Introduction to Security

Outline

1. Are cyberattacks reals?

2. What is Security?

3. Core Goals of Security (CIA Triad)

4. Security concepts: Treat, Vulnerability, Risk and Controls

Are cyberattacks reals?

- Is it possible to break-in my laptop ?

- Is it possible to hack my WiFi ?

- What about my Facebook account ?

- **This actually already happened [1]**
  - Ebay, 145M accounts, 2014
  - Yahoo, 500M accounts, 2014
  - British Airways, 500K accounts, 2015
  - Invest Bank, 40K accounts, 2016
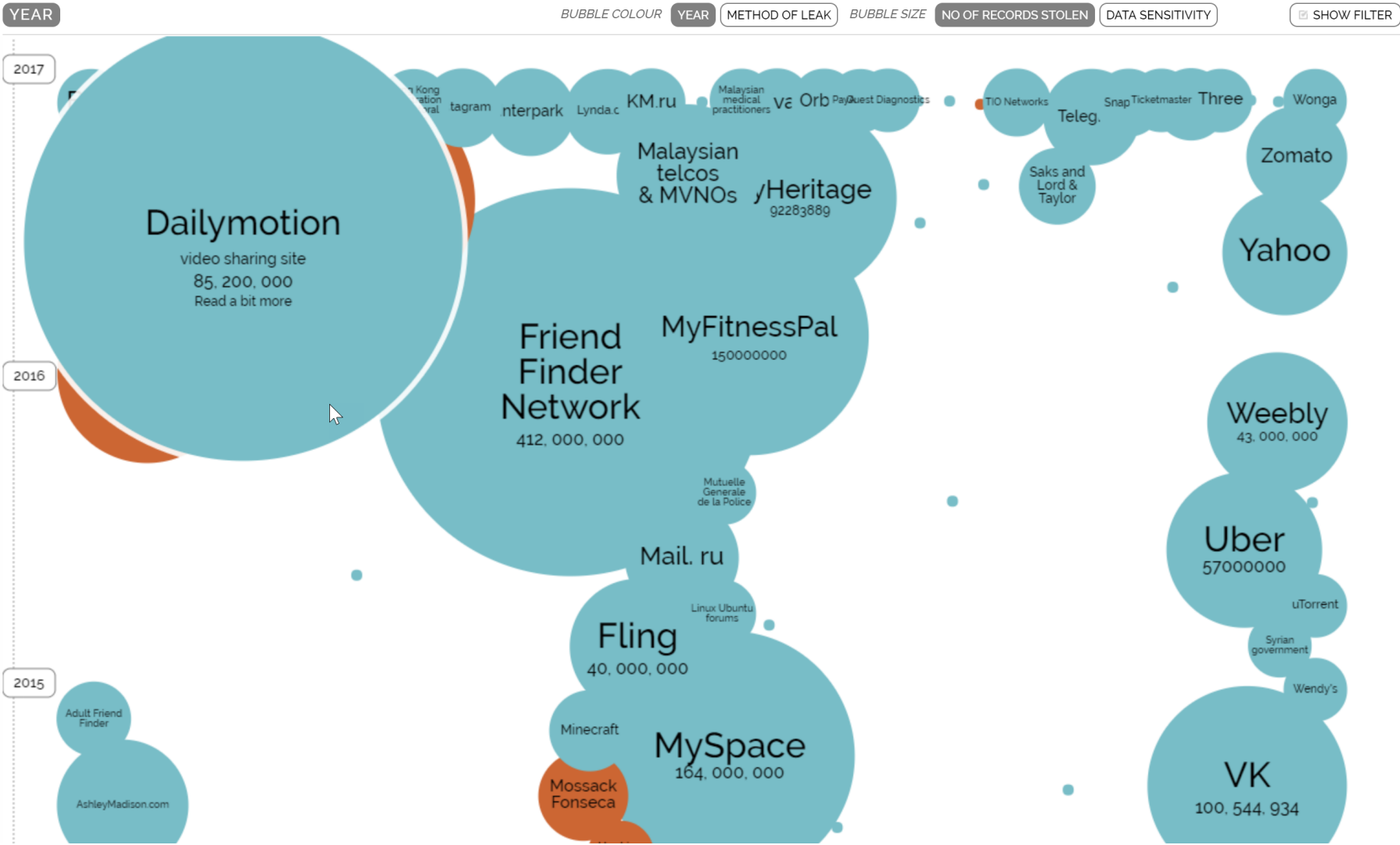 - QNB, 100K accounts, 2016

[1] http://informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

World's Biggest Data Breaches

Selected losses greater than 30,000 records
(updated 23rd Aug 2018)

interesting story

| YEAR | BUBBLE COLOUR | YEAR | METHOD OF LEAK | BUBBLE SIZE | NO OF RECORDS STOLEN | DATA SENSITIVITY | ☑ SHOW FILTER |

2017

tagram · nterpark · Lynda.c · KM.ru · Malaysian medical practitioners · vɛ · Orb · PayQuest Diagnostics · TIO Networks · Snap · Ticketmaster · Three · Wonga

Malaysian telcos & MVNOs · yHeritage 92283889 · Teleg. · Saks and Lord & Taylor

Zomato

Dailymotion
video sharing site
85, 200, 000
Read a bit more

Yahoo

MyFitnessPal
150000000

Friend Finder Network
412, 000, 000

Weebly
43, 000, 000

Mutuelle Generale de la Police

2016

Mail. ru

Uber
57000000

uTorrent

Linux Ubuntu forums

Fling
40, 000, 000

Syrian government

2015

Minecraft

Wendy's

Adult Friend Finder

MySpace
164, 000, 000

Mossack Fonseca

VK
100, 544, 934

AshleyMadison.com

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   f ● y ✉ < 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

5

Personal Data

BBC NEWS

Home UK

10 January 2014

Target customers

The cyber-thie

US retail gia card and pe December -

Target said t addresses, p

The data bre Friday, one o

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 B
The Guardian, Friday 21 J
💬 Jump to comments (34

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 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 | f | 🐦 | ✉ | 🖨

Viewpoint: Stuxnet shifts the cyber arms race up a gear

Mikko Hypponen
Chief research officer, F-Secure

THINKSTOCK

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...

RELATED STORIES

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

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?

- Security = protection from harm

- 3 main categories of harm:
  - **Theft of information** (e.g., corporate secrets, personal information, military intelligence)
  - **Alteration of information** (e.g., break in and deface a website, alter DB records to cover-up fraud).
  - **Denial of Service (DoS)** – system busy responding to attackers and no longer available to provide serve to legitime users

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: *Data*

- Protecting data is hard
  - Our data is stored and spread everywhere (PC, Laptop, Smartphones, Online services …)
  - Can be accessed electronically

- The internet has made this even harder

Who are the attackers?

- Script-kiddies
- Scammers, crooks
- Cyber-spies
- Insiders
- Cyber-hactivists
- Organized crime: Cyber-Mafia
- Secret agencies

Full underground economy based on cyber-crime: cybercrime as a service

Core Goals of Security

Also known as **CIA Triad**
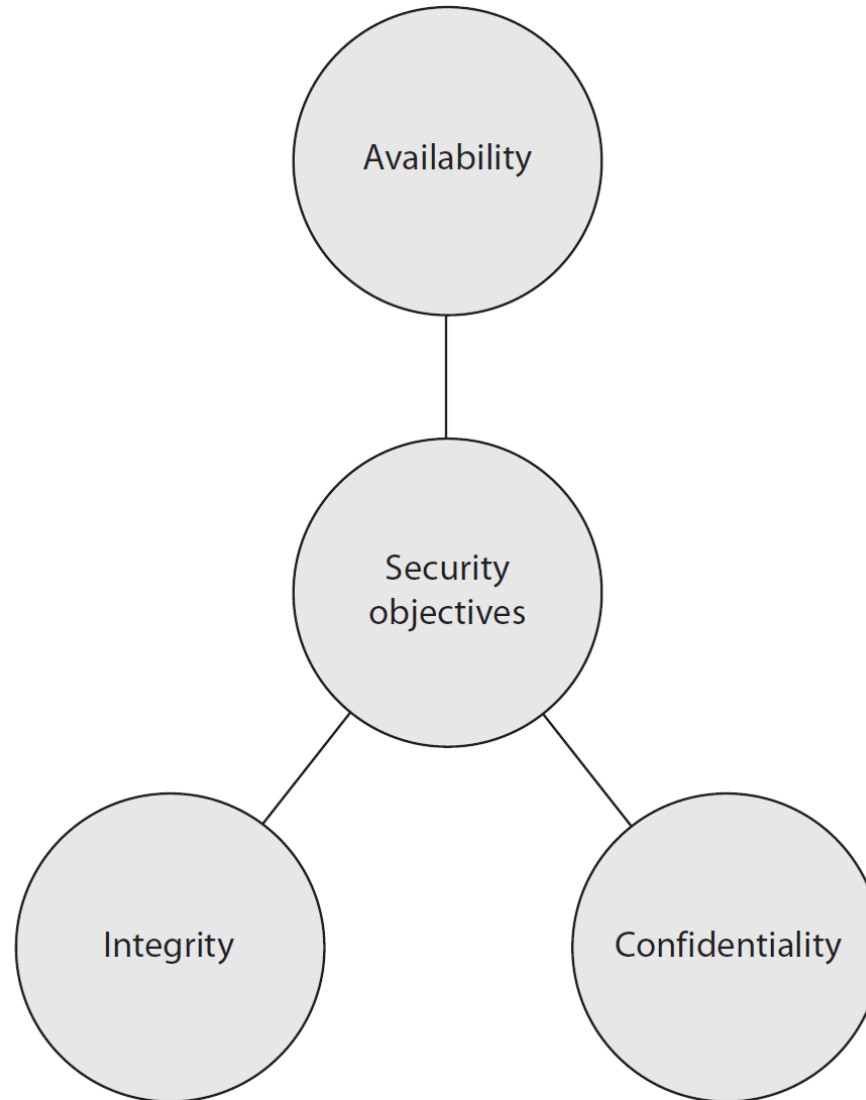
Three Security Properties

1. Confidentiality
   o Prevent unauthorized reading of confidential data

2. Integrity
   o Prevent unauthorized/malicious modification of data

3. Availability
   o Ensure data is available to authorized people
   o Systems remain operational, reachable, functional and available for legitimate users

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

About the adversary

- The adversary can be either **active** or **passive.**

Active:

- o He takes an active part in the scenario
- o He corrupts a transmitted messages
- o He prevents an ongoing communication
- o He injects a virus into a system

Passive:

- o He is silent and stealthy
- o He eavesdrops the radio communications
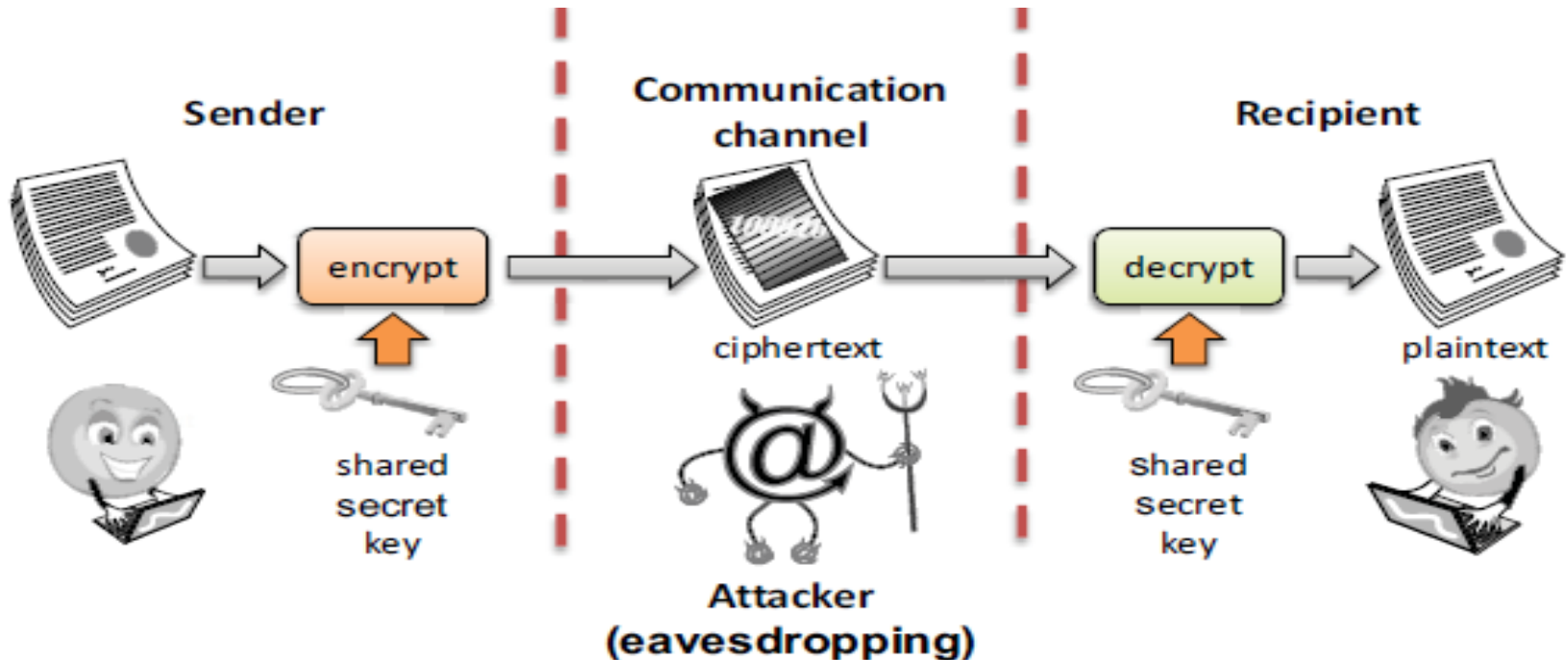- o He logs the messages transmitted in the local network

Attack Scenario of Availability

- Denial of Service: Possible to overwhelm and Online Service making it unavailable
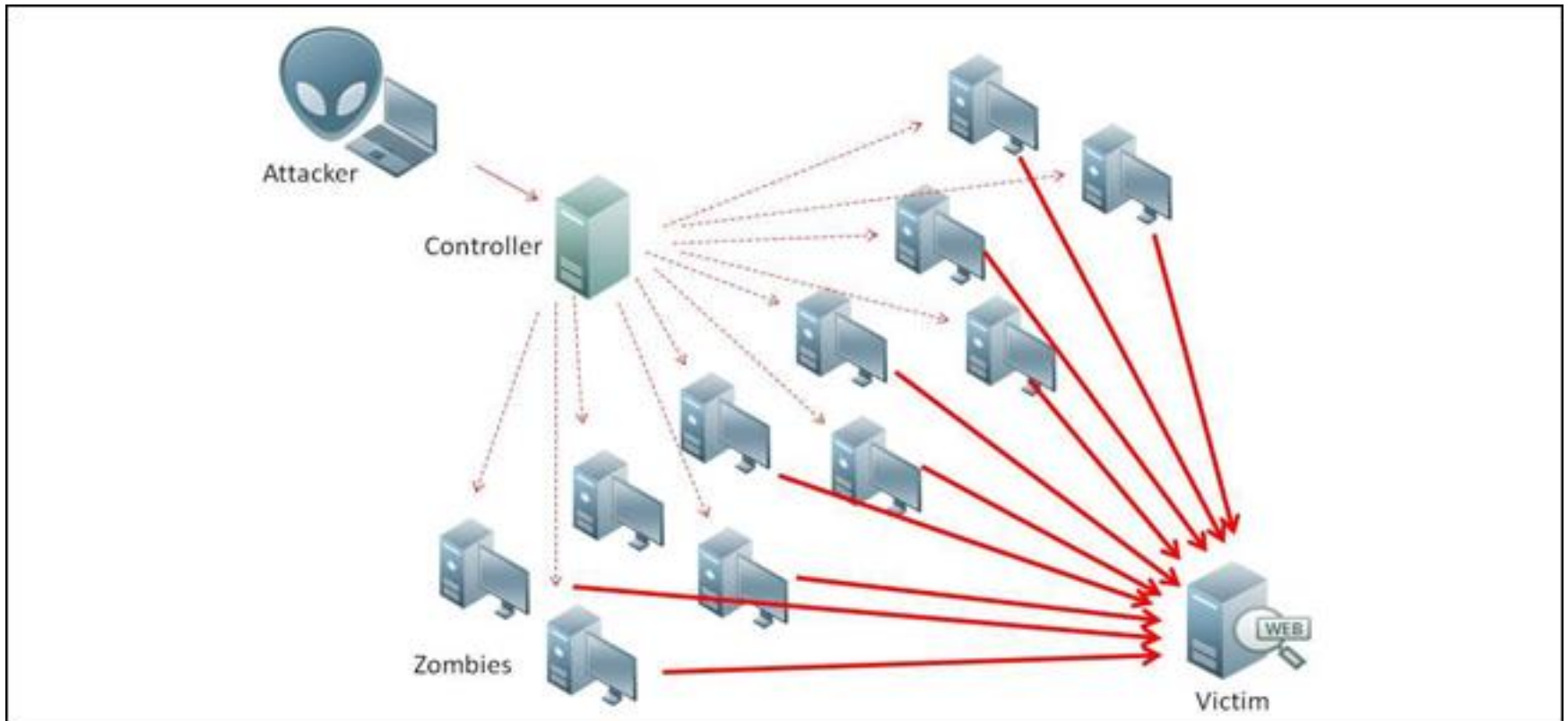
Tools for confidentiality (1/3)

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

Tools for confidentiality (2/3)

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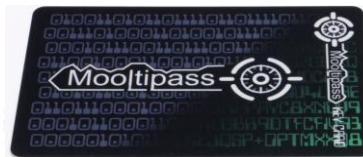 - Fingerprint, password, smart card / radio key

human with fingers and eyes

Something you are

***

Something you know

Mooltipass

Smartcard with secret key

Something you have

Tools for confidentiality (3/3)

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

- **Authorization:** determine 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

  o e.g., backup, multiple mail/DNS/DHCP servers, multiple network paths to ISP

- Firewall

  o 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
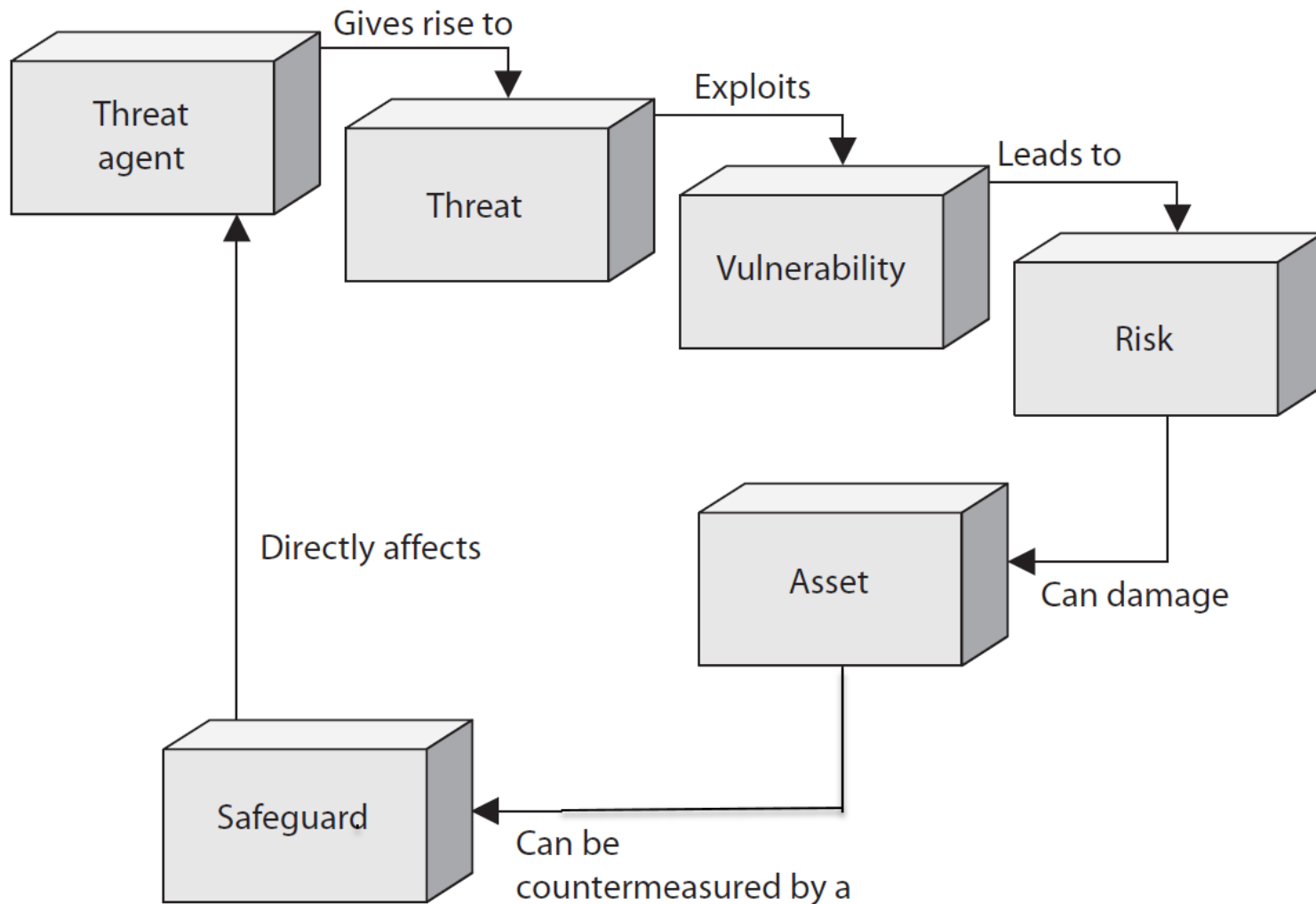
Vulnerability

- **Asset**: entity you want to protect, e.g., your data.

- A **vulnerability** is a weakness in a system that allows a threat to be realized, compromising CIA.
  - e.g., unpatched applications or OS, an unrestricted wireless access point

- Identifying vulnerabilities:
  - How is a system potentially affected by a threat?
  - What weaknesses are present in a system that enable a threat to materialize and compromise CIA?

Threat

- A *threat* anything that can exploit a vulnerability.

  - Possible dangers that could compromise the Confidentiality, Integrity, or Availability of a computer system or service

  - Can be malicious or accidental. May be external or internal

- Identifying:

  - How can a system be compromised?

  - What are the ways that the Confidentiality, Integrity, or Availability of the system can be reduced?

27

Risk

- *Risk* is assessed based **Likelihood** of a threat agent exploiting a vulnerability + **Impact** (passible harm and damages)

  - 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.

  - e.g., if strong password rules are not enforced, the company is exposed to the possibility of having users' passwords leaked and used in an unauthorized manner

Risk Martix
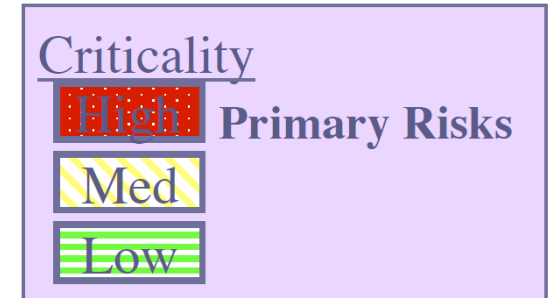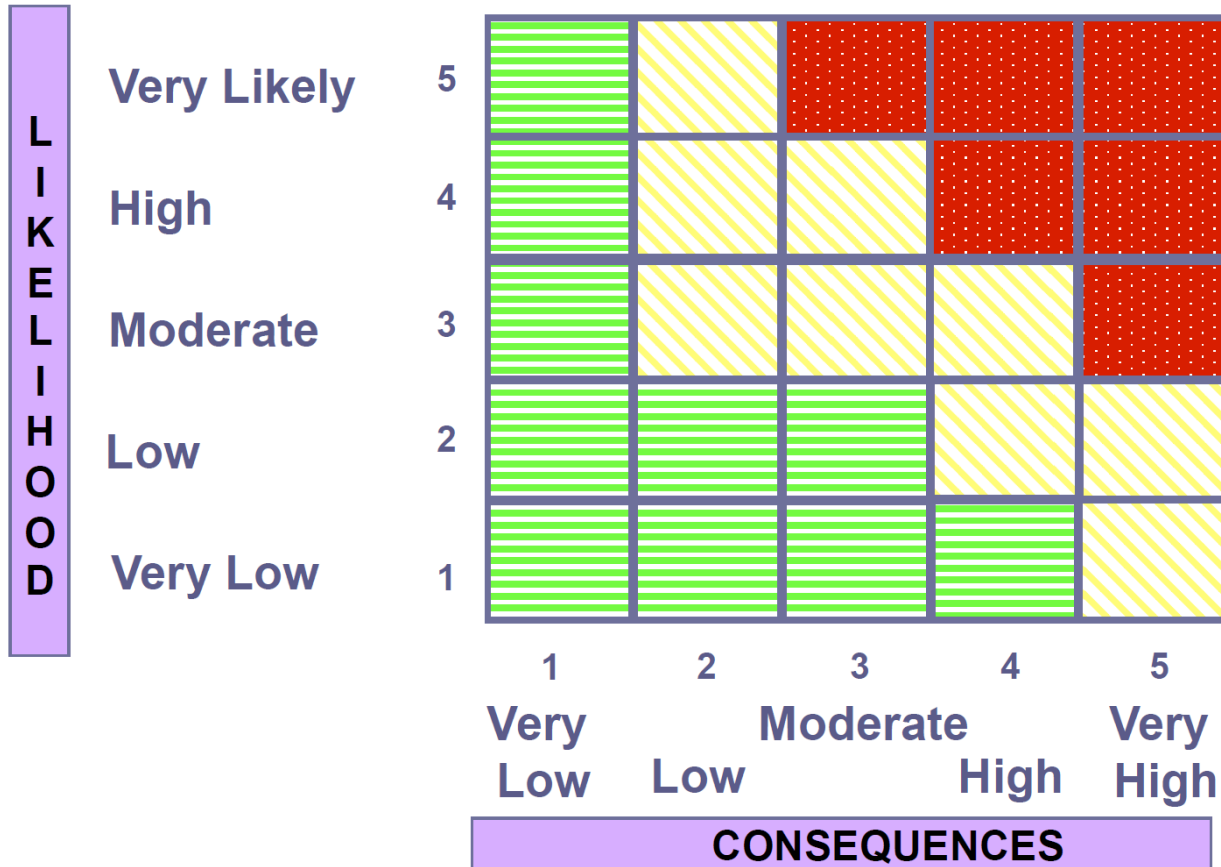
Control

- A ***control***, countermeasure or safeguard, that can be implemented to close vulnerabilities and mitigate (reduce) the potential risk in order to protect CIA of the system
  - e.g., strong password management, firewalls, Intrusion Detection System, access control mechanisms, encryption, and security-awareness training
- Identifying controls:
  - How can vulnerabilities be closed and/or threats mitigated?
  - What safeguards (protective measures) can be put in place to make a system less vulnerable to a threat?
 - Controls should be proportional to the risk

Vulnerability, Threats: Cat Example

- Cat can threaten the pen:
  - Denying its availability by kick it under fridge
  - Affect integrity by chewing on pen
- Pen vulnerabilities:
  - Small size relative to the cat
  - Light weight permits easy manipulation

Controls: Cat Example

- Increase the size or weight of the pen
    - Close the vulnerability directly
    - Tradeoff: pen usability will be significantly reduced

- Secure the pen where the cat cannot reach it
    - Close the vulnerability by
    preventing its exploitation
    - Tradeoff: reduced availability … I need to open the
    draw when I need the pen

- Prevent the cat from taking the pen
    - Mitigate the threat of the cat directly (No kitty don't)
    - Impractical in cybersecurity (e.g., cannot lock-up all hackers)

⇒ Focus on reducing the vulnerabilities

- Put pen with other pens in a coffee cup
    - Control reduces vulnerability but maintains availability
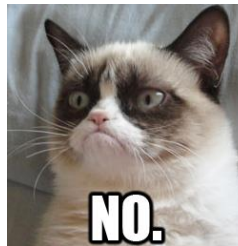
Controls Tradeoffs

- Controls can negatively affect other quality attributes such as availability, performance, and usability

  - Unplug the server and place it in a vault => high confidentiality at the expense of availability.

- Select alternative controls that are equally effective, with fewer side effects

- In many cases, a certain amount of risk must be accepted in order to operate the system (risk cannot be fully eliminated)

  - Security controls in practice must safeguard system to an acceptable level of risk, while maintaining availability

  - Controls must be sufficient to prevent most attacks from succeeding but not necessary 100% completely effective

Vulnerability, Threats: Cybersecurity example

- **Asset**: Your private photo on your mobile-phone

- **Vulnerability**: Bug on Android/IOS

- **Threat**: Someone aware of the vulnerability can steal your selfies

More examples of threats on assets

	Availability	Confidentiality	Integrity
Hardware	Equipment is stolen or disabled, thus denying service.		Hardware firmware modified maliciously
Software	Programs are deleted, denying access to users.	An unauthorized copy of software is made.	A working program is modified, either to cause it to fail during execution or to cause it to do some unintended task.
Data	Files are deleted, denying access to users.	An unauthorized read of data is performed.	Existing files are modified or new files are fabricated.

Summing Up

- Security = protection from harm

- Secure computer system adheres to the principles of the CIA Triad:
  - o Confidentiality
  - o Integrity
  - o Availability

- Fundamental trade-offs exist between security and functionality, as well as between CIA Triad principles

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