Introduction to Cyber Security

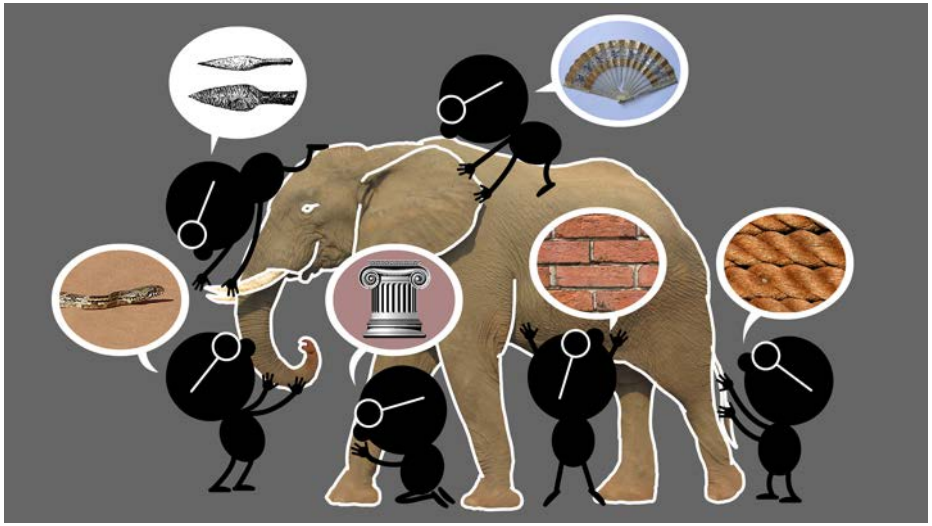
Prof. Ravi Sandhu
Executive Director and Endowed Chair

Lecture 1

ravi.utsa@gmail.com
www.profsandhu.com

Natural vs Cyber Science

Elephant Problem



Cyber-Elephant Problem

The cyber-elephant problem requires Applied and Basic research Combined (ABC)

*** The New ABCs of Research, Ben Schneiderman, 2016**

Cyber Security is Dynamic

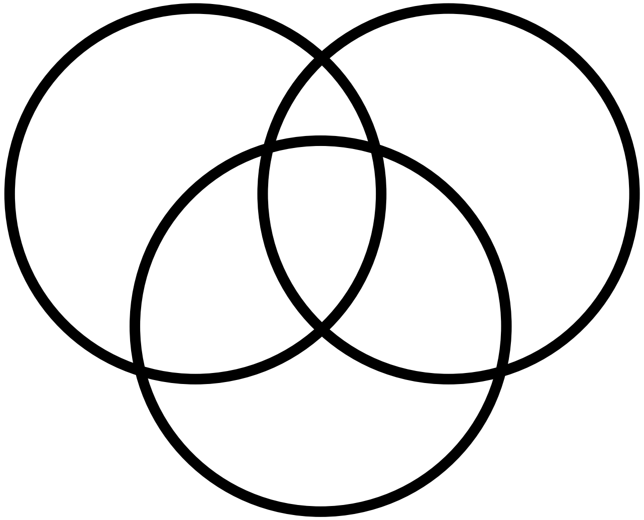
"My dear, here we must run as fast as we can, just to stay in place. And if you wish to go anywhere you must run twice as fast as that."

— Lewis Carroll, Alice in Wonderland

Prognosis

- Cyberspace will become orders of magnitude more complex and confused very quickly
  - Cyber and physical distinction will blur
  - Threats will go beyond money to physical harm and danger to life and body
- Overall this is a very positive development and will enrich human society
- It will be messy but need not be chaotic!
- Cyber security research and practice are loosing ground

Security Objectives



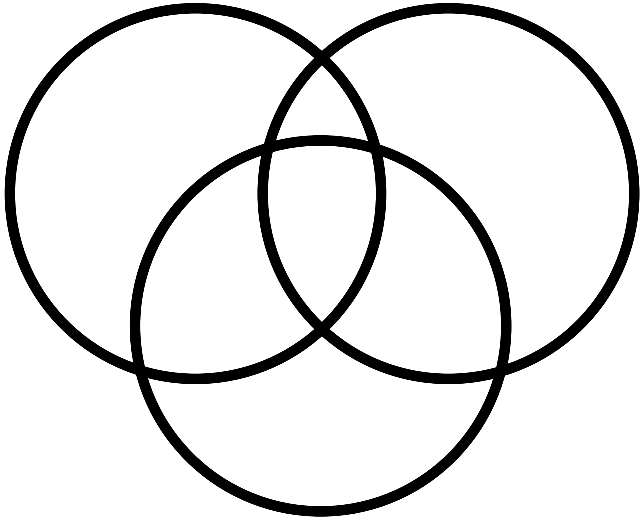
INTEGRITY
modification

AVAILABILITY
access

CONFIDENTIALITY
disclosure

Security Objectives

Control of read and write is fundamental to all three



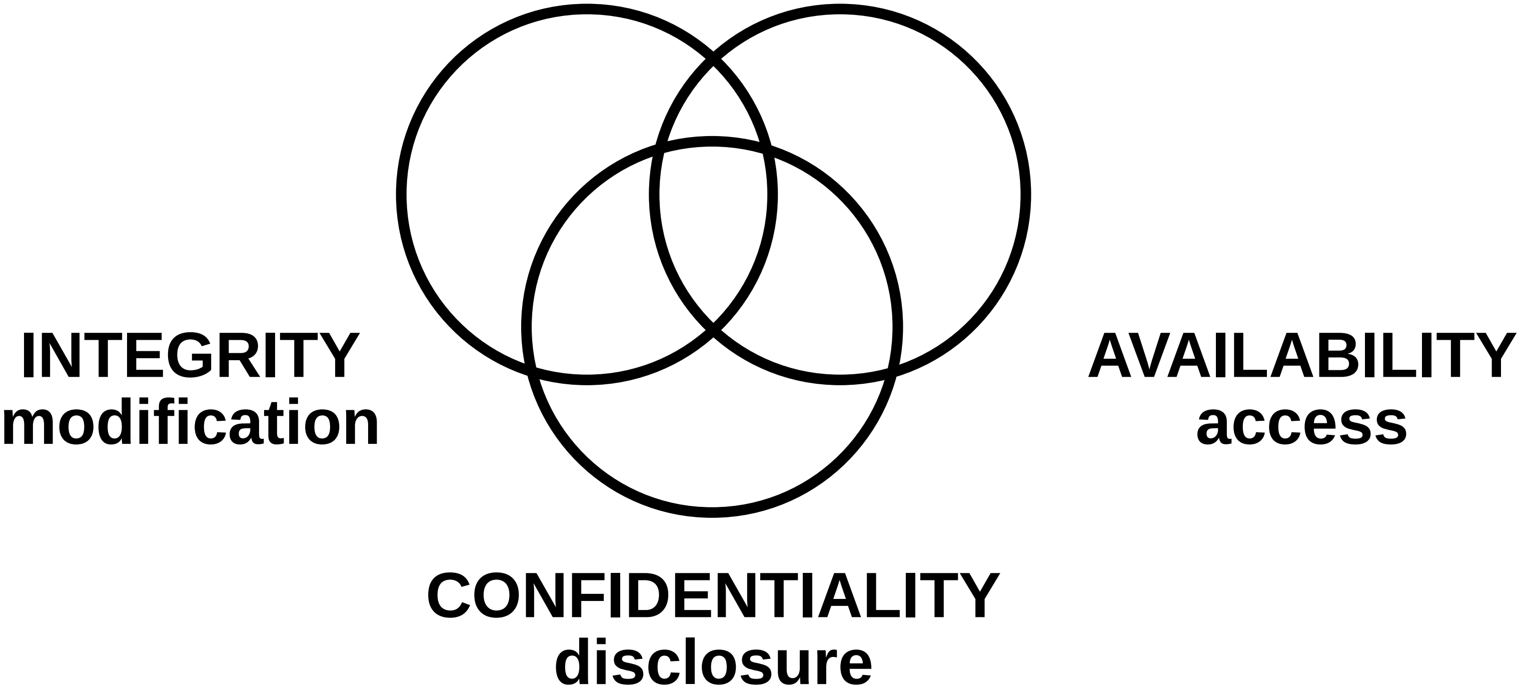
INTEGRITY
modification

AVAILABILITY
access

CONFIDENTIALITY
disclosure

Security Objectives

Cannot have it all
Need to compromise



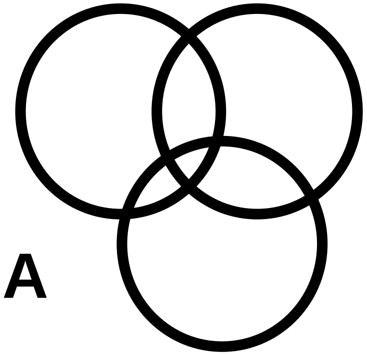
INTEGRITY
modification

AVAILABILITY
access

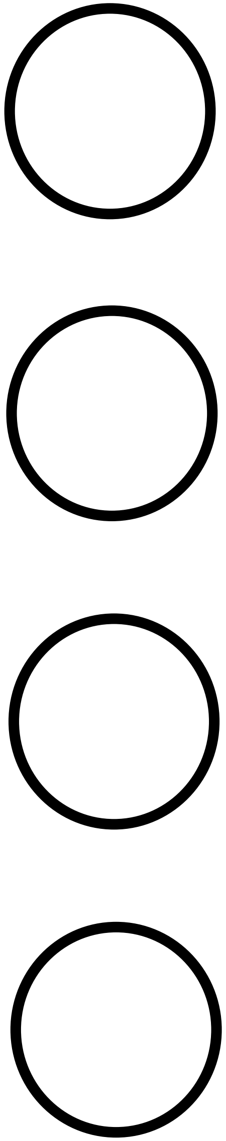
CONFIDENTIALITY
disclosure

Security is Secondary

Cannot have it all
Need to reconcile
with non-Security Objectives



CIA



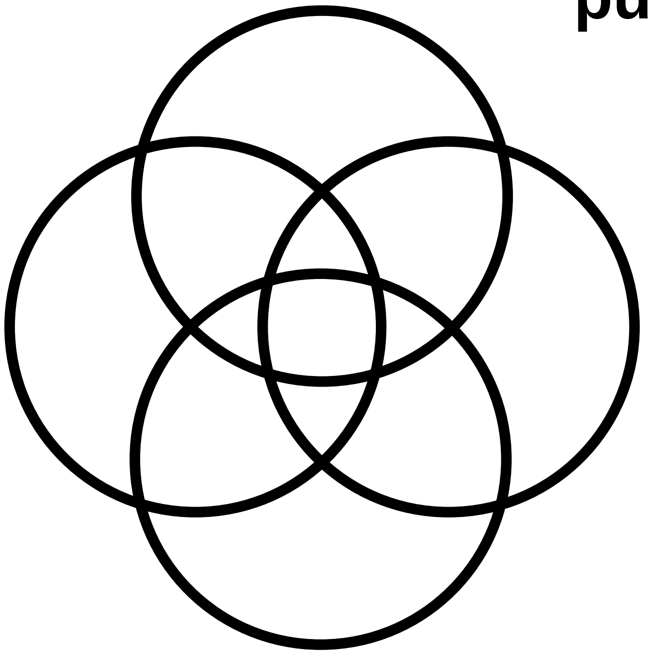
Cost

Convenience

Growth

Safety

Security Objectives



USAGE
purpose

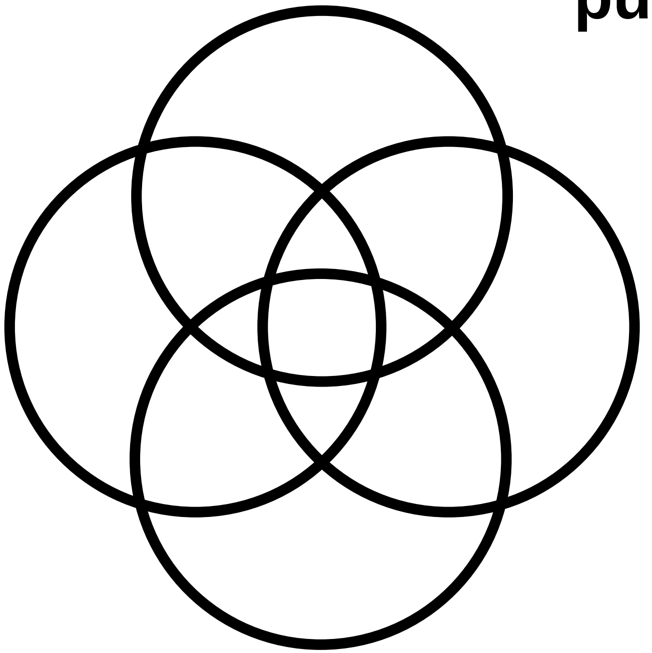
INTEGRITY
modification

AVAILABILITY
access

CONFIDENTIALITY
disclosure

Security Objectives

USAGE
purpose



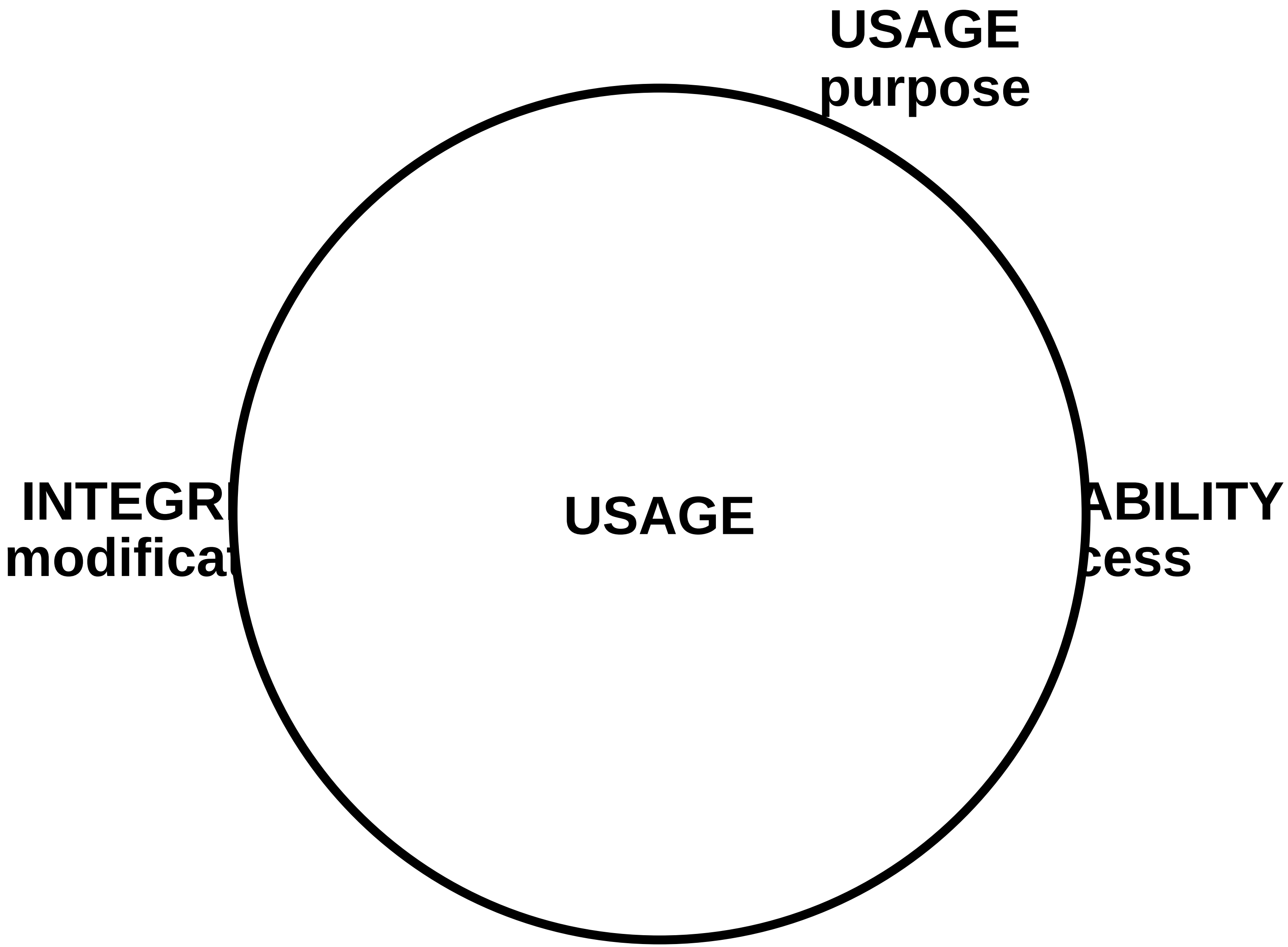
Covers privacy and intellectual property protection

INTEGRITY
modification

AVAILABILITY
access

CONFIDENTIALITY
disclosure

Security Objectives

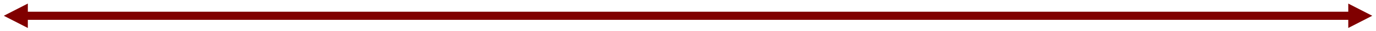

USAGE
purpose

INTEGRI
modificat

USAGE

ABILITY
cess

Security Objectives



Single Enterprise

- **owns all the information**
- **employs all the users**

Multiple Interacting Parties

- **no one owns all the information**
- **no one can unilaterally impose policy on all the users**

Cyber Security Scope

- Computer security
- Information security =
  - Computer security + Communications security
- Information assurance
- Mission assurance
  - Includes cyber physical

Cyber Security Goal

- Enable system designers and operators to say:

  This system is secure

Cyber Security Goal

- Enable system designers and operators to say:

  This system is secure

  Not attainable

- Conflicting objectives need political and social compromise
- There is an infinite and escalating supply of attacks

Cyber Security Goal

- Enable system designers and operators to say:

  This system is secure enough OR
  This system is as secure as it needs to be and no more

Many successful examples

Cyber Security is Dynamic

“My dear, here we must run as fast as we can, just to stay in place. And if you wish to go anywhere you must run twice as fast as that.”

— Lewis Carroll, Alice in Wonderland

Low Assurance Systems

- The ATM (Automatic Teller Machine) system is
  - secure enough
  - global in scope
- Similarly
  - on-line banking
  - e-commerce payments

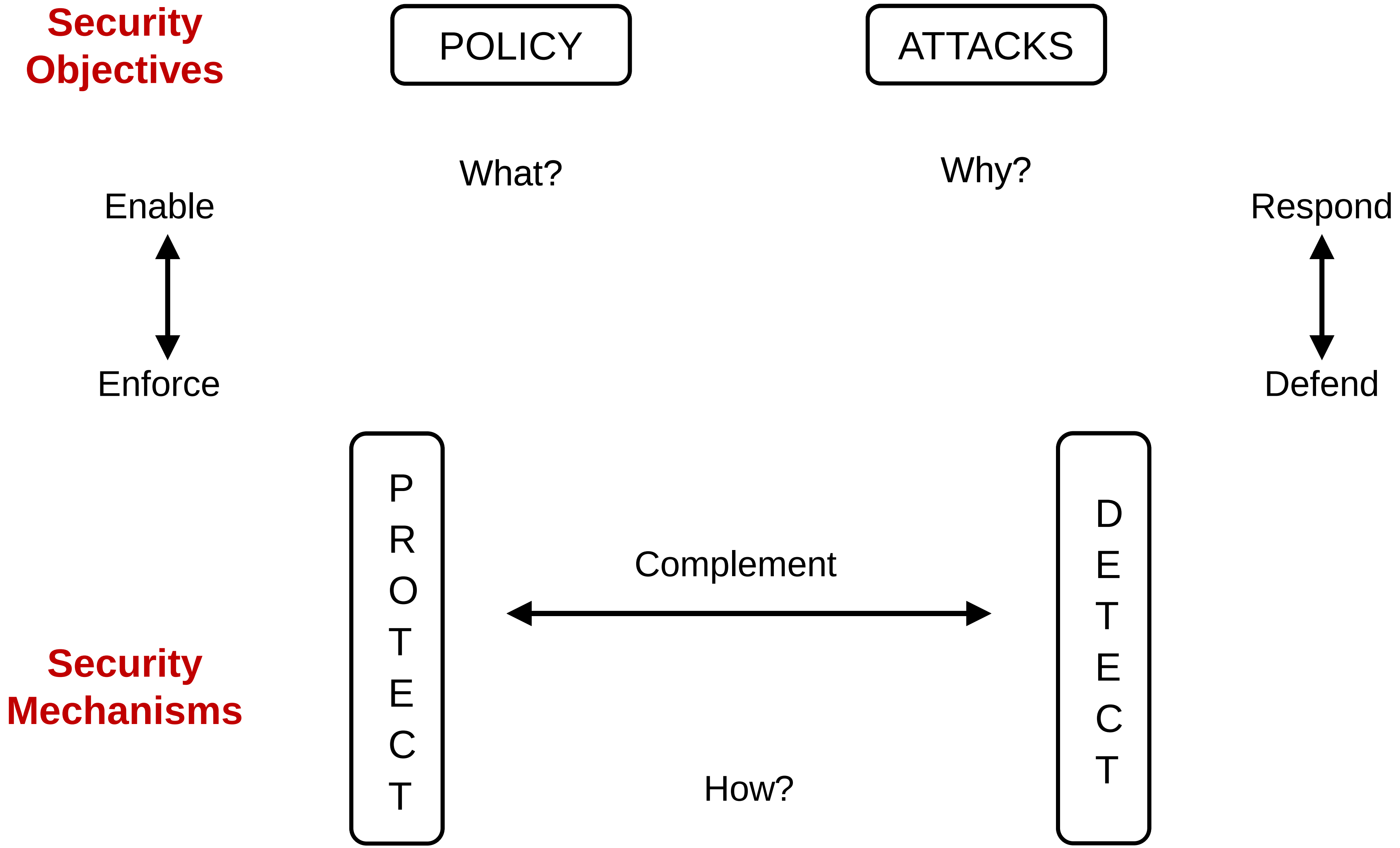
High Assurance Systems

- US President’s nuclear football
- Secret formula for Coca-Cola

Limits to Security

- Analog hole
- Inference
- Side channels
- Insider threat
- Detection is impossible
- Protection is impossible
- …..

Cyber Security Landscape



Security Objectives

POLICY

ATTACKS

What?

Why?

Enable

Enforce

Respond

Defend

P R O T E C T

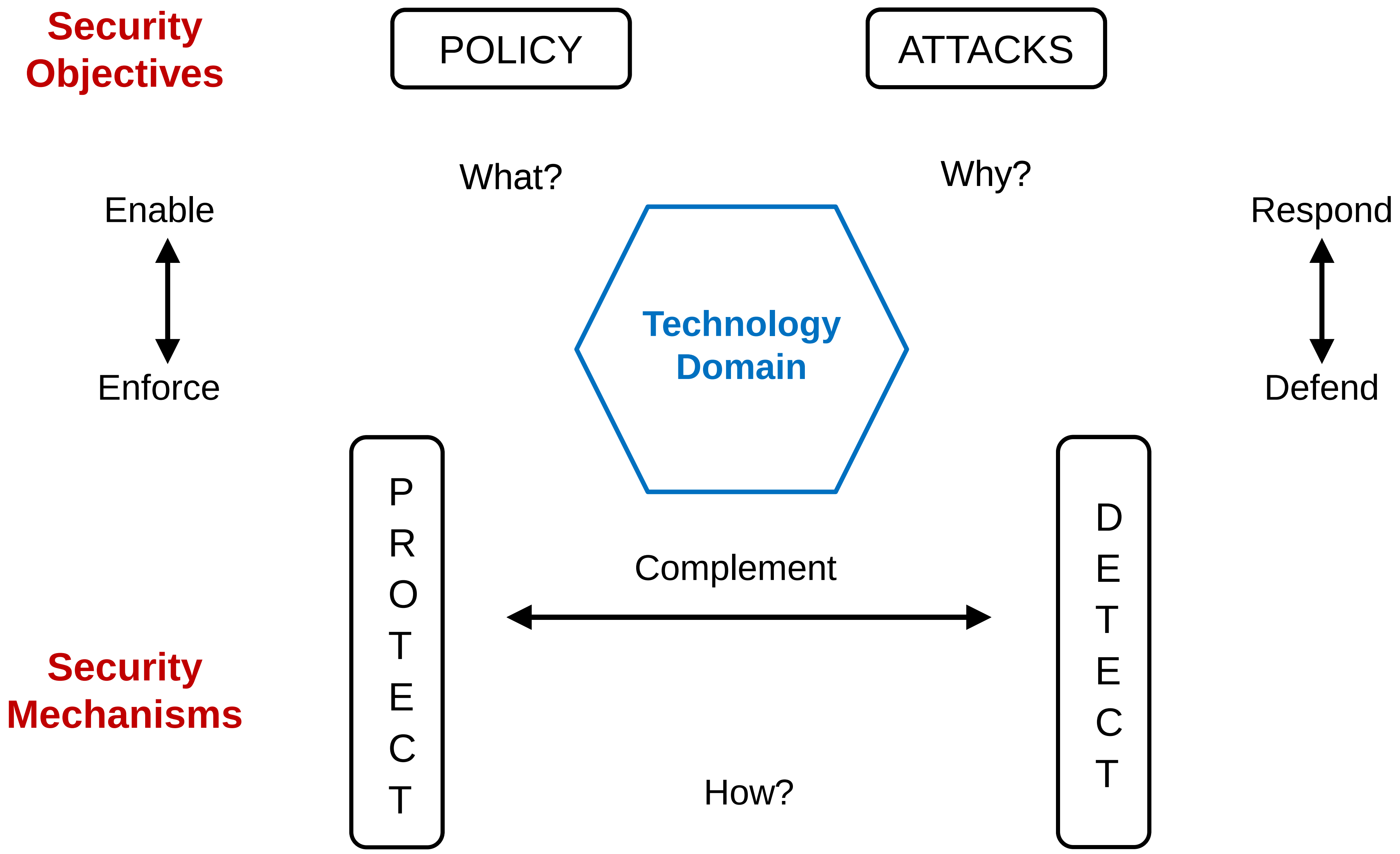
Complement

D E T E C T

How?

Security Mechanisms

Cyber Security Landscape



Security Objectives

POLICY

ATTACKS

What?

Why?

Enable

Enforce

Respond

Defend

Technology Domain

PROTECT

DETECT

Complement

How?

Security Mechanisms