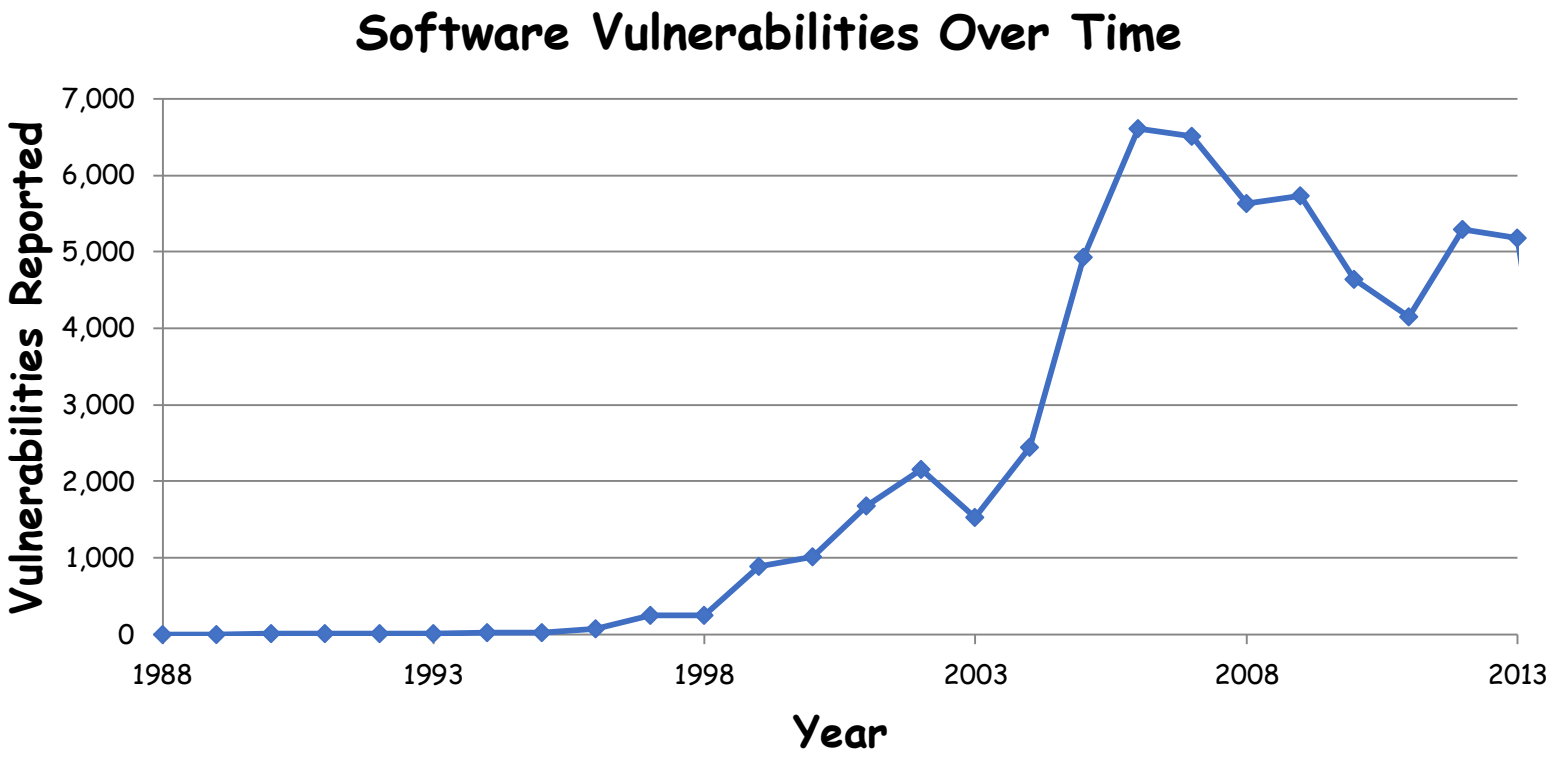
Introduction to Security

Outline

1. Single Page Application (SPA) Architecture
2. Web and HTTP
3. Web API
4. Web API using Node.js Express

Vulnerabilities Growing



Source: National Vulnerability Database
https://web.nvd.nist.gov/view/vuln/statistics

Qatar News Agency hacked…

BBC Sign in News Sport Weather Shop Earth Travel More

NEWS

Home Video World UK Business Tech Science Stories Entertainment & Arts H

World Africa Asia Australia Europe Latin America Middle East US & Canada

Qatar says state news agency hacked after report cites emir criticising US

24 May 2017 Share

Donald Trump urged Qatar's emir and other Arab leaders on Sunday to "isolate" Iran

Qatar has blamed hackers for a story on its state news agency website that quoted the emir as criticising US "hostility" towards Iran.

On Tuesday, the Qatar News Agency (QNA) quoted Sheikh Tamim Al Thani as

Personal Data

BBC

News | Sport | Weather | Capital | Future | Shop

NEWS

Home | UK

10 January 2

Targe
custo

The cyber-thie

US retail gia
card and pe
December -

Target said t
addresses, p

The data bre
Friday, one c

The company said customers would have "zero liability" for any fraud losses.

Payment card data theft jumps five-fold

5:22 PM, Jan 2

英文中國郵報
The China Post

News | Opinion | Taiwan Living | Learn English | The China Post | Subscribe | RSS Feeds

Asia

REGIONAL | China | Australia | India | Indonesia | Japan | Korea | Malaysia | New Zealand | Pakistan

Angry South Koreans flood banks after data leak affects 20 million

AFP
January 22, 2014, 12:13 am TWN

Print | Email | Share

SEOUL--Tens of thousands of South Koreans flooded banks and call centers Tuesday to cancel credit cards following the unprecedented theft of the personal data of at least 20 million people.

Foreign Governments

theguardian

News | Sport | Com

News › UK news

GCHQ taps
access to wo

Exclusive: British s
of global email mes
calls, and shares th
Snowden reveal

Follow The NSA File

Ewen MacAskill, Julian E
The Guardian, Friday 21 .

Jump to comments (3

EDITION: INTERNATIONAL | U.S. | MÉXICO | ARABIC

TV: CNNi | CNN en Español

Set edition preference

Home | Video | World | U.S. | Africa | Asia

NSA hacks China, le

By **Jethro Mullen** and **Chelsea J. Carter**, CNN
June 13, 2013 -- Updated 0932 GMT (1732 HKT)

Notable leakers and whi

<< < 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 > >>

BBC News Sport Weather Capital Future Sho

NEWS TECHNOLOGY

Home | UK | Africa | Asia | Europe | Latin America | Mid-East | US & Canada | Business | Health | Sci/Enviro

13 July 2012 Last updated at 23:01 GMT

Share

Viewpoint: Stuxnet shifts the cyber arms race up a gear

Mikko Hypponen
Chief research officer, F-Secure

Governments are busy developing secret weapons in preparation for any potential cyber conflict, Mikko Hypponen says

Regional Industry

The A

Data Centre Software N

SECURITY

Hack on Sa
oil firm adm

First hacktivist-

By John Leyden, 29th Au

4

Analy
days a

In a st
intern
firm sa
attack
of a fe
also s

RELATED STORIES

No woman, no drive: Saddo hackers lob Android nasty at Saudi women's

REUTERS EDITION: IN SIGN IN

HOME BUSINESS MARKETS IN

UPDATE 1-Qata
computer virus

Thu Aug 30, 2012 7:59pm IST

0 COMMENTS Link t

(Adds background, comment)

By Daniel Fineren

Aug 30 (Reuters) - Qatar's Rasgas h
world's second-biggest liquefied natu
weeks after the world's biggest oil pr

"The company's office computers ha
identified on Monday," Rasgas, one

Corp. [US] | https://www.bankinfosecurity.com/qatar-national-bank-suffers-massive-breach-a-9068

Ikea AC Stool Reg. Forms CQAC Save to Mendeley City Hotel Duqm, Om QU ClassRooms Lib

Qatar National Bank Suffers Massive Breach

Customer Details, Card Data Apparently Leaked Online

Varun Haran (APACinfosec) • April 26, 2016 0 Comments

Twitter Facebook LinkedIn Credit Eligible Get Permission

What is Security?

- Oxford Dictionary Definition:
  The state of being free from danger or threat

Real-World Security

- Protecting valuable things
  - Physical stuff (money, jewelry, cars, etc.)
  - People
  - Access to somewhere (parking?)

- We think of an item as secure if no one can take it, harm it, or use it without our permission.

Computer Security

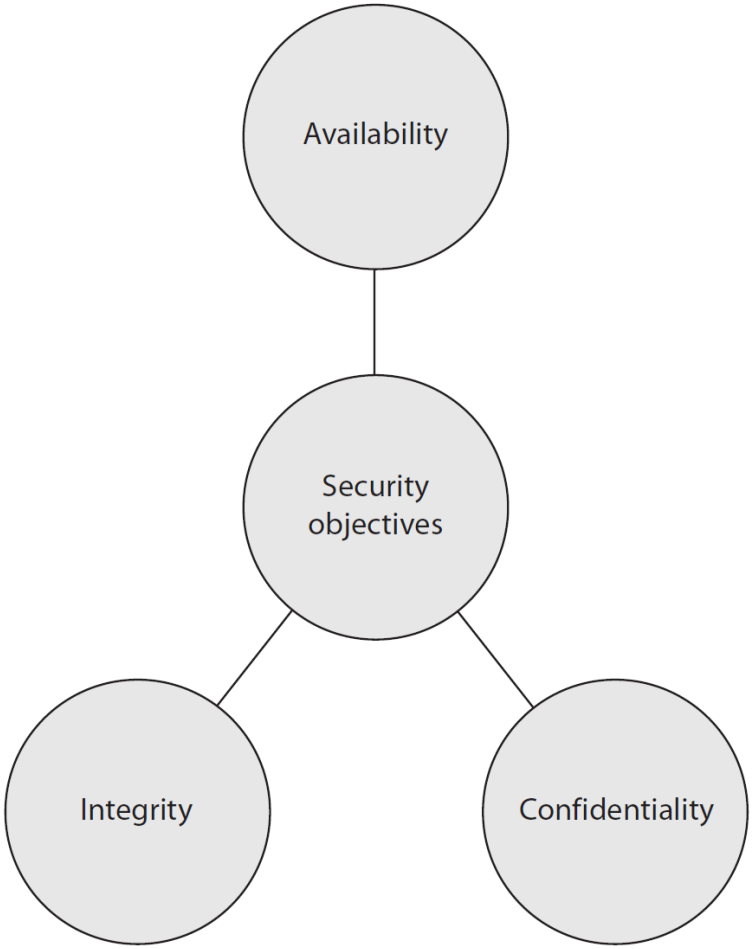
- Only one type of digital asset: *Information*

- Protecting information is hard
  - Stored on small, portable devices
  - Can be accessed electronically

- The internet has made this even harder

Core Goals of Security

Also known as **CIA Triad**



Three Security Properties

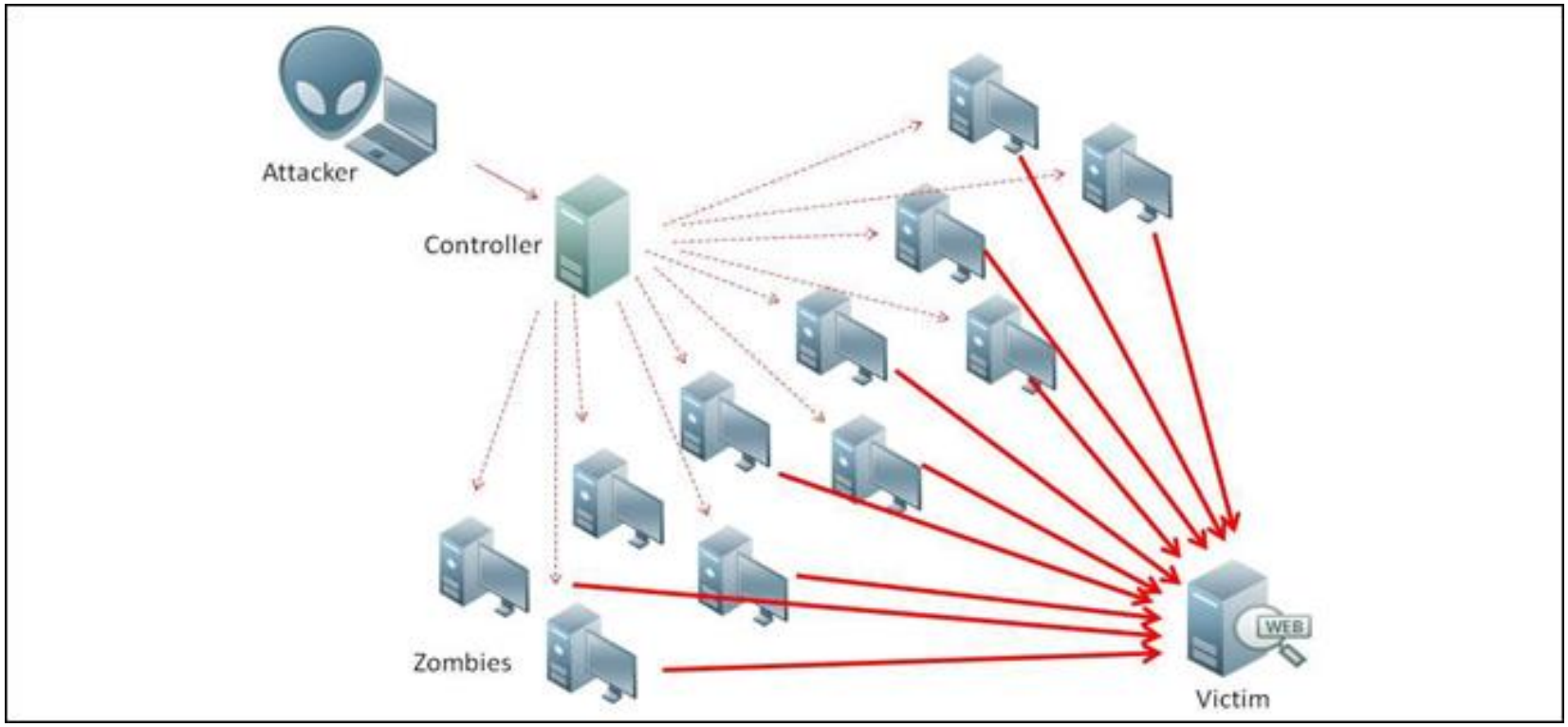
1. Confidentiality
   - Prevent unauthorized reading of data
2. Integrity
   - Prevent unauthorized modification of data
3. Availability
   - Ensure data is available to authorized people

How to achieve security goals?

- Understand the adversary.
  - what are the resources available?
  - what is the goal of the attack?
- Understand the modes of attack.
  - in what ways can the attack be launched?
  - what are the vulnerabilities?
- Understand the security/usability tradeoff.

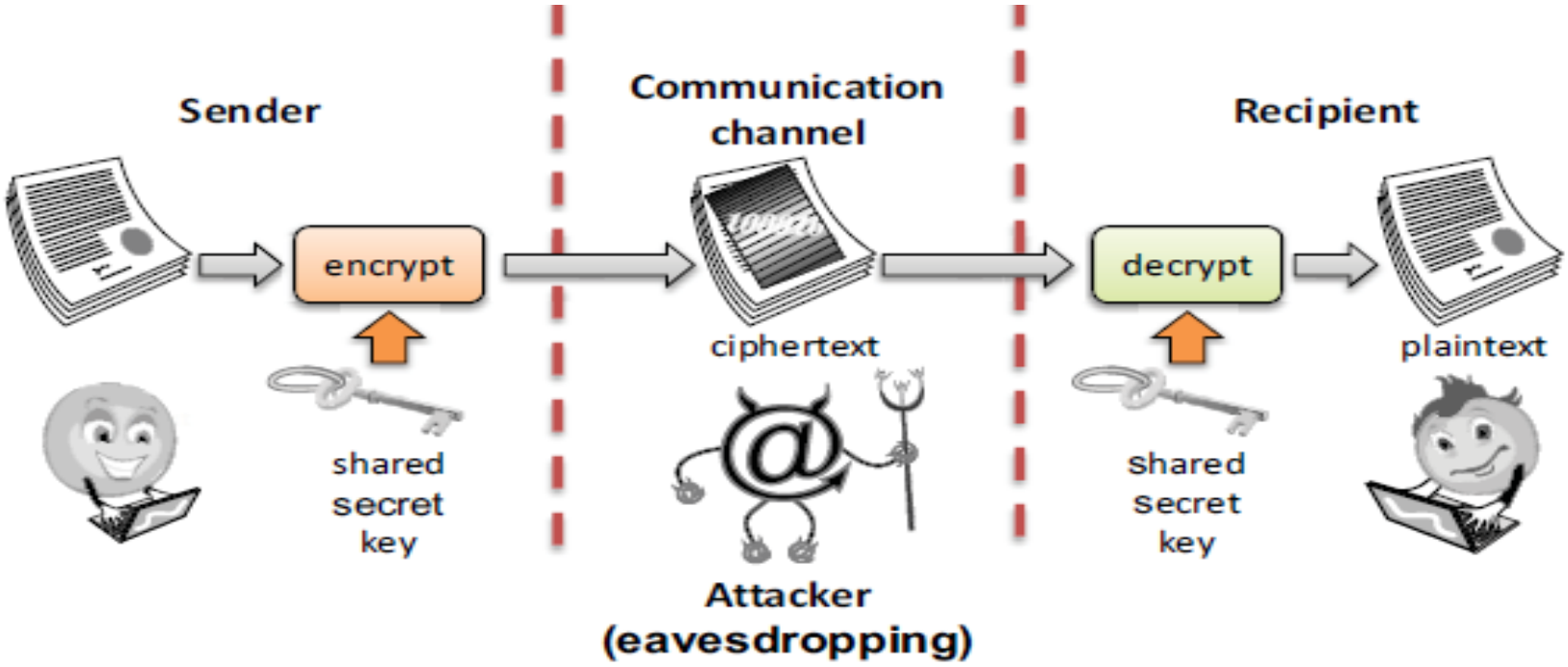
Attack Scenario of Availability

- Denial of Service: Possible to overwhelm Online Services, making them unavailable



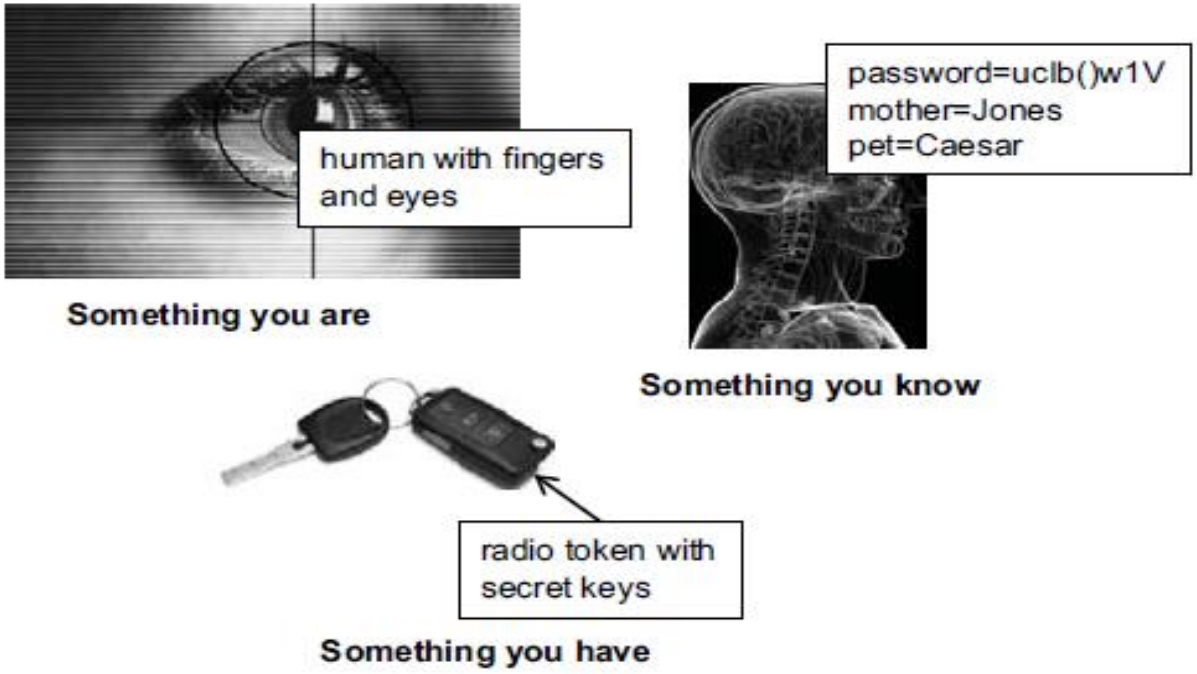
Tools for confidentiality (1/3)

- **Encryption**: encrypt data using an encryption key



Tools for confidentiality (2/3)

- **Authentication:** determination of the identity or role that someone has.
  - Fingerprint, password, smart card / radio key,



Tools for confidentiality (3/3)

- **Access Control:** rules and policies that limit access to confidential information to those with a permission .

- **Authorization:** determination if a person or a system is allowed access to resources, based on an access control policy.

Tools for integrity

- Prevention Mechanisms
  - Access controls
  - Authentication
- Detection Mechanisms
  - Message signing: cryptographic technique to detect whether bits have been modified
  - Intrusion detection and prevention: try and understand normal behavior and detect anomalous
  - Monitors the characteristics of a single host for suspicious activity
  - Monitors network traffic and analyzes network, transport, and application protocols to identify suspicious activity
    - *Deep packet inspection:* look at packet contents (e.g., check character strings in packet against database of known virus, attack strings)

Tools for availability

- Redundancies
  - e.g., backup, multiple mail/DNS/DHCP servers, multiple network paths to ISP
- Firewall
  - isolates organization's internal net from larger Internet, allowing some packets to pass, blocking others
- Intrusion prevention

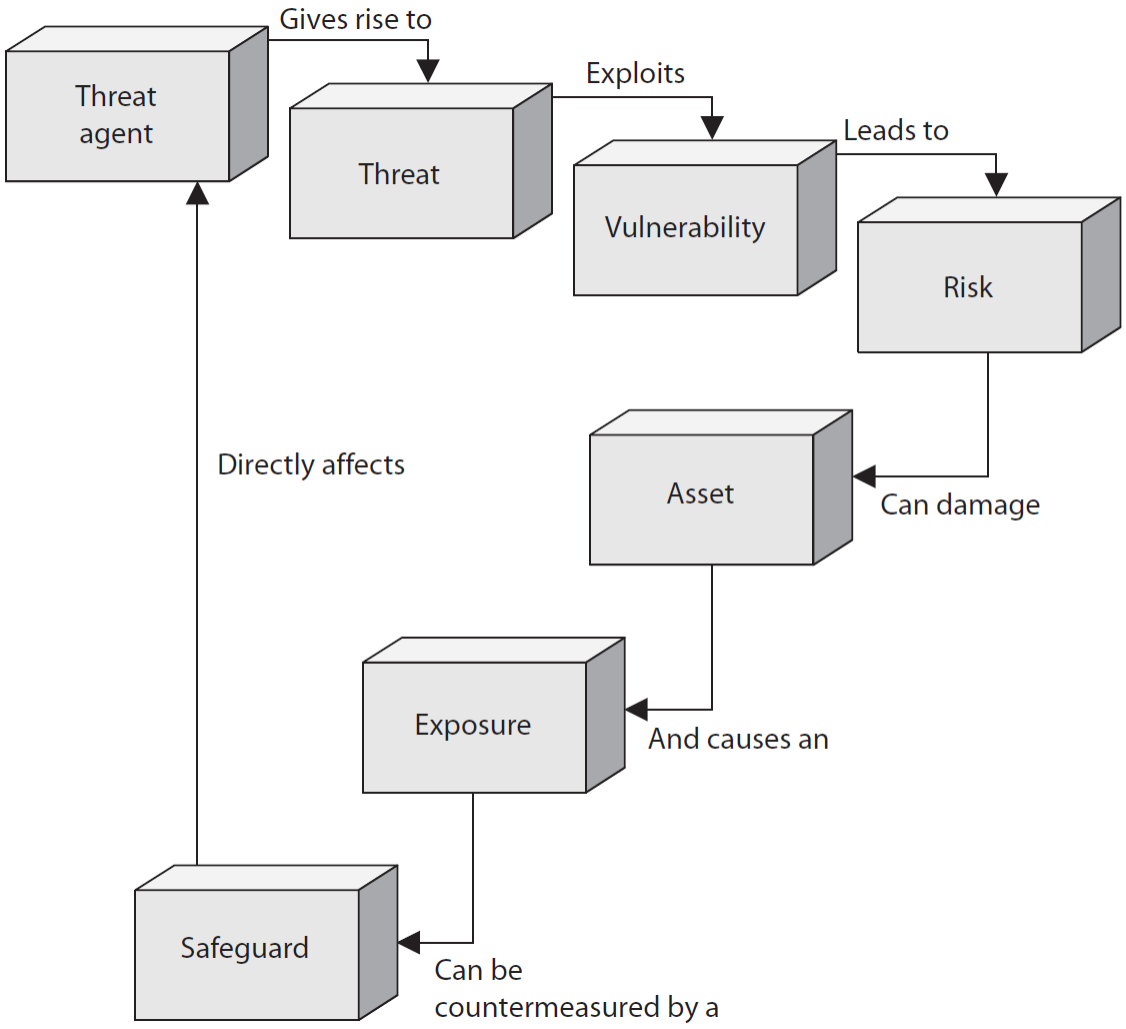
Tools to achieving CIA

- Confidentiality
  - Encryption
  - Access Control
  - Authorization
- Integrity
  - Prevention Mechanisms
  - Detection Mechanisms
- Availability
  - Redundancy
  - Intrusion Detection/Prevention

Exercise

- Classify each of the following as a violation of confidentiality, of integrity, of availability, or of some combination
  - Ali logs into Fatima's Facebook, posts a photo
  - Steve sees network traffic of Apple's earning projections and sells Apple stock
  - Jenny forges a request to Banner to change her Computer Security homework grade
  - Ali Taleh causes the power system to fail, taking the submission server offline

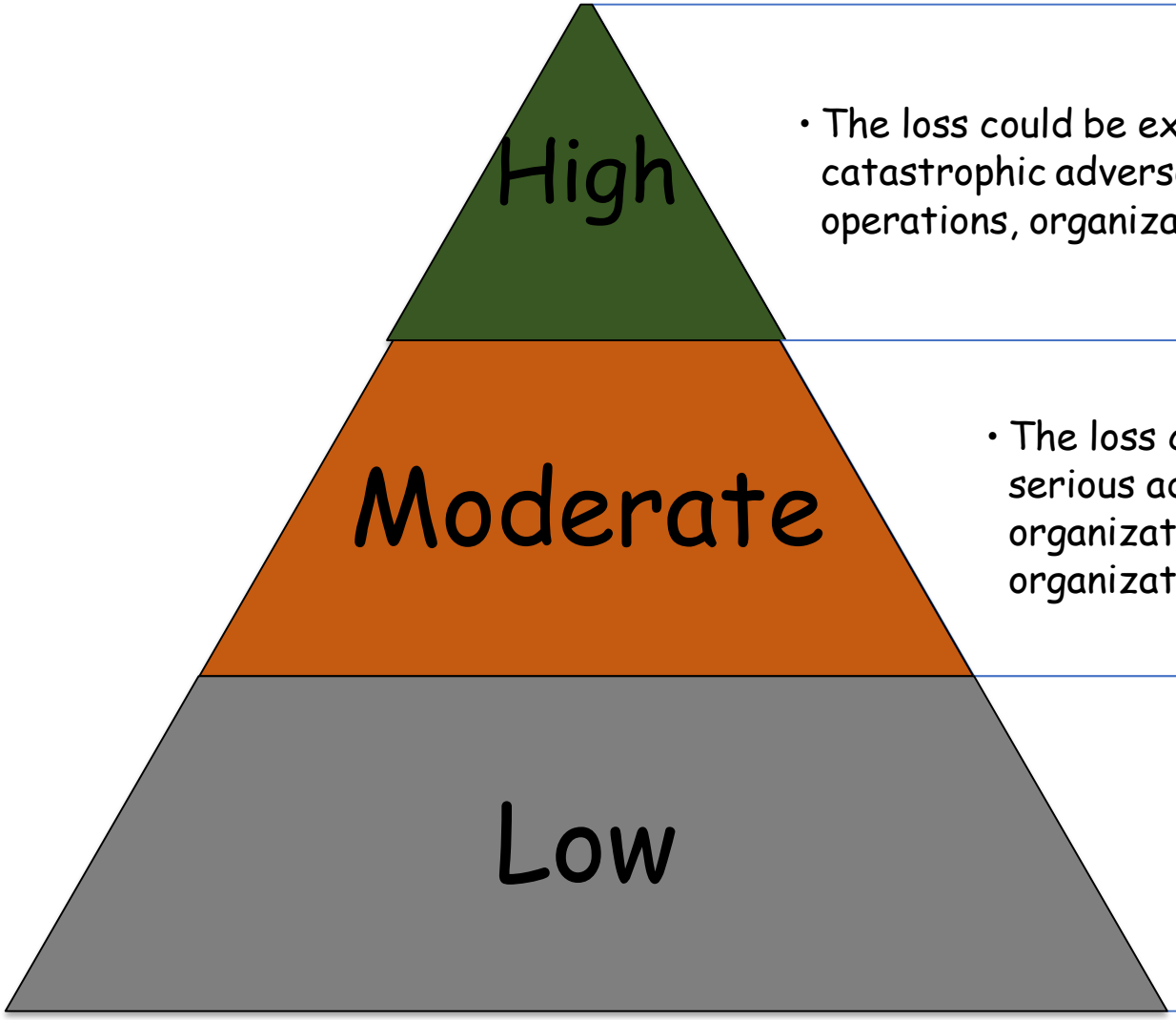
The relationships among the different security concepts



Security Concepts

- A **vulnerability** is a weakness in a system that allows a threat source to compromise its security.
  - e.g., unpatched applications or OS, an unrestricted wireless access point
- A ***threat*** is any potential danger that is associated with the exploitation of a vulnerability.
- A ***risk*** is the likelihood of a threat source exploiting a vulnerability.
  - e.g., if a firewall has several ports open, there is a higher likelihood that an intruder will use one to access the network in an unauthorized method.
- An ***exposure*** is an instance of being exposed to losses. A vulnerability exposes an organization to possible damages.
  - e.g., if strong password rules are not enforced, the company is exposed to the possibility of having users' passwords compromised and used in an unauthorized manner
- A ***control***, countermeasure or safeguard, is put into place to mitigate (reduce) the potential risk.
  - e.g., strong password management, firewalls, Intrusion Detection System, access control mechanisms, encryption, and security-awareness training.

Breach of Security - Levels of Impact



- The loss could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals

- The loss could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals

- The loss could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals

Summing Up

- Attacks are growing
- They affect real people
- Three main properties in computer security:
  - Confidentiality
  - Integrity
  - Availability
- A system is as secure as its weakest component
  - Partly why security so hard: attacker just needs to find the weakest link

Resources

- SecTools.Org: Top 125 Network Security Tools

http://sectools.org/

- A collection of awesome penetration testing resources and tools
  - https://github.com/enaqx/awesome-pentest

- SANS Penetration Testing Blog

https://pen-testing.sans.org/blog