CS396: Security, Privacy & Society

Fall 2022

Lecture 1: Introduction

Instructor: Abrar Alrumayh

September 7, 2022

Outline

- Introduction to the fields of Security, Privacy, and Society
  - Basic concepts and terms
  - in-class discussion with real-world examples
    - secure computation outsourcing

1.1 Basic security concepts & terms

What is IT security?

IT security is the prevention of, or protection against

- access to information by unauthorized recipients
- intentional but unauthorized destruction or alteration of that information

Definition from: *Dictionary of Computing,* Fourth Ed. (Oxford: Oxford University Press 1996).

IT security (informal definition)

- the protection of information systems from
  - theft or damage to the hardware, the software, and to the information on them, as well as from disruption or misdirection of the services they provide
  - any possible threat

Security properties

- General statements about the value of a computer system
- Examples
  - The C-I-A triad
    - **confidentiality**, **integrity, availability**
  - (Some) other properties
    - **authentication / authenticity**
    - **non-repudiation / accountability / auditability**
    - **anonymity**

Security properties

- General statements about the value of a computer system
- Examples
  - **The C-I-A triad**
    - **confidentiality, integrity, availability**
  - (Some) other properties
    - **authentication / authenticity**
    - **non-repudiation / accountability / auditability**
    - **anonymity**

The C-I-A triad

- Captures the three fundamental properties that make any system valuable

Computer security seeks to prevent unauthorized viewing (confidentiality) or modification (integrity) of data while preserving access (availability)

Confidentiality

- An asset is viewed only by authorized parties
  - e.g., conforming to originally-prescribed “read” rules <subject, object, access mode, policy> via access control
  - some other tools
    - encryption, obfuscation, sanitization, …

Integrity

- An asset is modified only by authorized parties
  - beyond conforming to originally-prescribed “write” access-control rules
  - precise, accurate, unmodified, modified in acceptable way by authorized people or processes, consistent, meaningful and usable
  - authorized actions, separation & protection of resources, error detection & correction
  - some tools
    - hashing, MACs

Availability

- An asset can be used by any authorized party
  - usable, meets service's needs, bounded waiting/completion time, acceptable outcome
  - timely response, fairness, concurrency, fault tolerance, graceful cessation (if needed)
  - some tools
    - redundancy, fault tolerance, distributed architectures

1.2 Secure outsourced computation

Example: Tax return preparation…

Involves information collection & processing

- calculate financial data
  - payroll, profits, stock quotes, …
- manage data
  - search emails, store records, …
- submit – done!

… by many unknown machines!

Data & computation outsourcing

Cloud-based services

- hardware, OS, software, apps, …
- storage, computation, databases, analytics, …

Transformative multi-platform technology

- businesses, organizations or individuals
- client-server, distributed, P2P, Web-based, …

Internet protocols

social networks

big-data analytics

sharing economy

FinTech

Security consequences

Fact: Untrusted interactions

- information is processed outside one's administration control or "trust perimeter"

Risk: Falsified / leaked information

- information may unintentionally altered by or shared with unauthorized entities

Goal: Integrity / privacy safeguards for outsourced assets

- need to protect information against change, damage / unauthorized access

What can go wrong?

Fact: Untrusted interactions

- information is processed outside one's administration control or "trust perimeter"

Risk: Falsified / leaked information

- information may unintentionally altered by or shared with unauthorized entities

Goal: Integrity / privacy safeguards for outsourced assets

- need to protect information against change, damage / unauthorized access

Threats:

- misconfigurations, erroneous failures, limited liability
- economic incentives of cost-cutting providers
- compromises, attacks, advanced persistent threats (APTs)

Limited liability

"[We will] not be responsible for any damages arising in connection with any unauthorized access to, alteration of, or the deletion, destruction, damage loss or failure to store any of your content or other data."

Amazon Web Services customer agreement

Advanced Persistent Threats (APTs)

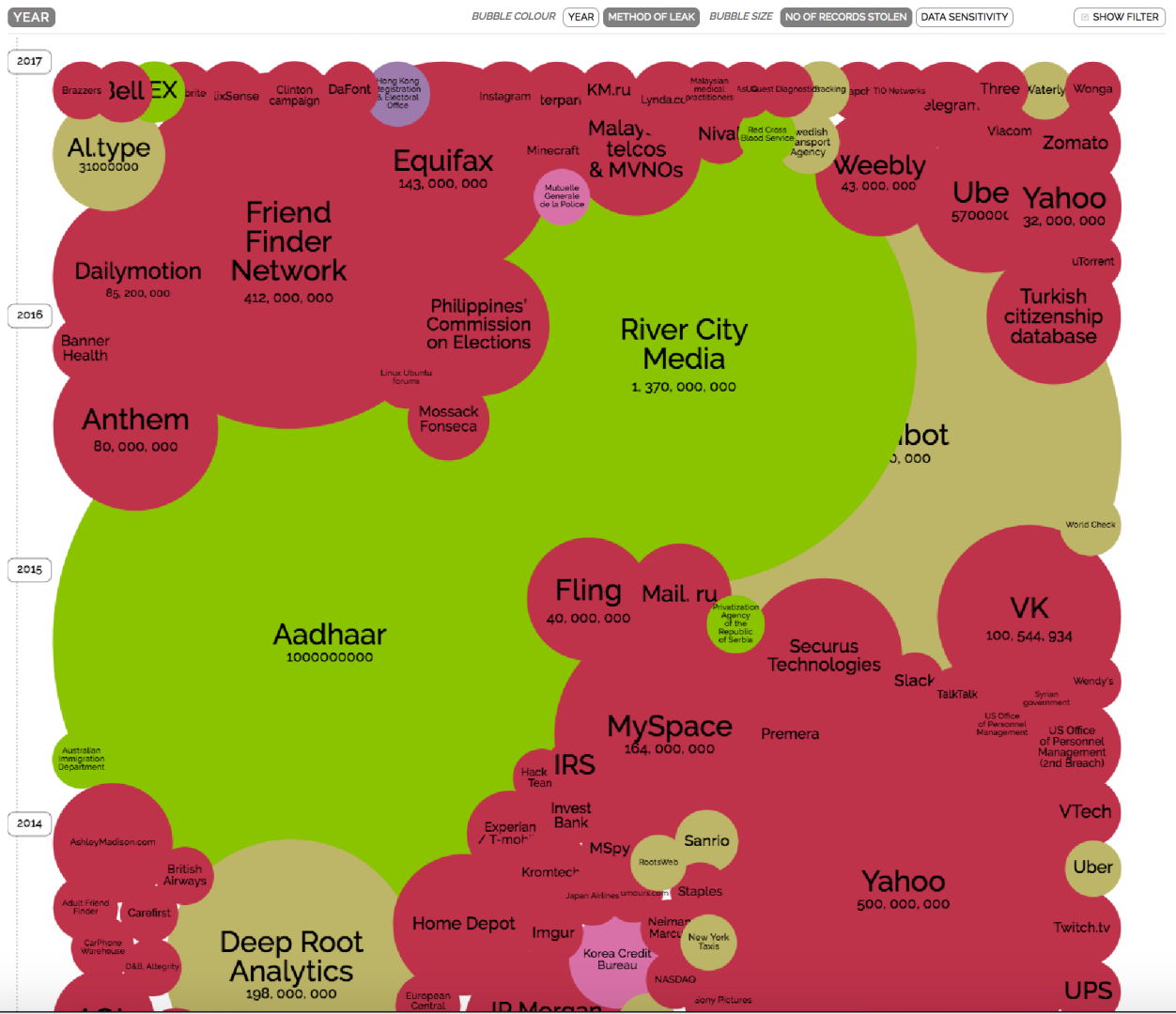
Sophisticated well-targeted cyber-attack campaigns

- aim for unauthorized data manipulation or exfiltration
- employ rich attack vectors & highly adaptive strategies
  - social engineering
  - zero-day vulnerabilities
  - low-and-slow progression
  - intelligence

extremely hard-to-defend
or even hard-to-detect

…	
RSA	(2011)
Bit9	(2013)
Dyn	(2016)
Equifax	(2017)
…	

World's biggest data breaches

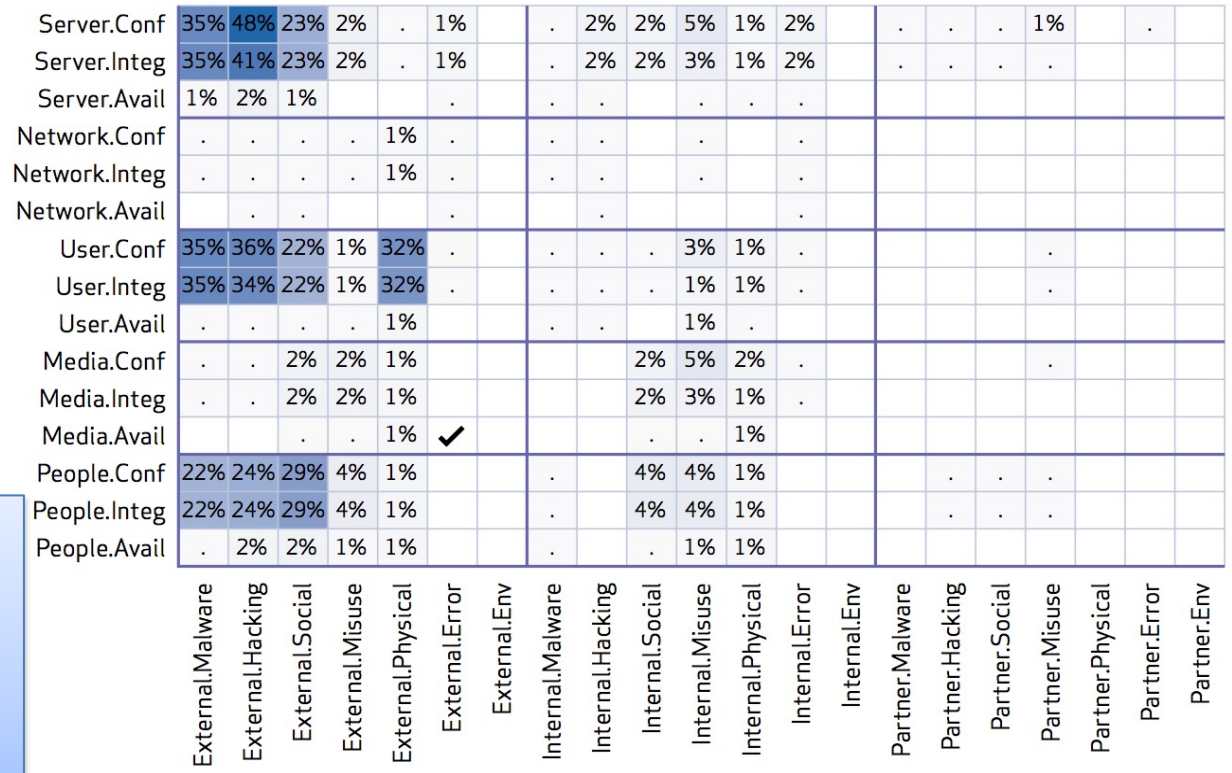


"Information is beautiful" by David McCandless

- world's biggest data breaches
  - losses > 30K records
  - up to 2/2/18

Real cases: Threats against integrity Vs. confidentiality

Figure 6: VERIS A⁴ grid depicting associations between actors, actions, assets, and attributes



	External.Malware	External.Hacking	External.Social	External.Misuse	External.Physical	External.Error	External.Env	Internal.Malware	Internal.Hacking	Internal.Social	Internal.Misuse	Internal.Physical	Internal.Error	Internal.Env	Partner.Malware	Partner.Hacking	Partner.Social	Partner.Misuse	Partner.Physical	Partner.Error	Partner.Env
Server.Conf	35%	48%	23%	2%	.	1%		.	2%	2%	5%	1%	2%		.	.	.	1%		.	
Server.Integ	35%	41%	23%	2%	.	1%		.	2%	2%	3%	1%	2%		.	.	.	.			
Server.Avail	1%	2%	1%			.		.	.		.	.	.								
Network.Conf	.	.	.	.	1%	.		.	.		.		.								
Network.Integ	.	.	.	.	1%	.		.	.		.		.								
Network.Avail		.	.			.			.				.								
User.Conf	35%	36%	22%	1%	32%	.		.	.	.	3%	1%	.					.			
User.Integ	35%	34%	22%	1%	32%	.		.	.	.	1%	1%	.					.			
User.Avail	.	.	.	.	1%			.	.		1%	.									
Media.Conf	.	.	2%	2%	1%					2%	5%	2%	.					.			
Media.Integ	.	.	2%	2%	1%					2%	3%	1%	.								
Media.Avail			.	.	1%	✓				.	.	1%									
People.Conf	22%	24%	29%	4%	1%			.		4%	4%	1%				.	.	.			
People.Integ	22%	24%	29%	4%	1%			.		4%	4%	1%				.	.	.			
People.Avail	.	2%	2%	1%	1%			.		.	1%	1%									

Data Breach Investigations Report by Verizon (2013)

- servers are a high-value target
- compromises / attacks affect both confidentiality and integrity

The “new” big threat: Data manipulation

US Officials’ View

- data manipulation is the new big threat