CS306: Introduction to IT Security

Fall 2020

Lecture 1: Introduction

Instructor: **Nikos Triandopoulos**

September 1, 2020

STEVENS
INSTITUTE *of* TECHNOLOGY
THE INNOVATION UNIVERSITY®

Today

- Course logistics
- Introduction to the field of IT security
  - in-class discussion with a real-world example

1.1 Course logistics

CS306: Topic of study

“Introduction to IT Security”

- “IT” = Information Technology
  - the study or use of information systems (especially computers, the Internet and telecommunications) for storing, retrieving, and sending information
- “IT security” = “computer security” = “cyber security”
  - 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
- “Introduction to IT Security”
  - introductory course, broad topics w/ focus on basic tools & applications

CS306: Who can take it

- **Undergraduate** course
- Prerequisite course is **CS135** or **MA134** (i.e., discrete math)
- **Required** course for Cyber-security & Computer Science concentrations
  - in study plans of CyS sophomores & CS seniors
- **Full-credit** course (w/ grade)

PLEASE contact me any of the above does not apply to you

CS306: Lectures & labs

CS306 is offered in **2 required sessions**, each offered in **multiple sections**

- lectures
  - CS306-A Tue 2:00pm - 4:30pm **Online** 67 / 69
  - CS306-B Tue 6:30pm - 9:00pm **Online** 63 / 69
- labs
  - CS306-Lx Thursdays

x	A	B	C	D	E	F
time	8 - 8:50	9:30 - 10:20	11:00 - 11:50	12:30 - 13:20	2:00 - 2:50	3:30 - 4:20
enrollment	1	18	29	29	29	24

PLEASE contact me if you have not enrolled to any lab section

CS306: Lectures & labs (continued)

- Lecture/lab sections will cover the same materials
- Changes in lecture or lab sections
  - **allowed** (if need be) but **generally discouraged** (for planning purposes)
- In any case, if a section change is necessary
  - **students must let the TAs or instructor know well in advance**

Disclaimer on lecture format

- Lectures take place in 2.5h slots

CS306-A	Tue 2:00pm - 4:30pm	**Online**	67 / 69
CS306-B	Tue 6:30pm - 9:00pm	**Online**	63 / 69

- Highly **problematic** & **undesirable** for **both students & instructor**
- Unfortunately **unavoidable** due to existing **scheduling restrictions**
  - namely, finding two time slots that *allow both CyS sophomores and CS seniors to enroll*, without conflicting with other required CS courses, is nearly impossible
  - let alone satisfying other Institute–wide policies and finding high-capacity rooms

Please provide suggestions on what can make class experience better despite 2.5h lectures

CS306: Staff

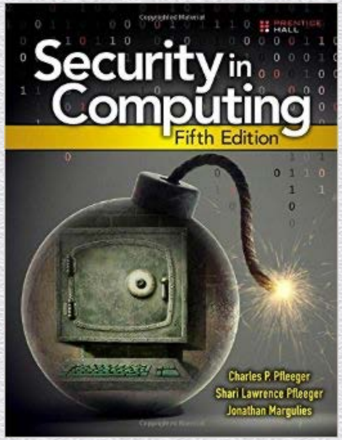
- Instructor
  - **Nikos Triandopoulos**, ntriando@stevens.edu
  - course organization / management, lectures, assignments, grades, …
    - all mistakes will be also mine ☺
  - office hours: Tuesdays 1 – 2pm or by appointment
  - office location: GS 428 – **not available in Fall 2020**
  - virtual office hours: Zoom ID 91463728672
- Teaching assistants
  - assistance w/ labs, assignments, "help sessions" as needed, some grading, demos
  - TAs & office hours: TBA

CS306: Course organization – what is offered

- Weekly lectures
  - materials covered via presentations, demos and whiteboard or in-class discussions
  - two ~10 min breaks (on the 50min marks in the lecture)
- Weekly labs
  - guided recitation of basic concepts, discussions, preparation of homework sets
- 3 - 4 homework sets
  - revision and application of covered materials
- TA hours
- Office hours by instructor

CS306: Learning materials

- Lectures
  - lecture notes: slides in pdf available online after class
  - additional materials covered via demos and whiteboard or in-class discussions
- Lab & homework assignments
  - Canvas quizzes, practice code, online resources
- Optional textbook
  - *Security in Computing*, 5th edition,
    by Pfleeger, Pfleeger & Margulies, Prentice Hall
  - available as hardcopy or e-book



CS306: Grading (tentative*)

- 20% Participation (labs attendance & in-class quizzes)
- 40% Homework assignments
- 40% 2 exams (midterm & final)
- 110% Total (w/ extra credit opportunities via homework assignments)
- Tentative* grading scheme

A	90-100
B	80-89
C	70-79

PLEASE don't estimate your grade;
if you have concerns, just contact me!

*Adapted as needed to fairly benefit the class

CS306: Course workload – what is expected from you

- Attend online lectures regularly & participate
  - e.g., you are expected to ask questions and provide comments
- Attend labs
- Hand-in homework assignments
- Pass exams
- Work independently (unless otherwise explicitly specified)
  - collaboration policy is governed by Honor System
- Provide feedback

PLEASE don't underestimate this; protect yourself and your classmates!

CS306: Policies (not complete list)

- All class matters will be handled through Canvas
- Attendance of lectures & labs is required
  - only one missed lab is allowed
  - there are no make-up labs or quizzes
- Laptops
  - **required**
- Late assignments
  - 3 free late days, after which 10% per-day reduction
  - an exception may be granted by the instructor, if there is an important reason

CS306: Announcements

- Course materials will appear on Canvas
  - I’ll make any effort to be complete, consistent and accurate in all updates
  - please be patient as I set up the processes and finalize course materials
  - communication (e.g., questions about course materials, announcements, etc.)
- No lab session this week
- TA hours & office hours will start next week, from Wednesday, September 9

CS306: Tentative Syllabus

Week	Date	Topics	Reading	Assignment
1	**Sep 1**	**Introduction**	**Lecture 1**	**-**
2	Sep 8	Symmetric-key crypto I		
3	Sep 15	Symmetric-key crypto II		
4	Sep 22	Public-key crypto I		
5	Sep 29	Public-key crypto II		
6	Oct 6	Access control & authentication		
-	Oct 13	**No class (Monday schedule)**		
7	Oct 20	**Midterm**	All materials covered	

CS306: Tentative Syllabus (continued)

Week	Date	Topics	Reading	Assignment
8	Oct 27	Software & Web security		
9	Nov 3	Network security		
10	Nov 10	Database security		
11	Nov 17	Cloud security		
12	Nov 24	Privacy		
13	Dec 1	Economics		
14	Dec 8	Legal & ethical issues		
15	Dec 10 (or later)	**Final** (closed “books”)	All materials covered*	

* w/ focus on what covered after midterm

CS306: Course outcomes

- Terms
  - describe common security terms and concepts
- Cryptography
  - state basics/fundamentals about secret and public key cryptography concepts
- Attack & Defense
  - acquire basic understanding for attack techniques and defense mechanisms
- Impact
  - acquire an understanding for the broader impact of security and its integral connection to other fields in computer science (such as software engineering, databases, operating systems) as well as other disciplines including STEM, economics, and law
- Ethics
  - acquire an understanding for ethical issues in cyber-security

Questions?

- Please ask questions during class!

Today

- Course logistics
  - topic of study, enrollment eligibility, sessions
  - staff, learning materials, course organization
  - expectations, grading, policies, announcements
  - syllabus overview, course objectives/outcomes
- Introduction to the field of IT security
  - in-class discussion with a real-world example

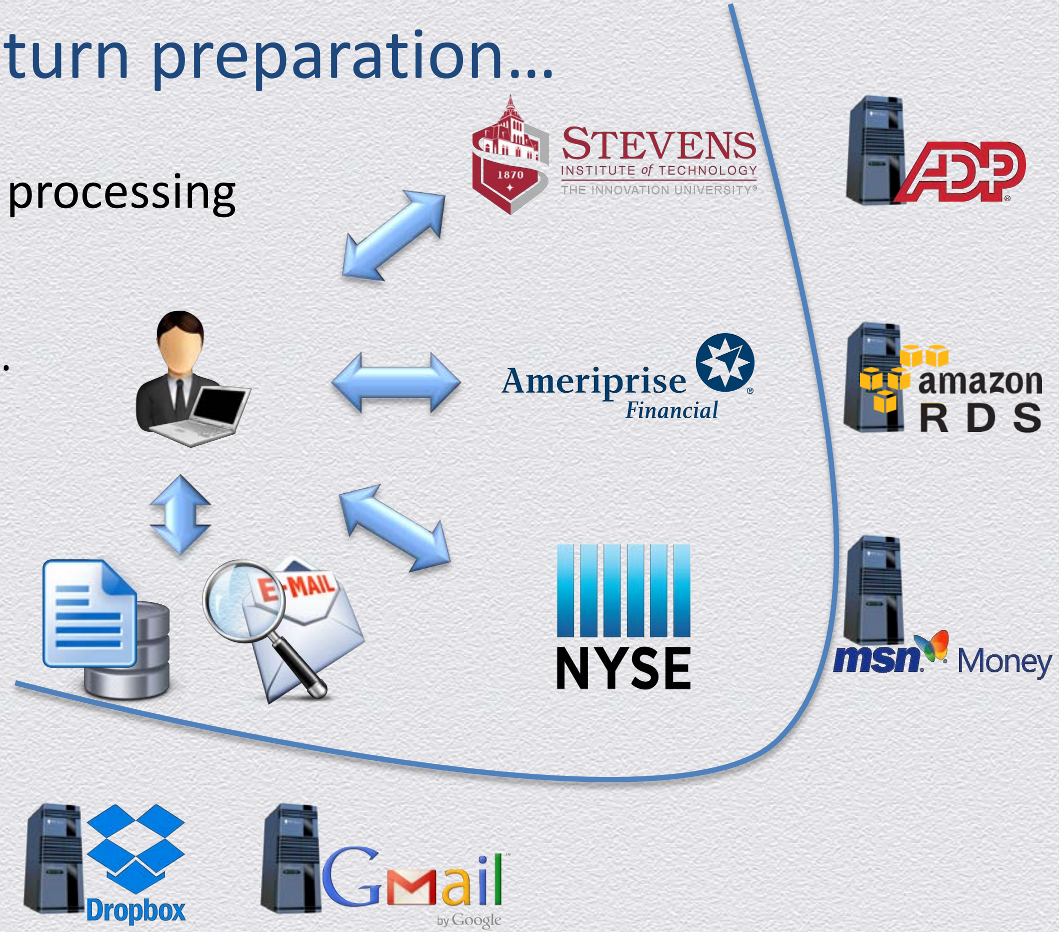
1.2 Secure outsourced computation

Another 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, …

*aaS

Internet protocols

social networks

big-data analytics

sharing economy

UBER

airbnb

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)

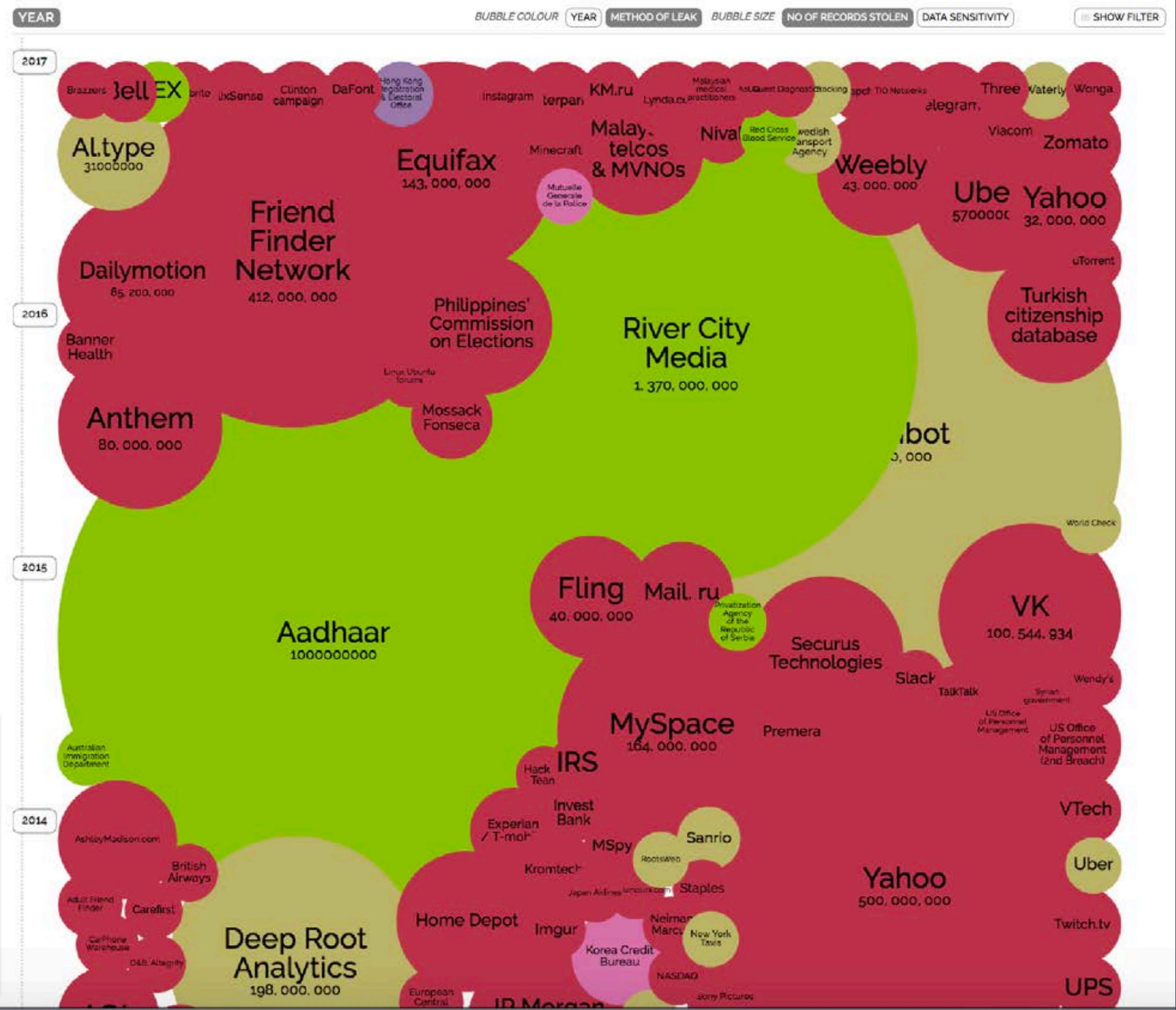
Sophisticated well-targeted cyber-attack campaigns

- 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

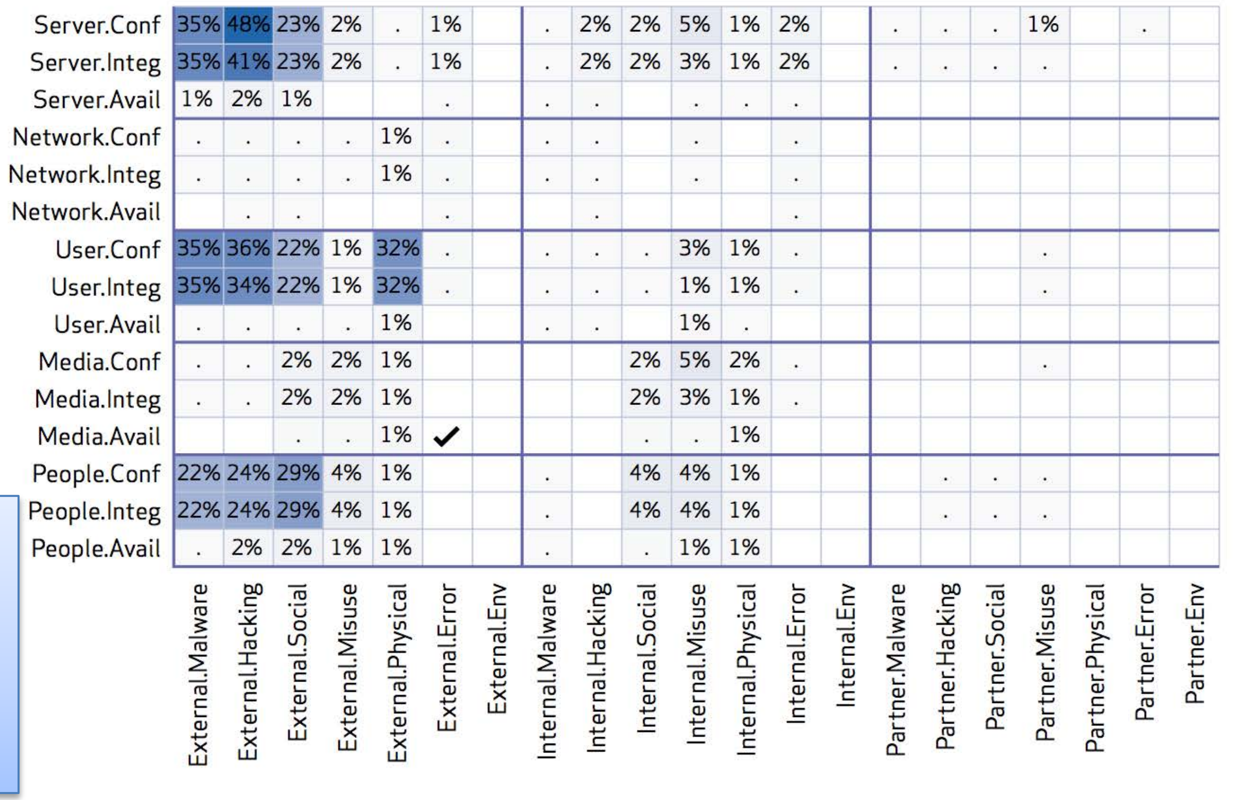


“Information is beautiful”
by David McCandless

- 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

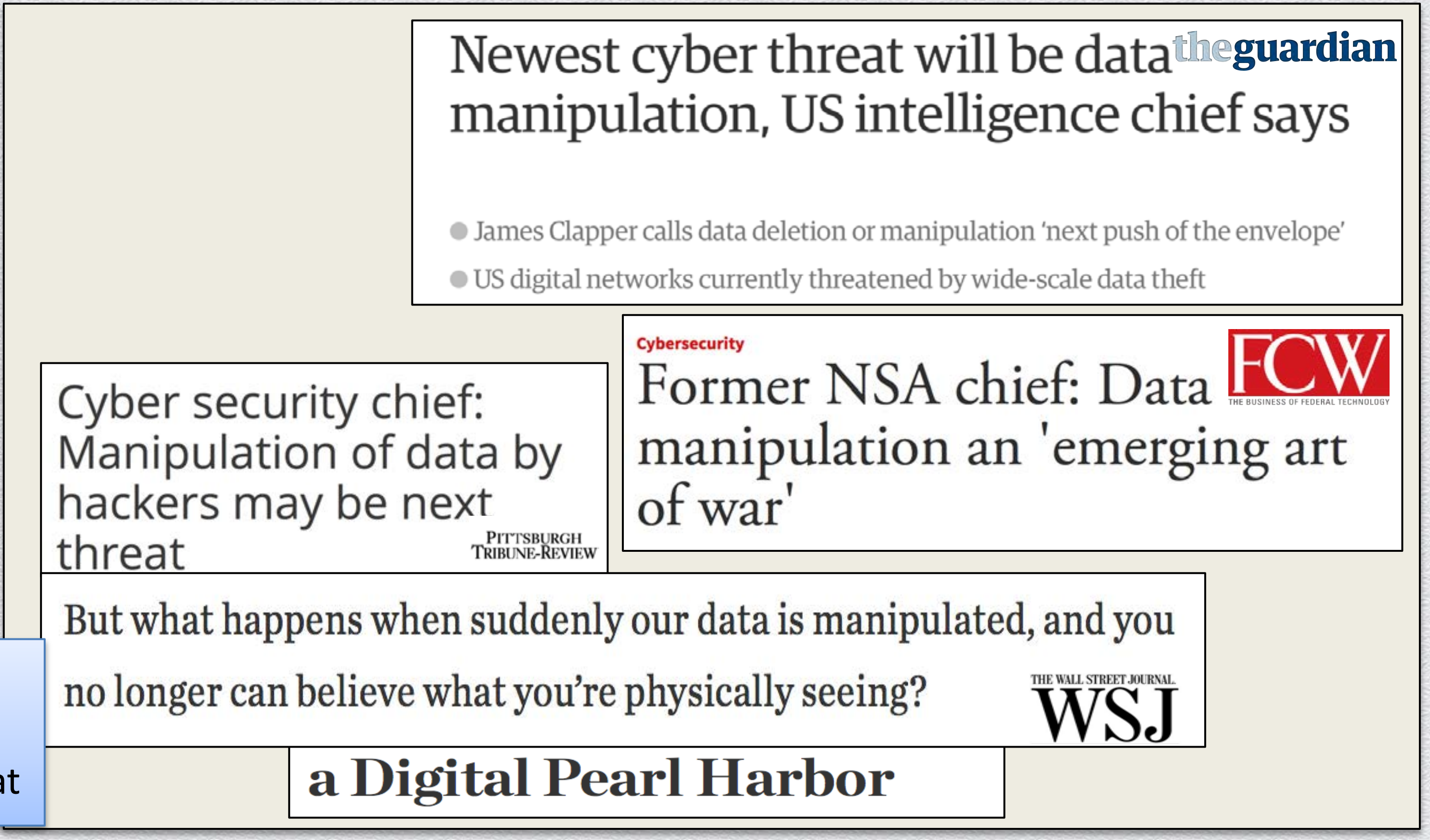


	External.Malware	External.Hacking	External.Social	External.Misuse	External.Physical	External.Error	External.Env	Internal.Malware	Internal.Hacking	Internal.Social	Internal.Misuse	Internal.Physical	Internal.Error	Internal.Env	Partner.Malware	Partner.Hacking	Partner.Social	Partner.Misuse	Partner.Physical	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



theguardian

Newest cyber threat will be data manipulation, US intelligence chief says

- James Clapper calls data deletion or manipulation ‘next push of the envelope’
- US digital networks currently threatened by wide-scale data theft

Cybersecurity

Former NSA chief: Data manipulation an 'emerging art of war'

FCW THE BUSINESS OF FEDERAL TECHNOLOGY

Cyber security chief: Manipulation of data by hackers may be next threat

PITTSBURGH TRIBUNE-REVIEW

But what happens when suddenly our data is manipulated, and you no longer can believe what you’re physically seeing?

THE WALL STREET JOURNAL. WSJ

a Digital Pearl Harbor

US Officials’ View

- data manipulation is the new big threat

Today

- Course logistics
  - topic of study, enrollment eligibility, sessions
  - staff, learning materials, course organization
  - expectations, grading, policies, announcements
  - syllabus overview, course objectives/outcomes
- Introduction to the field of IT security
  - in-class discussion with a real-world example
  - coverage of basic concepts & terms