یا ذالامن والامان

فصل اول: مفاهیم پایه‌ای امنیت

توسط: حمید رضا شهریاری

دانشگاه صنعتی امیرکبیر

دانشکده مهندسی کامپیوتر

http://aut.ac.ir/shahriari

http://atlas.aut.ac.ir

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 غیرعمدی

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، داده‌ها و اطلاعات و ارتباطات)

*National Institute of Standards and Technology

امنیت اطلاعات: گذشته و حال

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

امنیت اطلاعات در دنیای نوین

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

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 داده‌ها استفاده می‌شود.

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

1. بازارهای خرید و فروش آسیب پذیری
2. بازارهای خرید و فروش سیستمهای تحت کنترل
3. روشهای متعدد سوءاستفاده از سیستمهای تحت کنترل

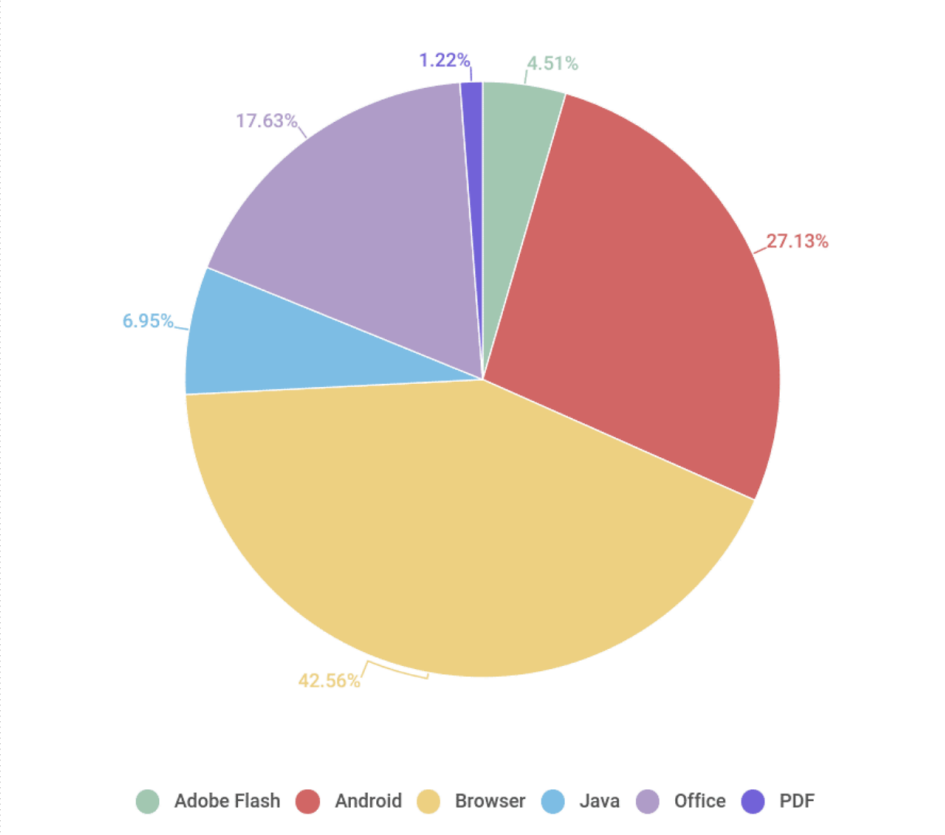
Top 50 Products By Total Number Of "Distinct" Vulnerabilities in 2018

Go to year: 1999 2000 2001 2002 2003 2004 2005 2006 2007 2008 2009 2010 2011 2012 2013 2019 All Time Leaders

	Product Name	Vendor Name	Product Type	Number of Vulnerabilities
1	Debian Linux	Debian	OS	950
2	Android	Google	OS	611
3	Ubuntu Linux	Canonical	OS	494
4	Enterprise Linux Server	Redhat	OS	394
5	Enterprise Linux Workstation	Redhat	OS	378
6	Enterprise Linux Desktop	Redhat	OS	369
7	Firefox	Mozilla	Application	333
8	Acrobat Reader Dc	Adobe	Application	286
9	Acrobat Dc	Adobe	Application	286
10	Windows 10	Mic[illegible]	OS	255

Screenshot

Vulnerable applications being exploited



Source: Kaspersky Security Bulletin 2017

مقدمه

برخی حملات نمونه

چرا تسخیر سیستم‌ها؟

1- 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

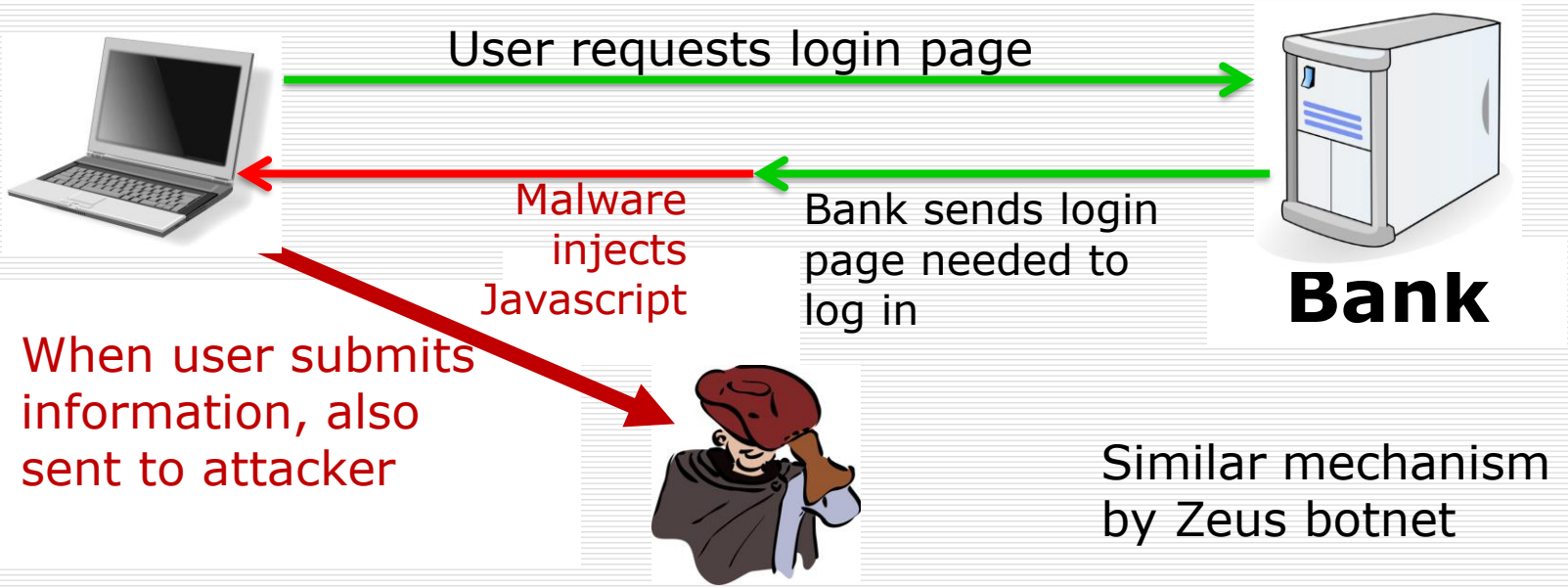
  1:260K greeting card spams leads to infection

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

چرا تسخیر سیستمها؟
2- سرقت اطلاعات مهم کاربر

استفاده از keylogger برای سرقت گذرواژه‌ها

مانند SilentBanker (و بسیاری نمونه های مشابه)



Similar mechanism used by Zeus botnet

Man-in-the-Browser (MITB)

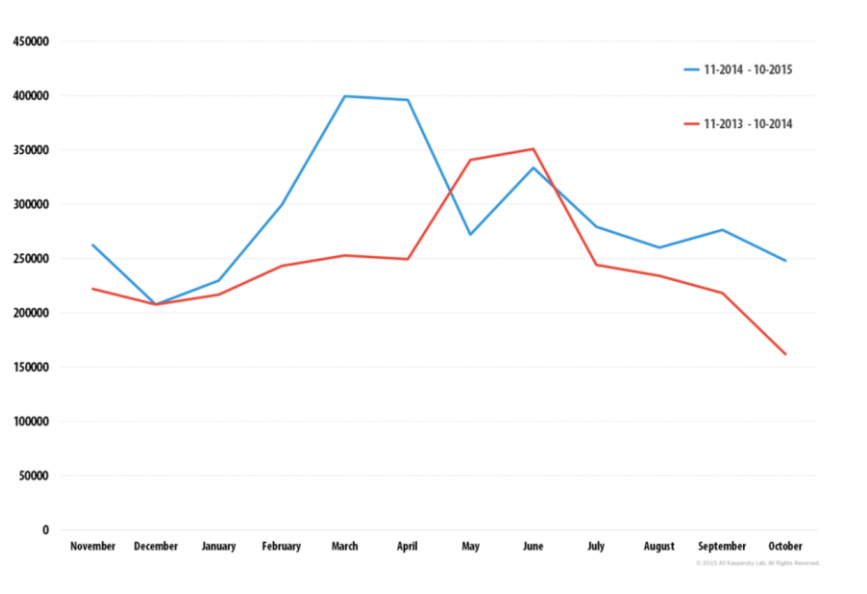
وجود تعداد زیادی بدافزار مالی

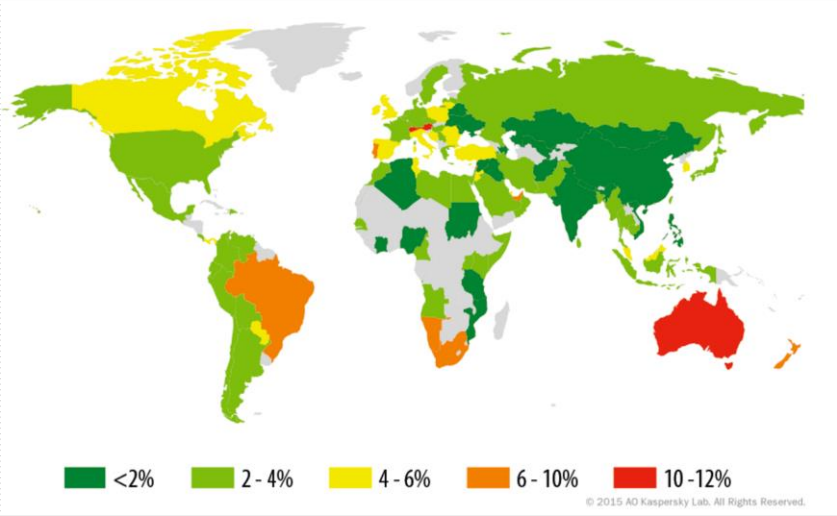
1	Trojan-Downloader.Win32.Upatre
2	Trojan-Spy.Win32.Zbot
3	Trojan-Banker.Win32.ChePro
4	Trojan-Banker.Win32.Shiotob
5	Trojan-Banker.Win32.Banbra
6	Trojan-Banker.Win32.Caphaw
7	Trojan-Banker.AndroidOS.Faketoken
8	Trojan-Banker.AndroidOS.Marcher
9	Trojan-Banker.Win32.Tinba
10	Trojan-Banker.JS.Agent

- 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؟
3- 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

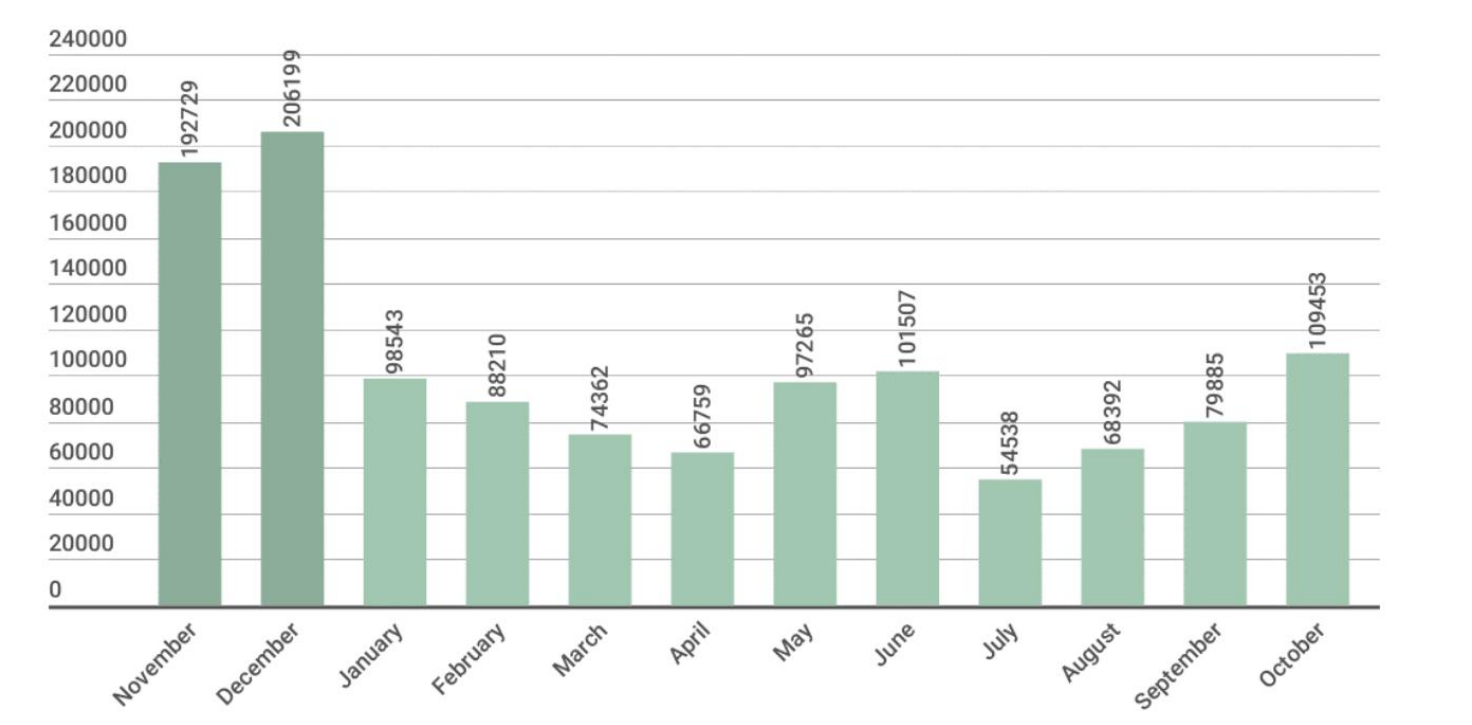
CryptoWall (2014-)
- targets Windows
- spread by spam emails

≈ 200,000 machines in 2015

A worldwide problem.

WannaCry ransomware

Ransomware in 2017: # users attacked



Source: Kaspersky Security Bulletin 2017

چرا تسخیر سیستمها؟
4- انتشار به سیستمهای ایزوله شده

مثال: **Stuxtnet**

Windows infection ⇒

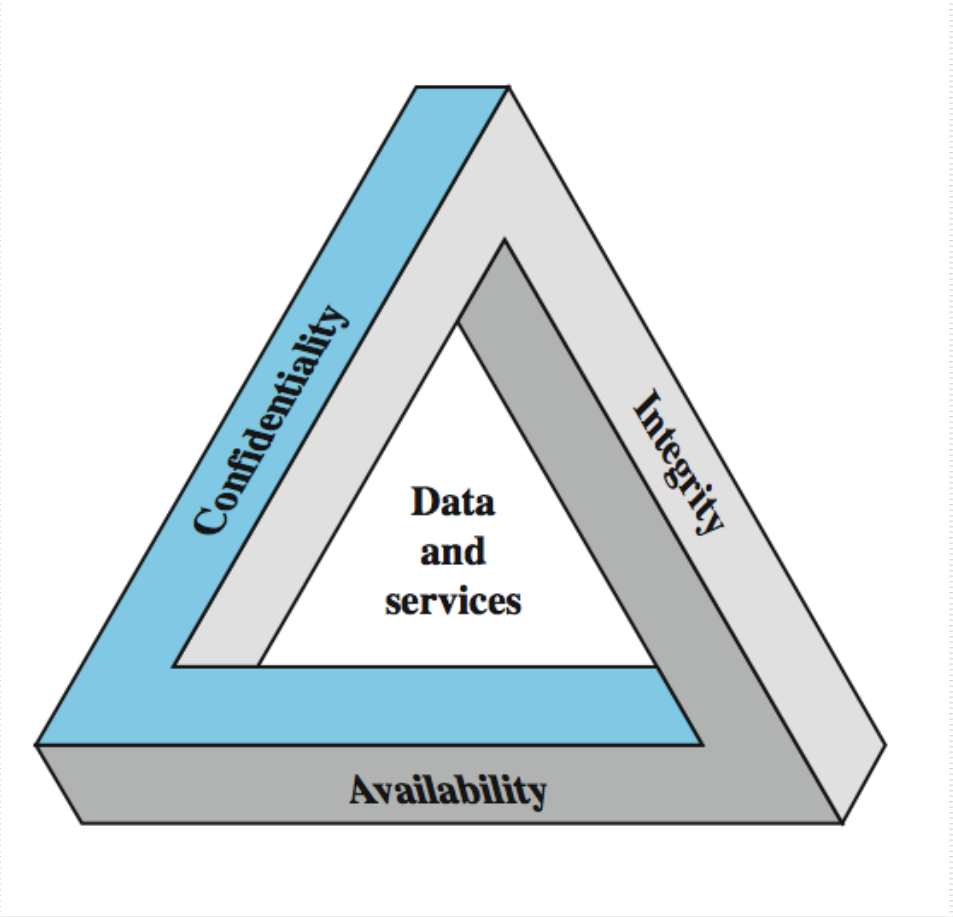
Siemens PCS 7 SCADA control software on Windows ⇒

Siemens device controller on isolated network

مقدمه

نیازمندی‌های امنیت

ابعاد امنیت


Confidentiality
Integrity
Data
and
services
Availability

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
- **دسترس‌پذیری (Availabiltiy)**: منابع در دسترس افراد به ویژه افراد مجاز باشند.

ابعاد امنیت

- انکارناپذیری (Non-Repudiation): جلوگیری از انکار انجام کار توسط هر یک از دو طرف ارتباط یا کاربران
  - مثال:
    - انکار نکردن فرستادن دستور خرید سهام
    - انکار نکردن دریافت دستور خرید سهام
    - انکار نکردن فرستادن ایمیل
- نیازمندی عدم انکار/انکارناپذیری تا حدی توسط ویژگی صحت قابل برآورده کردن است. (چگونه؟)

مثال‌هایی از نیازمندی‌های امنیتی

- **محرمانگی**: محرمانه بودن نمره‌های دانشجویان
- **صحت**: صحت اطلاعات بیماران و خدشه‌دار نبودن
- **دسترس‌پذیری**: در دسترس بودن سایت بانکداری اینترنتی

دشواری برقراری امنیت

- تعامل پروتکل‌ها پیچیدگی را افزایش داده و امنیت را تهدید می‌کند.
- امنیت معمولاً قربانی افزایش کارآیی و مقیاس پذیری می‌شود.
- امنیت بالا هزینه‌بر است.
- کاربران عادی امنیت را به عنوان مانع در برابر انجام شدن کارها تلقی می‌کنند و از خط مشی‌های امنیتی پیروی نمی‌کنند.

دشواری برقراری امنیت

- اطلاعات و نرم افزارهای دور زدن امنیت به طور گسترده در اختیار می‌باشند.
- برخی دور زدن امنیت را به عنوان یک مبارزه در نظر می‌گیرند و از انجام آن لذت می‌برند.
- ملاحظات امنیتی در هنگام طراحی های اولیه سیستم‌ها و شبکه‌ها در نظر گرفته نشده است.

چالش‌های برقراری امنیت

1. ساده نیست.
2. حملات بالقوه باید در نظر گرفته شود.
3. فرایندها حالت مقابله‌ای دارند و با معلوم بودن تهدید مفهوم پیدا می‌کنند.
4. شامل الگوریتم‌ها و اطلاعات محرمانه می‌شود.
5. باید در رابطه با محل قرار دادن مکانیزم‌ها تصمیم‌گیری کرد.
6. نبردی دائم میان مهاجم و مدیر سیستم وجود دارد.
7. تا زمانی که سیستم دچار نقص امنیتی نشود، به عنوان یک مزیت محسوب نمی‌شود.
8. نیاز به کنترل منظم دارد.
9. بیشتر پس از طراحی اعمال می شود.
10. مانعی برای استفاده از سیستم محسوب می‌شود.

معماری امنیتی OSI

- ITU-T X.800
- روشی نظام‌مند برای 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.

مفاهیم امنیت

- مفاهیم مهم:

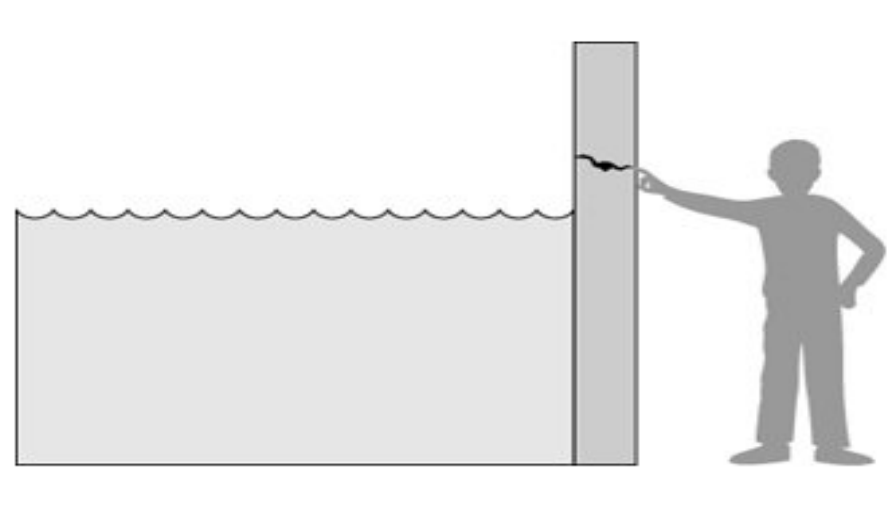
- حمله (یورش، تک) امنیتی : **تلاش** برای نقض امنیت
- مکانیزم (راهکار) امنیتی یا کنترل امنیتی : روش، ابزار یا فرآیندی برای مقابله با حملات امنیتی (با تشخیص، جلوگیری یا بازسازی)
- سرویس (خدمت) امنیتی: سرویس‌های فراهم کننده امنیت با استفاده از مکانیزم‌های امنیتی
- تهدید (Threat): یک عامل بالقوه برای نقض امنیت
- خط مشی امنیتی (Security Policy): بیان نیازمندی‌های امنیت سازمان یا سیستم

آسیب پذیری

- آسیب پذیری (Vulnerability):
  ویژگی (نقطه ضعف) در سیستم که ممکن است از آن سوءاستفاده شود و امنیت سیستم نقض شود.

آسیب پذیری و تهدید

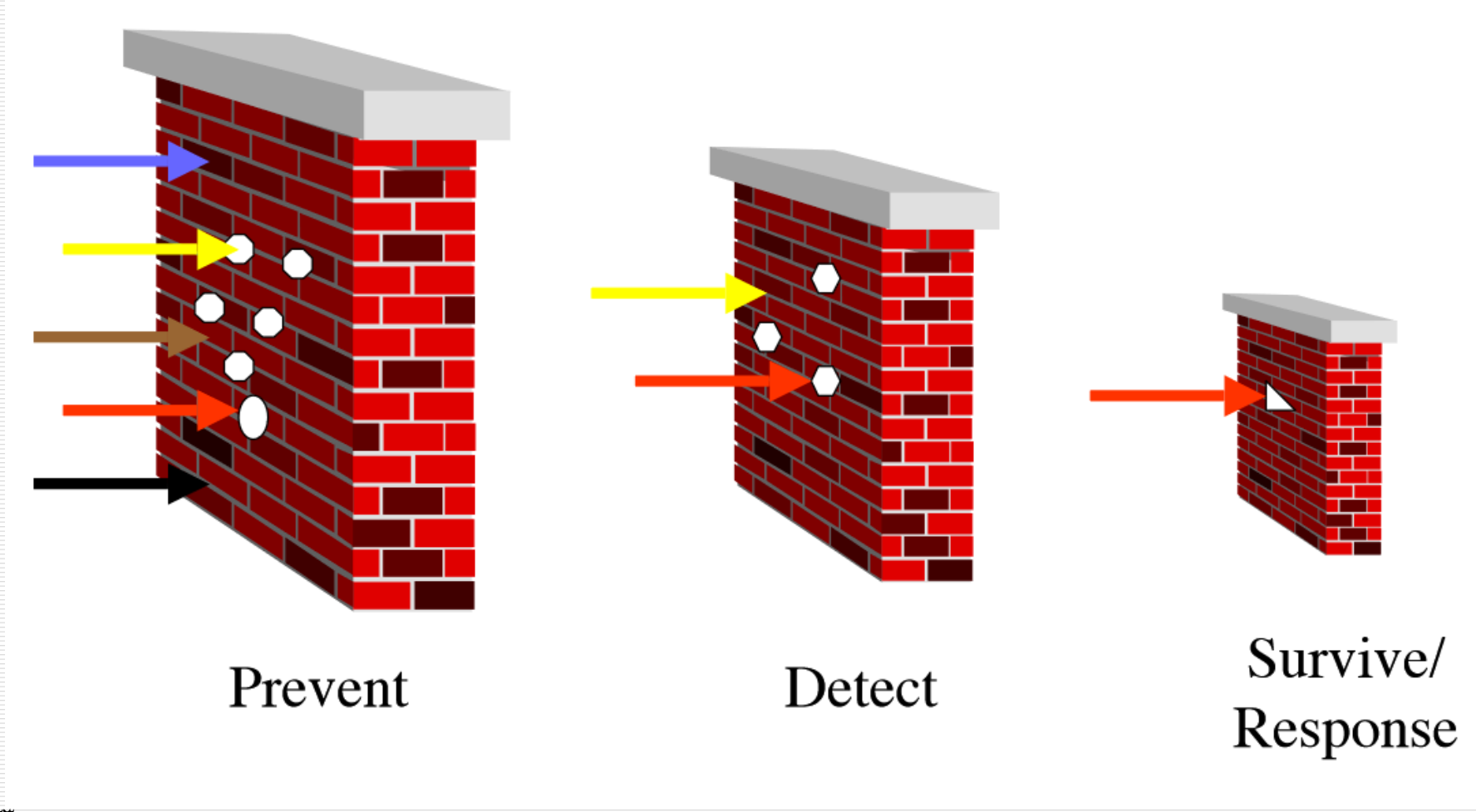
- تفاوت میان تهدید و آسیب پذیری:
  - آب موجود پشت سد به علت امکان شکستن سد، یک تهدید برای شخص است.
  - تَرک موجود در سد به عنوان یک آسیب پذیری شناخته می شود.



مکانیزم امنیتی

- انواع مکانیزمهای امنیتی (کنترلهای امنیتی)
  - بازدارنده یا Prevention: از نقض امنیت جلوگیری می‌کنند.
  - تشخیص یا Detection: در صورت وقوع حمله یا نقض امنیت آن را تشخیص و اعلام می‌کنند.
  - 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 بر می‌گردانند.

نقش مکانیزم‌های امنیتی

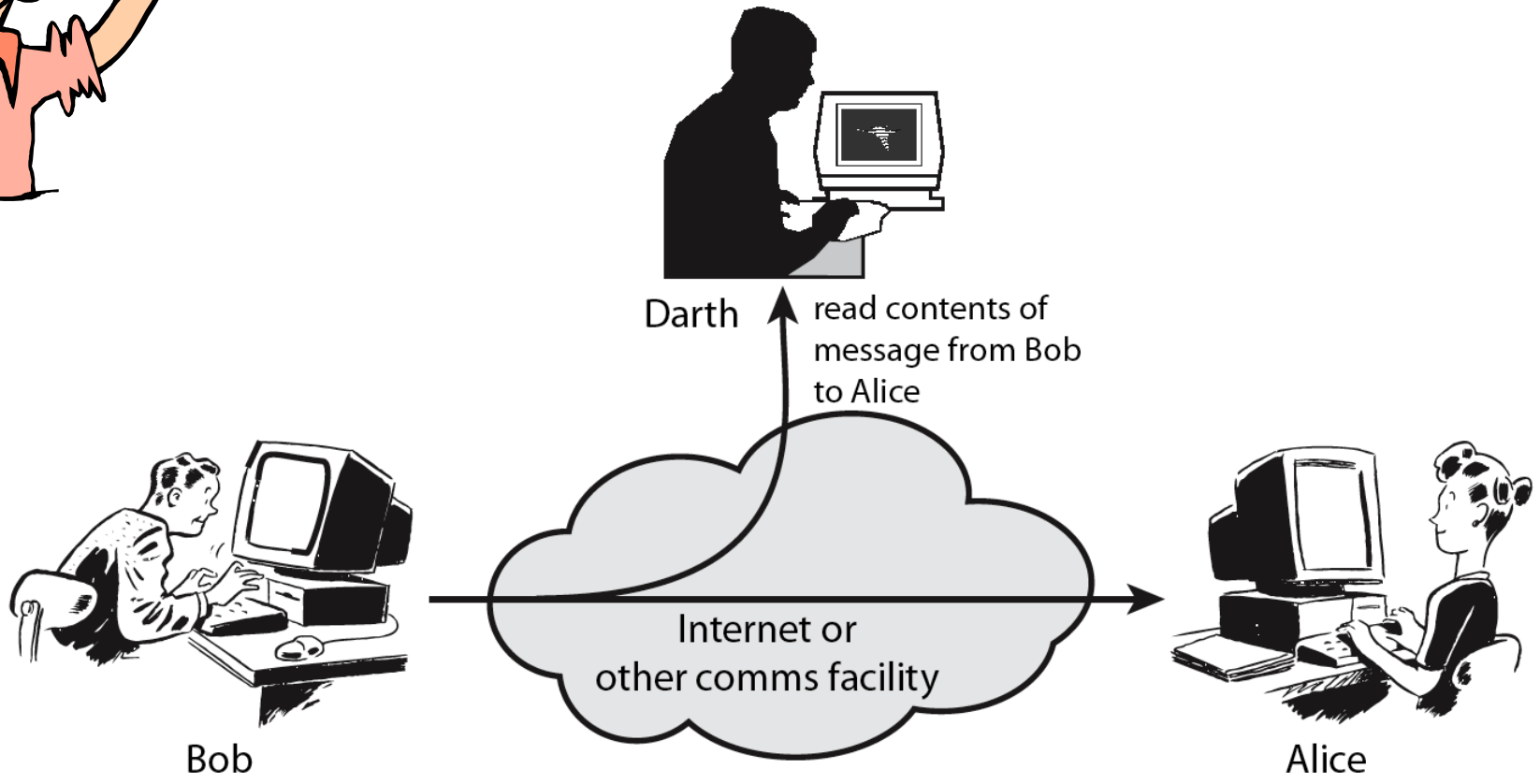


انواع حملات

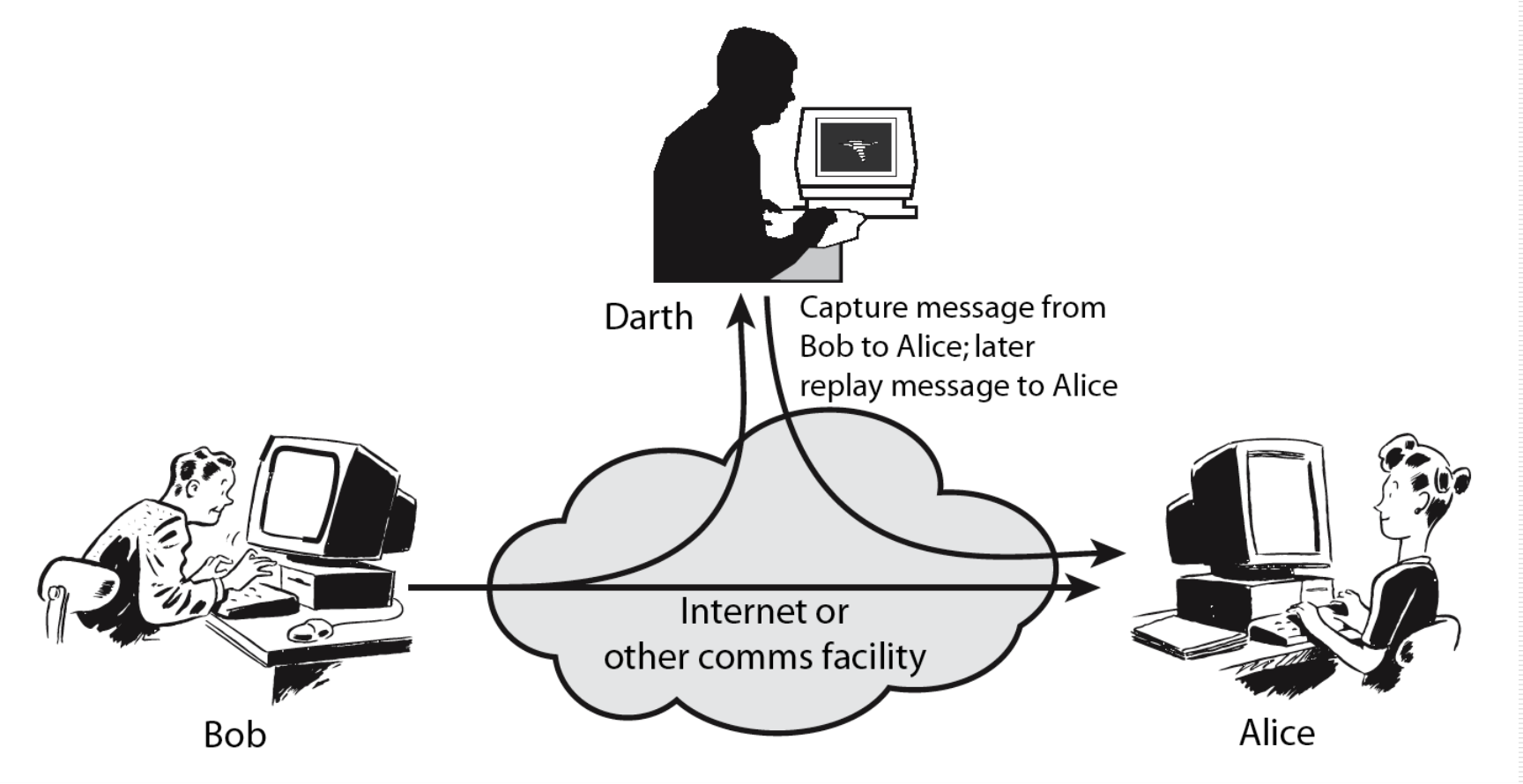
انواع حملات از نظر تأثیر در منابع سیستم یا ارتباط:

- حملات غیرفعال (Passive attack):
  - حملاتی که در آن اطلاعاتی از سیستم جمع‌آوری می‌شود. مثال:
    - انواع حملات شنود و افشای پیام (release of message content)
    - تحلیل ترافیک
- حملات فعال (Active attack)
  - حملاتی که در آن سعی می‌شود 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 غیرفعال



حملات فعال


Darth
Capture message from
Bob to Alice; later
replay message to Alice
Internet or
other comms facility
Bob
Alice

انواع حملات فعال

جعل Masquerade

- هنگامی که یک کاربر به جای یک کاربر دیگر خود را جا می‌زند.
- معمولا شامل یک یا دو نوع از حملات فعال می‌شود.

ارسال مجدد Replay

- شنود داده‌ها و ارسال مجدد آنها به منظور کسب نتایج غیرمجاز

دستکاری

Modification of messages

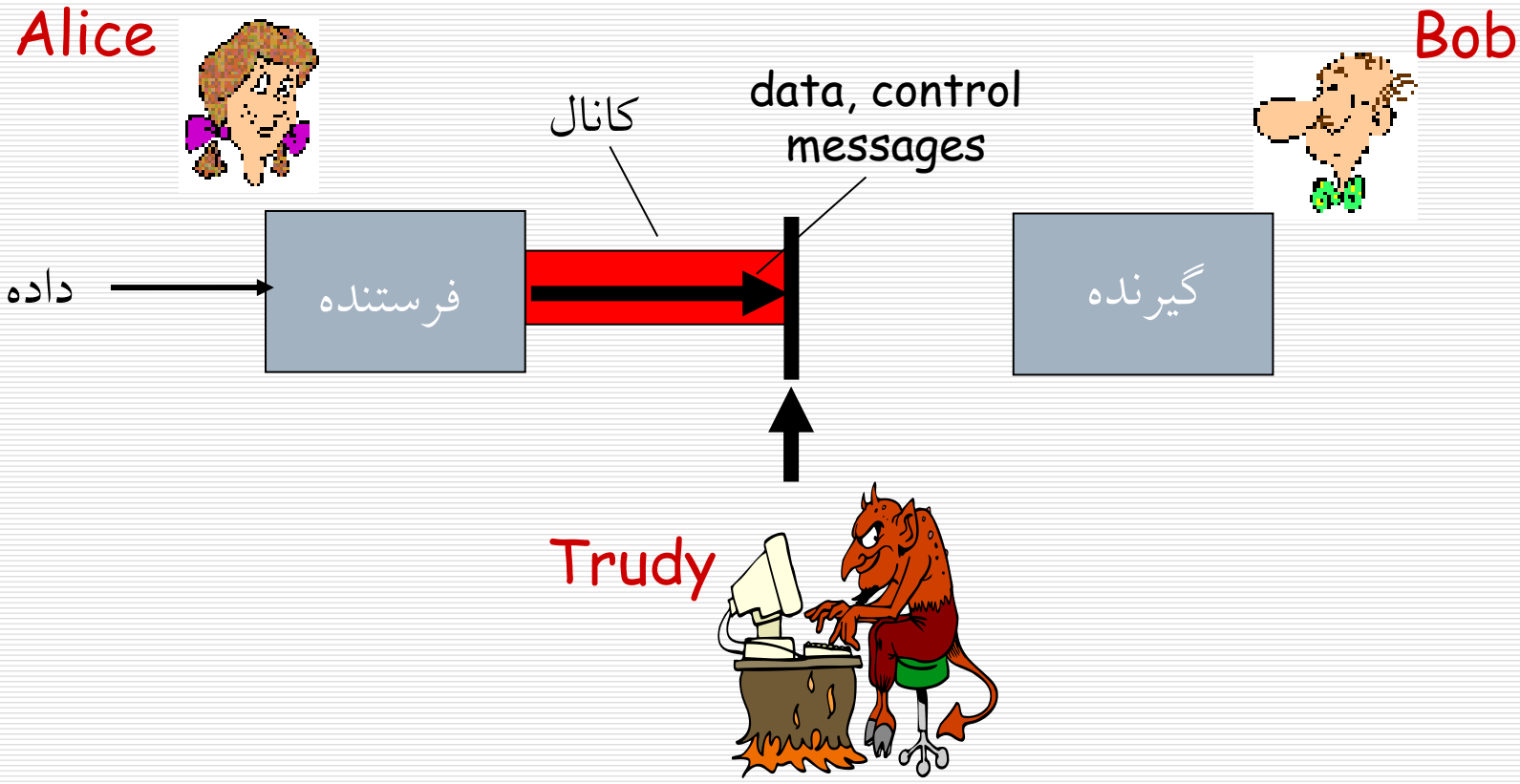
- تغییر در بخشی از پیام مجاز، یا ترتیب پیامها یا زمان ارسال (به منظور کسب نتایج غیرمجاز)

منع خدمت

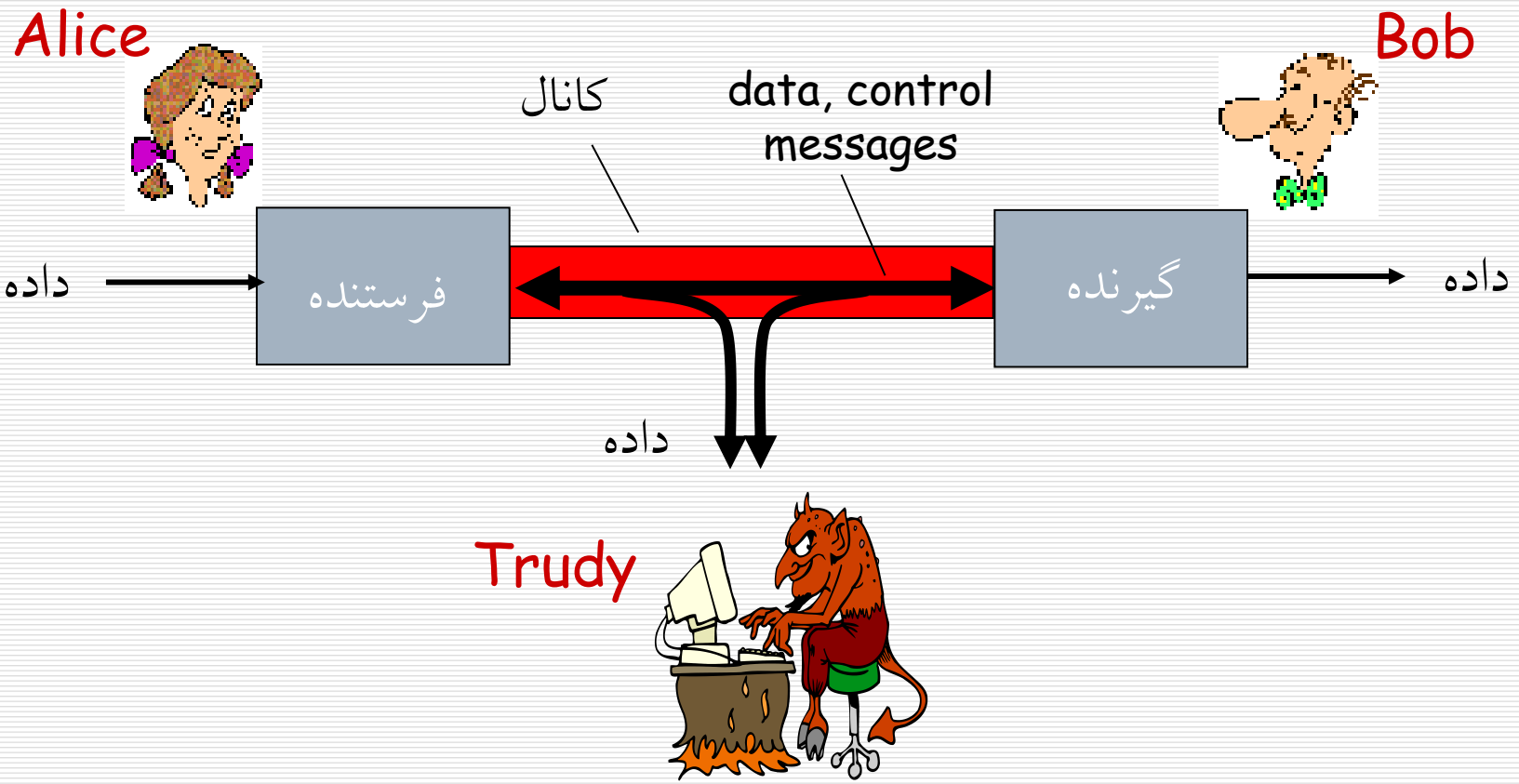
Denial of service

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

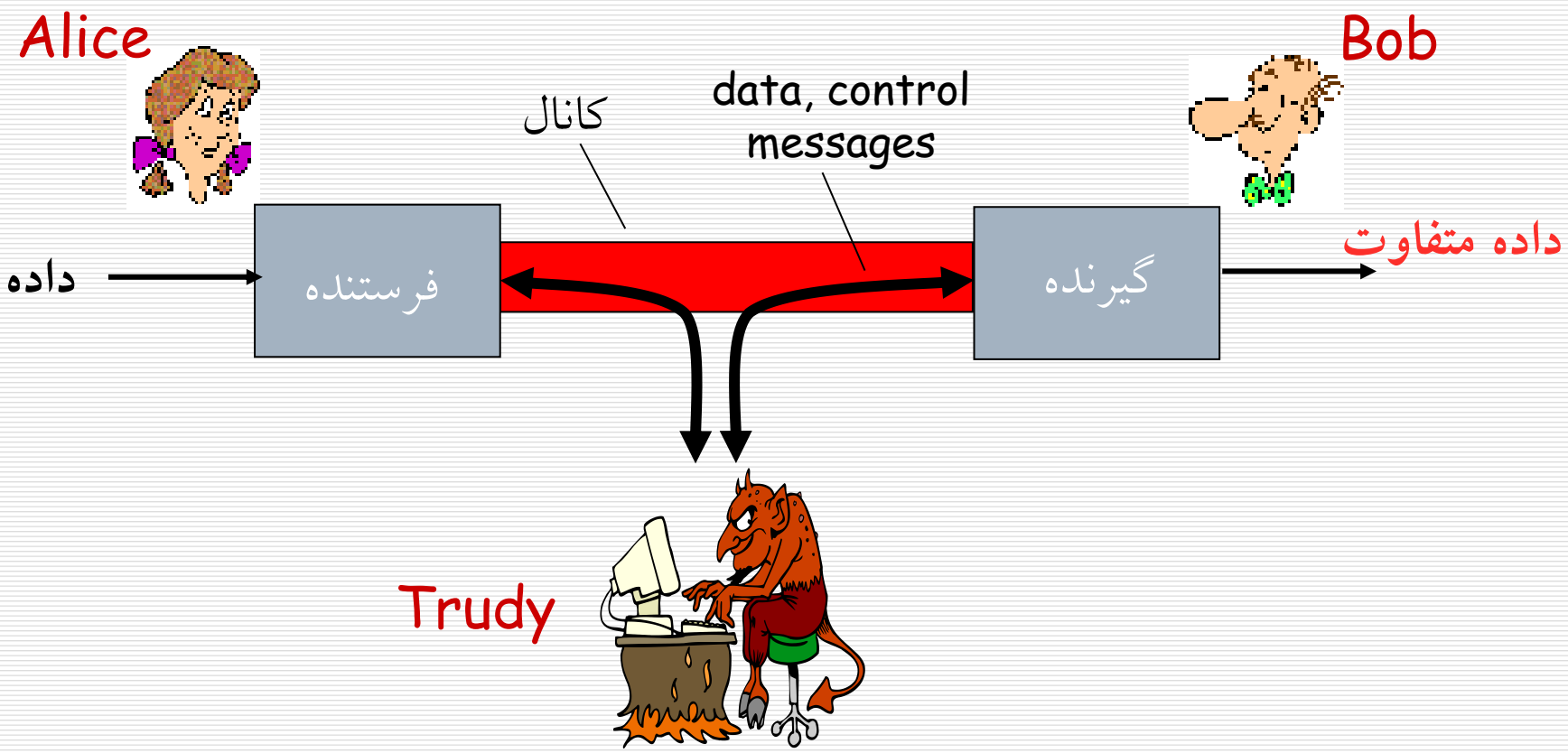
حمله امنیتی: وقفه



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 مانند 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.

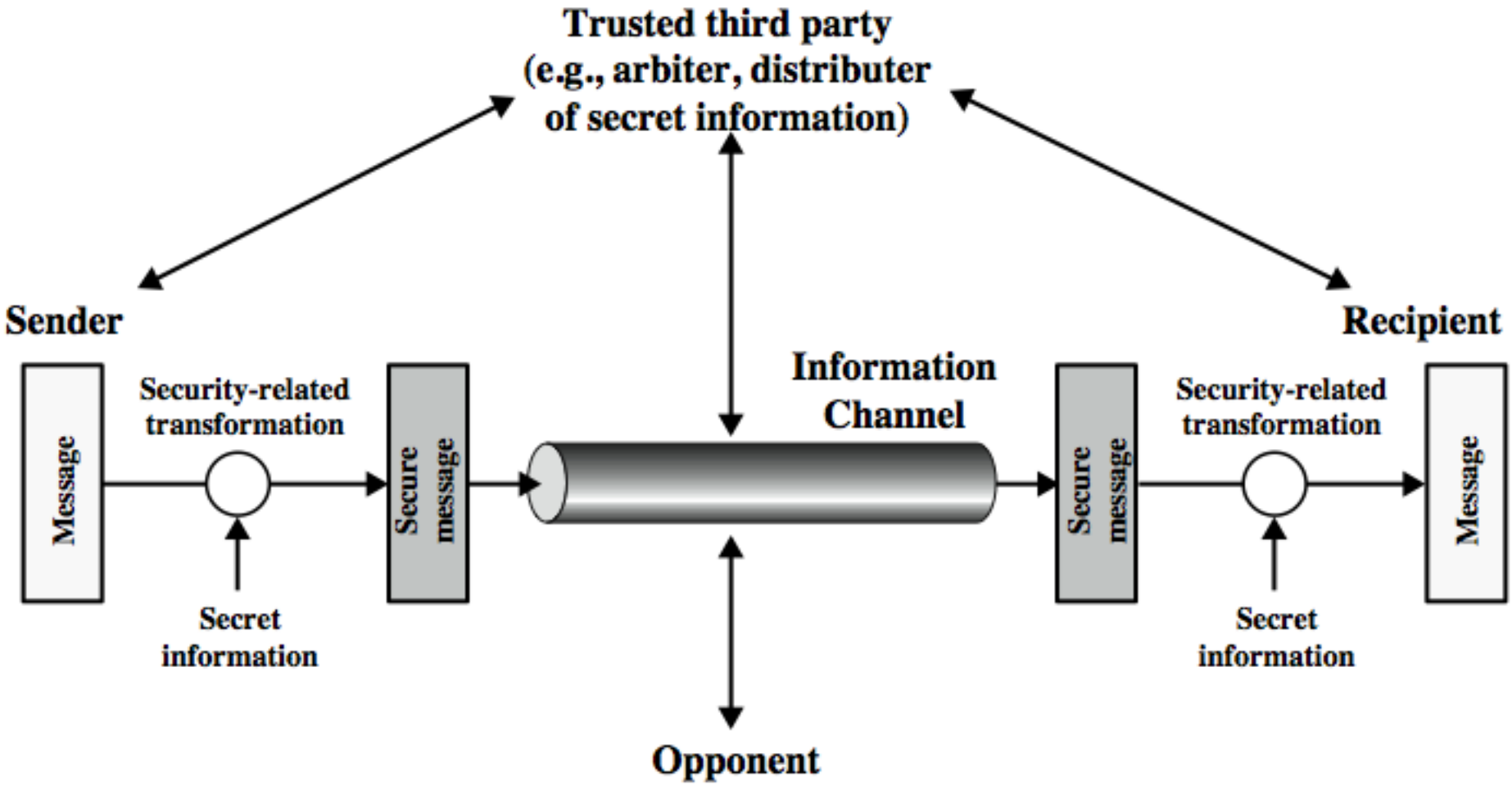
سرویس‌های امنیتی (X.800)

- 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 این‌که داده‌ها همان گونه که توسط یک موجودیت مجاز ارسال شده، دریافت شده‌اند.
- عدم انکار (انکارناپذیری) (Non-Repudiation): جلوگیری از انکار توسط هر یک از طرفین ارتباط
- دسترس پذیری: در دسترس بودن منابع

مکانیزم امنیتی

- روش یا 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 تکنینک‌های "رمزنگاری" در اکثر مکانیزم‌های امنیتی مورد استفاده قرار می‌گیرند.
  - به همین دلیل این موضوع مورد توجه ما نیز قرار خواهد گرفت.

مدل امنیت شبکه

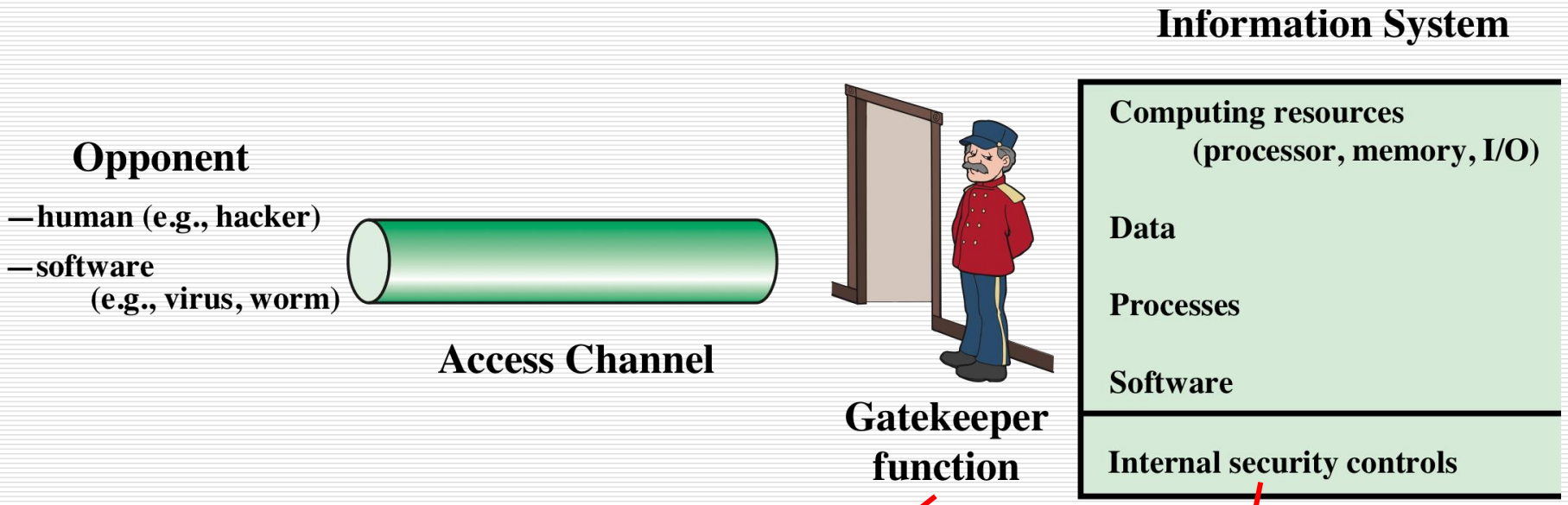


مدل امنیت شبکه

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

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

مدل دسترسی امنیتی شبکه



کنترل ورود افراد و نیز کنترل بدافزارها 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:

1. انتخاب عملیات مناسب برای gatekeeper جهت شناسایی کاربران
2. پیاده سازی کنترل‌های امنیتی برای حصول اطمینان از این‌که تنها کاربران مجاز به اطلاعات و منابع مورد نظر دسترسی دارند.

دسترسی های غیر مجاز

- انواع تهدیدهای ناشی از برنامه ها:
  - تهدیدهای دسترسی به اطلاعات
    - خواندن یا تغییر داده ها از طرف کاربرانی که نباید دسترسی داشته باشند
  - تهدیدهای سرویس ها
    - سوءاستفاده از ضعف های سرویس برای دسترسی

خلاصه

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

Threat Consequence	Threat Action (Attack)
Unauthorized Disclosure A circumstance or event whereby an entity gains access to data for which the entity is not authorized.	**Exposure:** Sensitive data are directly released to an unauthorized entity. **Interception:** An unauthorized entity directly accesses sensitive data traveling between authorized sources and destinations. **Inference:** A threat action whereby an unauthorized entity indirectly accesses sensitive data (but not necessarily the data contained in the communication) by reasoning from characteristics or byproducts of communications. **Intrusion:** An unauthorized entity gains access to sensitive data by circumventing a system's security protections.
Deception A circumstance or event that may result in an authorized entity receiving false data and believing it to be true.	**Masquerade:** An unauthorized entity gains access to a system or performs a malicious act by posing as an authorized entity. **Falsification:** False data deceive an authorized entity. **Repudiation:** An entity deceives another by falsely denying responsibility for an act.
Disruption A circumstance or event that interrupts or prevents the correct operation of system services and functions.	**Incapacitation:** Prevents or interrupts system operation by disabling a system component. **Corruption:** Undesirably alters system operation by adversely modifying system functions or data. **Obstruction:** A threat action that interrupts delivery of system services by hindering system operation.
Usurpation A circumstance or event that results in control of system services or functions by an unauthorized entity.	**Misappropriation:** An entity assumes unauthorized logical or physical control of a system resource. **Misuse:** Causes a system component to perform a function or service that is detrimental to system security.

Threat Consequences, and the Types of Threat Actions That Cause Each Consequence

Based on RFC 4949

**Table is on page 20 in the Stallings Book (Computer Security).