Quantitative Security

Yashwant K Malaiya

CS559

How to do research

CSU Cybersecurity Center

Computer Science Dept

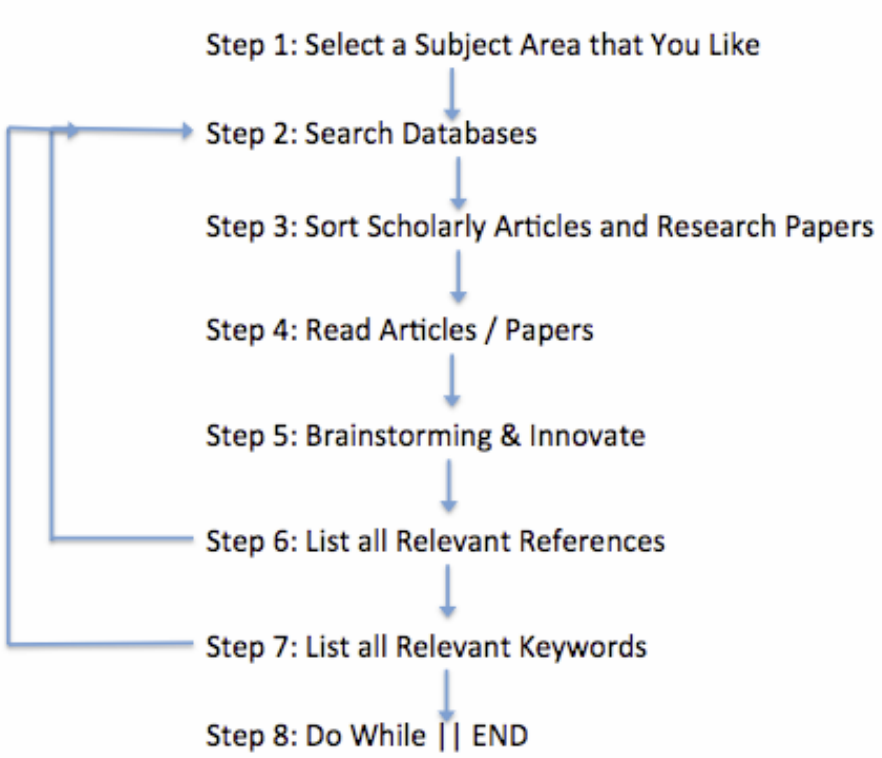
Research Objective

- 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 type

- 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.
- A meaning 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

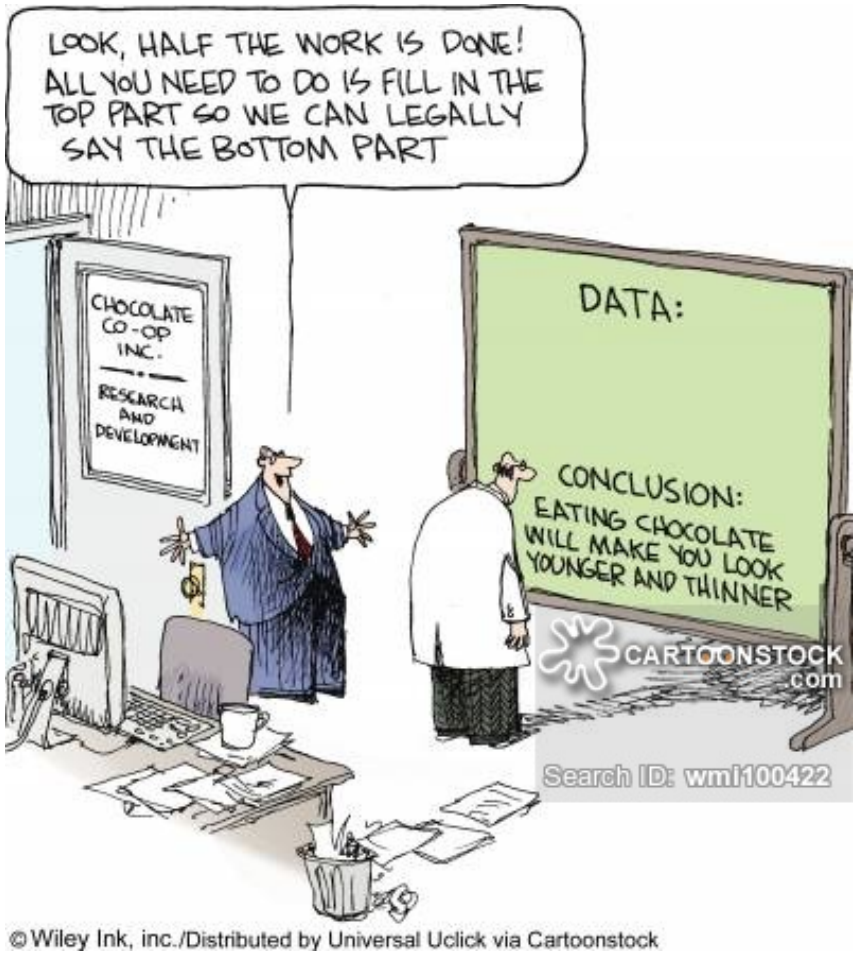
- Journals: published several times a year
  - Rigorously reviewed, long publication delay
  - Journal, Transactions, …
- Conferences: held once a year, proceedings published
  - Conference, Symposium, …
- Research groups
  - Industry, academic, consultants: web site
- Industry publications
  - Magazines, blogs, white papers, product website
- Books: often well known stuff

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 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



Key Questions

- What problem are you trying to solve?
  - Why is it important?
- What recent advances or interesting ideas are there?
  - what have others done?
  - what have others not done yet?
- What have you done (so far)?
  - What is your next step?
  - how does it relate to your goal?
  - why is it important?
- How will you know when …
  - you've made progress?
  - you're done?

William J. Rapaport, How to Write

Proper formatting

- Proper citations: IEEE/ACM format
  - Including authors, title, publication, page numbers, date.
- Two column IEEE/ACM format
  - Title, name(s) of the author(s), name of the class and professor
  - Abstract
  - Your contribution and what is new
  - Introduction (background & related work, objectives & methods),
  - Assumptions/schemes/models/problem-formulation
  - Comparison/discussion/derivation etc. of the results,
  - Conclusions and suggestions for improvements
  - References.
  - Appendixes (if need)

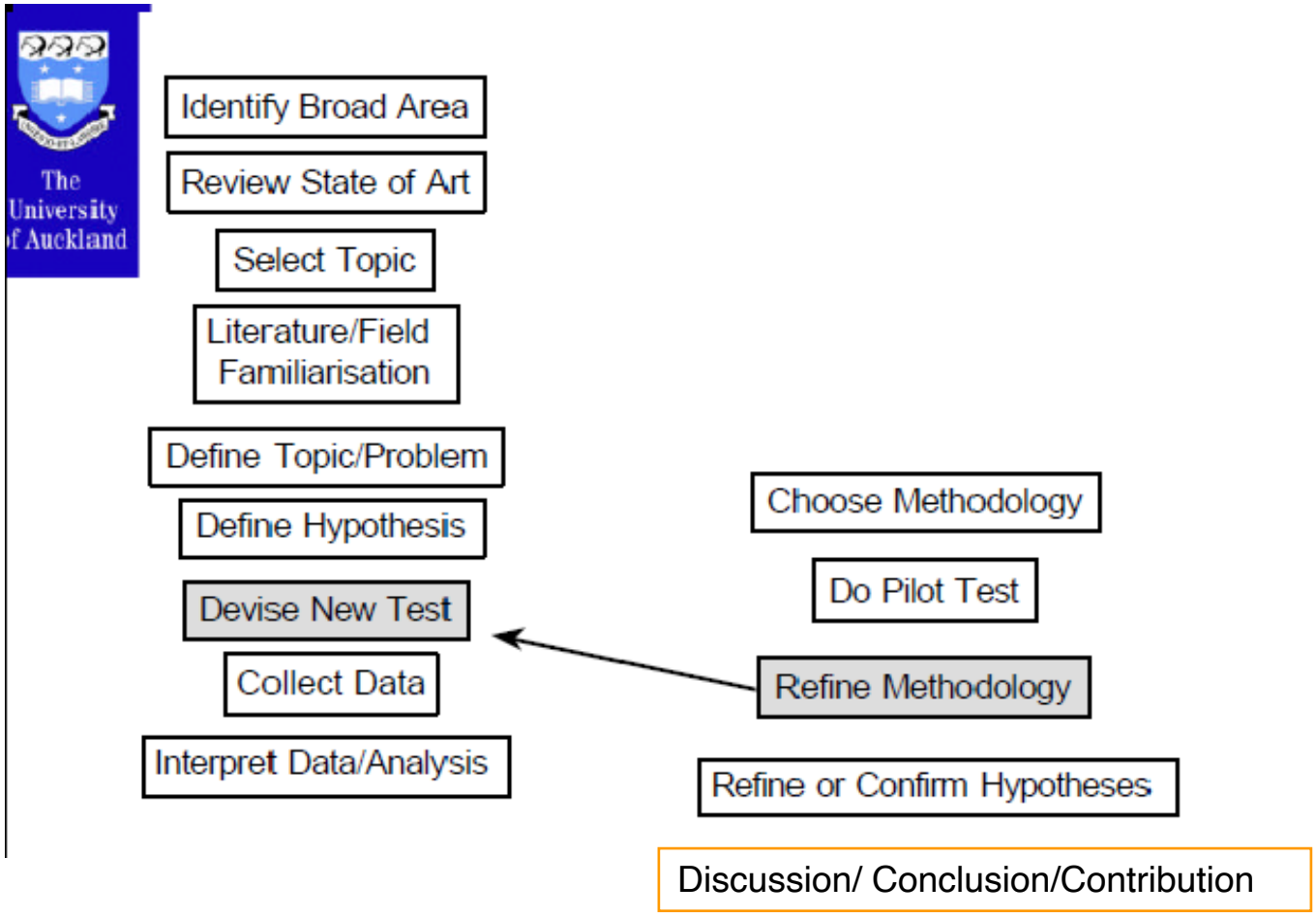
Must have diagrams and hard technical info (equations/tables/plots/screen-shots etc)

Evaluation

Similar to paper review for conferences/journals

- **Significance and originality**
- **Thoroughness of research**
- **Depth of understanding displayed**
- **Presentation**
- Final report is submitted through TurnItIn using Canvas
  - Checks for overlap with other documents (plagiarism)
  - Some overlap OK
  - Cite sources of definitions, ideas, data, figures etc.
  - Any text copied and pasted must be enclosed in quotes and cited
    - Exception: references (cite only those you have seen)

Typical Original Research Process



Introduction to Research in Computer Science - Ian Watson

About the Term Project

Yashwant K. Malaiya
Colorado State University

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**
- ***Do it (if your expertise and time allows)***
- **Present your work**
  - **Briefly (presentation) and in detail (paper)**

Deliverables

- A *one-page* proposal
  - motivation, brief scope of study and *some specific references*.
  - Identify key sources of information
- Progress report: should have completed a major part of the project.
- Slides based on findings thus far
  - Post in Canvas Discussions and present in class
  - Should demonstrate
    - thoroughness of literature search
    - Understanding of the key technical concepts
  - Peer review required
- Final report (two column format)

Progress report

- **Documentation:** http://www.cs.colostate.edu/~cs530dl/f18/project
- **Progress report (3-5 pages)** It should indicate that you have finished at least half of the work.
- Partial version of the final report
- Abstract, Background
- Summary of the findings
- What the final report will contain , any refinements of the objectives as a result of the recent study,
- Applicable references in proper format.

You Must Do Research

Not enough:

- Summary of a couple of papers
- Summary of work of a single research group
- Rephrasing of existing surveys

You must know (and should be able to answer related questions):

- Current state of the art
- Alternative approaches and how they can be evaluated
- Technology trend
- Find data describing the technology
- Existing issues and challenges

Citing Sources

"IEEE" "ACM" etc:

- These are professional organizations that organize numerous conferences and published journals
- You must specify the author, title of paper, specific names of conference/journal, associated details, date, page numbers
- A simple URL is not a valid citation
- URL not needed for conference, journal publications. Needed for on-line publications (Organizational reports, Industrial white-papers, News etc)

Omar H., Alhazmi and Yashwant K. Malaiya, "Application of vulnerability discovery models to major operating systems", IEEE Transactions on Reliability, Volume: 57 , Issue: 1, pp. 14-22, March 2008,

Ambrose Andongabo, Ilir Gashi, "vepRisk - A Web Based Analysis Tool for Public Security Data", 13th European Dependable Computing Conference (EDCC) 2017, pp. 135-138, 2017.

You must include

- Title, your name, class, year, professor's name
- Abstract: What does it include and why is it important
- Background: Other existing work and background ideas
- Technical discussion: detailed discussion of findings with non-text material (charts, plots, tables. algorithms etc)
- Discussion & Summary
- References

Quantitative Security

Colorado State University

Yashwant K Malaiya

CS 559

Frameworks

CSU Cybersecurity Center

Computer Science Dept

List-based vs Quantitative Approaches

Management Approaches

- **List based approach (binary/compliance):**
  - **Compile lists of all possible things, actions.**
  - **Subdivide items into finer sub-items to make sure everything is considered.**
  - **Identify policies/standards to ensure everything is covered.**
  - **Check the boxes.**
- **Quantitative approach**
  - **Includes lists of items/sub-items**
  - **Quantitatively evaluate possible outcomes and assign weights.**
  - **Compute overall figure of merit. Optimize if possible.**

This is how I see things. YKM

Quantitative Approaches

- Determine exact/approximate numbers using measurements or models.
  - Numbers may be hard to get
- Use intuitive numbers (perhaps 0-10) etc using some description.
- No numbers, but use mental quantification based on past experiences.
- Binary: Yes/No, Done/Not Done

This is how I see things. YKM

Security Frameworks

Several frameworks/standards have been identified to organize security concerns and controls. Major frameworks include

- **NIST Cybersecurity Framework (CSF) for Critical Infrastructures (V 1.0 Feb 2014)**
- **PCI: Payment Card Industry Data Security Standard v2.0**
- **Center for Internet Security (CIS) Critical Security Controls (CSC)**

Note: Managers use/understand jargon specific in the field. You may need to translate jargon into what you understand. Talmud.

NIST Cyber security Framework

NIST: National Institute of Standards and Technology

- **Agency of U.S. Department of Commerce**
  - **Federal, non-regulatory agency around since 1901**
- **develops and promotes measurement, standards and technology to enhance productivity, facilitate trade, and improve the quality of life.**

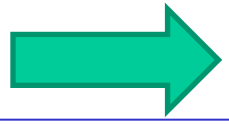
NIST Cybersecurity

- **Cybersecurity since the 1970s**
- **Computer Security Resource Center – csrc.nist.gov**

The Framework for Improving Critical Infrastructure Cybersecurity, April 2018

NIST Framework - Motivation

- The NIST framework is “Risk-based” (semi-quantitative) and not compliance based.
- Core “Functions”
  - Identify: defines the actions related to the understanding of policies, governance, assets, risks, and priorities.
  - Protect: activities related to the development and implementation of safeguards and training
  - Detect: monitoring and detection activities to identify events.
  - Respond: activities related to actions to respond to detected cybersecurity event.
  - Recover: plans and processes to recover.
- Functions are divided into categories.



Framework Categories

	Function	Category
What processes and assets need protection?	Identify	Asset Management
		Business Environment
		Governance
		Risk Assessment
		Risk Management Strategy
		Supply Chain Risk Management[1.1]
What safeguards are available?	Protect	Identity Management, Authentication and Access Control[1.1]
		Awareness and Training
		Data Security
		Information Protection Processes & Procedures
		Maintenance
		Protective Technology
What techniques can identify incidents?	Detect	Anomalies and Events
		Security Continuous Monitoring
		Detection Processes
What techniques can contain impacts of incidents?	Respond	Response Planning
		Communications
		Analysis
		Mitigation
		Improvements
What techniques can restore capabilities?	Recover	Recovery Planning
		Improvements
		Communications

Colorado State University

Implementation Levels

Quantification Approaches by Dedeke '17

1. Implementation Level

- **fully implemented (76–100),**
- **largely implemented (51–75),**
- **somewhat implemented (26–50),**
- **partially implemented (1–25),**
- **not implemented (0).**

Cybersecurity Framework Adoption: Using Capability Levels for Implementation Tiers and Profiles,
Dedeke, IEEE Security & Privacy, Sept/Oct 2017

Colorado State University

Maturity Levels

Characterize an organization's practices over a range

- from Partial (Tier 1) to Adaptive (Tier 4)
  - Partial: risks are managed in an ad hoc manner
  - Risk Informed: Risk management practices are approved by management but may not be established as organizational-wide policy.
  - Repeatable: Risk management practices are formally approved and expressed as policy.
  - Adaptive: The organization adapts its cybersecurity practices based on lessons learned and predictive indicators derived from previous and current cybersecurity activities.
- Reflect a progression from informal, reactive responses to approaches that are agile and risk-informed.
- Ex: Maturity level 2 means that 70 percent or more of the categories are assigned a capability level 2 rating, and so on (Dedeke '17)

Compare with SEI CCMM Capability Maturity Model

Effort Priorities Needed

- For each category, assess current and target capability levels
- Assign a weight to each capability.
- Compute weighted capability improvement need.
- An example by Dedeke next.

Computing priorities

Table 3. Example of an organization's current and target profiles based on capability levels.

Function	Category	Current		Target		Capability gap (G)	Weight (W)	Priority (W * G)
		Capability profile	Maturity	Capability profile	Maturity			
Detect	Anomalies and events	20	Level 1	55	Level 3	35	3	105
	Security continuous monitoring	20		65		15	2	30
	Detection processes	10		50		40	3	120
Respond	Response planning	28	Level 2	35	Level 2	7	3	21
	Communication	25		35		10	2	20
	Analysis	30		55		25	2	50
	Mitigation	35		60		25	2	50
	Improvements	12		20		8	1	8
Recover	Recovery planning	25	Level 1	35	Level 2	10	3	30
	Improvements	20		30		10	2	20
	Communication	10		28		10	1	18

Colorado State University

CIS Critical Security Controls

- 20 Critical High-Level Controls
  - 148 sub-controls
  - 125 Foundational, 23 Advanced
  - 9 System, 5 Network and 6 Application
- 96 Measures, metrics and thresholds
  - Each Measure has lower, moderate and higher risk thresholds
- 30 Effectiveness tests
- 4 Governance items and 15 Governance topics
- 23 Attack Types

Top 20 CIS Critical Security Controls

Center for Internet Security (CIS) Critical Security Controls (CSC)

Basic, Foundational, Organizational

1. Inventory of Authorized and Unauthorized Devices
2. Inventory of Authorized and Unauthorized Software
3. Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
4. Continuous Vulnerability Assessment and Remediation
5. Controlled Use of Administrative Privileges
6. Maintenance, Monitoring and Analysis of Audit Logs
7. Email and Web Browser Protections
8. Malware Defenses
9. Limitation and Control of Network Ports
10. Data Recovery Capability
11. Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
12. Boundary Defense
13. Data Protection
14. Controlled Access Based on the Need to Know
15. Wireless Access Control
16. Account Monitoring and Control
17. Security Skills Assessment and Appropriate Training To Fill Gaps
18. Application Software Security
19. Incident Response and Management
20. Penetration Tests and Red Team Exercises

CIS Critical Security Controls

Colorado State University

Mapping among frameworks

- **Frameworks attempt to ensure everything is covered.**
- **Some components of a framework may correspond to a component in another framework, partially or completely.**
- **An organization may choose to follow a framework based on its need.**

Quantitative Security

Colorado State University

Yashwant K Malaiya

CS 559

Risk and its components

CSU Cybersecurity Center

Computer Science Dept

Perspective

Technological advances are driven by economics.

- **Intel's x86 architecture with upward compatibility defeated competing other architectures.**
- **Moore's law (and other laws) have held well.**
- **Public clouds.**

Defining Risk

An organization needs to identify the security risk and take measures to limit the risk.*

- **Is risk the list of potential attacks?**
- **Is risk the set of system vulnerabilities?**
- **Is risk the probability of an attack?**
- **Is risk the information that may be potentially compromised.**
- **Is the financial cost of a successful attack?**

Answer: Risk includes all of the above

- **What is the dimension of risk value**
  - **a probability (number between 0 to 1)?**
  - **Ordinal scale: (Very Low, Low, … Very High)? Number between 1 to 10?**
  - **US$**
- **Answer: Risk is generally measured in $/time unit.**

*** You can take it for granted that risk cannot be eliminated.**

Defining "Vulnerability"

- Risk is a well-defined concept in management/finance.
- It makes sense to use the same term/concept in cyber-security
- There is one issue. The term "vulnerability" is used with different meanings in classic risk literature and cyber-security. It can cause great confusion if the term is used with both meanings.
- We will use the term vulnerability only in the computer security sense.

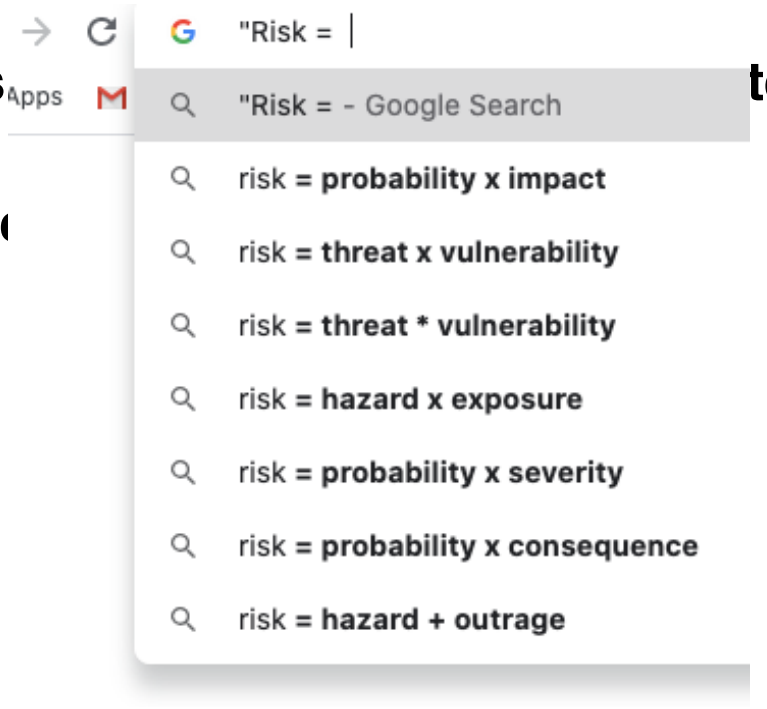
Definition: A vulnerability is a system bug that can be potentially be exploited to violate security requirements.

- The term is mostly used for software bugs, although it can be used for hardware or system-level bug.
- Note that most software bugs are ordinary bugs, but some software bugs, which are security related are called vulnerabilities. We have found that 1-5% of the software bugs may be vulnerabilities*.
- A vulnerability is a thing. It is not a quality or a probability.

* Alhazmi, Malaiya , Ray, " Measuring, Analyzing and Predicting Security Vulnerabilities in Software Systems," Computers and Security Journal, May 2007

Googling “Risk =”

- Type in the search bar: “Ris te suggestions
- It suggests following search



- What is correct? Many depend on the meaning of the terms. We will use the terminology used in the next slide

* In classical risk literature the term “vulnerability” has a different meaning.

Colorado State University

Risk: Formal definition

Definition: The Risk due to an adverse event e_i is

$$\text{Risk}_i = \text{Likelihood}_i \times \text{Impact}_i$$

- **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 .

Colorado State University

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**

Extent of the problem: IoT

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**

  $Likelihood_i$ = P{A security $hole_i$ is exploited}.

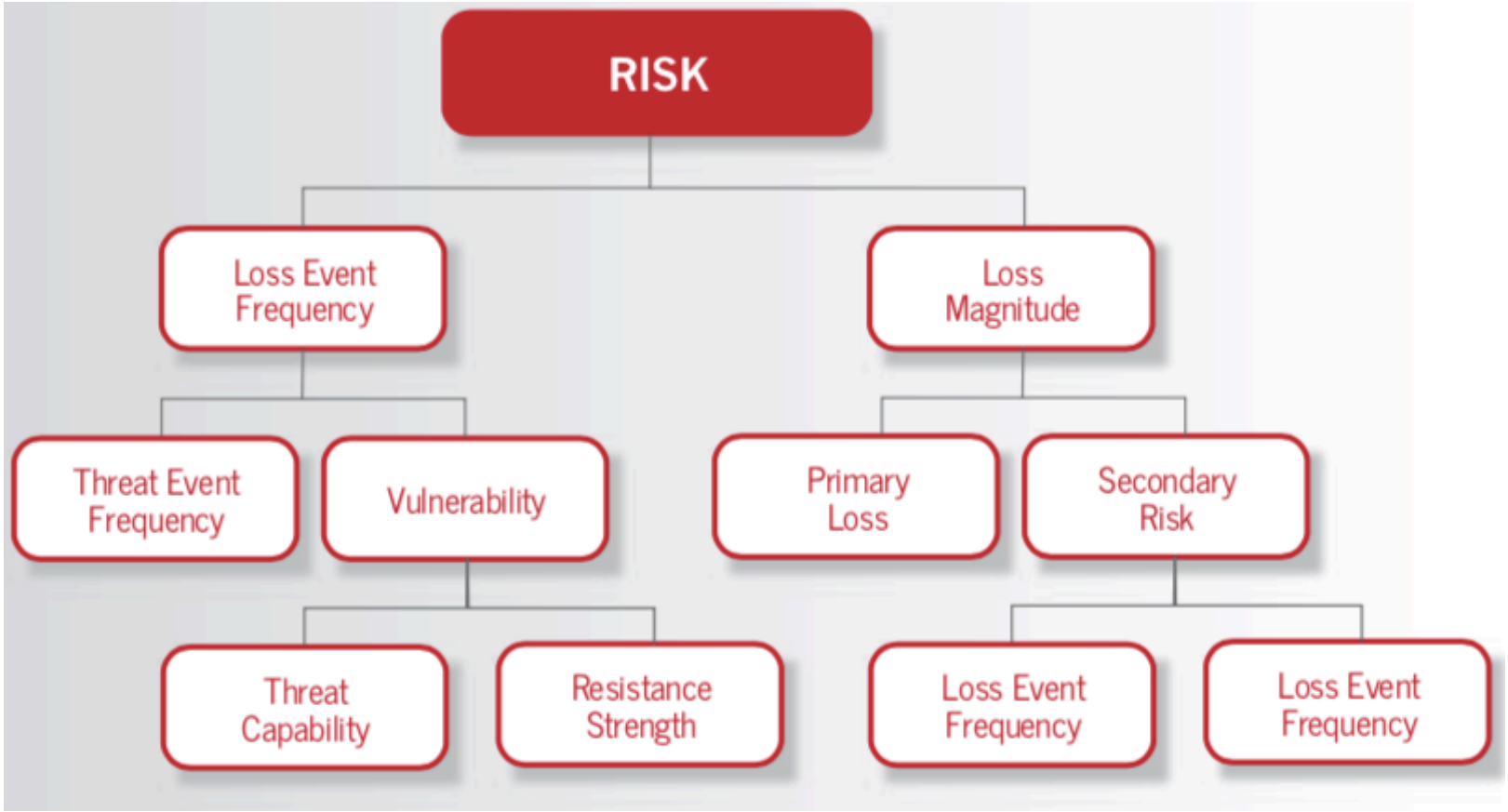
  = P{$hole_i$ present}.

  P{exploitation|$hole_i$ present}

- **P{$hole_i$ present}: an internal attribute of the system.**
- **P{exploitation|$hole_i$ present}: depends on circumstances outside the system, including the adversary capabilities and motivation.**
- **In the literature, the terminology can be**

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.

Risk Components (?)



An Adoption Guide For FAIR, Jack Jones, RiskLens 2019.
Note that some of the terminology is traditional for Risk literature, and is not the one we are using.

Colorado State University

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 (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.

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

Colorado State University

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

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**

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

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**

Colorado State University