Quantitative Cyber-Security

Colorado State University
Yashwant K Malaiya

CS559 L3

Authentication, Risk

CSU Cybersecurity Center
Computer Science Dept

Today

- Access control
- Authentication
- Risk

Course notes:

- Assignment 1 Quick Research will be available on Thursday..
- Pledge form for permission to use a device in the class is available.

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.

HW1: Quick Research

In this assignment, you need to do some quick research on a selected topic to find out the following

- Discuss the current status of technology in the field.
- Recent development, say past 2-4 years.
- Current related products and mature technologies available.
- Identify 3 organizations (industry, research labs or academic) that have an influential role in advancing the field.

Search using these in this sequence: Google News, Google Scholar, available data bases at CSU library (IEEE Explore, ACM, Science Direct etc), and finally general Google search.

Use of AI is restricted.

See Canvas for details. Report due Wed. Sept 9 (HW1), Slides due Fri. Sept 11, in Discussions.

What is not good “Research”

Locating sources of information should involve significant effort.
Examples of inadequate research

- Finding information that anyone can find with a few clicks.
- Finding a couple of high level overview articles and rephrasing them.
- Finding a few papers and giving a brief summary of each of them, without considering a logical relationship among them.
- Finding work of a single research group and summarizing what they have done.
- Searching of information using a only limited number of keywords such as just “Economics of ransomware”
- Mechanically generated using GenAI tools

AI Guidelines

Overarching Principles in the Use of AI by Graduate Students

- Students remain fully responsible for all scholarly work produced with AI assistance.
- AI may assist but does not assume authorship or accountability
- Transparency is expected whenever AI makes a substantive contribution.
- Human judgement is indispensable for scientific reasoning, interpretation, and ethical decision making. AI should not replace human judgment.
- Compliance with legal, ethical, contractual, and sponsor requirements is mandatory.

Using Generative AI to Support Writing Papers and Theses

- The use of generative AI tools and technologies to create content is permitted but must be fully disclosed.
- See department policies.

Do not use AI at the beginning of literature search. Use only after the the problem and the preliminary approach is identified.

Quantitative Security

Colorado State University
Yashwant K Malaiya

CS 559
Access Control

CSU Cybersecurity Center
Computer Science Dept

Access Control

Definition according to RFC 4949:

> "Access control is a process by which use of system resources is regulated according to a security policy and is permitted only by **authorized entities** (*users, programs, processes, or other systems*) according to that policy"

RFC 4949 defines security as

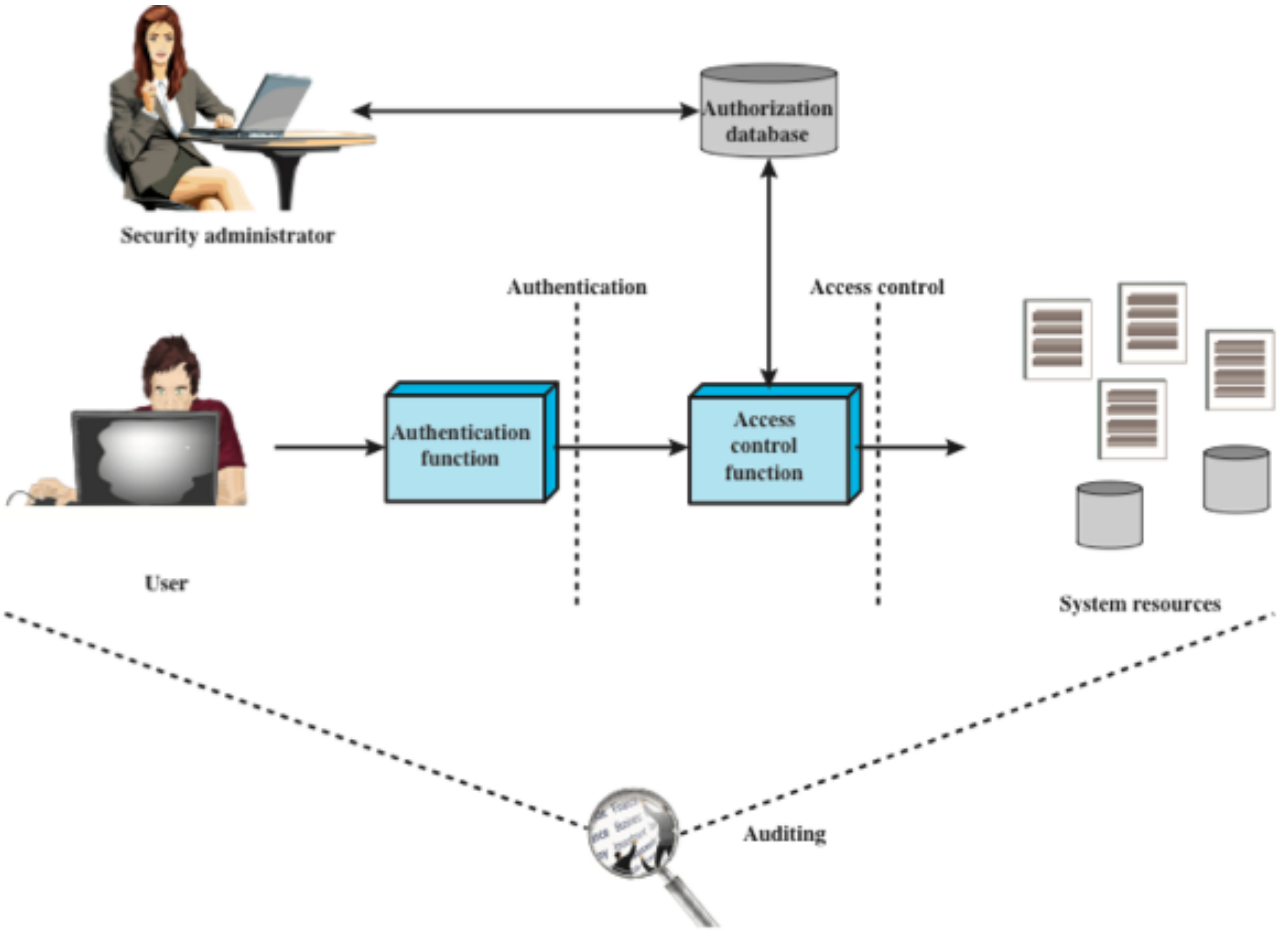
> "measures that implement and assure security services in a computer system, particularly those that assure access control service"

Thus all of computer security is concerned with access control.

Enforced by the Trusted Computing Base (OS) which performs

- authentication
- authorization

Access Control as a Security Function



Subjects, Objects, and Access Rights

- A **subject** is an entity capable of accessing objects.
  - represented by a process. A user/application gains access to an object by means of a process that represents that user/application. The process takes on the attributes of the user, such as access rights.
  - Held accountable for the actions.
  - Classes: Owner (u in linux), Group (g), World (o), people with specific roles
- An object is a resource to which access is controlled.
  - an entity used to contain and/or receive information.
  - Examples: pages/segments, files/directories/programs, ports, devices etc.

Subjects, Objects, and Access Rights

An access right describes the way in which a subject may access an object.

- **Read**: User may view information in a system resource (e.g., a file, selected records in a file, selected fields within a record, or some combination). Read access includes the ability to copy or print.
  - Directory: ability to list the directory.
- **Write**: User may add, modify, or delete data in system resource (e.g., files, records, programs). Write access includes read access.
  - Directory: create new files
- **Execute:** User may execute specified programs.
  - Directory: enter it to access the files within it.

- Delete: User may delete certain system resources, such as files or records.

- Create: User may create new files, records, or fields.

- Search: User may list the files in a directory or otherwise search the directory.

Access Control Schemes

Discretionary Access Control (DAC): Scheme in which an entity may be granted access rights that permit the **owner** entity, by its own violation, to enable another entity to access some resources.

- Ex: Linux. Provided using an access matrix

Mandatory Access Control: **Centralized authority** sets security policy for all resources

- Example: SELinux

Role based access control: based on the roles that users have within the system and on rules specifying the accesses are allowed to users in given roles.

Example: Access Control Matrix

		OBJECTS			
		File 1	File 2	File 3	File 4
SUBJECTS	User A	Own Read Write		Own Read Write	
	User B	Read	Own Read Write	Write	Read
	User C	Read Write	Read		Own Read Write

(a) Access matrix

Access Control List (ACL): Every object has an ACL that identifies what operations subjects can perform. Each access to object is checked against object's ACL.

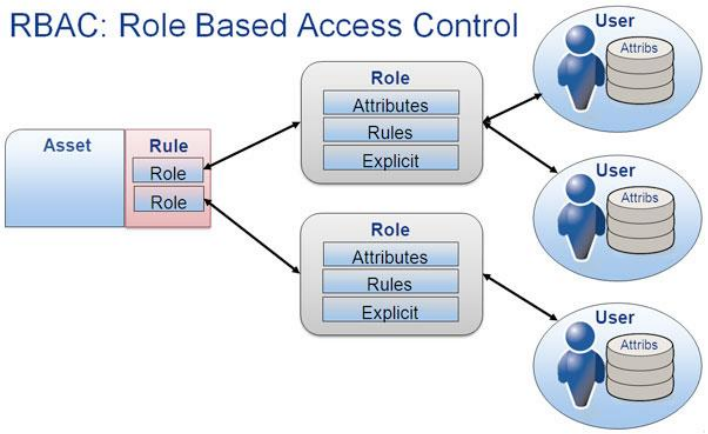
May be kept in a relational database. Access recorded in file metadata (inode).

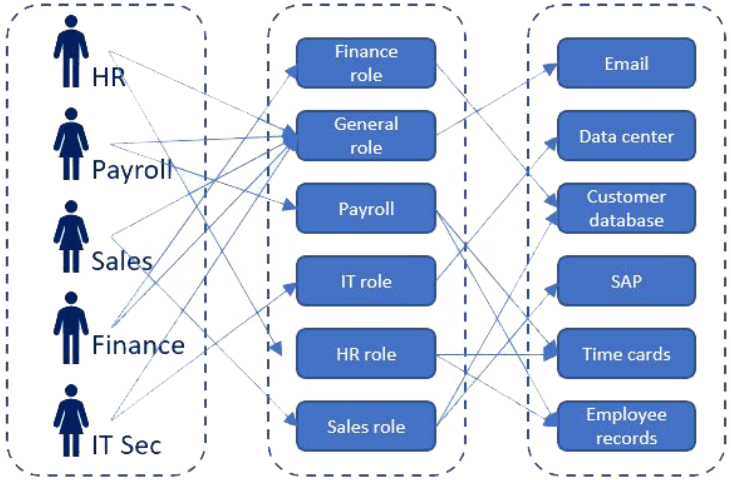
Unix Access Control

- Subjects (Who?)
  - Users
- Objects (What?)
  - Files, directories
  - Files: sockets, pipes, hardware devices, kernel objects, process data
- Access Operations
  - Read, Write, Execute
  - Set by root or owner of the object
- Linux is an example of *discretionary access control*.
  - Resource owners can set the security policy for objects they own
- Superuser (root) allowed to do anything.
  - System administrators assume superuser role to perform privileged actions – Good practice to assume superuser role only when necessary

Role Based Access Control (RBAC)

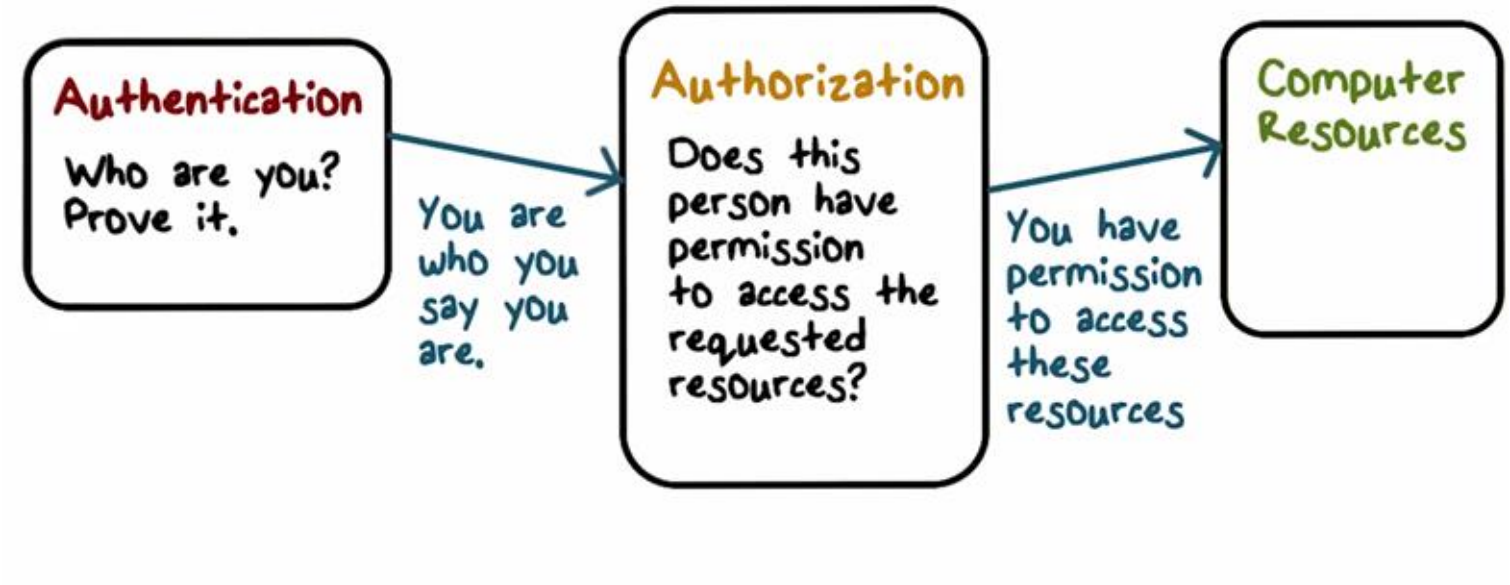
- **Role-based access control (RBAC):** based on the roles that users have within the system and on rules specifying the accesses are allowed to users in given roles.
- Widely used commercially in larger organizations.





Colorado State University

Authentication



Georgia Tech

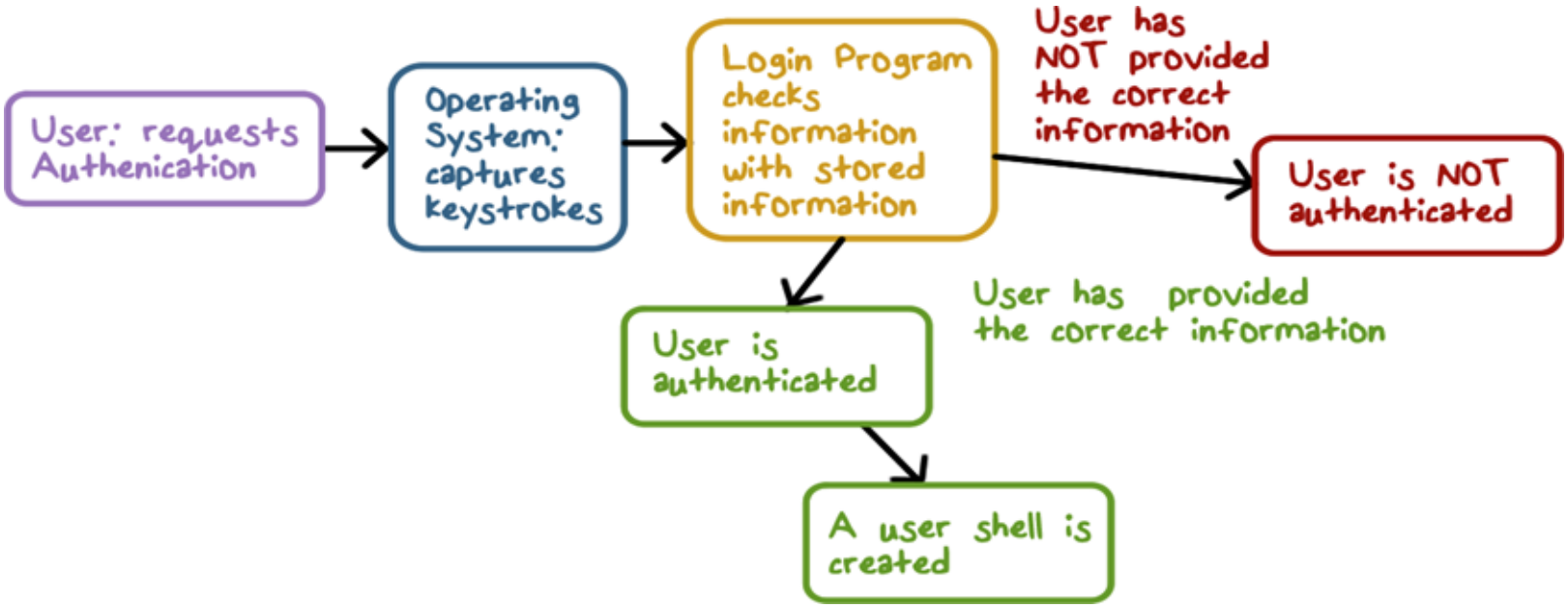
Authentication

- OS (Trusted Computing Base) needs to know who makes a request for a protected resource
- A process that makes the request does it on behalf of a certain user
- Authentication handles the question: on whose behalf the requesting process runs?
- Involves
  - claims about an identity and
  - verification of the claimed identity
- Goals
  - No false negatives
  - No false positives (major consideration)

Authentication Methods

- Something a user knows
  - password
- Something a user has
  - Ex. Id card, smartphone
- Something a user is
  - Biometric (face or fingerprint)
- Multifactor authentication to reduce false positives
  - Ex. OTP (*one-time password*

Implementation: Password based Authentication



The system must provide a trusted path from keyboard to the OS.

Georgia Tech

Password authentication

Possible approaches

1. Store a list of passwords, one for each user in the system file, readable only by the root/admin account
   - Why the admin need to know the passwords?
   - If security is breached, the passwords are available to an attacker. No longer used.
2. Do not store passwords, but store something that is derived from them
   - Use a hash function and store the result
     - More about that later
   - The password file is readable only for admin

Security Challanges

- Password guessing
  - List of bad passwords. 123456, password, ..
- Brute force guessing
  - more later
- Good passwords are the ones harder to remember
- May be stolen using
  - keyloggers,
  - compromised websites where same password was used
  - eavesdropping *(Alice, Bob and Eve?)*

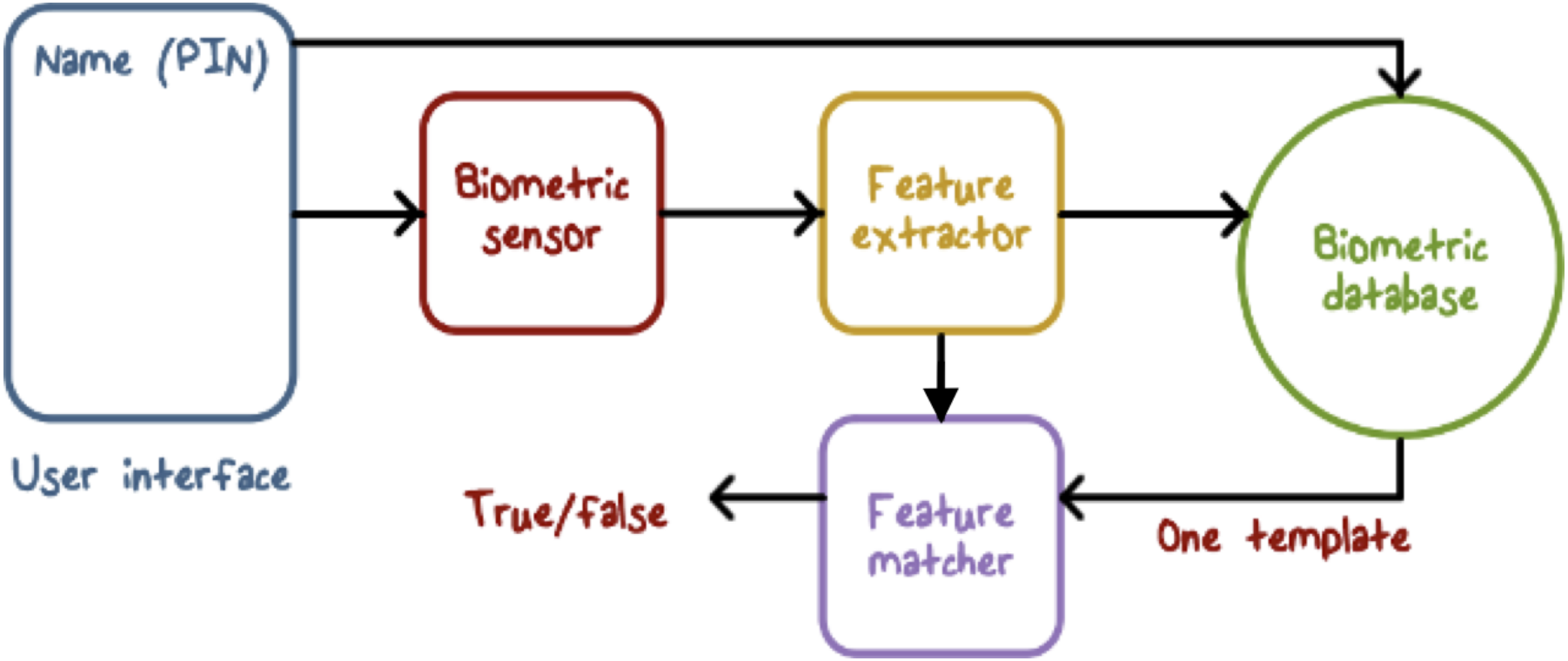
Biometric Authentication

- Fingerprints (finger swipes)
- Keystroke dynamics
- Voice
- Retina scans

Issues

- Feature value distribution or a range
- False positives and negatives

Implementing Biometric Authentication



Summary

Access control

- Who can access what
- Authentication

Quantitative Security

Colorado State University
Yashwant K Malaiya

CS 559

Risk and its components

CSU Cybersecurity Center
Computer Science Dept

Risk

Topics

- Risk and its components
  - Visualization using Risk matrix
  - FAIR
- Insurance

Risk: Formal definition

Definition: The Risk due to an adverse event e_i is

$$Risk_i = Likelihood_i \times Impact_i$$

- $Likelihood_i$: Probability of the adverse event i occurring within a specific time-frame.
  - The time-frame is often chosen to be a year. Note that the probability of an adverse event happening depends on the duration of the time-frame.
  - Probability is a number between 0 and 1.
- $Impact_i$: The impact of the adverse event, measured in monetary terms.
  - Note that impact me be direct or indirect.
  - Common units are dollars (US$)#.

US$ is a common and convenient scale. Non-monetary losses, including human life, can be converted into US$, if you are a business or insurance company .

Risk: Possible Actions

How to handle risk?

Example: Credit card fraud

- Risk acceptance
  - Ex: fraud cost paid through fees charged to merchants
- Risk mitigation
  - Ex: install anti-fraud technology, adds to costs
- Risk avoidance
  - downgrade high-risk cardholders to debit or require additional verification: lost time/business
- Risk transfer
  - buy cyber-insurance to cover excess losses

Risk as a composite measure

Formal definition:

- **Risk** due to an adverse event e_i

  $Risk_i = Likelihood_i \times Impact_i$

- A specific time-frame, perhaps a year, is presumed for the likelihood.
- $Likelyhood_i$ may be replaced by $frequency_i$, when it may happen multiple times a year.
- This yields the expected value. Sometimes a worst-case evaluation is needed.

In classical risk literature, the internal component of Likelihood is termed “Vulnerability” and external “Threat”. Both are probabilities. There the term “vulnerability” does not mean a security bug, as in computer security.

Risk as a composite measure

- Likelihood can be split in two factors

  $\text{Likelihood}_i = P\{\text{A security hole}_i \text{ is exploited}\}.$

  $= P\{\text{hole}_i \text{ present}\}.$

  $P\{\text{exploitation} \mid \text{hole}_i \text{ present}\}$

- $P\{\text{hole}_i \text{ present}\}$: an internal attribute of the system.
- $P\{\text{exploitation} \mid \text{hole}_i \text{ present}\}$: depends on circumstances outside the system, including the adversary capabilities and motivation.
- In the literature, the terminology can be inconsistent.

Caution: In classical risk literature, the internal component of Likelihood is termed "Vulnerability" and external "Threat". Both are probabilities. There the term "vulnerability" does not mean a security bug, as in computer security.

Annual Loss Expectancy (ALE)

Note the terminology is from the Risk literature.

- Single loss expectancy (SLE)

  SLE = AV x EF,

  – AV is the value of the asset. EF is exposure factor which describes the loss that will happen to the asset as a result of the threat, expressed as fractional (or %) value.

- Annual loss expectancy (ALE)

  ALE = SLE x ARO

  – Where ARO is Annualized rate of occurrence.

- Example: Asset value is $100,000, exposure factor is 30%, and ARO is 0.5/year (once every two years). Thus
  – ALE = ($100,000 x 0.30) x 0.5 = $15,000.
- Note that ALE is essentially what we term as “risk”, with an annual time frame.

Annual value of the countermeasure

Cost/benefit analysis of countermeasures

- A countermeasure reduces the ALE by reducing one of its factors.

  COUNTERMEASURE_VALUE
  = (ALE_PREVIOUS – ALE_NOW) – COUNTERMEASURE_COST

  Where ALE_PREVIOUS: ALE before implementing the countermeasure.
  ALE_NOW: ALE after implementing the countermeasure
  COUTERMEASURE_COST: *annualized* cost of countermeasure
- The COUNTERMEASURE_VALUE should be positive.

ROI

- Businesses often use a term Return on Investment (ROI. it can be defined as

  ROI =

  COUNTERMEASURE_VALUE/COUNTERMEASURE_COST

- Given the following, what is the ROI?
  - ALE_PREVIOUS = $50,000
  - ALE_NOW=$25,000
  - COUNTERMEASURE_COST = $10,000
  - ROI = (50,000-25,000-10,000)/10,000 = 1.5

  (This assumes an annual perspective)

Likelihood & Impact scales

- Quantitative or descriptive levels
  - Number of levels may depend on resolution achievable
- Scale: Logarithmic, Linear or combined
  - A logarithmic scale is natural when the numbers involved vary by several orders of magnitude.
- Risk = Likelihood x Impact
  - May be rewritten as

    Log(Risk) = Log(Likelihood) + Log(Impact)
- If the term "Score" is proportional to Log value
  - Risk score = Likelihood score + Impact score
  - Adding scores valid if scores represent logarithmic values.
  - Example:
    - Likelihood = 10%, impact = $100,000 ⇒ **Risk = $10,000**
    - Scores: Log(0.10) = -1, log (100000) = 5 ⇒ **Risk score = 4**

$10^2 = 100$
$\text{Log}_{10}\ 100 = 2$
Log implies base 10, if not specified

Risk Matrix

- Likelihood and Impact divided into levels
  - Each level quantitatively/qualitatively defined
- Cells marked by the overall risk
  - Low, Medium, High, Extreme etc.
- *Equal risk regions* along the diagonal, valid provided score scales are logarithmic.

Likelihood	Consequences				
	Insignificant	Minor	Moderate	Major	Severe
Almost certain	M	H	H	E	E
Likely	M	M	H	H	E
Possible	L	M	M	H	E
Unlikely	L	M	M	M	H
Rare	L	L	M	M	H

Colorado State University

35

Risk Matrix: Example

LIKELIHOOD (probability) How likely is the event to occur at some time in the *(Linear Scale time specific matrix)*	**CONSEQUENCES** What is the Severity of injuries /potential damages / financial impacts (if the risk event actually occurs)? *(Logarithmic Scale, property industry specific matrix)*				
	Insignificant	Minor	Moderate	Major	Catastrophic
	No Injuries First Aid No Envir Damage << $1,000 Damage	Some First Aid required Low Envir Damage << $10,000 Damage	External Medical Medium Envir Damage <<$100,000 Damage	Extensive injuries High Envir Damage <<$1,000,000 Damage	Death or Major Injuries Toxic Envir Damage >>$1,000,000 Damage
Almost certain - expected in normal circumstances (100%)	MODERATE RISK	HIGH RISK	HIGH RISK	CRITICAL RISK	CRITICAL RISK
Likely – probably occur in most circumstances (10%)	MODERATE RISK	MODERATE RISK	HIGH RISK	HIGH RISK	CRITICAL RISK
Possible – might occur at some time. (1%)	LOW RISK	MODERATE RISK	HIGH RISK	HIGH RISK	CRITICAL RISK
Unlikely – could occur at some future time (0.1%)	LOW RISK	MODERATE RISK	MODERATE RISK	HIGH RISK	HIGH RISK
Rare - Only in exceptional circumstances 0.01%)	LOW RISK	LOW RISK	MODERATE RISK	MODERATE RISK	HIGH RISK

Example:

Likely x Moderate
= (10/100) x $100,000
= $10,000 High

Colorado State University

Scales

Note the use of logarithmic scales.

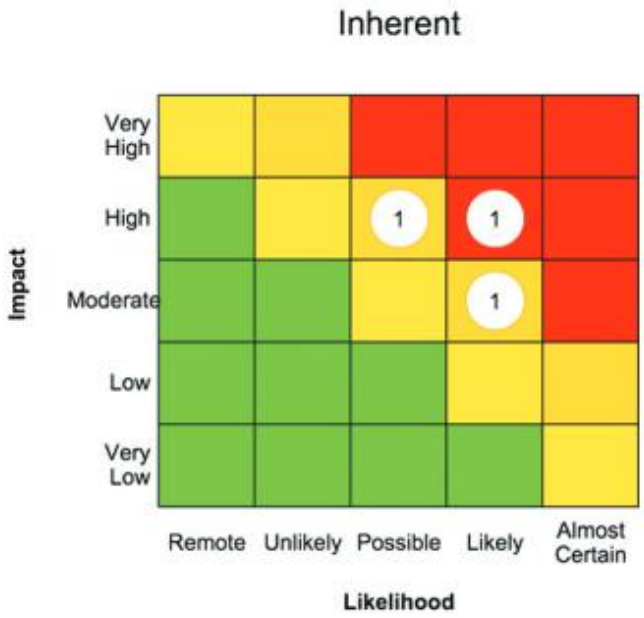
Likelihood	
Almost certain	≈ 100%
Likely	≈ 10%
Possible	≈ 1%
Unlikely	≈ 0.1%
Rare	≈ 0.01%

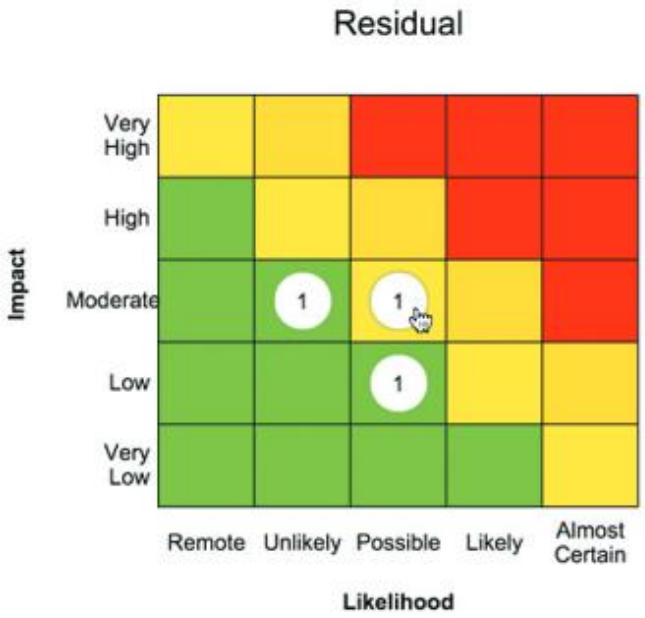
Consequence	
Insignificant	<< $1,000
Minor	<< $10,000
Moderate	<< $100,000
Major	<< $1,000,000
Catastrophic	>> $1,000,000 death

Advantages of Risk Matrices

- Visual representation of distribution of risks in a system.
  - Similar to “Heat Maps” for the stocks in a market
- Change in overall risk due to a system redesign can be visualized.
  - Attempt to move risks from red region to green region.
- Allow expert estimates to be used instead of exact numbers.
  - Calibration or training may be needed to make estimates more accurate.

Visualizing Risk Reduction





Risks reset

Risk Title	Business Unit	Risk No	Category	Subcategory	Inherent Rating	Residual Rating
IT Infrastructure Failure	TF Group	R006	Operational	IT Disaster Recovery Planning		
Bribery and Corruption	TF Group	R005	Conduct of Business	Financial Crime		
Loss of Key Staff	TF Group	R007	Strategic	Loss of Key Staff		

RISK MANAGEMENT FOR FINANCIAL SERVICES

Colorado State University

Limitations of Risk Matrices

The main limitations of Risk Matrices arise because

- Limited resolution: continuous to discrete scales
- The scales are generally logarithmic
- May rely on subjective judgement, which may not be accurate.

- Cox, L.A. , 'What's Wrong with Risk Matrices?', Risk Analysis, April 2008, Vol. 28, No. 2, pp. 497-512
- Julian Talbot, What's right with risk matrices? 2018

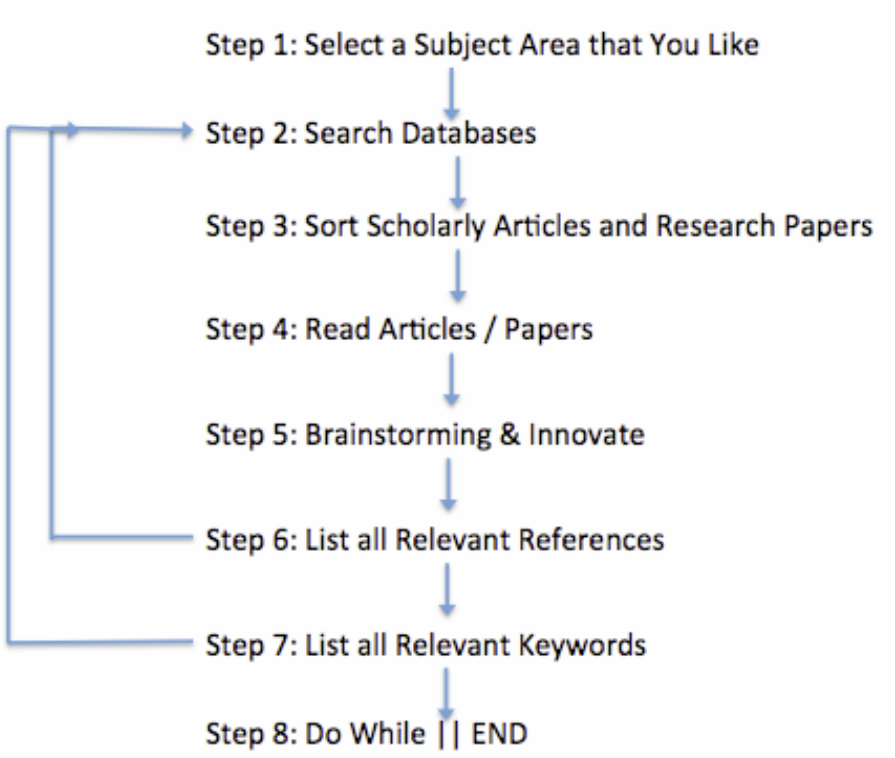
Research Objective

- Become familiar with technical topic of current interest
  - Current state of the art
  - Where the field is going (thus what to expect next)
- Become an expert in the field
  - Should be able to answer important questions
- Original contributions
  - What needs to be done
  - Suggest how it would be addressed
- Present your work
  - Briefly (presentation) and in detail (paper)

Project types

- A thorough survey of a topic, with original insight
- A development of a new scheme
  - or a fresh implementation of an existing scheme
- Modeling and analysis of an existing scheme.
  - If it has not been done/done adequately before
- Development of a hypothesis and evaluating it.
  - Standard statistical methods
- A meaningful combination

Steps for Identifying Sources



How to Start a Research Work in Computer Science:
A Framework For Beginners Somdip Dey
https://xrds.acm.org/article.cfm?aid=2627954

Search Databases

Specific sources: database indexes

- Google Scholar
  - Forward links: Paper X Cited by
  - Backward Links: Paper X cites
- Researcher sites
  - Personal/Group Website
  - DBLP
  - Google Scholar: researcher
- CSU Library etc.

General (*accessible through CSU Library*)

- ACM Digital Library
- IEEEXplore Digital Library
- ScienceDirect etc

Source types

- Journals: published several times a year
  - Rigorously reviewed, long publication delay
  - Journal, Transactions, …
- Conferences: held once a year,
  - Refereed Proceedings: Conference, Symposium, …
  - Workshops: Mildly refereed, often no proceedings
- Research groups
  - Industry, academic, consultants: web site
- Industry publications
  - Magazines, blogs, white papers, product website
  - Annual threat reports
- Books:
  - Textbooks/Trade books: well known things
  - Research monographs/collections

How to Read a Paper: THE THREE-PASS APPROACH

- The first pass: Read
  - the title, abstract, and introduction
  - section and sub-section headings, but ignore everything else
  - the conclusions
- The second pass: Read
  - figures, diagrams, tables and other illustrations
  - mark relevant unread references for further reading
  - Do you need to read it in detail?
- The third pass: Read critically
  - identify and challenge assumption and views
  - Loop up references needed

Keshav, S., How to Read a Paper, ACM SIGCOMM, http://ccr.sigcomm.org/online/files/p83-keshavA.pdf

Avoid Prior Bias