Quantitative Cyber-Security

Colorado State University
Yashwant K Malaiya

CS559 Fall 2026
Course Introduction

CSU Cybersecurity Center
Computer Science Dept

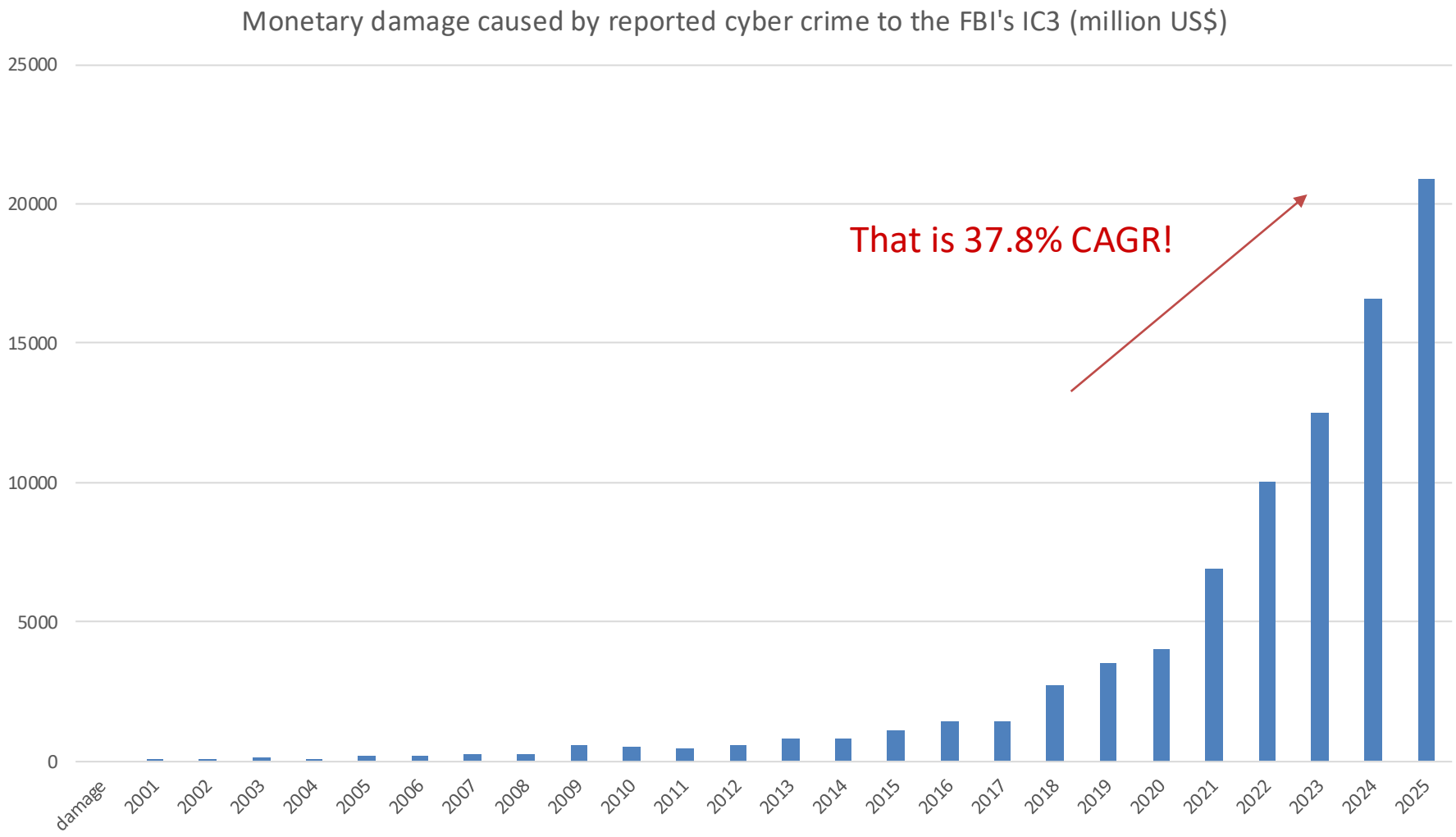
Welcome

Colorado State University

About the course

- **Quantitative and algorithmic view of cyber-security**
- **Intended for students from**
  - **computer science**
  - **engineering and business**
- **One semester graduate course**
  - **On-campus section (S001)**
  - **Distance section (S801)**
  - **Mostly identical work requirements, however with some individual section optimization**
- **Course materials:**
  - **Lectures slides, videos**
  - **linked reading materials**
- **Evaluation:**
  - **on-line quizzes, assignments**
  - **Exams: Midterm, Final**
  - **term project: research**
  - **Interaction**
- **Technology requirement: use of excel, some open-source tools**

Cyber crime losses

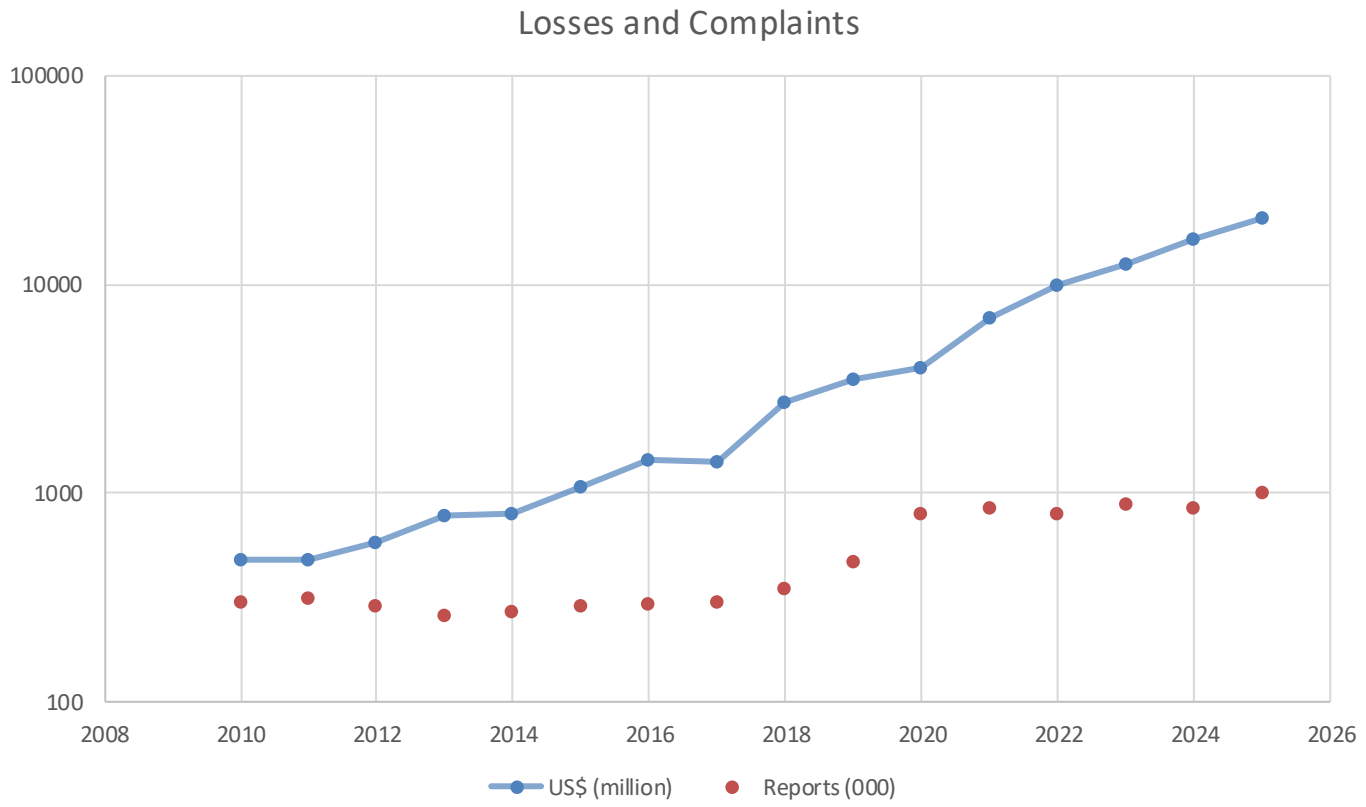


CAGR: Compound Annual Growth Rate

FBI's Internet Crime Complaint Center (IC3)

Colorado State University

Cyber crime complaints & Losses



Losses growing exponentially, although complaints have risen only marginally.

FBI's Internet Crime Complaint Center (IC3

Colorado State University

Some recent Cyber breaches

Instructure (Canvas) Extortion Attack: Records Stolen/Exposed: 275 million records across nearly 9,000 institutions. Executed by the ShinyHunters group via voice phishing (vishing) and vulnerabilities in account programs, compromising student and staff details and private internal messages.

PowerSchool (2025 Highlight): 71.9 million records. Recognized by the Identity Theft Resource Center as the single largest U.S. corporate/ed-tech breach event of 2025

Charter Communications (Spectrum): 40 million+ records claimed (with ~4.9 million unique email/customer identifiers confirmed). Compromised in April 2026 after a Microsoft Entra account credential was handed over via voice phishing, giving attackers an entry point into Salesforce data environments.

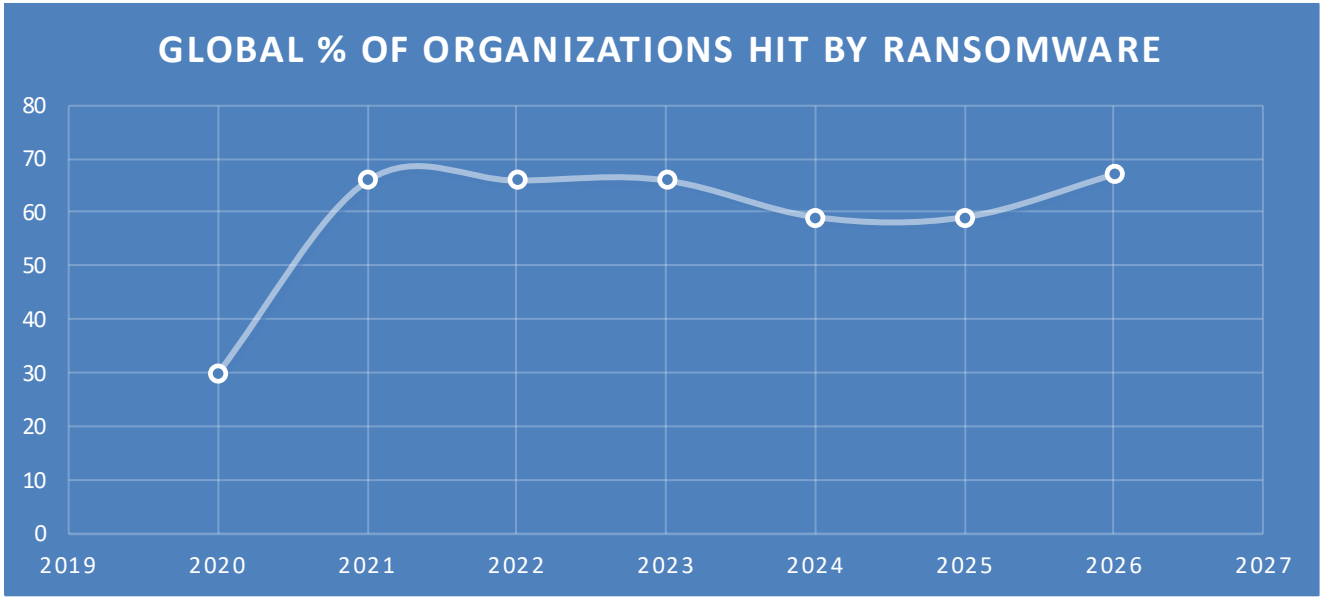
Mexican Government Agencies Attack: Over 415 million combined records (including taxpayer identities and civil registry records). Between the end of 2025 and the start of 2026, a cyberattack hit nine Mexican government agencies. A single hacker, using Claude Code and OpenAI's GPT-4.1, ran the operation.

NYC Health + Hospitals: 1.8 million individuals. A third-party vendor compromise led to sensitive medical records, Social Security numbers, and rare biometric indicators (such as fingerprints and palm prints) being accessed.

Some recent Cyber breaches

- **Salesforce attack**: In the summer of 2025, the hacker group. Victims included Google, Workday, and Allianz Life.
- **Microsoft SharePoint vulnerabilities**: In July 2025, multiple Chinese nation-state threat groups exploited zero-day vulnerabilities in on-premises Microsoft SharePoint servers, compromising over 400 systems.
- **Qantas data breach**: In July 2025, a cyber incident in one of the Australian airline's call centers inked to the Scattered Spider group, affected customer records for 6 million people.
- **Bybit cryptocurrency heist**: In February 2025, North Korea's Lazarus Group stole an estimated $1.5 billion in cryptocurrency from the Bybit exchange.
- **Yale New Haven Health System breach**: In April 2025, a likely ransomware attack affected 5.5 million patients of the Yale New Haven Health System.
- **Oracle Cloud breach**: In March 2025, a threat actor was discovered selling 6 million records from Oracle Cloud's Single Sign-On and LDAP systems.

Ransomware



Use backups to restore data	Paid the ransom and got data back	Use other means to get data back
68%	56%	26%

Colorado State University

ABOUT ME: Yashwant K. Malaiya

- My Research approach
  - Explore what has not been examined
  - Concepts contributed: Antirandom testing, Detectability Profile, New Vulnerability Discovery models (inc. AML model), new Software reliability models

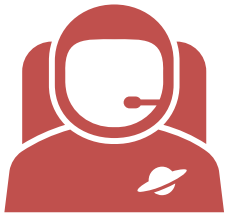
Areas in which I have published:

- Computer security
  - Vulnerability discovery
  - Risk evaluation
  - Assessing Impact of security breaches
  - Vulnerability markets
- Hardware and software
  - Testing & test effectiveness
  - Reliability and fault tolerance
- Results have been used by industry, researchers and educators
- I will use some of our results in this class.

About me

- Teaching
  - Computer Organization (CS270)
  - Operating systems (CS370 on-campus/on-line)
  - Computer Architecture (CS470 on-campus/on-line)
  - Fault tolerant computing (CS530 on-campus/on-line)
  - Quantitative Security (CS599 First! on-campus/on-line)
- Professional
  - Organized International Conferences on Microarchitecture, VLSI Design, Testing, Software Reliability
  - Computer Science Accreditation: national & international
  - Professional lectures
  - Advised more than 65 graduate students ..

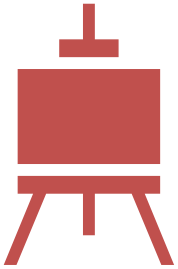
Contacting me



Professor: Yashwant Malaiya

Office hours: 3:30-4:30 Wednesday (tent)

Computer Science (CSB 356)



Platforms:

Canvas https://canvas.colostate.edu

- Discussions, including announcements
- quizzes, homeworks, project, exams, videos

Topics we will cover in CS 599

1. Introduction: state, terms, concepts
2. Risk: breach likelihood and breach cost, scales
3. Probability and modeling
4. Vulnerabilities: taxonomy, life cycle, markets
5. Metrics, data bases
6. Attack types
7. Risk components:
    1. Breach likelihood components
    2. Breach cost components
8. Testing: coverage and effectiveness
9. Risk mitigation
10. Emerging issues and trends

Books and resources

- Required text-books: none
- will also use materials from other sources including
  - Research publications
    - You have access to CSU library digital resources (IEEE Explore/ACM/ScineceDirect etc)
    - Off campus access
  - Government, vendor and expert reports
  - System Documentation, articles, news etc.
  - Vulnerability related Data-bases
  - Selected Books

Grading

- Quizzes, Assignments, participation 40%
  - Quizzes 15%
  - Assignments 15%
  - Participation 10%
- Exam 25%
  - Midterm 25%
  - ~~Final~~
- Project: 35%
  - Topic search/proposal, Progress report
  - Presentations & interaction
  - Final report

iClicker Cloud

- In the on-campus class we will use iClicker Cloud for interactive activities.
  - Download an install iClicker Cloud on your smartphone.
  - Please use only one iClicker login with your exact student id and email address used for registration. Bring it daily.
- Distance students: You will be able to see the questions/discussion but not participate in it. You should interact more often on canvas.

Grading

- This is a graduate class.
- Default dividing lines:
  - **≥ 98 is an A+, Near perfect**
  - **≥ 90 is an A, Excellent**
  - **≥ 88 is an A-, Very good**
  - ≥86 is a B+, Good
  - ≥80 is a B, Good enough
  - ≥78 is a B-, ≥76 is a C+, ≥70 is a C, ≥60 is a D, and <60 is an F.
- I will not cut higher than this, but I may cut lower.
- I expect most students will work for A+, A, A-.

Evolution of Cyber-security subfields

- Cyber-security field has several subfields. There are individuals and organizations that are experts in their subfield.
- The subfields have evolved separately, with specialists becoming experts in specific subfields, using their own terminology and framework.
- Inconsistent terminology leads to increased effort needed to understand developments and to cross-link them.
- Cyber-security is an emerging field, but there are well developed disciplines that are related:
  - Testing (hardware/software)
  - Fault tolerance (systems/hardware/software/network/data)
  - Reliability and risk evaluation (Quantitative/qualitative)
  - Investments and insurance (economic issues)
- Is it possible to connect different perspectives using a single framework?

Need for well-defined terminology

- In cyber-security field, some key terms are often used in a very ad-hoc manner.
- Consider for example the term ***risk*** a key concept.
- ***Risk*** may refer to
  - Attack types: "Ransomware, Social Engineering, Vendor Exposure"
  - "Cyber risk = probability of threat exploiting weak point of assets"
  - "Risk: The effect of uncertainty on objectives"
  - Etc.
- Which is the right definition of the term ***risk***?

Collaborative Learning

An old saying

आचार्यात् पादमादत्ते पादं शिष्यः स्वमेधया ।
पादं सब्रह्मचारिभ्यः पादं कालक्रमेण च ॥

ācāryāt pādam ādhatte pādaṃ śiṣyaḥ svamedhayā ।
pādaṃ sabrahmacāribhyaḥ pādaṃ kālakrameṇa ca ॥

महाभारत: उद्योग पर्व:

Trans: 1. A student learns a quarter from his teacher, 2. another quarter using his own intelligence, 3. receives yet another quarter from his classmates and 4. the quarter in due course of time.

Electronic devices in lecture room

- Use of Laptops, phones and other devices are not permitted.
- Exception: only with the required pledge (see Canvas) that you will
  - Must have a reason for request
  - use it only for class related note taking, which must be submitted on 1st and 15th of each month.
  - not distract others, turn off wireless, last row
- Laptop use lowers student grades, experiment shows, Screens also distract laptop-free classmates
- The Case for Banning Laptops in the Classroom
- Laptop multitasking hinders classroom learning for both users and nearby peers

Use of GenAI is restricted

- ChatGPT and other LLM models are an exciting development, made possible by hardware and software advances. Use them in your profession and in classes where their use is expected.
- AI is permitted to a limited extent in this class.
  - You must be able to understand and explain your work and writing.
  - University and department rules apply.
  - Simply copying and pasting text from ChatGPT etc will not lead to any learning.
  - I will share a detailed policy later.

Introductions

Can each of you briefly briefly introduce yourself?

- First and last name
- Where you are from (mention city if it is a large country)
- What are you doing here? (major/year)
- Technical (and personal, if you like) Interests
- In class and on Canvas discussions

Quantitative Security

Colorado State University

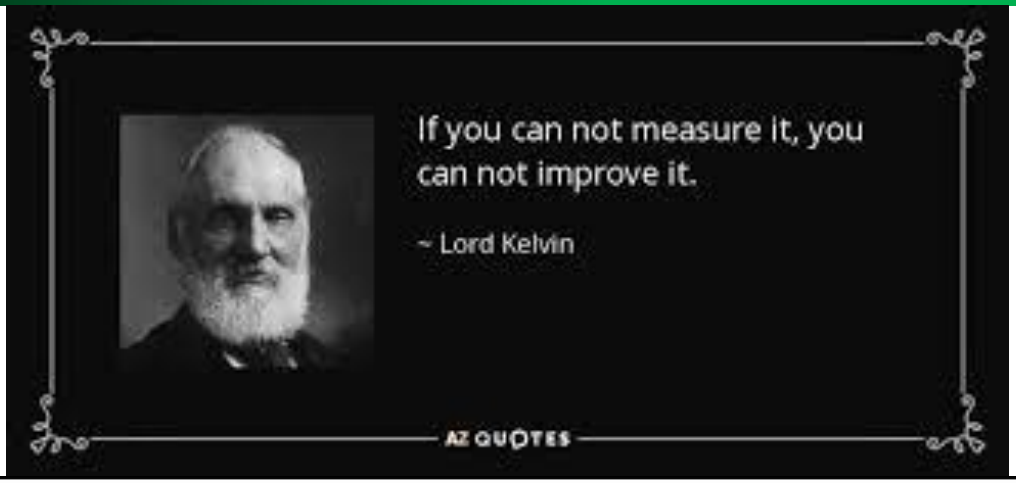
Yashwant K Malaiya

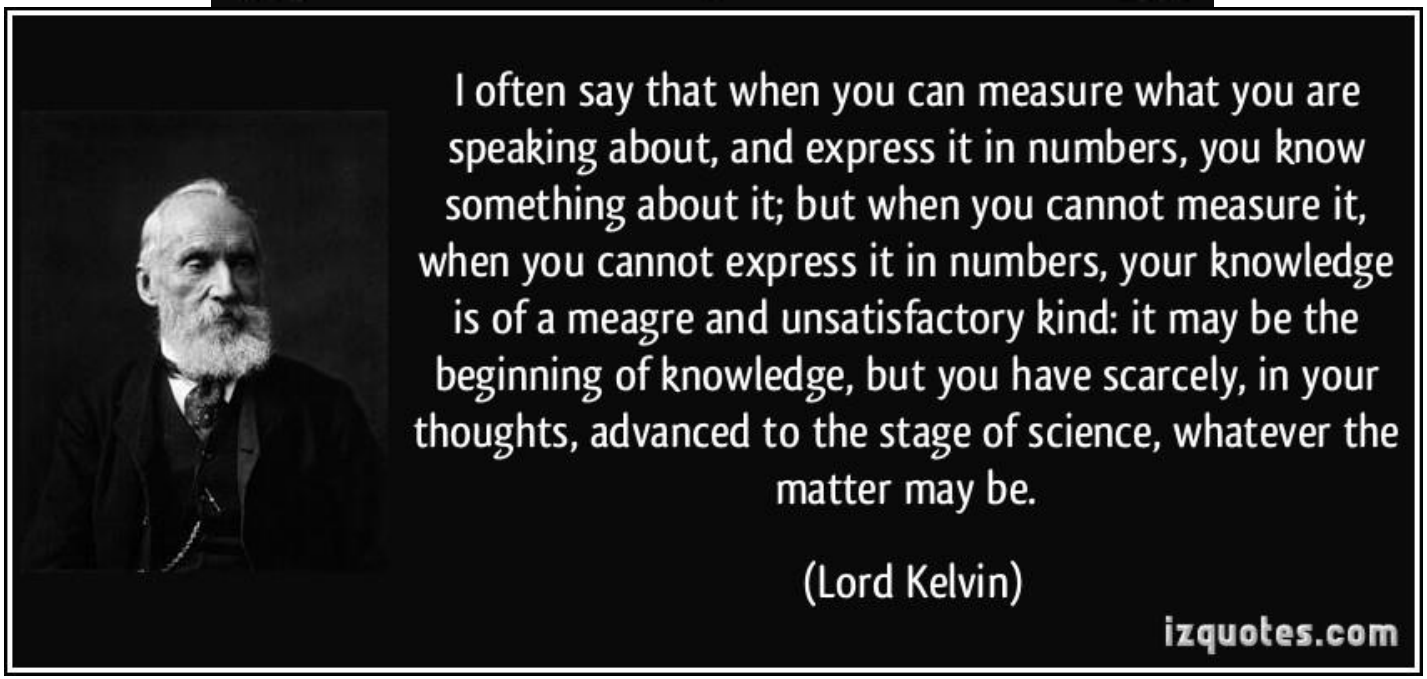
CS 559

Course Outline

CSU Cybersecurity Center
Computer Science Dept

Lord Calvin (1824-1907)





Colorado State University

Course Outline 1

Course Introduction/Background:

- Introduction, Outline, Current state
- Key terms, Access control, Security framework

Risk:

- as the product of breach likelihood and breach cost and their components, conflicting definitions of risk
- Linear/logarithmic scales, Risk Matrix, Time-frame: per event (single breach) vs per year (annual loss expectancy).
- Insurance

Course Outline 2

Probability/distributions/Modeling

- A review of essential concepts from probability, conditional probabilities, Bayes' rule
- Common distributions used in risk evaluation, Monte Carlo simulation
- Modeling approaches, Regression
- Combinatorics (Ciphers and password)

System Security Architecture: Networked system components, placement of protection schemes

Course Outline 3

Vulnerabilities

- Types: Software: defect vs vulnerabilities, System/network/configuration, Social engineering: exploitation of human weaknesses
- Life cycle: Introduction, discovery, disclosure, patching, exploitation.
- Vulnerability Discovery process in individual and evolving programs, Longer-term trends
- Metrics: Metrics, CVSS v2/v3 metrics and scores., Temporal (patches and exploits), Environmental metrics CVSS,
- Databases: NVD, CVEDetails, VulnDB, ExploitDB

Course Outline 4

Testing for bugs and vulnerabilities

- Testing as exercising input or structure space, Testing Profiles
- Coverage metrics, Fuzzing and Pen Testing
- Probabilistic vs deterministic testing, Test effectiveness

Research methodology

- Potential sources of information
- Identifying research threads and trends
- Information extraction and consolidation
- Assessing promise of a research direction

Course Outline 5

Attacks

- Attack types, Intrusion detection, Mitre ATT&CK framework
- **Breach likelihood components:** Vulnerability presence, Breach Probability, Vulnerability exploitability, and reachability, Motivation/skill/tool support of potential adversaries, Impact of management policies.
- **Breach cost components:** Investigation costs, crisis mitigation costs, cost of sanctions and lawsuits. Question of insurance coverage, tax breaks. Longer-term costs: loss of reputation and business opportunity**.**
- **Costs to a government/nation:** loss of industrial IP, defensive secrets, tempering with national infrastructure or defenses

Quantitative Security

Colorado State University
Yashwant K Malaiya

CS559

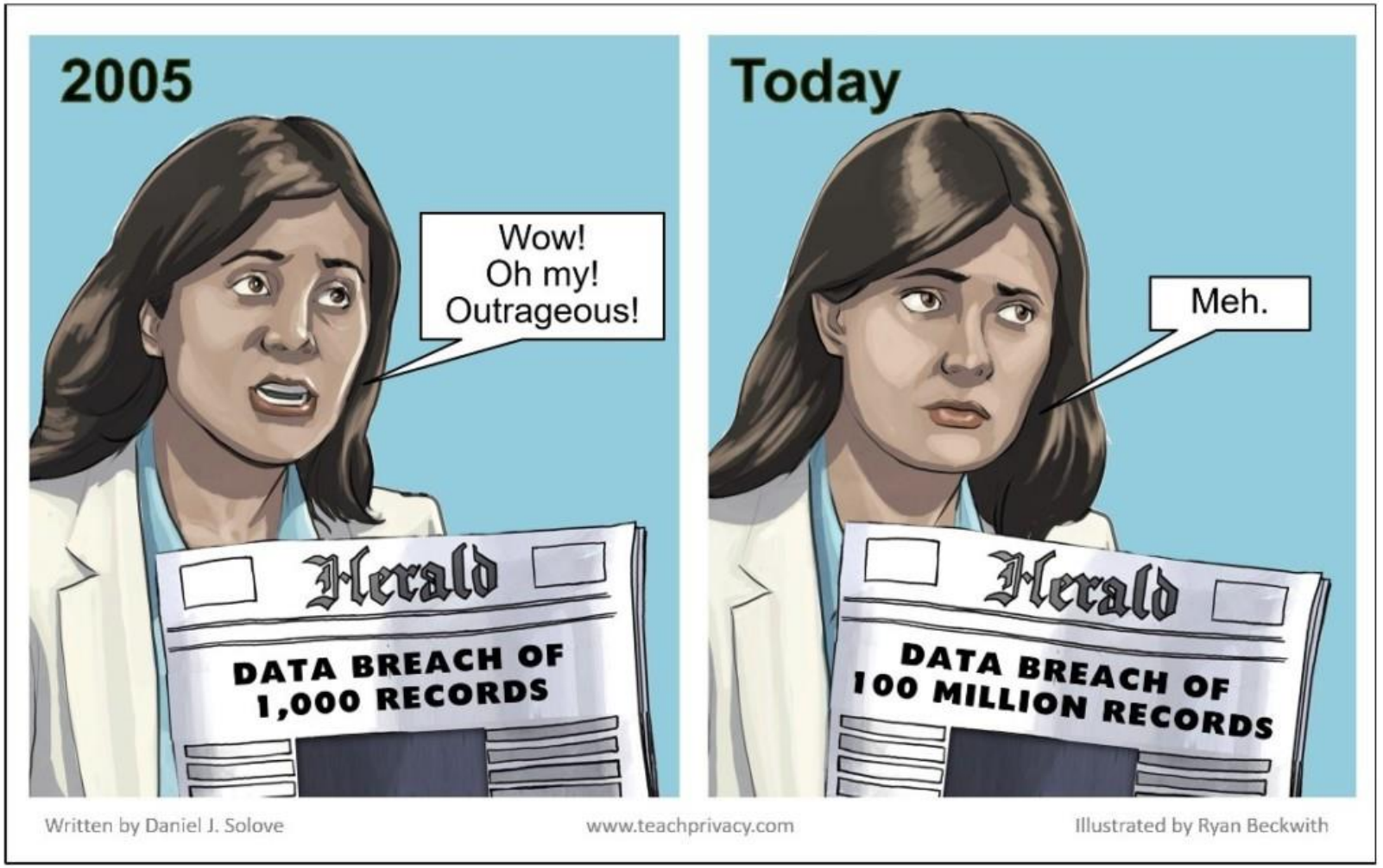
Recent Security Statistics

CSU Cybersecurity Center
Computer Science Dept

What can you do with numbers?

- Assess relative magnitude of problems
  - Even if the data is limited or anecdotal
- Construct models
  - If there is enough data
  - Make projections
  - Understand causes and engineer for desired behavior
- Where to find data?
  - Someone has already compiled data
  - Doing experiments to collect data
  - Search and search for pieces of data. You might be able to link them.

Progress in Cyber-security



Colorado State University

Cyber Security Statistics

- **Breaches:**
  - **in most cases, it takes half a year to detect a data breach.**
  - There were 8,854 recorded breaches between January 1, 2005 and April 18, 2018. Price per record ranging anywhere from $120-$600
  - ~~**31%**~~ **39% of organizations have experienced cyber attacks on operational infrastructure. 2020**
  - 43% of all cyber attacks are aimed at small businesses. In 2017, 61% of data breach victims were companies with less than 1000 employees.
  - Around 50% of the risk companies face, come by way of having multiple security vendors!
  - **Just 38% of global organizations claim that they are equipped and able to handle a complex cyber attack**

Cyber Security Statistics

- **Phishing:**
  - **94% ~~91%~~ of attacks launch with a phishing email 2020**
  - 30% of U.S. users open phishing emails.
  - **12% of those who opened phishing emails later opened the infected links or attachments.**
  - 85% of all attachments emailed daily are harmful for their intended recipients.
  - In the last year, 76% of businesses reported that they had been a victim of a phishing attack.
  - 38% of malicious attachments are masked as one Microsoft Office type of file
- **Human errors:**
  - **65% of companies have over 500 employees that have never changed their password.**
  - **95% of data breaches have cause attributed to human error**

Cyber Security Statistics

- **Attacks**
  - **Over 24,000 malicious mobile apps are blocked from the various app stores each day.**
  - IoT attacks were up by 600% in 2017.
  - DDoS attacks account for 5% of monthly traffic related to gaming.
  - **Around 60% of malicious web domains are associated with spam campaigns.**
  - **Cyber criminals managed to exploit the credit cards of 48% of Americans back in 2016.**
- **Malware**
  - There was an 80% increase in malware attacks on Mac computers in 2017.
  - **75% of the healthcare industry has been infected with malware at some point in time.**
- **Ransomware**
  - **Ransomware attacks are growing more than 350% annually**.
  - The damage costs of ransomware will rise to $10 billion in 2019.
  - A business falls victim to a ransomware attack every 13.275 seconds.

Cyber Security Statistics

- **Weaknesses:**
  - Of all files, 21% remain completely unprotected.
  - Reported system vulnerabilities went up by 16% in 2017.
- **Costs and Opportunities**
  - **$4.35 ~~$2.4~~ million is the average cost of a malware attack in 2022 ~~2017~~.**
  - **The global cost of online crime is expected to reach $6 trillion by 2021.**
  - **Cybersecurity expenditures are expected to reach $1 trillion by 2024.**
  - The annual cost of cybercrime damages is expected to hit $5 trillion by 2020.
  - The global cost of online crime is expected to reach $6 trillion by 2021.
  - Cybersecurity expenditures are expected to reach $1 trillion by 2024.
  - The annual cost of cybercrime damages is expected to hit $5 trillion by 2020.
  - Cybersecurity expenditures are expected to reach $1 trillion by 2024.
- **Jobs**
  - Cybersecurity job postings are up 74% over the past five years.
  - There are over 300,000 unfilled cybersecurity jobs in the United States, with the demand rising each year.
  - **By 2021, the number of unfilled cybersecurity jobs is expected to balloon to 3.5 million**.
  - Cybersecurity job postings are up 74% over the past five years.

https://www.cyberdefensemagazine.com/cyber-security-statistics-for-2019/

Colorado State University

Course Outline 6

Risk mitigation

Reducing the breach likelihood, Reducing the breach cost.

Security Economics, Security investment ROI, Attack surfaces and connectivity, Threat containment strategies and their effectiveness.

Emerging topics

Vulnerability markets: Legitimate (for example rewards programs), Gray (vulnerability brokers) and black markets, Potential buyers and sellers of Zero-day vulnerabilities and exploits

People: Well known Vulnerability finders/cyber criminals

Readings/Discussion

- The course will involve reading some assigned articles and discussing them
  - May involve looking up background and recent developments
  - Quick Research Project: Available soon this week

Term Project

- Term project: You will choose a topic from a given list. Other topics may be permitted by the instructor. Need to be aligned with the objectives of the class.
- Project will involve
  - Preliminary research to identify the sources of information and the topic/problem to be investigated.
  - Proposal (Oct), Progress report (Nov), Final report (Early Dec)
    - Must have some some original ideas
    - Report format: ACM/IEEE conferences
    - Dates to be determined soon
  - Presentations and discussions are required
  - Peer reviews/interaction and comments needed

Quantitative Cyber-Security

Colorado State University
Yashwant K Malaiya

CS 559
Security System Architecture

CSU Cybersecurity Center
Computer Science Dept

Fault-Tolerance vs Seurity

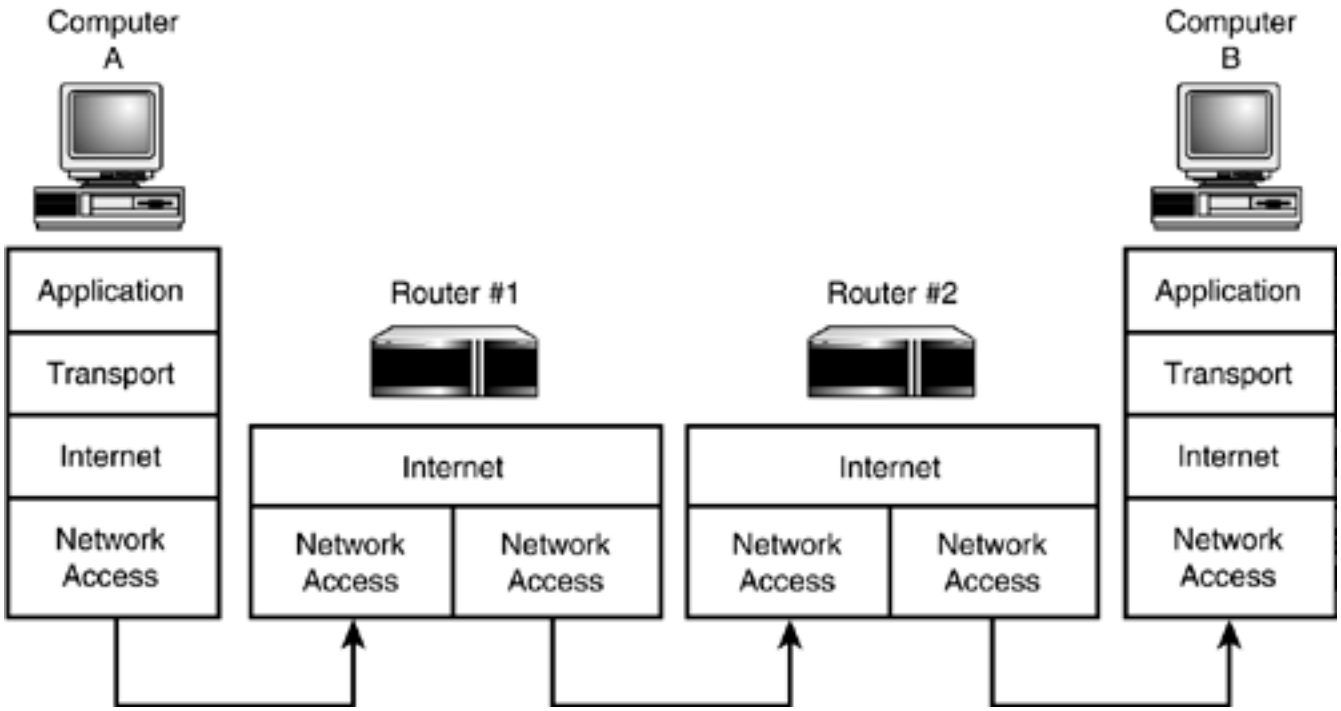
- Fault-tolerance:
  - Errors are unintentional
  - Testing: reduce number of faults that cause errors
  - Objective: block propagation of error, spatially or temporally
- Security:
  - Intrusions are intentional
  - Testing: reduce number of vulnerabilities that allow intrusions black hat: find vulnerabilities so that they can be exploited
  - Objective: block path of intrusion

Security System Architecture

- Networked systems
  - Use of firewalls to block intrusions/extrusions
- Single computing System: OS
  - Isolation of processes
    - Threads are not isolated
  - Isolation in containers: cgroups
  - Isolation of virtual machines
- Isolation mechanism may be imperfect.

Internet architecture

Connections identified by IP addresses and port numbers.

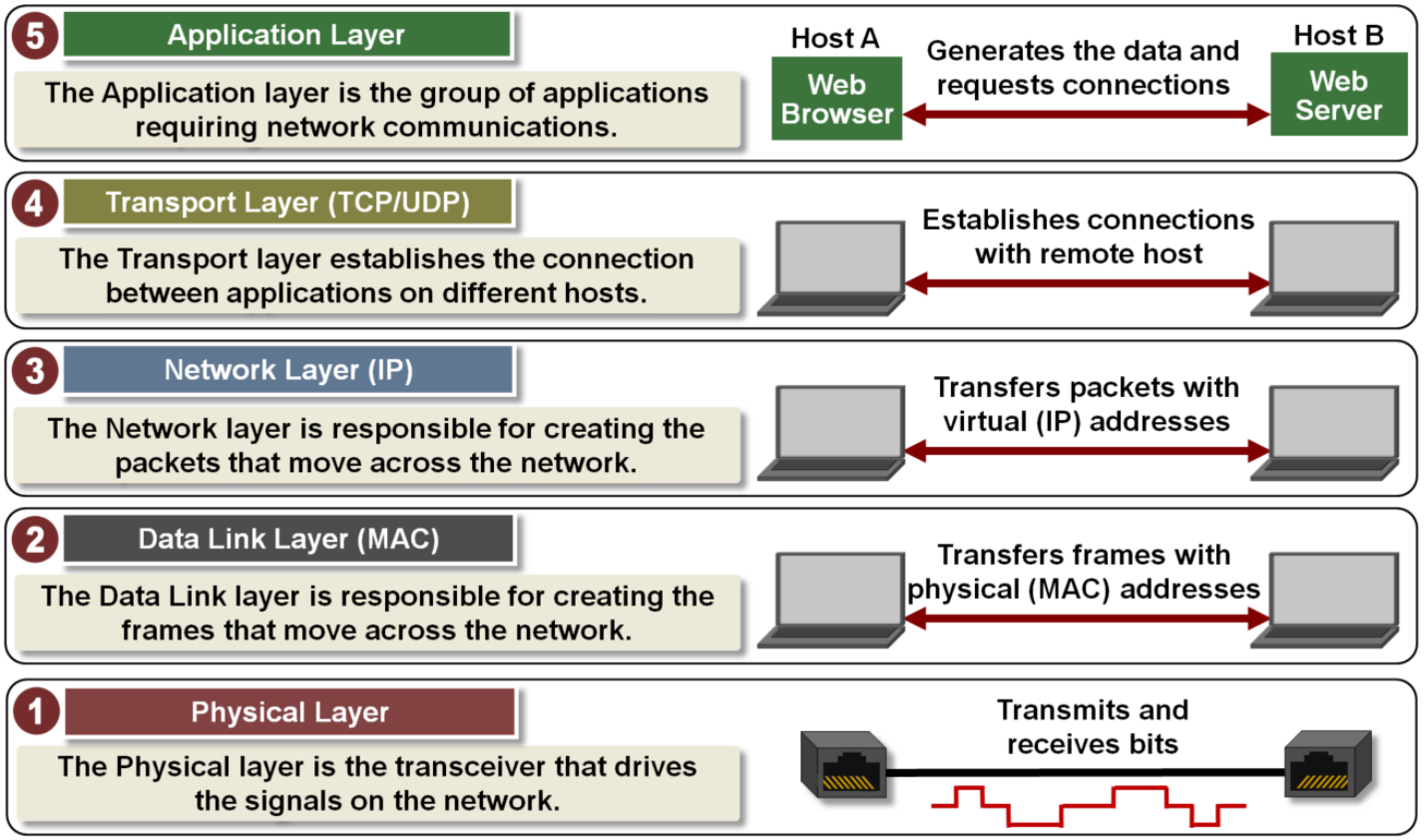


https://www.yaldex.com/tcp_ip/FILES/06fig07.gif

Colorado State University

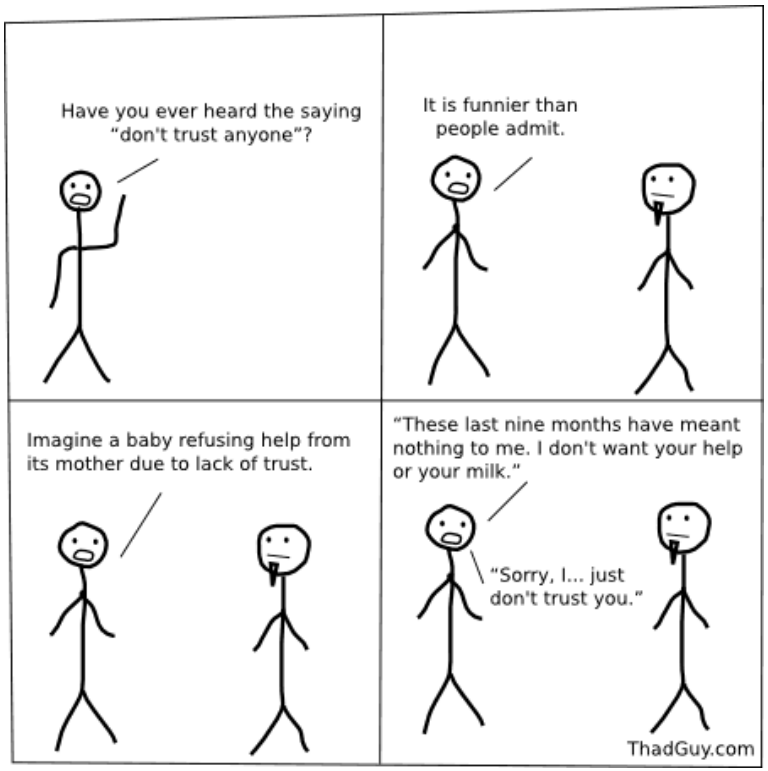
Internet: IP, TCP

- Networking protocols have multiple layers.



https://microchipdeveloper.com/tcpip:tcp-ip-five-layer-model

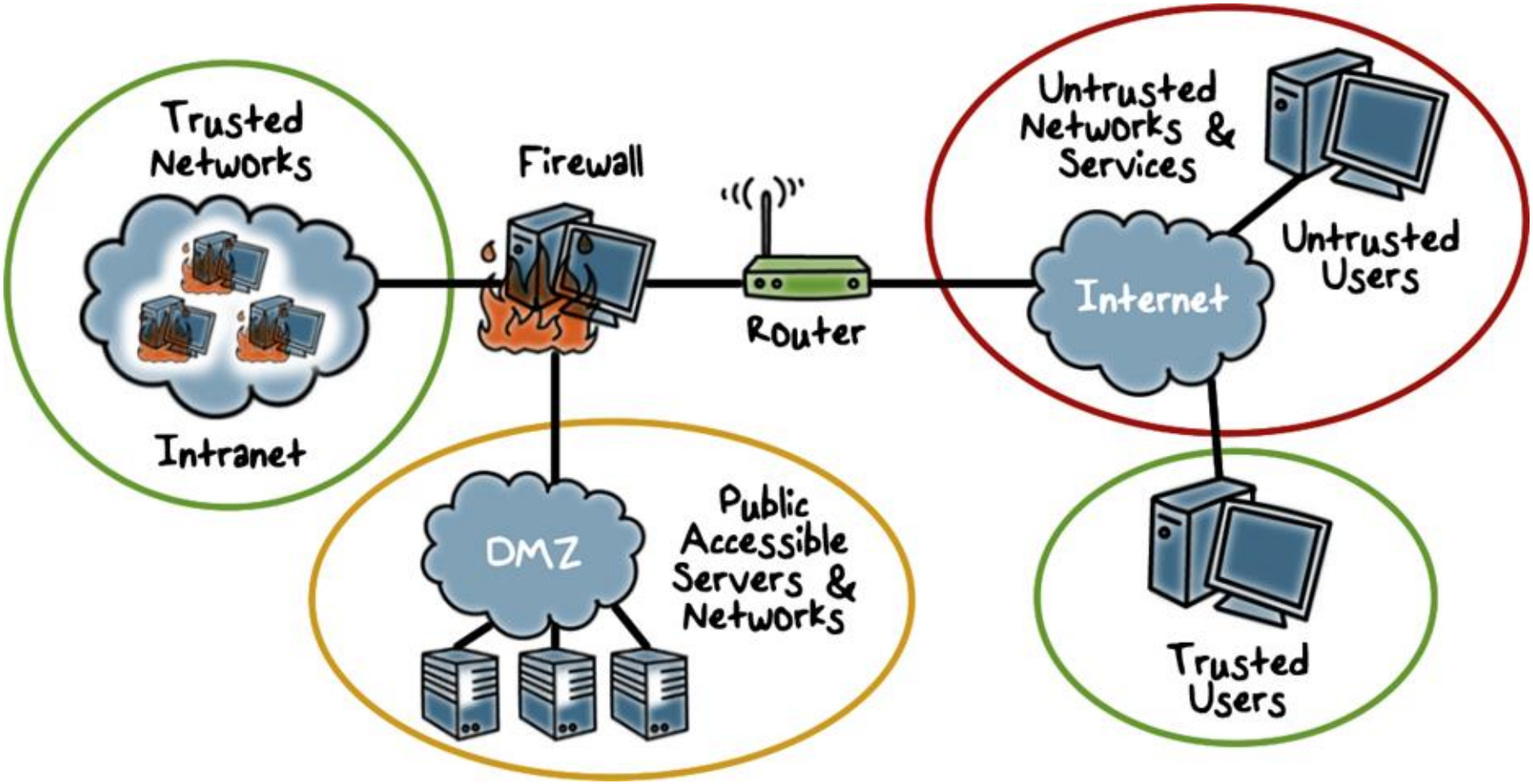
Trusted and Untrusted Actors



A binary trusted/untrusted classification is an **approximation**.

Colorado State University

Firewalls



DMZ: “Demilitarized zone”, distributed firewalls, From Georgia Tech
Note multiple levels of trust.

Firewalls

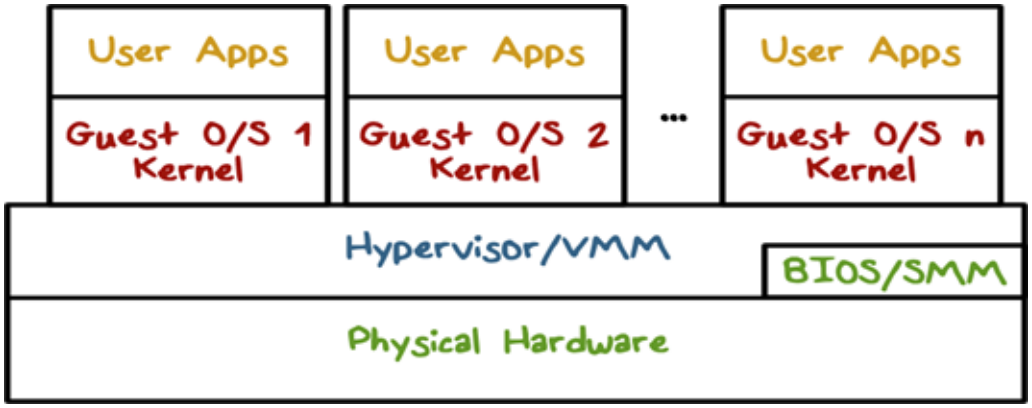
- A firewall checks traffic (packets or sessions) passing through it
- Can be programmed to check address ranges (IP addresses, ports), protocols, applications and content types.
- Can provide address translation, encryption

Operating System

- The operating system serves as as trusted computing base (TCB) that controls access to protected resources.
  - Must establish the source of a request for a resource (authentication is how we do it)
  - Authorization or access control
  - Mechanisms that allow various policies to be supported
- How
  - Hardware support for memory protection
  - Processor execution modes (system and user modes)
  - Privileged instructions - can only be executed in system mode
  - System calls - transfer control between user and system code

Isolation in a system

- OS isolates address spaces of different processes using address translation. Also data vs code isolation.
  - Page tables governed by OS.
- In virtualization, hypervisor isolates virtual machines.
- Containers (Docker): Linux cgroups isolate process groups.



Colorado State University

Summary

Security must be a consideration in a

- Networked system
- Operating Systems
- Security protocols, cryptography (later)