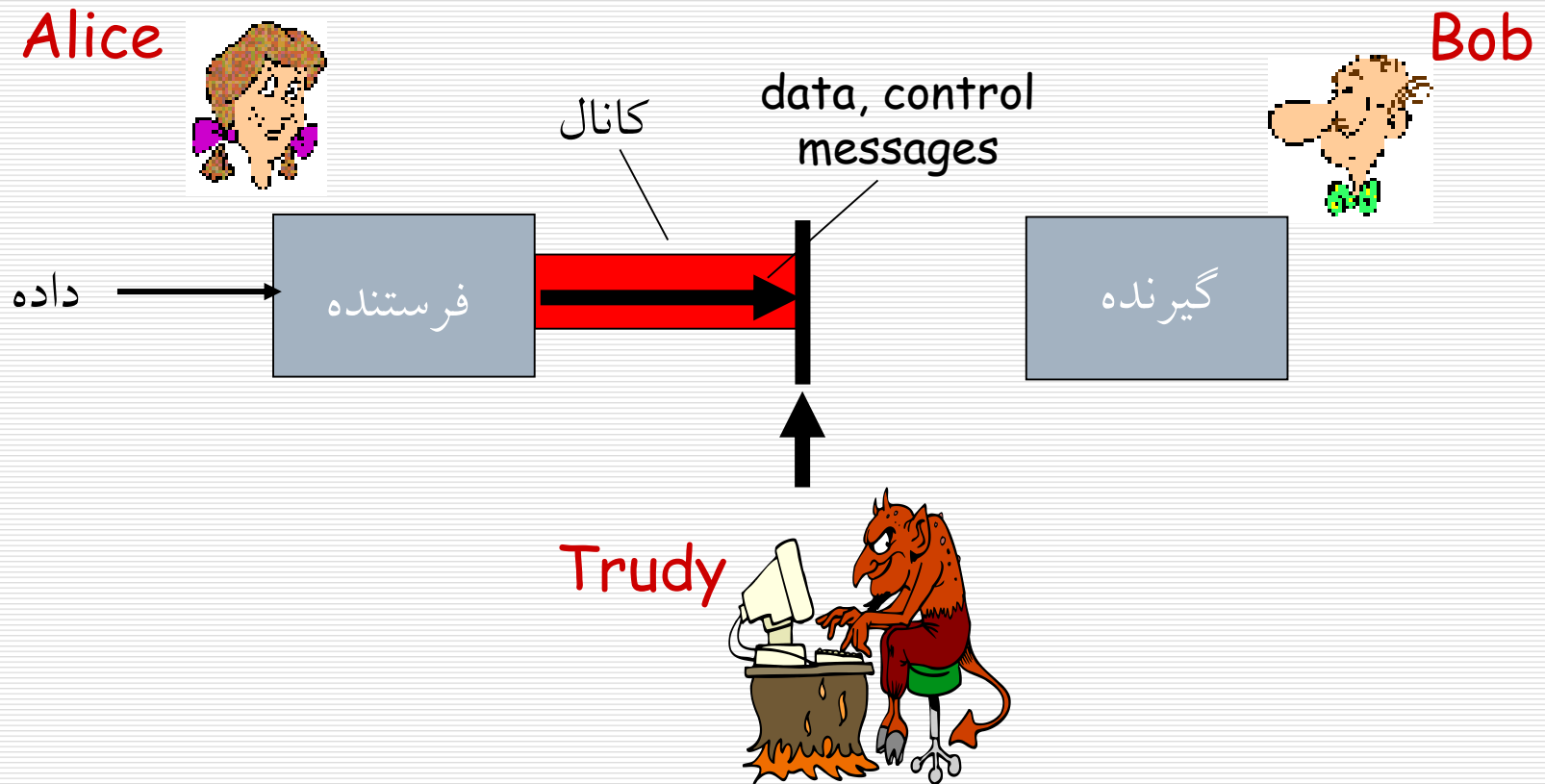
Modification of messages

- جلوگیری یا منع از استفاده از یک سرویس یا امکانات ارتباطی

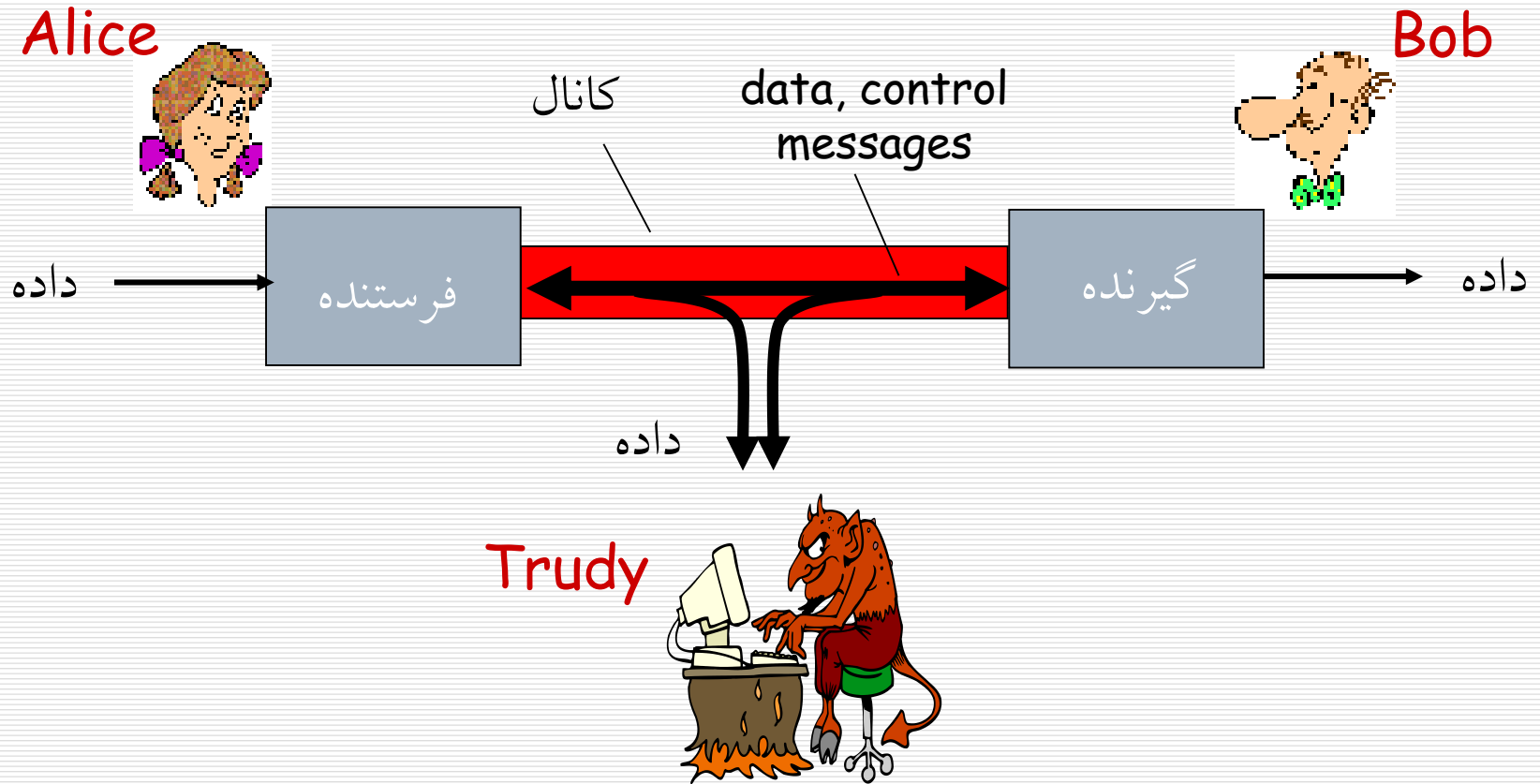
منع خدمت

Denial of service

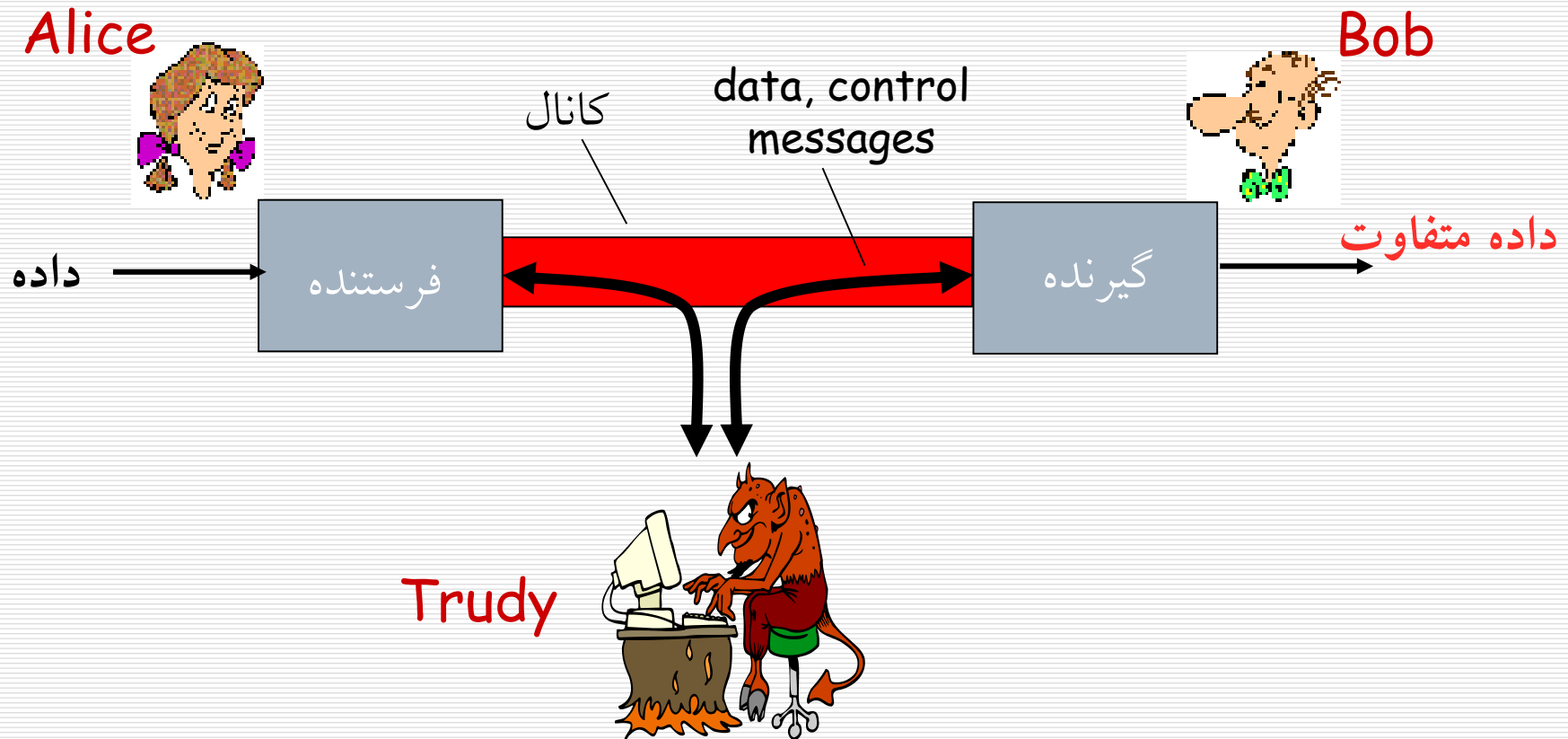
حمله امنیتی: وقفه



حمله امنیتی: شنود



حمله امنیتی: دستکاری



سرویس امنیتی

- هدف: مقابله با حملات امنیتی
- افزایش امنیت سیستم‌های پردازش اطلاعات و تبادل اطلاعات سازمانها
- استفاده از یک یا چند مکانیزم امنیتی
- معمولاً اعمالی که در اسناد کاغذی مد نظر است در اینجا نیز تکرار می شود.
- کارهایی نظیر قرار دادن امضا و تاریخ، حفاظت در برابر افشا یا خرابی، ثبت شدن و امثال آنها

سرویس امنیتی

□ تعریف سرویس امنیتی:

■ X.800

□ سرویسی که توسط یک پروتکل ارتباطی فراهم شده و امنیت کافی برای سیستم‌ها و یا انتقال داده‌ها فراهم می‌آورد.

■ RFC 2828

□ یک سرویس ارتباطی یا پردازشی که توسط یک سیستم تعیین می‌شود تا نوع خاصی از حفاظت منابع سیستم را فراهم کند.

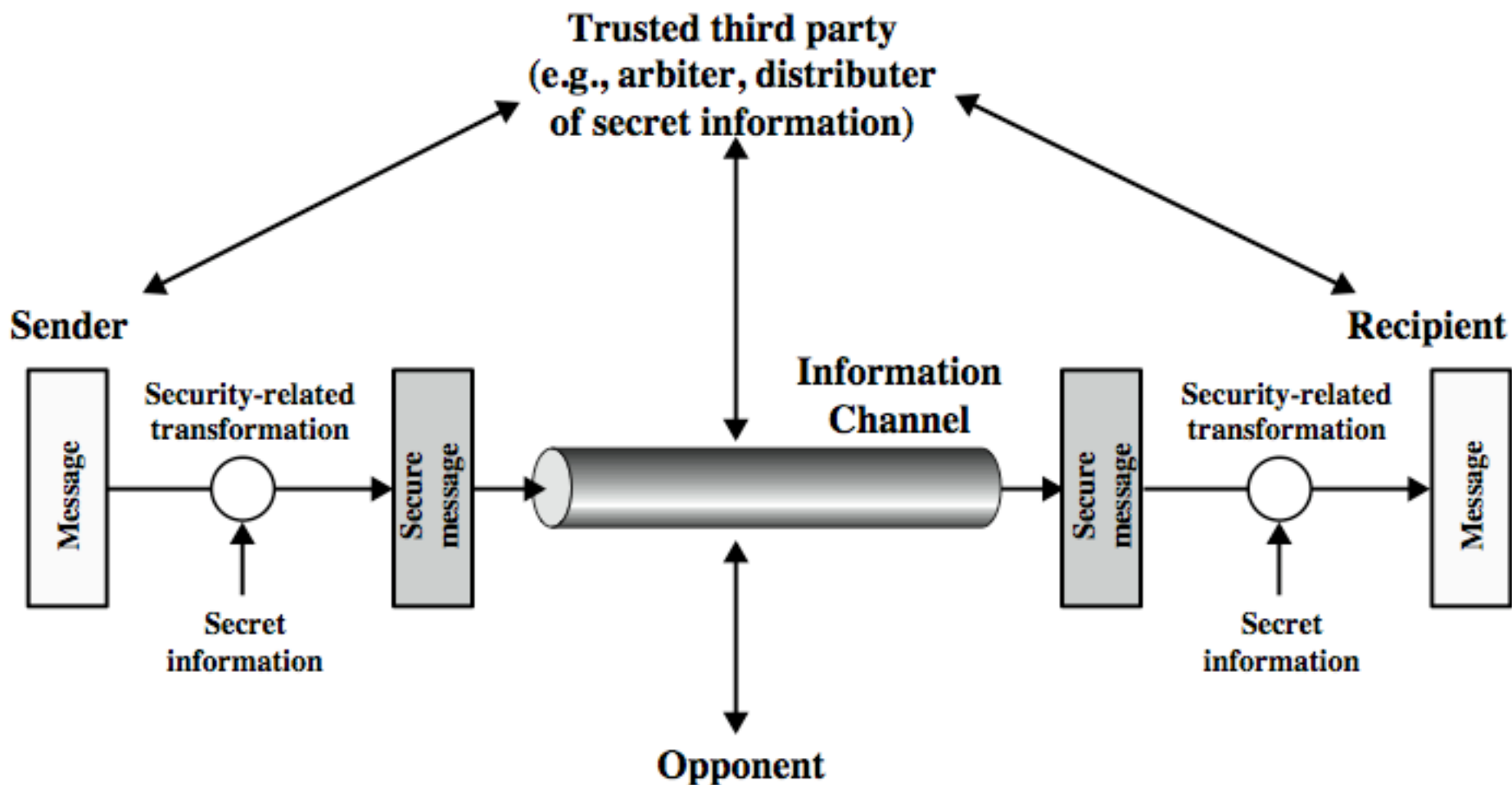
سرویس‌های امنیتی (X.800)

- تصدیق اصالت: اطمینان از اینکه طرف ارتباط همان است که ادعا می‌کند.
■ تصدیق اصالت داده و طرف ارتباط
- کنترل دسترسی: جلوگیری از دسترسی غیرمجاز به منابع
- محرمانگی داده: جلوگیری از افشای غیرمجاز داده‌ها
- صحت داده: حصول اطمینان از این که داده‌ها همان گونه که توسط یک موجودیت مجاز ارسال شده، دریافت شده‌اند.
- عدم انکار (Non-Repudiation): جلوگیری از انکار توسط هر یک از طرفین ارتباط
- دسترس پذیری: در دسترس بودن منابع

مکانیزم امنیتی

- وسیله‌ای برای تشخیص یا جلوگیری از حمله و یا بازسازی سیستم پس از وقوع حمله
- همه سرویس‌های امنیتی توسط یک مکانیزم واحد فراهم نمی‌شوند. هرچند تکنیک‌های “رمزنگاری” در اکثر مکانیزم‌های امنیتی مورد استفاده قرار می‌گیرند.
- به همین دلیل این موضوع مورد توجه ما نیز قرار خواهد گرفت.

مدل امنیت شبکه

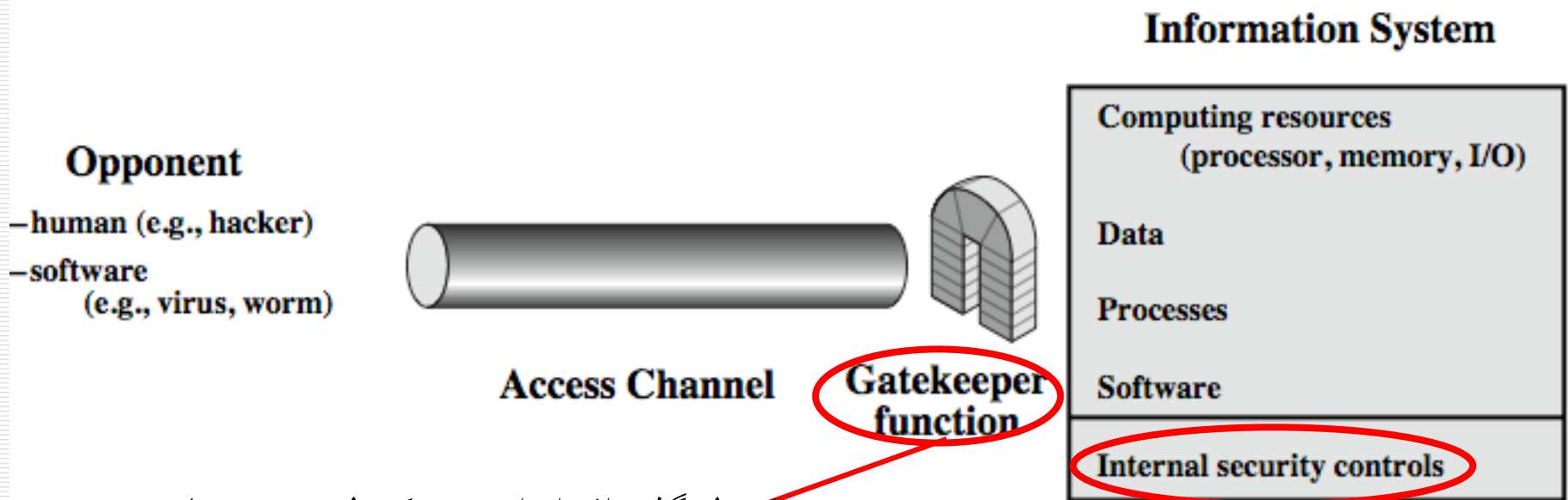


مدل امنیت شبکه

□ برای استفاده از این مدل موارد زیر مورد نیاز است:

۱. طراحی الگوریتمی مناسب برای عملیات «تبدیل»
۲. تولید اطلاعات محرمانه (کلید) برای استفاده در الگوریتم
۳. ایجاد روش‌هایی جهت توزیع و به اشتراک گذاشتن کلید
۴. مشخص کردن پروتکلی که طرفین را قادر به استفاده از «تبدیل» و اطلاعات محرمانه برای یک سرویس امنیتی می‌کند.

مدل دسترسی امنیتی شبکه



کنترل گذرواژه افراد و نیز کنترل ویروس‌ها
و کرم‌ها و جلوگیری از نفوذ آنها

نظارت و تحلیل اطلاعات ذخیره شده جهت
تشخیص وجود مهاجمین احتمالی

مدل دسترسی امنیتی شبکه

□ برای استفاده از این مدل موارد زیر مورد نیاز است:

۱. انتخاب عملیات مناسب برای gatekeeper جهت شناسایی کاربران
۲. پیاده سازی کنترل‌های امنیتی برای حصول اطمینان از این که تنها کاربران مجاز به اطلاعات و منابع مورد نظر دسترسی دارند.

خلاصه

- مفاهیم امنیتی
- محرمانگی، صحت و دسترس پذیری
- معماری امنیتی X.800
- حملات، سرویس‌ها و مکانیزم‌های امنیتی
- مدل‌های امنیت شبکه و دسترسی