# Fundamentals of Enterprise Security

Mohammad Saidur Rahman, Ph.D.

Department of Computer Science
The University of Texas at El Paso (UTEP)

https://www.rahmanmsaidur.com/

June 15, 2025

# Agenda

About Me

IQSeC Lab

Defining Security

Enterprise Security

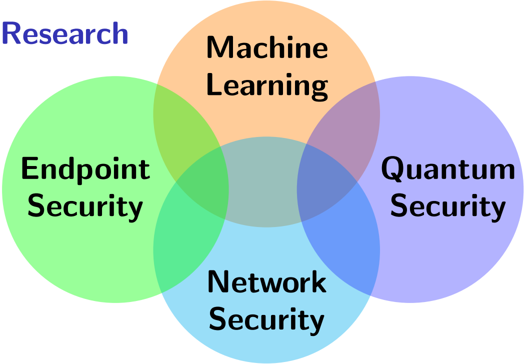
Four Pillars of Security

- Sample network and other problems
- Ten Laws for Security

# About Me

- Bachelor's in MIS (2016), University of Dhaka, Bangladesh
- MS in Cybersecurity (2018) and PhD in CIS (2024), Rochester Institute of Technology

## Research



IEEE S&P, ACM CCS, PoPETS, IEEE TIFS, IEEE QCNC, AAAI, CoLLAs

## Industry Research

- Cisco Quantum Lab, Cisco
- Nokia Bell Labs
- Mandiant (now part of Google Cloud)

# IQSeC Lab and Ongoing Research Projects

**I**ntelligent and **Q**uantum **Se**cure Advanced **C**yber Defense Research (**IQSeC**) Lab

https://iqseclab.rahmanmsaidur.com/

## ML and Endpoint Security

- Continual Learning/Lifelong Learning
- Concept Drift Detection and Adaptation
- Continual Machine Unlearning
- Explainable Continual Learning

## ML and Network Security

- LLM for Voice-over-IP (VoIP) fingerprinting
  - Attacks and Defense
- LLM for Video Fingerprinting
  - Attacks and Defenses

## Quantum Security

- Quantum Secure Communication
  - Classical and Satellite Networks
- Quantum Machine Learning

# IQSeC Lab

## PhD Students

- Md Ahsanul Haque
- Saeefa Rubaiyet R Nowmi
- Md Mahmuduzzaman Kamol (UTEP Incoming)
- Ismail Hossain (UTEP Collab)
- Md Jahangir Alam (UTEP Collab)
- Monjur Bin Shams (UTEP Collab)
- Zahra Asadi Naderabadi (UTEP Incoming)

## BS Students

- Cristina L Alarcon
- Jesus Lopez
- Viviana Cadena

# IQSeC Lab +

- Suresh Kumar Amalapuram, Postdoc, University of Edinburgh
- Scott Coull, Google
- Arifur R. Khan, Associate Professor of Instruction, UTEP
- Samee Khan, Professor and Chair, ECE, Kansas State University
- Khoa Luu, Assistant Professor, University of Arkansas
- Miralem Mehic, Associate Professor, University of Sarajevo
- David Mohaisen, Professor, University of Central Florida
- Se Eun Oh, Assistant Professor, Ewha Womans University
- Aritran Piplai, Assistant Professor, UTEP
- Shahrooz Pouryousef, PhD Candidate, UMass Amherst
- Alireza Shabani, CEO, Entangled Space
- Saeid Tizpaz Niari, Assistant Professor, University of Illinois Chicago
- Sajedul Talukder, Assistant Professor, UTEP

# IQSeC Lab +

## Students

- Se Eun Oh's Group
    - Jimin Park
    - Jungmin Park
    - Ahyun Ji
    - Sohyun Han
    - Saeyeon Hong
    - Haeseung Jeon
- Md Mahmudul Alam Imon (BD)

# Lecture Overview

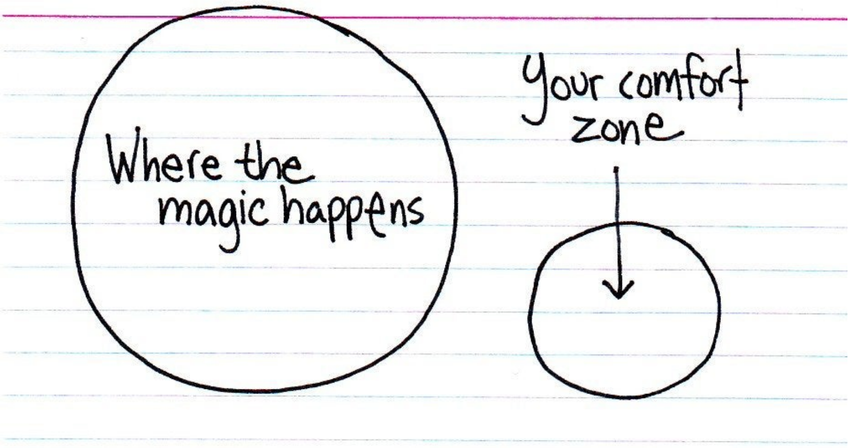
- Defining *Security*
- Contrast this to Enterprise Security
  - How does one “scale up”?
  - What are the “hard” vs “easy” parts?
- Foundations / Pillars
- Policies
- Organizational issues & organizational IMPACT

- What is a “security mode”?
  - an attack tree
  - a kill chain

# Defining Security

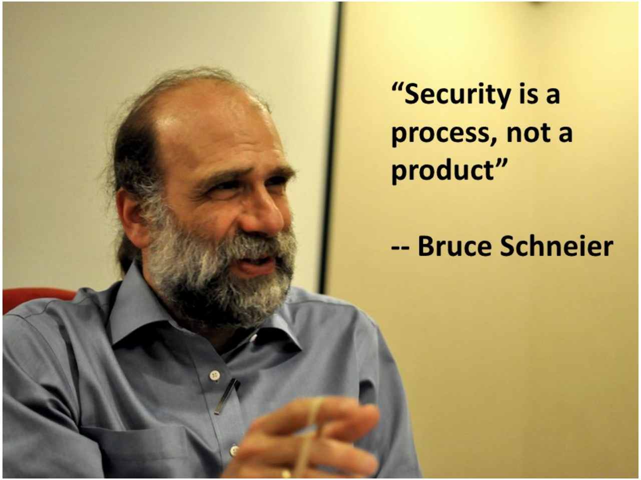
Security might be broken into areas such as:

- Network security
- Computer System / workstation security
- Server security
- Cloud security
- Mobile Device security
- AI Security
- Physical security
- Enterprise security


Where the magic happens
Your comfort zone

# NOT only ONE Action

*Security is NOT usually implemented with only ONE action.*



“Security is a process, not a product”

-- Bruce Schneier

# Example: Personal security

*How do you ensure your own* **personal security***?*

# Example: Personal security

*How do you ensure your own* **personal security***?*

- Pay attention to surroundings (what are the dangers?)
- Recognize potential threats (and how did you learn to do so?)
- Avoid dangerous conditions (falling into a hole, tripping on something)

# Example: Family security

*Scaling up - How might you ensure your* **Family's security***?*

# Example: Family security

*Scaling up - How might you ensure your* **Family's security***?*

You STILL need to:

- Pay attention to surroundings (what are the dangers?)
- Recognize potential threats (and how did you learn to do so?)
- Avoid dangerous conditions (falling into a hole, tripping on something)

BUT NOW you're responsible for doing this for someone OTHER than yourself.

# Example: Scaling up...

*What happens when we scale the participants* **EXPONENTIALLY***?*

What if you're responsible for EVERYONE at:

- A rock concert (Times Square on New Year's Eve)
- Convocation
- An amusement park (Disney Land / World)
- FIFA World Cup

# Scale is likely to change your approach...

# Classifying

*Do you consider yourself an adult?*

- *When did this happen?*

*Are you a "security professional"?*

- *What does this mean?*

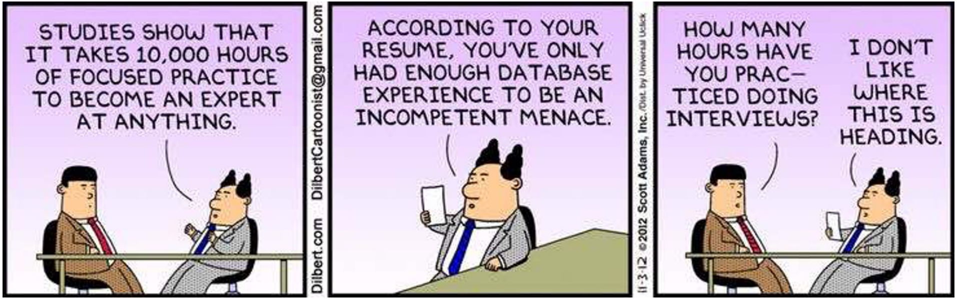
*Do other people have the same regard for your 31337 5k11lz*[1]*?*

[1] https://en.wikipedia.org/wiki/Leet

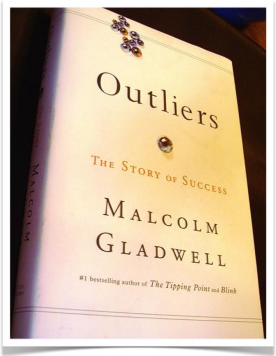
# How do you get to Carnegie Hall[2]?

[2] https://www.carnegiehall.org/About/Press/A-Short-History

# So how do you become an expert?


STUDIES SHOW THAT IT TAKES 10,000 HOURS OF FOCUSED PRACTICE TO BECOME AN EXPERT AT ANYTHING.
ACCORDING TO YOUR RESUME, YOU'VE ONLY HAD ENOUGH DATABASE EXPERIENCE TO BE AN INCOMPETENT MENACE.
HOW MANY HOURS HAVE YOU PRAC–TICED DOING INTERVIEWS?
I DON'T LIKE WHERE THIS IS HEADING.
Dilbert.com DilbertCartoonist@gmail.com
11-3-12 ©2012 Scott Adams, Inc./Dist. by Universal Uclick

# 10000 Hours



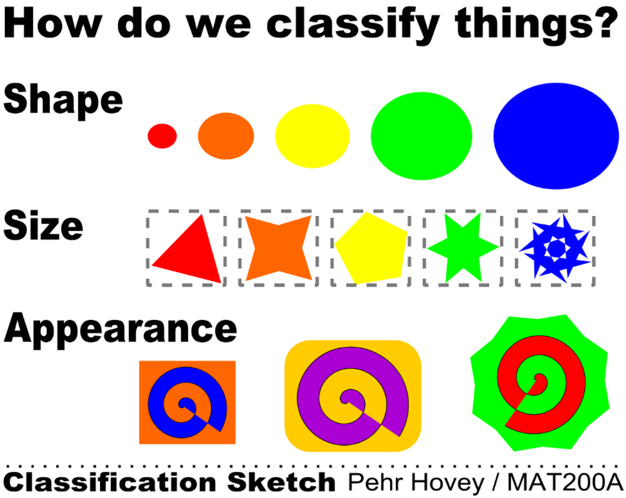
**10,000 hours**

**Gladwell says most experts accrue about 10,000 hours of practice before they develop their talent. For example, the Beatles spent two years in Germany playing long hours each day (8 hours a day, 7 days a week, for a good chunk of the year) before they became famous.**

# 10000 Hours

10000
hours to master your craft
1
8 hours a day
5 days a week
44 weeks a year
for 5½ years
Better get started!

# Back to classifying...



How do we classify things?

Shape

Size

Appearance

Classification Sketch Pehr Hovey / MAT200A

# What factors define an organization?

# Factors established!

STOP
SECURITY CHECK
SmartSign.com • 800-952-1457 • K2-4295

# Enterprise Security

Things to consider:

- What needs to be “secured”?
  - Can they (how can they) be secured?
  - What happens if they are NOT secured?
  - How will you ACTUALLY secure them? (and what will the impact be of those actions?)
- How to leverage policy/tech/education/people to address these questions?

# Four Pillars of Computing Security

- Computing fundamentals
- Networking
- Cryptography
- Human factors (or Psychology if that floats your boat)

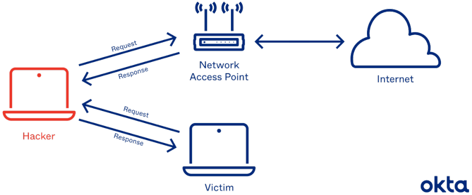
  *Computing security addresses these with regard to computers.*

  *Enterprise security will address real world interaction between the pillars.*

# What is “Enterprise Security” then?

Consider an attack such as ‘ARP poisoning’[3] in an academic “security” context...

1. How does it work?



[3] https://www.crowdstrike.com/en-us/cybersecurity-101/social-engineering/arp-spoofing/

# What is “Enterprise Security” then?

Consider an attack such as ‘ARP poisoning’[4] in an academic “security” context...

1. How does it work?
2. In this context, can you protect against it?
   - If YES, how?
   - If NO, then what should be done?

# What is “Enterprise Security” then?

Consider an attack such as ‘ARP poisoning’[5] in an academic “security” context...

1. How does it work?
2. In this context, can you protect against it?
   - Sure - static ARP entries!)
3. is this solution practical?(probably not - goes against the reason for ARP)

Compare to Enterprise Security

[5] https://www.crowdstrike.com/en-us/cybersecurity-101/social-engineering/arp-spoofing/

# Four Pillars of Security → Computer System Security

- Evaluates and addresses security of a SINGLE machine and the OS & applications run on that machine
- Define risks with metrics such as Common Vulnerabilities and Exposures (https://cve.mitre.org)
- Consider transitioning to “secure” operating systems or applications
- Address Underlying development concepts → access controls, design principles
- Secure the hosts (either manually or via tools / scripts such as MS-BSA, bastille, etc)

# Four Pillars of Security → Network Security

- Evaluate and address security of machines when connected via network
- Includes hardware / software managing network communications
  - client / server / everything in between
- Assess / evaluate / understand network protocols
  - recognizing when they need security and “bolting it on”
- Understanding services on a network, how they can be exploited / misused / misconfigured,
- Developing plans / processes / policies to minimize the risk
- All together these represent how one might go about “securing a network”.

# Four Pillars of Security → Cryptography

- Investigates the art and science of obscuring and securing data
- Can include both digital and non-digital approaches
- Protecting CIA (confidentiality, integrity, availability) (will talk more about this)
- Includes data in transit and at rest
- Encompasses things like Hashing[6] and Digital Signatures[7]
- Representing obscure or secure relationships between two pieces of data
- Also covers how we tend to attack such systems (Cryptanalysis[8])

[6] https://en.wikipedia.org/wiki/Hash_function
[7] https://en.wikipedia.org/wiki/Digital_signature
[8] https://en.wikipedia.org/wiki/Cryptanalysis

# Four Pillars of Security → Human factors/behavior/Psychology

- Not covered in as much depth as we should, but it's **IMPORTANT**
- The study of what people do and how they will do it
- The goal? Leverage well-known tactics to reduce the "attack surface"
  - social engineering attacks
  - physical security
- Insider Threat

# How does this impact “Enterprise” security?

- We have addressed some basics to consider — there are a few more things. These might include:
  - Scale
  - Budget
  - Systemic Nature
  - Control Selection
  - Policies

*When combining these factors in an enterprise environment, we are likely to make different choices than we might in an academic one. . .*

# Enterprise Security: BUDGETING

- Organizations do not *usually* have unlimited funds
- How does available funding impact security decisions?
- You will have to choose how you will apply your (limited) resources

| **PEOPLE** | **PROCESSES** | **TECHNOLOGY** |
|---|---|---|
| - training | - policies | - software |
| - employees | - vulnerability discovery | - log management |
| - structure | - incident response | - threat intelligence |

Table: People, Processes, Technology

# Enterprise Security: CONTROL SELECTION

- Controls not selected based solely on merit
- Other factors in play
    - Time?
    - Budget? (see previous slide)
    - Effectiveness?
        - in current environment
        - in conjunction w/ other defenses
    - Support
        - both how to fix & likely lifetime (how long it will be supported)
        - who will support? (consider open source tool vs commercial)

# Enterprise Security: SYSTEMIC NATURE

- Not only how controls play together, but also how interaction can introduce risk
- *Systemic Risk* is a term from economics
  - defines risk generated by interconnection between institutions
- Enterprises introduce unique situations such as stacked environments — these can introduce additional risk
  - consider the concept of “pivoting”
  - consider lack of physical security allowing a malicious USB to be inserted

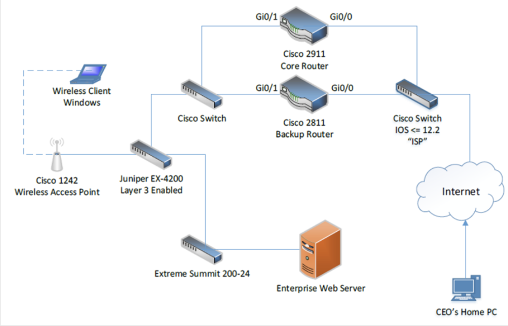
# Enterprise Security: SCALE

In terms of **SYSTEMS**:

- Do the systems change?
  - Consider how the following might impact your approach to "securing":
    - cloud / mainframes / thousands of desktops / multiple domains / virtualization
- Do the **SERVICES** change?
  - to accommodate bigger environments? to provide alternative deployment methods (DevOps)?
- Does the development change?
  - does Methodology, Continuous Integration (CI), etc., affect our scale?

# Sample network and other problems

- Is this a realistic network diagram?
- How does this compare to a real “modern” enterprise network?
- What about the code that runs an operating system?
  - How many lines?
  - Vulnerability in complexity.
- **TIME is AGAINST you!**
  - Secure today, vulnerable tomorrow.
  - Why pick a lock if you can break a window? (take the easy route whenever possible)



# Enterprise Security: POLICIES

- Enterprises involve **PEOPLE**
- Policies define limits on what a resource can do
  - and how it can interact w/ technology and internal processes
- Outside processes can **ALSO** influence policy
  - industry compliance
  - Privacy and data management laws
  - **Note:** these can **CHANGE** based on where your data is stored
    - Work for an international company? Rules can be different for other locales.

# Ten Laws for Security[9]

1. Attackers always find a way
2. Know the assets to protect
3. No “Security Through Obscurity”
4. Trust No One
5. *Si vis pacem, para bellum*
    - (if you want peace, prepare for war)
6. Security is no stronger than the weakest link
7. **YOU** are the weakest link
8. If you watch the internet, the internet is watching you
9. *Quis Custodiet Ipsos Custodes?*
    - (or “who will guard the guards themselves?”)
10. Security is not a product, security is a process.

[9] Diehl, Eric. Ten laws for security. Berlin: Springer, 2016.

## Summary/Takeaways

- **Enterprise security is DIFFERENT** from general cybersecurity
  - LOTS to think about
  - the issues are (usually) more complex
  - the implementation is more on the practical side and less on the academic approach to security
  - there are limits to what can be done
  - Guidelines and best practices exist

# Question?