midterm

امنیت شبکه – مروری بر مفاهیم پایه
Network Security - Concepts

Mohammad Sayad - محمد صیاد

دانشگاه تهران

[redacted]

برخی تجارب آمریکا در زمینه امنیت

$1.52B/y

هزینه ای که دزدی هویت به آمریکاییان
در سال تحمیل میکند
Huffington Post

46%

کاهش در تعداد حملات نفوذ به شبکه در
اثر استفاده از کارتهای هوشمند و PKI در
وزارت دفاع
Realized Value of FPKI

$2.9B/y

صرفه جویی از محل انجام
تراکنش ها بصورت دیجیتالی
بجای کاغذی
Economist

782%

میزان افزایش تعداد وقایع امنیتی سایبری
از سال ۲۰۰۶ تا ۲۰۱۲
GAO-13-187

17%

درصد وقایع امنیتی مربوط به
دسترسی غیر مجاز از کل وقایع
GAO-13-187

75%

کاهش هزینه های پردازش، حمل و
نقل و مدیریت کاغذی در اثر استفاده
از امضای دیجیتال
Signix.com

$7.2M

هزینه متوسط هر نشت اطلاعاتی در اثر
حمله در آمریکا
Bloomberg

$100/user/y

صرفه جویی از محل عدم
استفاده از پسورد های یک
بار مصرف توکنی
Tyntec

Story of a Hack…

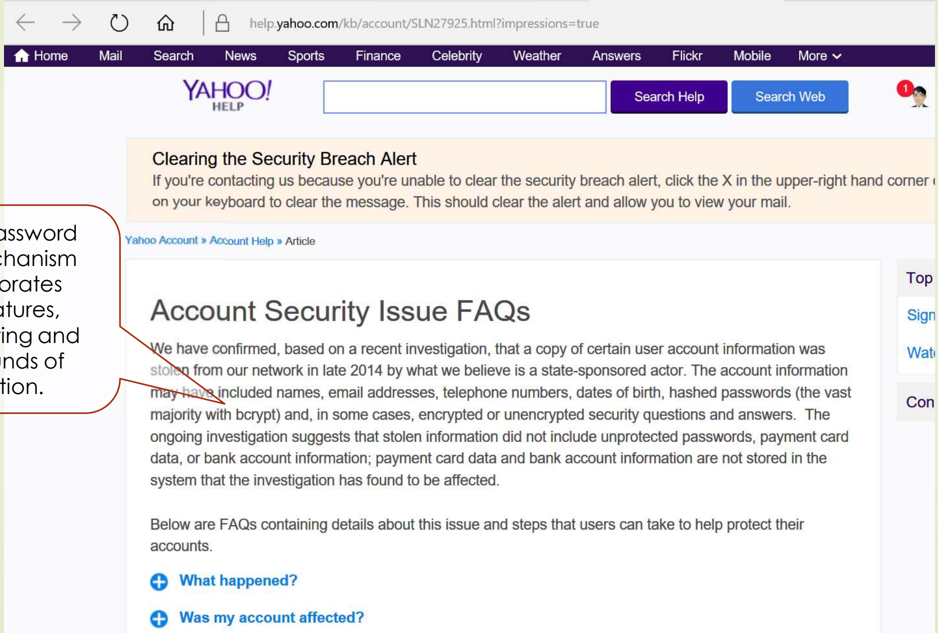
- November 24, 2014: A hacker group ("Guardians of Peace" (GOP)) leaked a release of confidential data from the film studio Sony Pictures Entertainment.
  - The data included personal information about Sony Pictures employees, e-mails between employees, executive salaries, and copies of unreleased Sony films.

(Wikipedia)

Story of a Hack…

- December 2014: The GOP demanded that Sony pull its film *The Interview*, and threatened terrorist attacks at cinemas screening the film.
  - Major U.S. cinemas decided not to screen the film. Sony wanted to cancel the release. Obama insisted on the release.
  - US officials, after evaluating the software, techniques, and network sources used, alleged that the attack was sponsored by North Korea. North Korea has denied all responsibility.

Yahoo Hack (publicized in 2016)



Clearing the Security Breach Alert

If you're contacting us because you're unable to clear the security breach alert, click the X in the upper-right hand corner on your keyboard to clear the message. This should clear the alert and allow you to view your mail.

Yahoo Account » Account Help » Article

Account Security Issue FAQs

We have confirmed, based on a recent investigation, that a copy of certain user account information was stolen from our network in late 2014 by what we believe is a state-sponsored actor. The account information may have included names, email addresses, telephone numbers, dates of birth, hashed passwords (the vast majority with bcrypt) and, in some cases, encrypted or unencrypted security questions and answers. The ongoing investigation suggests that stolen information did not include unprotected passwords, payment card data, or bank account information; payment card data and bank account information are not stored in the system that the investigation has found to be affected.

Below are FAQs containing details about this issue and steps that users can take to help protect their accounts.

⊕ What happened?

⊕ Was my account affected?

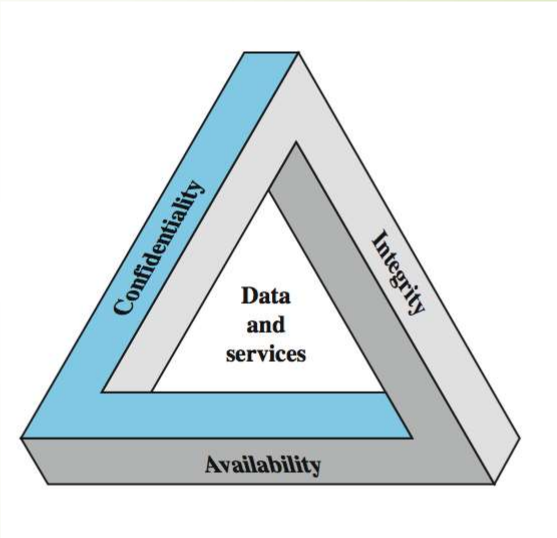
Bcrypt is a password hashing mechanism that incorporates security features, including salting and multiple rounds of computation.

Standards and Concepts

Fundamental Security Services

1- Confidentiality
2- Integrity
3- Availability
4- Authentication
5- Authorization
6- Non-repudiation

The first three are fundamental (C.I.A.) , others are derivatives.



Confidentiality

Confidentiality means keeping the information hidden from the eyes of others.

We usually encrypt the data to achieve this goal in the digital world.

Integrity

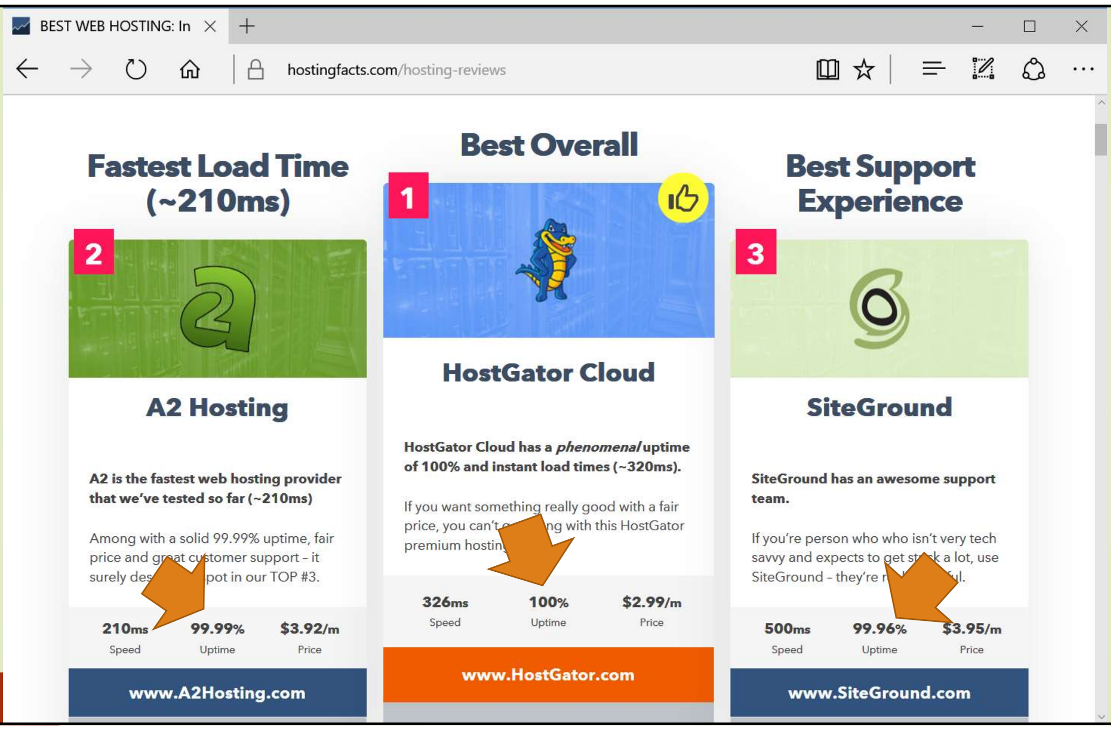
Means making sure the data is not modified or tampered with.

Even if the data is encrypted and is confidential, it can be modified.

Availability

Availability means the service should be up and available.

Some service provider show their availability rate by up-time: e.g. 99.9% up time



Fastest Load Time (~210ms)

2

A2 Hosting

A2 is the fastest web hosting provider that we've tested so far (~210ms)

Among with a solid 99.99% uptime, fair price and great customer support – it surely des[illegible]pot in our TOP #3.

210ms	99.99%	$3.92/m
Speed	Uptime	Price

www.A2Hosting.com

Best Overall

1

HostGator Cloud

HostGator Cloud has a *phenomenal* uptime of 100% and instant load times (~320ms).

If you want something really good with a fair price, you can't g[illegible]ng with this HostGator premium hostin[illegible]

326ms	100%	$2.99/m
Speed	Uptime	Price

www.HostGator.com

Best Support Experience

3

SiteGround

SiteGround has an awesome support team.

If you're person who who isn't very tech savvy and expects to get st[illegible]k a lot, use SiteGround – they're r[illegible]ul.

500ms	99.96%	$3.95/m
Speed	Uptime	Price

www.SiteGround.com

Authentication

Authentication means making sure the one who claims an ID, is really the one he says.

Authorization

Authorization means giving permission to access resources.

This is directly related to the access-control topic.

Examples are keys (to doors) in the real world.

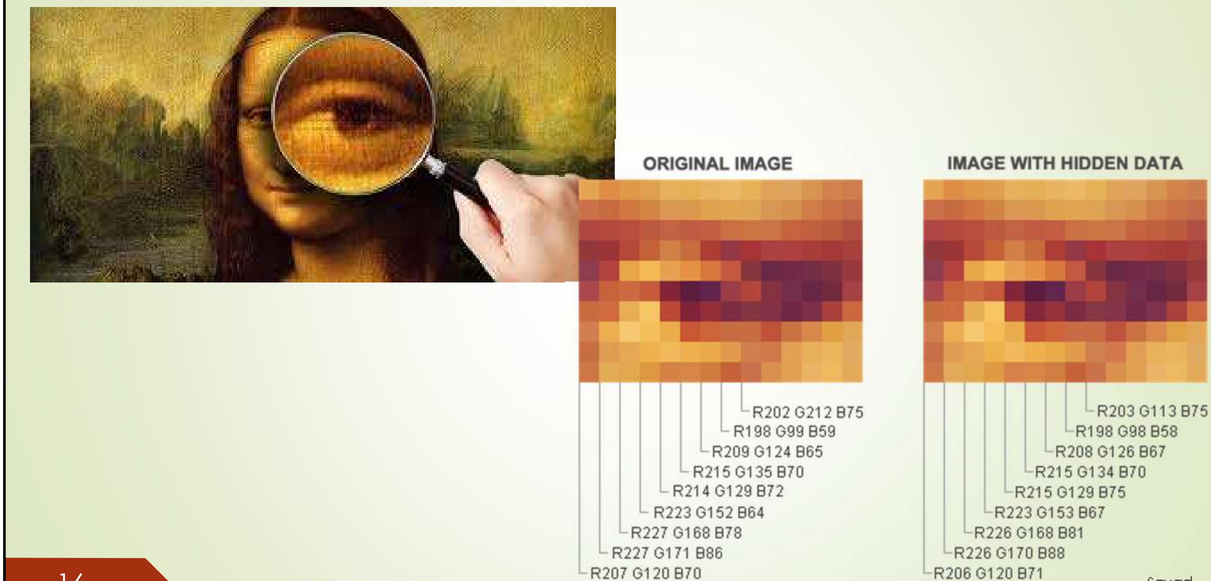
"First off, I'd like to categorically deny any wrongdoing...."

Non-repudiation

Non-repudiation is the service that makes sure no one can deny what he/she has done.

e.g. when you sign a contract digitally, you can't say I haven't done it.

Steganography



Key Definitions تعاریف کلیدی

- **Vulnerability** (آسیب پذیری):

  A weakness in the design, implementation or operation of a system

- **Threat** (تهدید) :

  The possibility/potential that an adversary takes advantage of the vulnerability

- **Attack** (حمله):

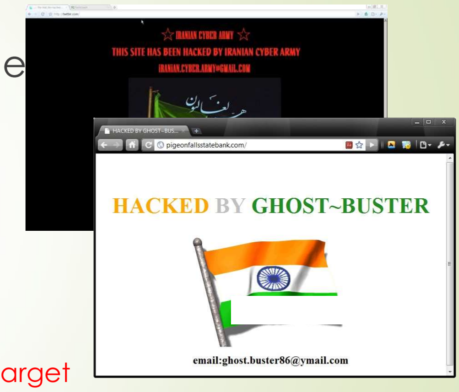
  Act of exploiting a vulnerability

Key Definitions تعاریف کلیدی

- **Asset:**

  Every valuable thing owned. Example are:

  - Devices, Tools, Machinery, …
  - Valuable information / data / plans
  - Bandwidth
  - Employees (people)
  - Reputation -> Website defacing attacks target this
  - …



☆ IRANIAN CYBER ARMY ☆

THIS SITE HAS BEEN HACKED BY IRANIAN CYBER ARMY

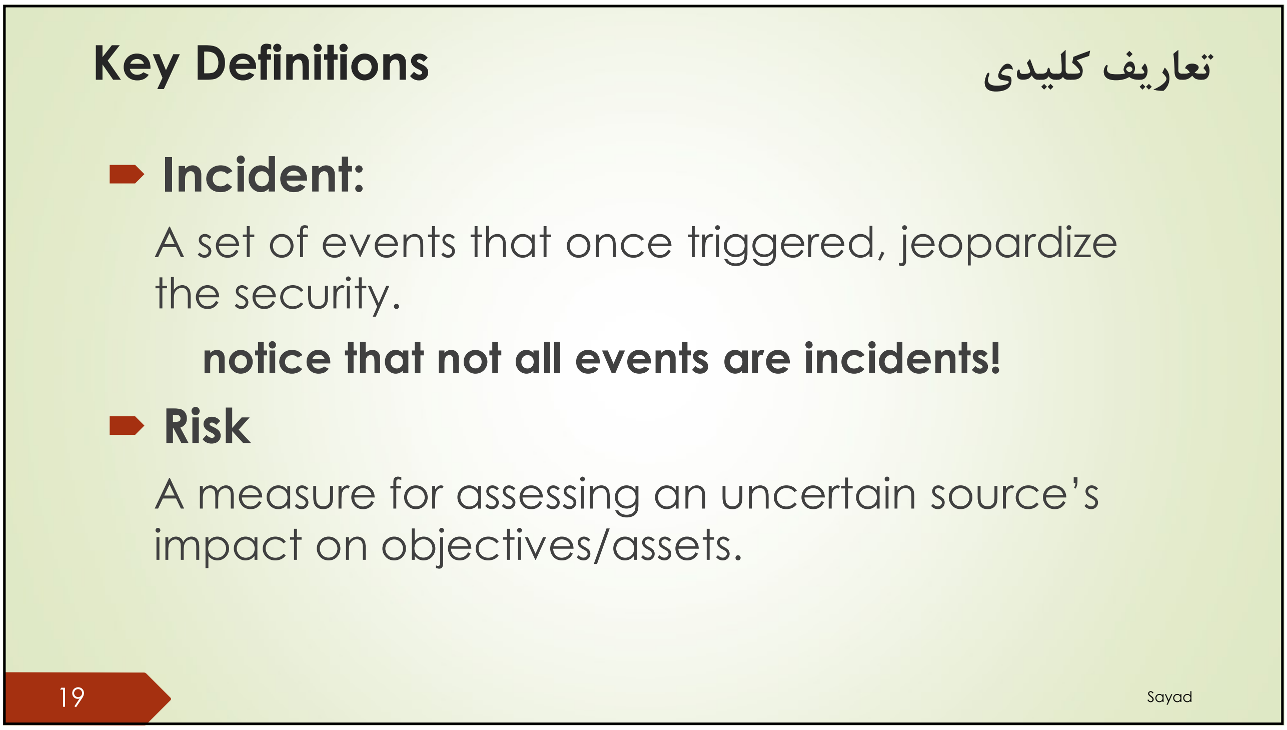
IRANIAN.CYBER.ARMY@GMAIL.COM

pigeonfallsstatebank.com/

HACKED BY GHOST~BUSTER

email:ghost.buster86@ymail.com

- In IoT, probably data is the most precious asset



Key Definitions تعاریف کلیدی

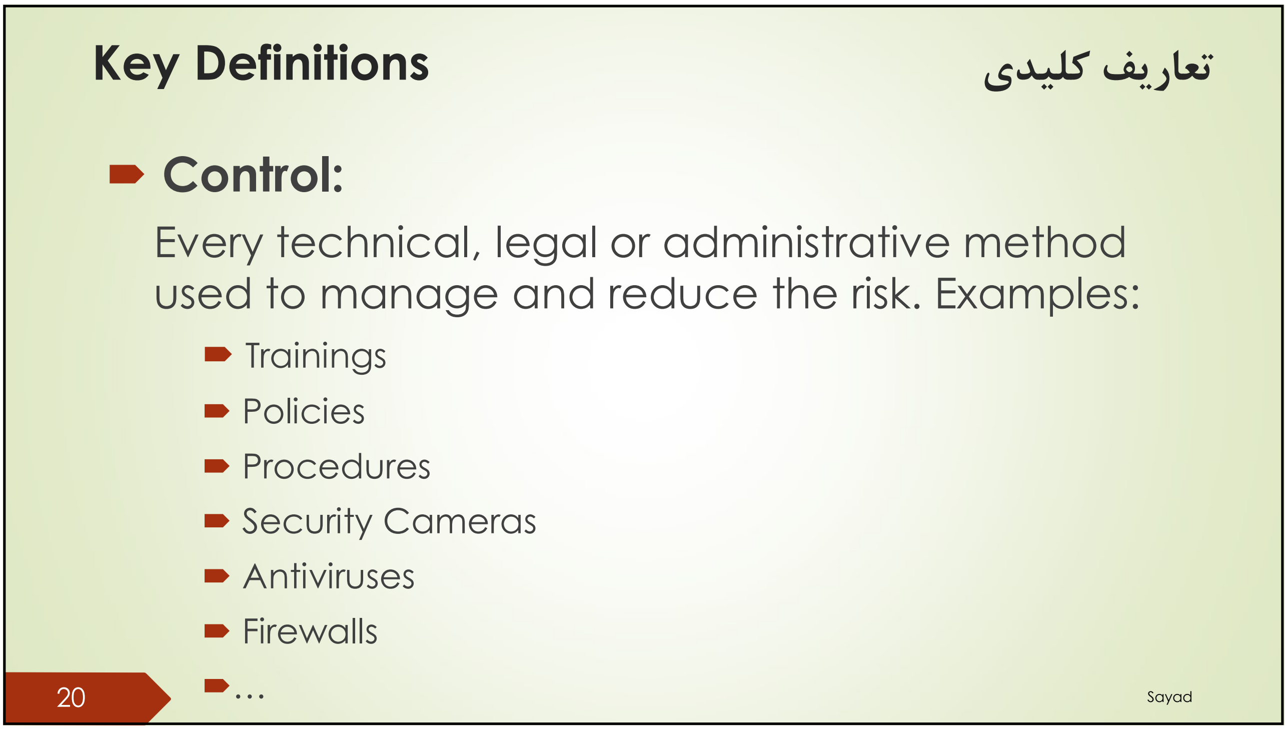
- **Incident:**

  A set of events that once triggered, jeopardize the security.

  notice that not all events are incidents!

- **Risk**

  A measure for assessing an uncertain source's impact on objectives/assets.



Key Definitions تعاریف کلیدی

- **Control:**

  Every technical, legal or administrative method used to manage and reduce the risk. Examples:

  - Trainings
  - Policies
  - Procedures
  - Security Cameras
  - Antiviruses
  - Firewalls
  - …

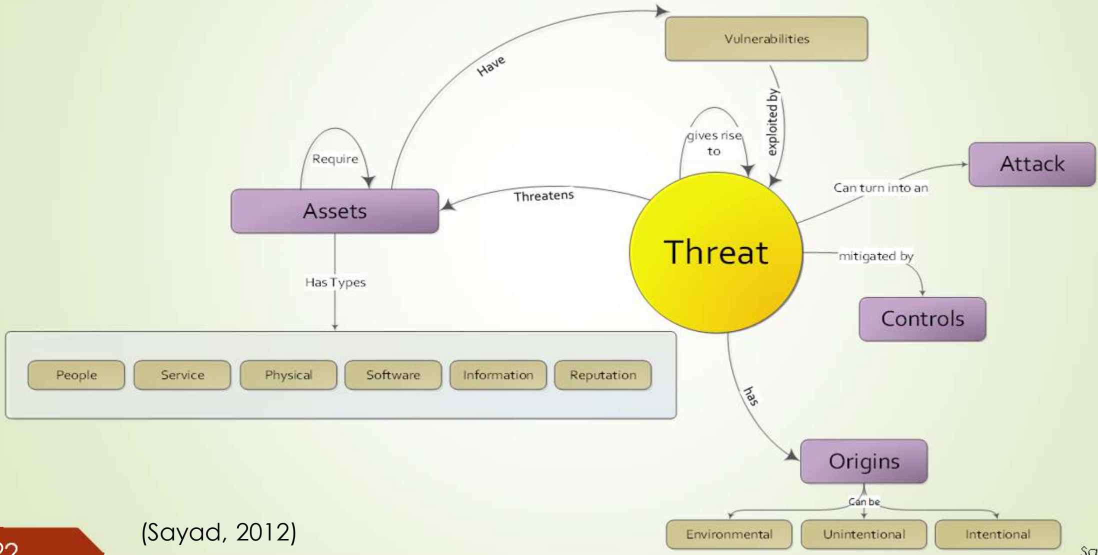
Key Definitions تعاریف کلیدی

- اجماعی بین المللی بر سر تعاریف پایه بصورت یکپارچه وجود ندارد و تعریفها در استاندارد های مختلفی همچون ISO، NIST، ENISA، ... با وجود داشتن شباهت، متفاوت است. برای مثال موسسه استاندارد ملی آمریکا (NIST) تهدید را هر واقعه یا موقعیتی تعریف می‌کند که کارایی سازمانی (شامل ماموریت ها، کارکردها، وجهه و یا شهرت)، اموال سازمانی، و یا افراد را از راه سیستمهای اطلاعاتی بصورت منفی تحت تاثیر قرار دهد که این خود می‌تواند از طریق دسترسی غیر مجاز، تخریب، آشکارسازی اطلاعات، تغییر اطلاعات و/یا جلوگیری از دسترسی به سرویس باشد. تهدید همچنین شامل وجود یک عامل که بطور بالقوه از یک نقطه ضعف امنیتی سیستم می‌تواند استفاده کند نیز می‌شود.
- اما موسسه استاندارد جهانی (ISO)، تهدید را عامل بالقوه ایجاد یک واقعه تعریف نموده که می‌تواند (با استفاده از یک آسیب پذیری) موجب صدمه رسیدن به سازمان شود.
- آنچه در تعاریف کلیدی ارایه شد، نسخه ای ساده و قابل استفاده در این درس است.

21

Sayad

Key Definitions Relationship رابطه تعاریف کلیدی با هم

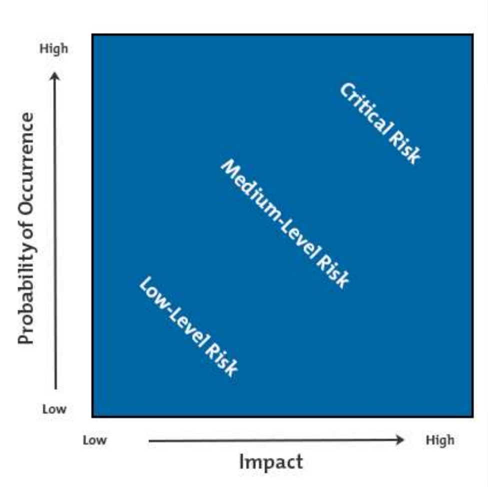


(Sayad, 2012)

22

Sayad

Risk Definition in Simple Words تعریف ریسک به زبان ساده



- ریسک تابعی از احتمال تهدید و میزان اثرگذاری آن در صورت وقوع است.
- یک تعریف ساده:

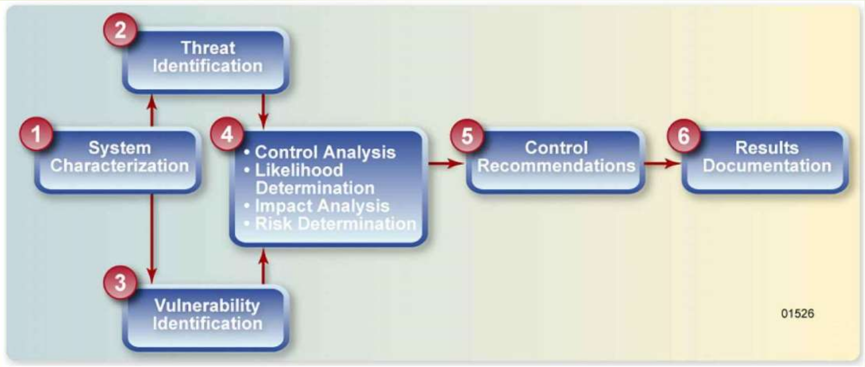
Risk=Threat Probability × Impact

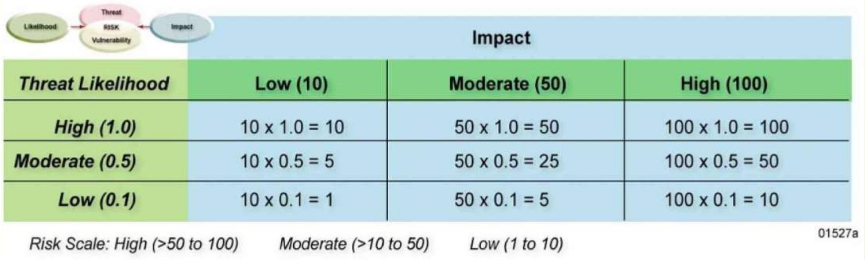
- ریسک زمانی بالاست که تهدید بالقوه خیلی محتمل باشد و اگر تبدیل به حمله شود، اثر تخریبی آن هم زیاد باشد.

23

Sayad

Example




Likelihood
Threat
RISK
Vulnerability
Impact

	Impact		
Threat Likelihood	Low (10)	Moderate (50)	High (100)
High (1.0)	10 x 1.0 = 10	50 x 1.0 = 50	100 x 1.0 = 100
Moderate (0.5)	10 x 0.5 = 5	50 x 0.5 = 25	100 x 0.5 = 50
Low (0.1)	10 x 0.1 = 1	50 x 0.1 = 5	100 x 0.1 = 10

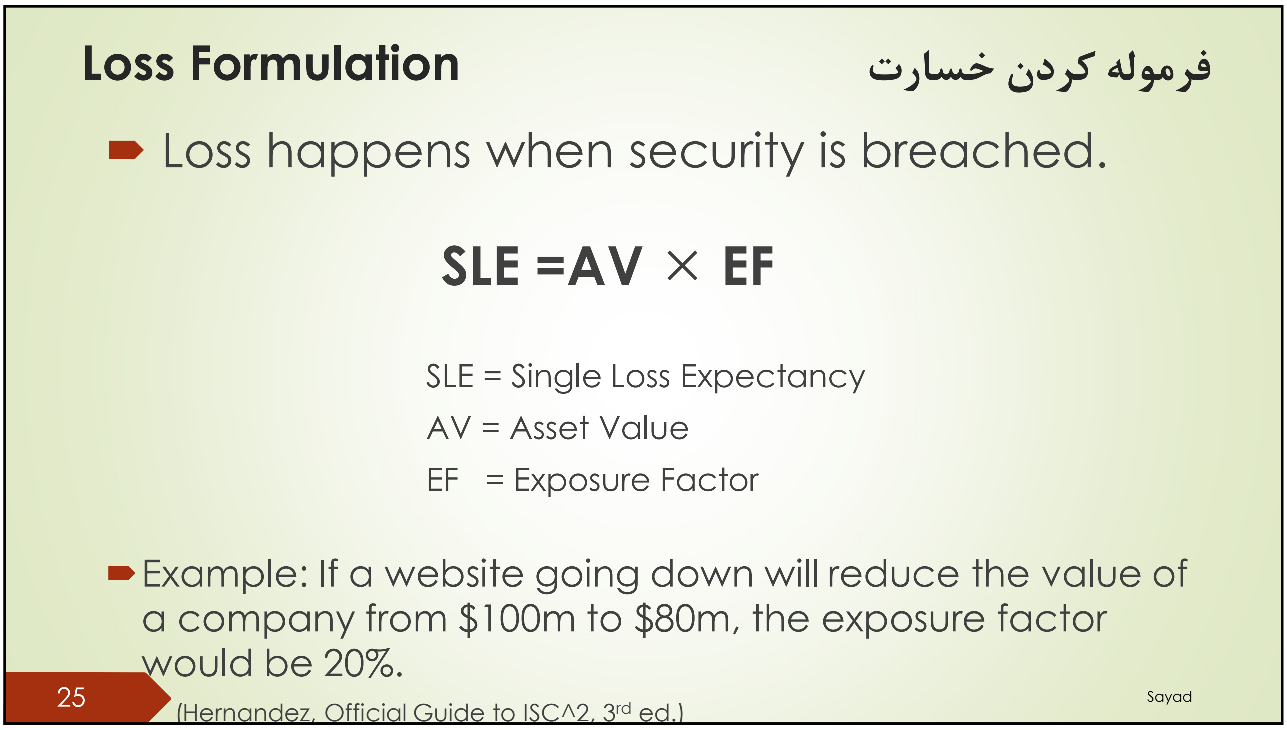
Risk Scale: High (>50 to 100) *Moderate (>10 to 50)* *Low (1 to 10)*

01527a

(Bowen, NIST 800-100, 2006)

24

Sayad



Loss Formulation فرموله کردن خسارت

- Loss happens when security is breached.

$$SLE = AV \times EF$$

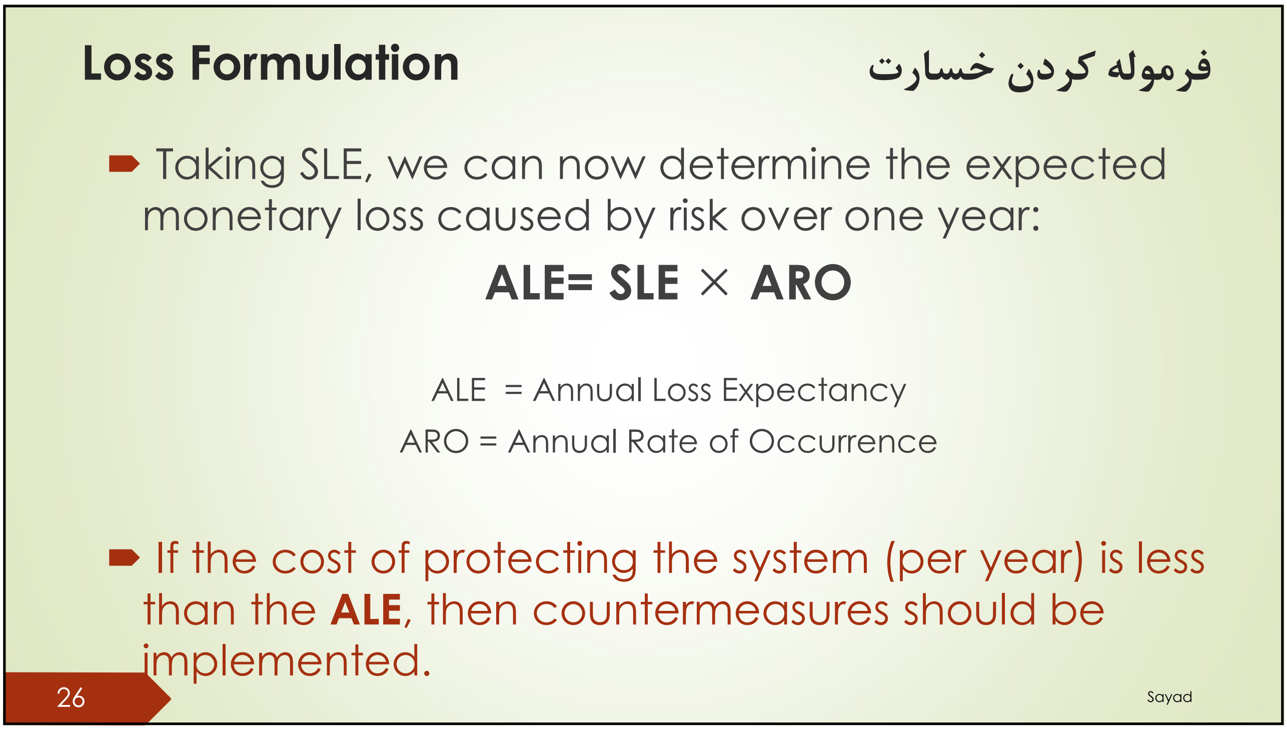
SLE = Single Loss Expectancy
AV = Asset Value
EF = Exposure Factor

- Example: If a website going down will reduce the value of a company from $100m to $80m, the exposure factor would be 20%.

(Hernandez, Official Guide to ISC^2, 3rd ed.)

25

Sayad



Loss Formulation فرموله کردن خسارت

- Taking SLE, we can now determine the expected monetary loss caused by risk over one year:

$$ALE = SLE \times ARO$$

ALE = Annual Loss Expectancy
ARO = Annual Rate of Occurrence

- If the cost of protecting the system (per year) is less than the **ALE**, then countermeasures should be implemented.

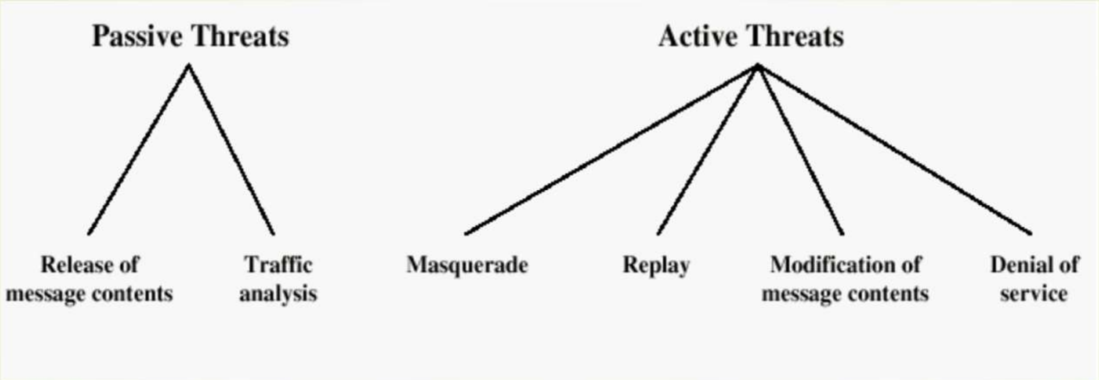
26

Sayad

دسته بندی حملات

Attacks Taxonomy

Attacks Taxonomy



Passive Threats

Release of message contents

Traffic analysis

Active Threats

Masquerade

Replay

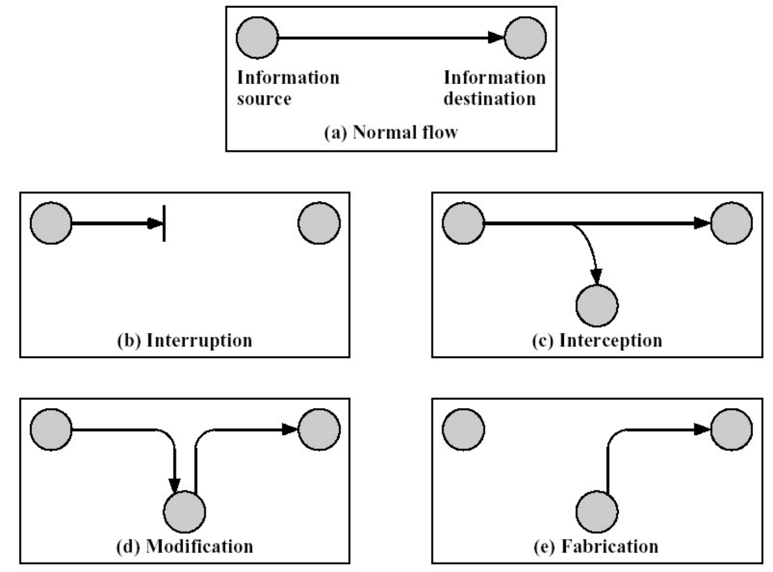
Modification of message contents

Denial of service

- There are many names and taxonomies in the market though they are the same in nature.
  - e.g. some call denial of service "interruption".

(Stallings, Network Security Essentials)

Attack Scenarios



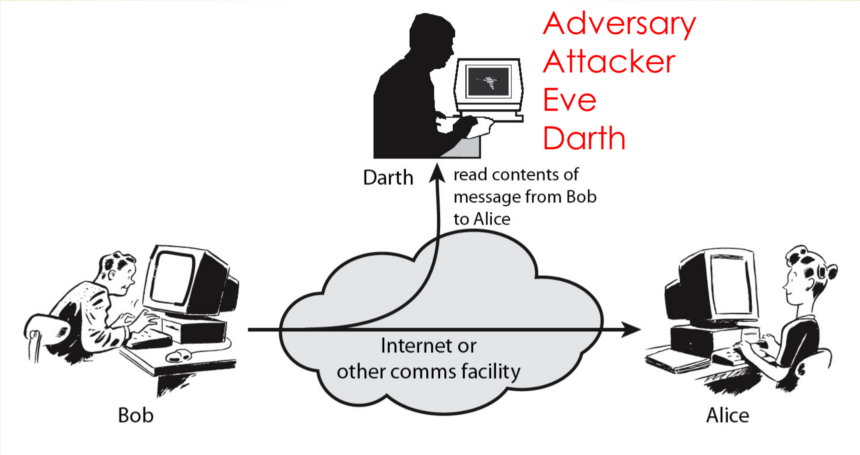
(Stallings, Network Security Essentials)

29

Sayad

Passive Attack – Interception (Eavesdropping)

- شنود یکی از حملات غیر تهاجمی است که به سختی آشکار سازی میشود. در روشهای نوین
(Quantum Cryptography) روی از بین بردن آن کار شده است.


Darth
read contents of message from Bob to Alice
Internet or other comms facility
Bob
Alice

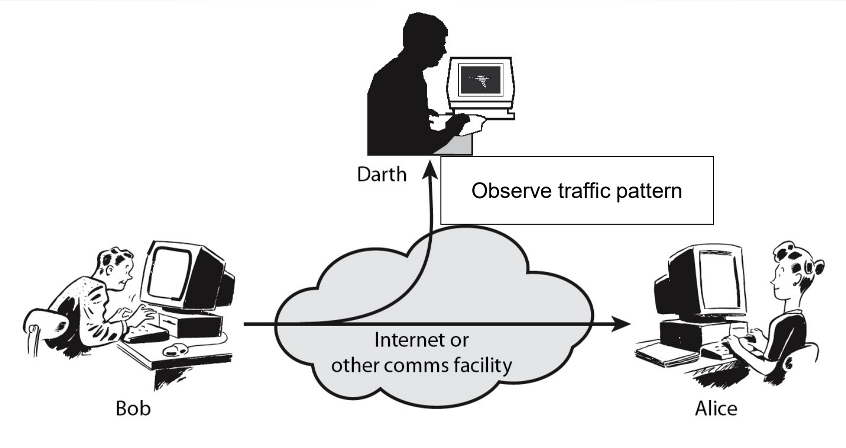
Adversary
Attacker
Eve
Darth

30

Sayad

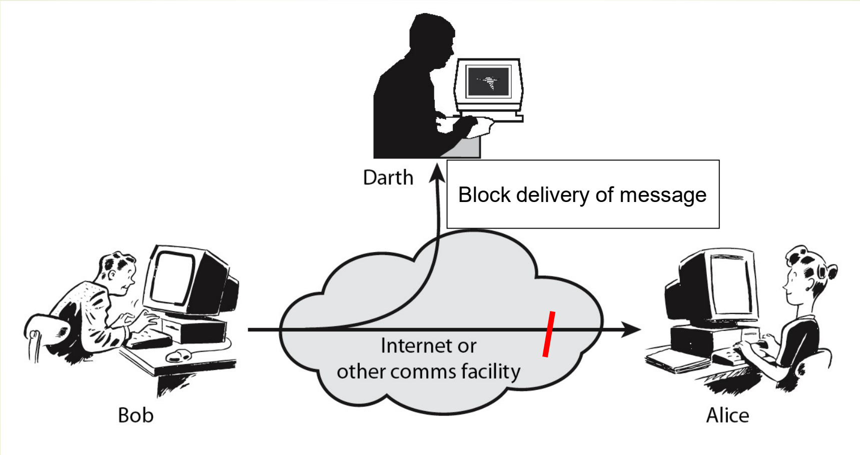
Passive Attack: Traffic Analysis

- در این حمله بیشتر از اطلاعات جنبی بدست آمده از مسیر ترافیک و ویژگیهای آن استفاده میشود. مثلا ترافیک به کجا میرود و یا جنس آن چیست.



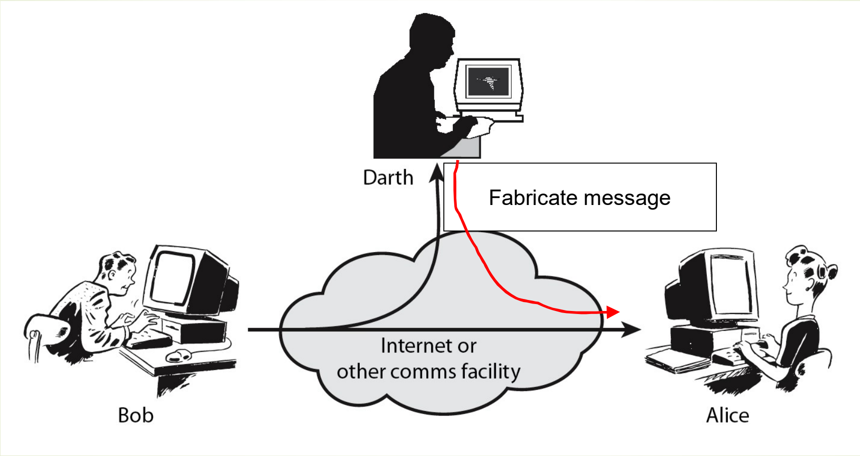
Active Attack: Interruption

- ایجاد وقفه در مخابره یکی از حملات فعال است. مثال حملات Denial of Service



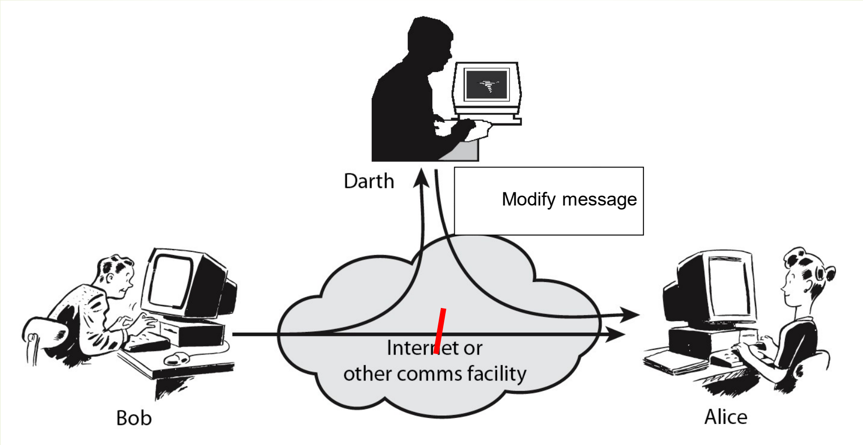
Active Attack: Fabrication

- جعل پیام از حملات فعال است. نمونه آن Replay Attack است.



Active Attack: Modification

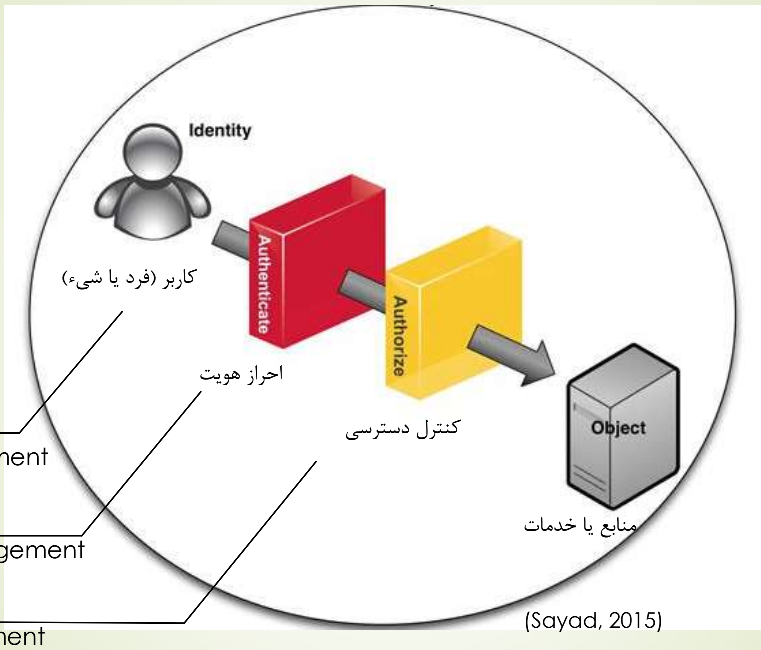
- تغییر پیام در حال تبادل نیز حمله فعال محسوب میشود.



مرز هویت، شناسه، احراز هویت و کنترل دسترسی

The boundaries of Identity, Identifier, Authentication and Access Control

Whole Problem Statement



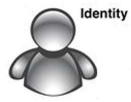
(Sayad, 2015)

مدیریت هویت
Identity Management

مدیریت اعتبارنامه
Credential Management

مدیریت دسترسی
Access Management

ID (شناسه)



دنیای واقعی

دنیای مجازی

هر مشخه و یا عدد یکتای
منتصب به شخص و یا شیء

کارت شناسائی ملی

شمارهٔ ملی: ۰۶۹_۳۲۷۶۹۸_۵

امیرحسین

پوردیلمی

۱۳۲۸ ۰۴ ۱۲

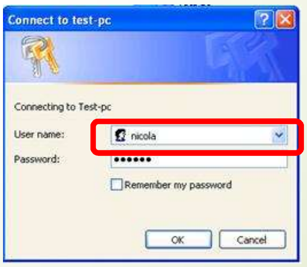
لاهیجان

۳۲۸

محمد جعفر

۱۳۷۸/۸/۱۱

نام کاربری


Connect to test-pc

Connecting to Test-pc

User name: nicola

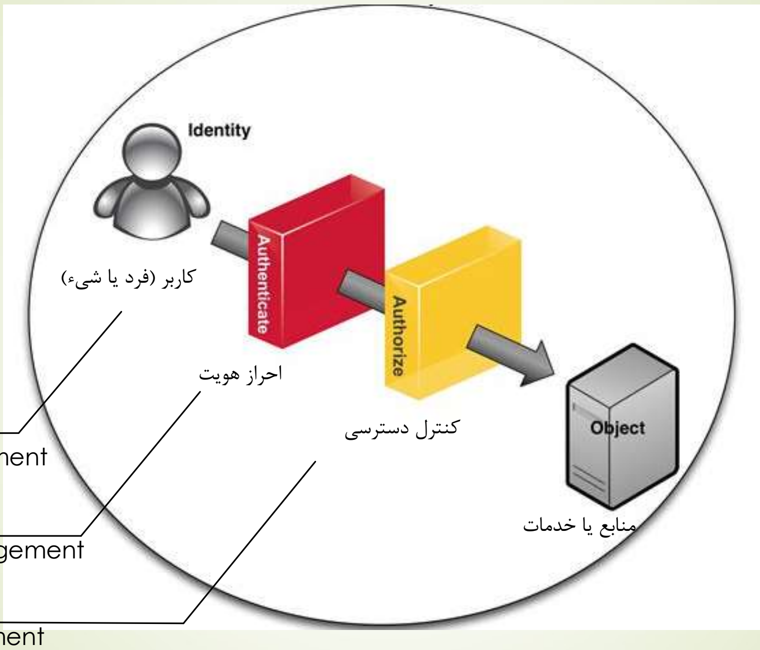
Password: ••••••

□ Remember my password

کد پرسنلی
#128340

بارکد

Whole Problem Statement



مدیریت هویت
Identity Management

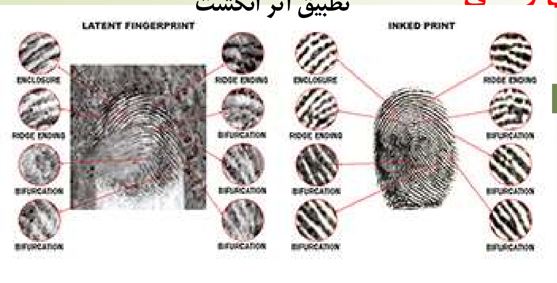
مدیریت اعتبارنامه
Credential Management

مدیریت دسترسی
Access Management

Authentication (احرازهویت)

دنیای واقعی

تطبیق اثر انگشت

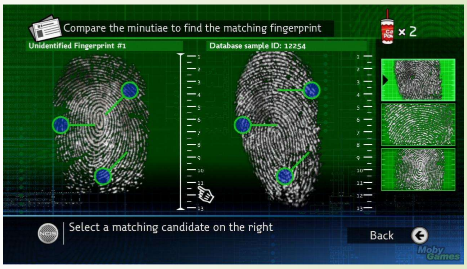


تطبیق چهره

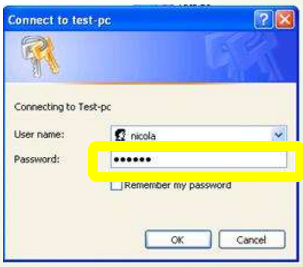
اسم شب،
رمز عملیات

دنیای مجازی

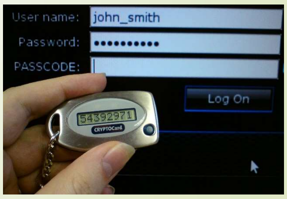
اثر انگشت بایومتریکی (چیزی که من هستم)


Compare the minutiae to find the matching fingerprint
× 2
Unidentified Fingerprint #1
Database sample ID: 12254
Select a matching candidate on the right
Back
Moby Games

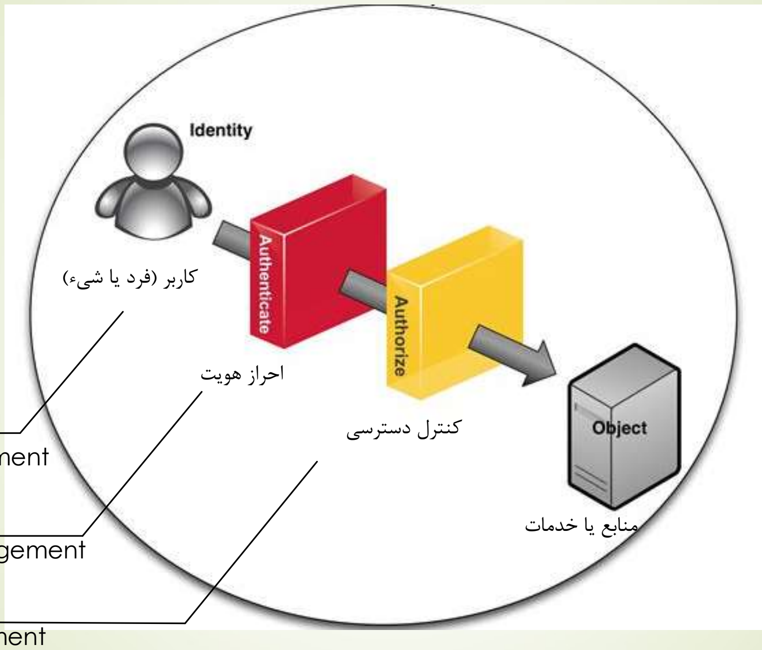
کلمه عبور (چیزی که من میدانم)



توکن یا کارت (چیزی که من دارم)



Whole Problem Statement



کاربر (فرد یا شیء)

احراز هویت

کنترل دسترسی

منابع یا خدمات

مدیریت هویت
Identity Management

مدیریت اعتبارنامه
Credential Management

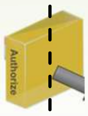
مدیریت دسترسی
Access Management

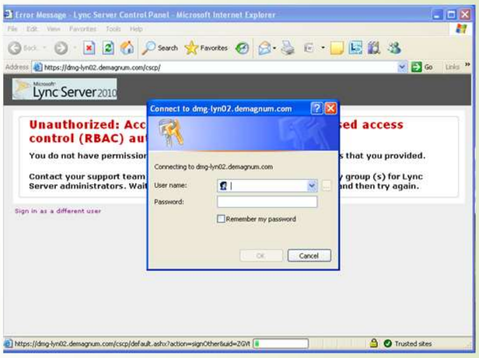
Authorization (مجوز دسترسی) کنترل دسترسی

کلید در (کلید، مجوز دسترسی است)

دنیای واقعی

دنیای مجازی





Error Message - Lync Server Control Panel - Microsoft Internet Explorer

https://dmg-lyn02.demagnum.com/cscp/

Unauthorized: Acc… …ed access control (RBAC) au…

You do not have permissio… …s that you provided.

Contact your support team … …y group (s) for Lync Server administrators. Wai… …nd then try again.

Sign in as a different user

Connect to dmg-lyn02.demagnum.com

Connecting to dmg-lyn02.demagnum.com

User name:

Password:

□ Remember my password

https://dmg-lyn02.demagnum.com/cscp/default.ashx?action=signOther&uid=ZGVt

دسترسی به حسابهای بانکی،
انتقال وجه و …

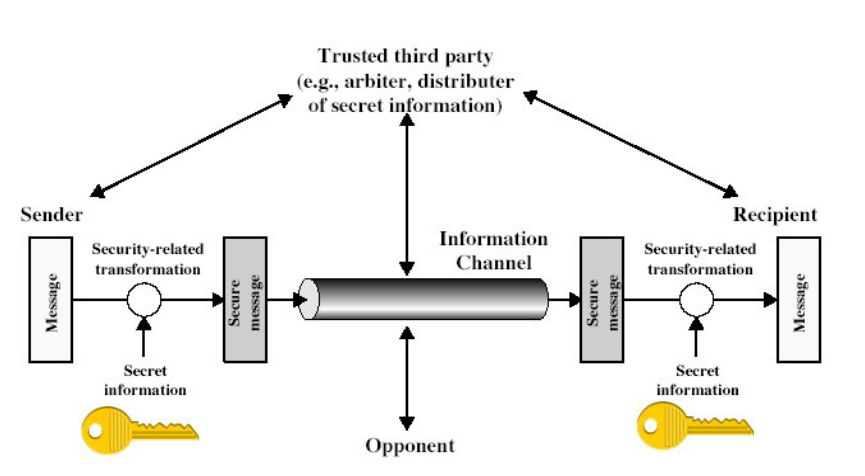
طبقه بندی اسناد

مدلهای پیشنهادی تامین امنیت (شبکه و دسترسی)

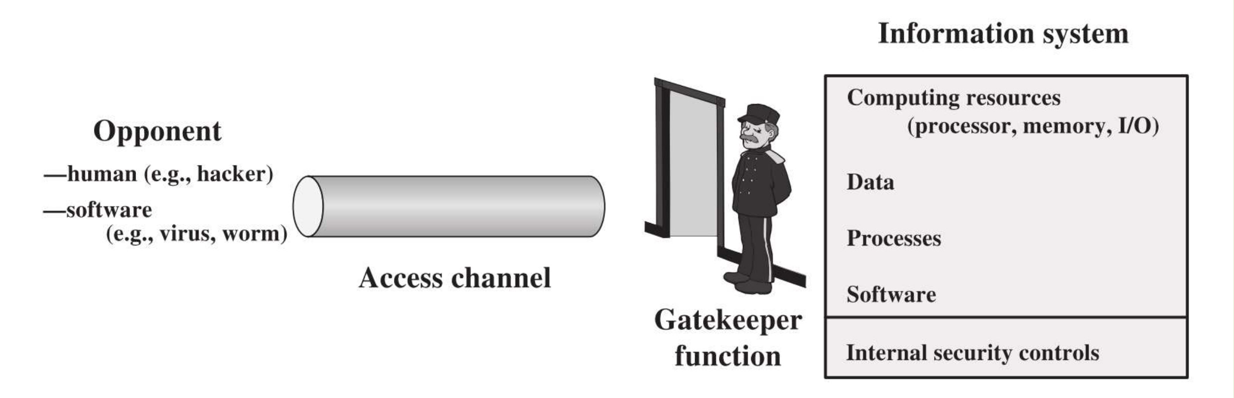
Stallings' Security Provisioning Model

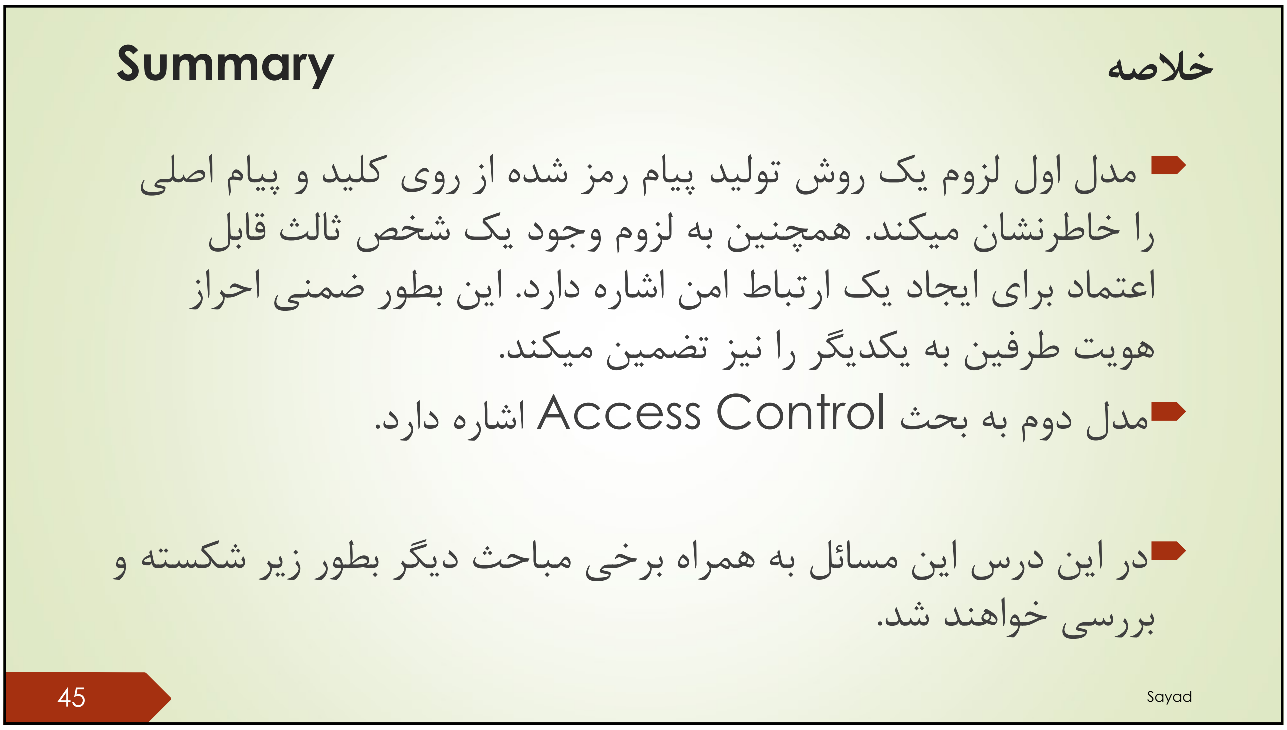
مدل تامین امنیت شبکه (امنیت تبادل داده)

- مدل کلی تامین امنیت ارتباطات چنین است. البته این مدل به تنهایی نمیتواند همه مسائل امنیت را پوشش دهد. برای مثال مشکلات Privacy ناشی از Traffic Analysis با چنین مدلی حل نمیشود.



مدل تامین امنیت دسترسی به یک سیستم کامپیوتری





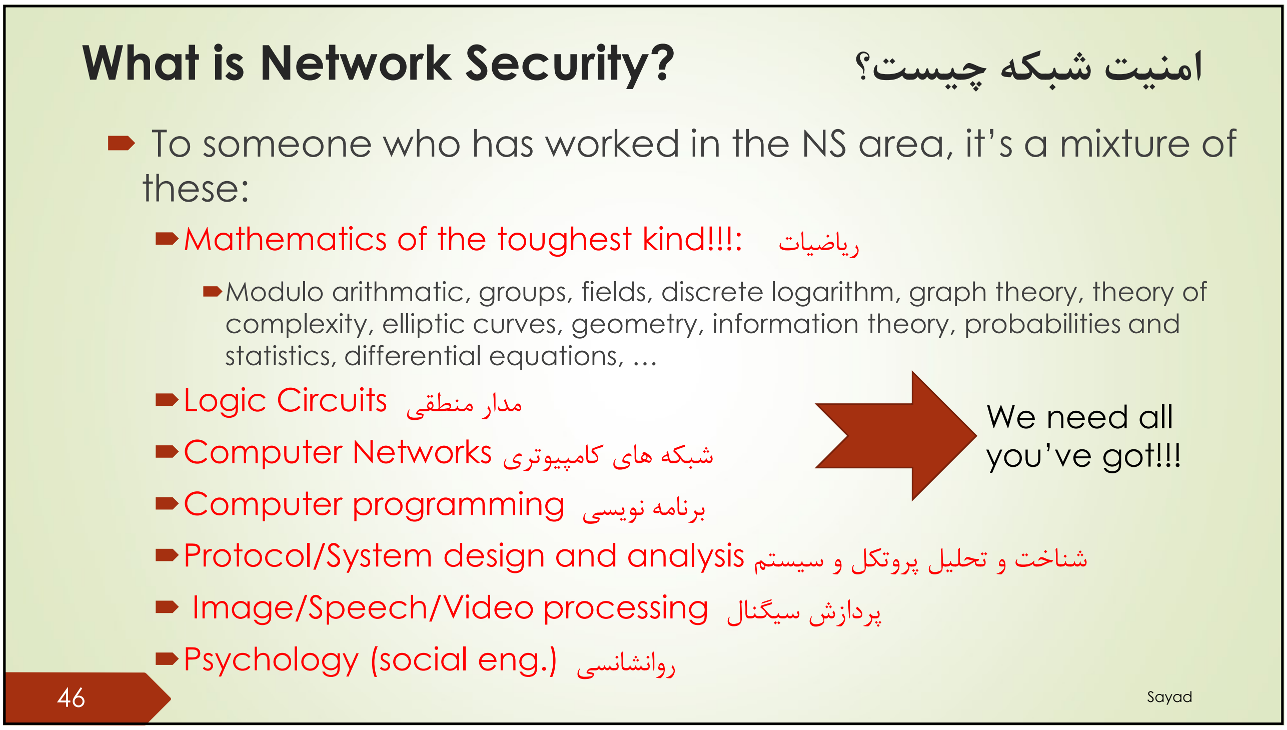
Summary خلاصه

- مدل اول لزوم یک روش تولید پیام رمز شده از روی کلید و پیام اصلی را خاطرنشان میکند. همچنین به لزوم وجود یک شخص ثالث قابل اعتماد برای ایجاد یک ارتباط امن اشاره دارد. این بطور ضمنی احراز هویت طرفین به یکدیگر را نیز تضمین میکند.
- مدل دوم به بحث Access Control اشاره دارد.

- در این درس این مسائل به همراه برخی مباحث دیگر بطور زیر شکسته و بررسی خواهند شد.

45

Sayad



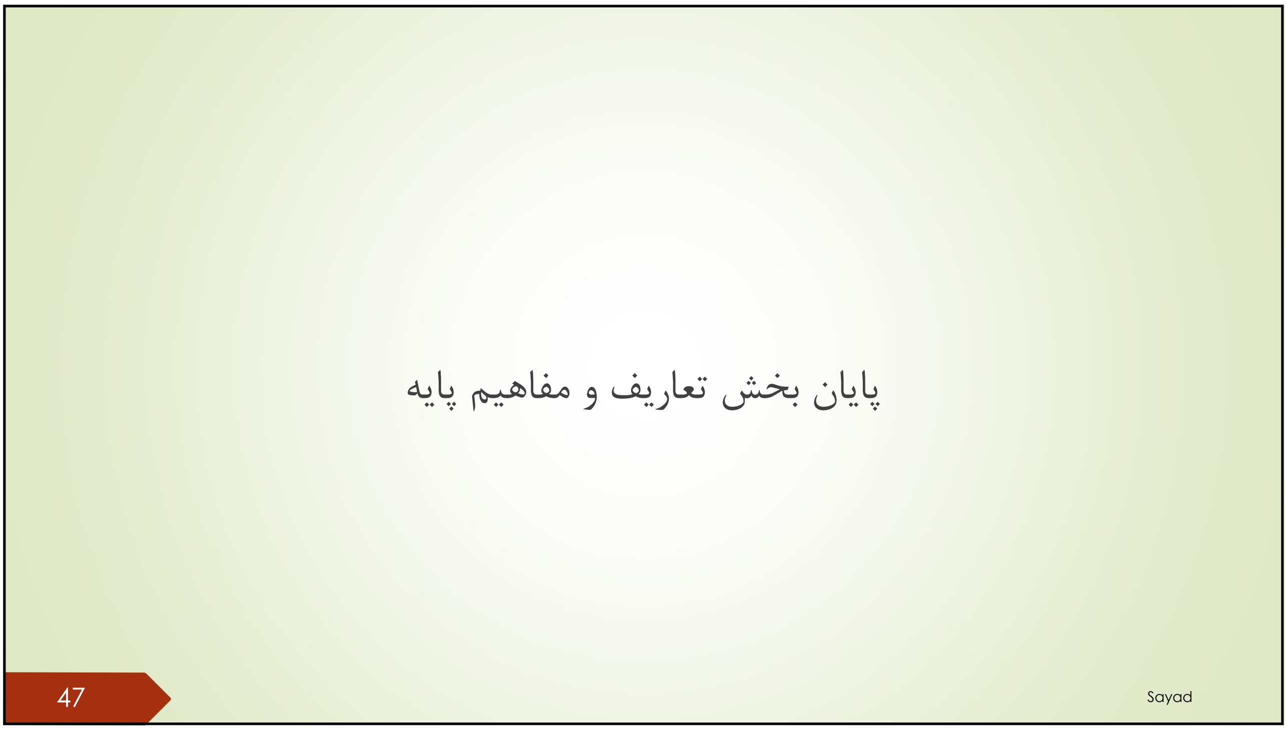
What is Network Security? امنیت شبکه چیست؟

- To someone who has worked in the NS area, it's a mixture of these:
  - Mathematics of the toughest kind!!!: ریاضیات
    - Modulo arithmatic, groups, fields, discrete logarithm, graph theory, theory of complexity, elliptic curves, geometry, information theory, probabilities and statistics, differential equations, …
  - Logic Circuits مدار منطقی
  - Computer Networks شبکه های کامپیوتری
  - Computer programming برنامه نویسی
  - Protocol/System design and analysis شناخت و تحلیل پروتکل و سیستم
  - Image/Speech/Video processing پردازش سیگنال
  - Psychology (social eng.) روانشناسی

We need all you've got!!!

46

Sayad



پایان بخش تعاریف و مفاهیم پایه

47

Sayad