Introduction and Basic Concepts
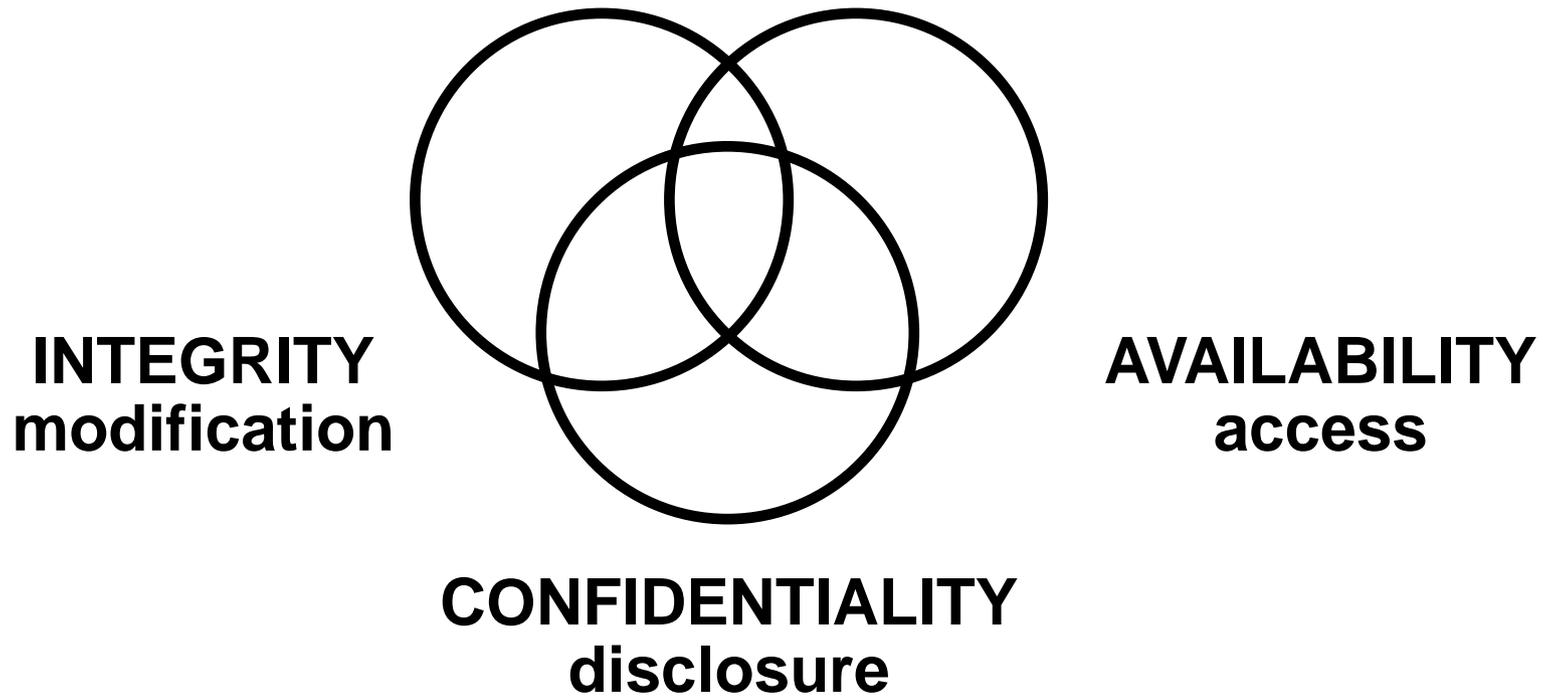
Prof. Ravi Sandhu
Executive Director and Endowed Chair
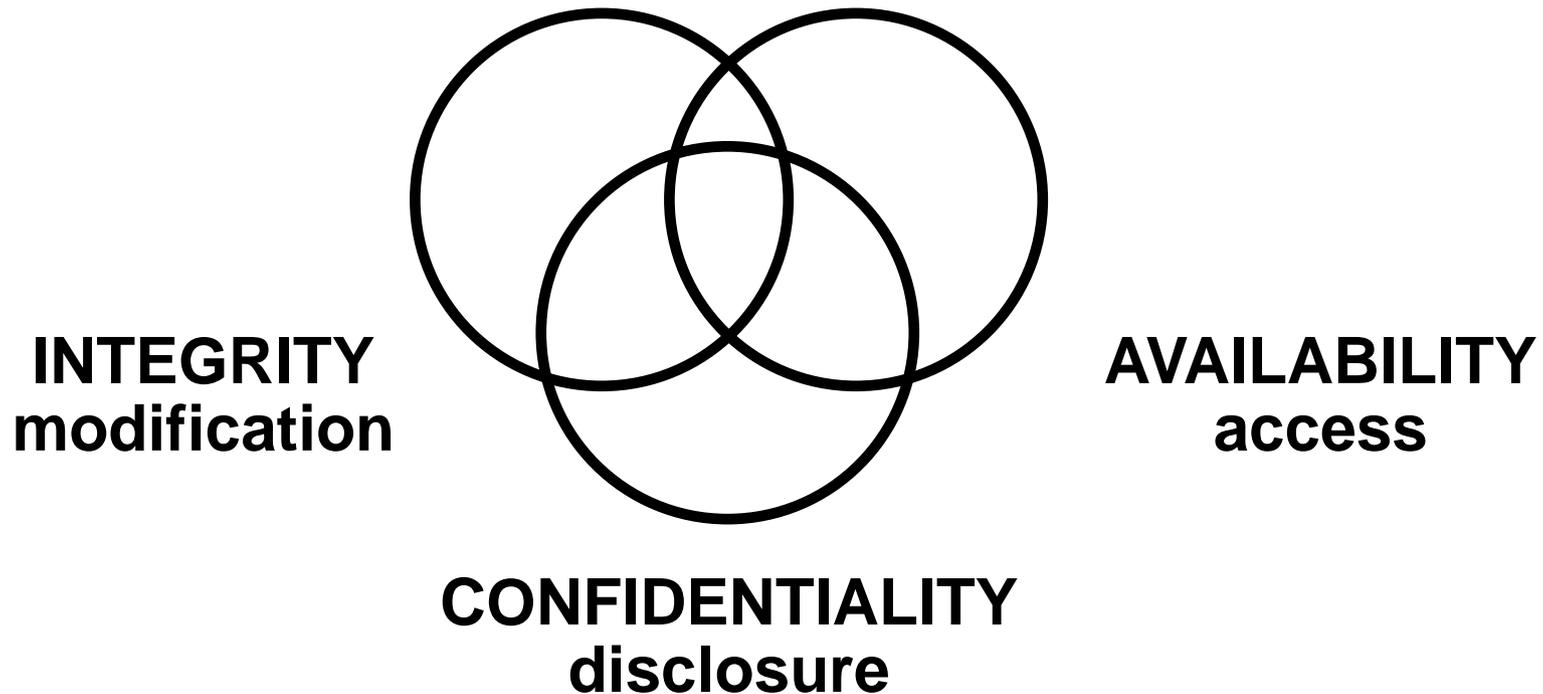
Lecture 1

ravi.utsa@gmail.com
www.profsandhu.com
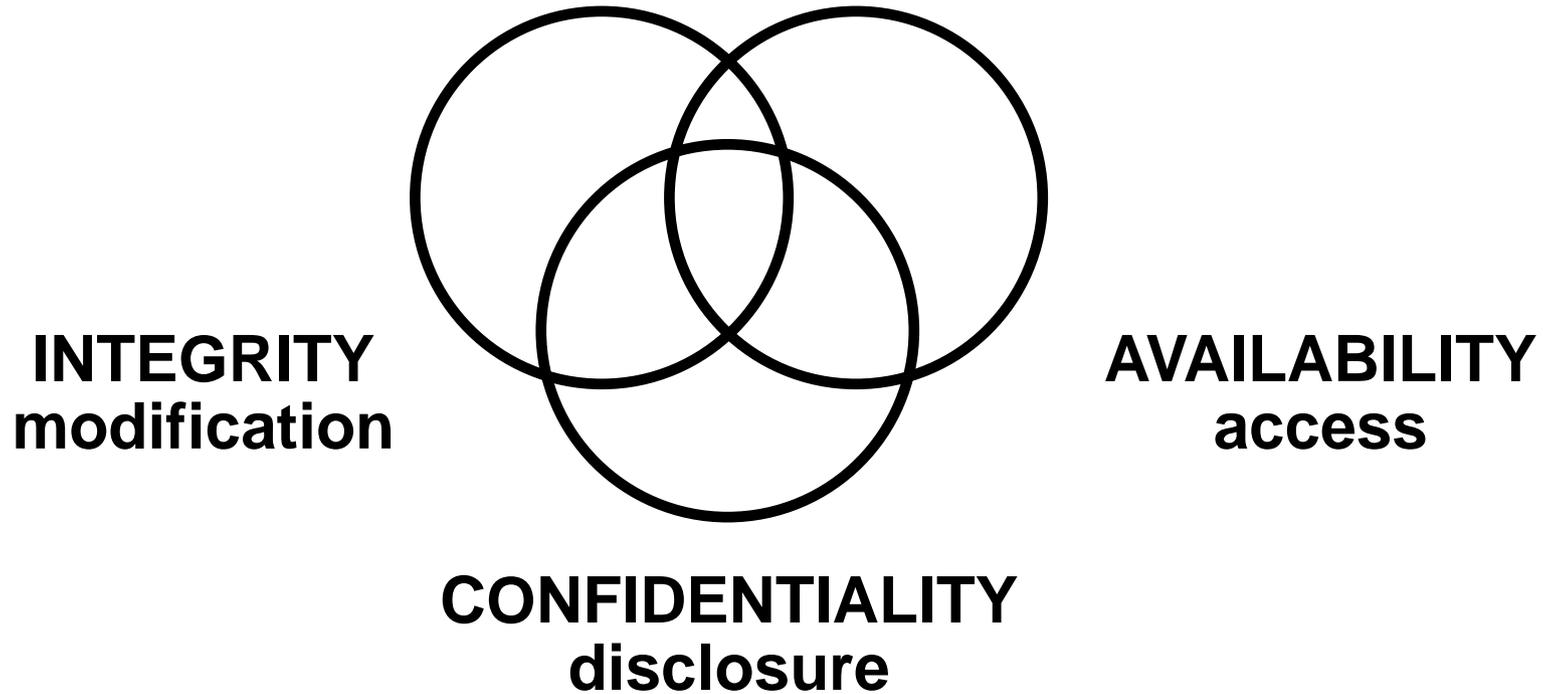
World-Leading Research with Real-World Impact!

➢ 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!

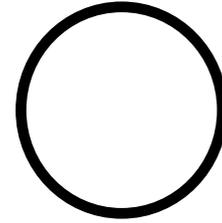➢ Cyber security research and practice are loosing ground

INTEGRITY
modification

AVAILABILITY
access

CONFIDENTIALITY
disclosure

World-Leading Research with Real-World Impact!

The Institute for Cyber Security

ICS

UTSA

Control of read and write is fundamental to all three

INTEGRITY
modification

AVAILABILITY
access

CONFIDENTIALITY
disclosure

**Cannot have it all
Need to compromise**

**INTEGRITY
modification**

**AVAILABILITY
access**

**CONFIDENTIALITY
disclosure**

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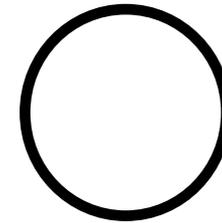
Cannot have it all
Need to reconcile
with non-Security Objectives

CIA
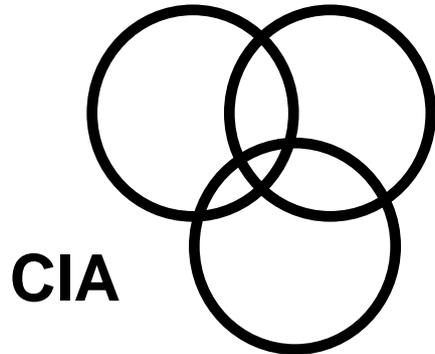
Cost
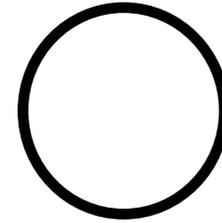
Convenience

Growth

Safety

World-Leading Research with Real-World Impact!

Security Objectives

USAGE
purpose

INTEGRITY
modification

AVAILABILITY
access

CONFIDENTIALITY
disclosure

World-Leading Research with Real-World Impact!

Security Objectives

USAGE
purpose

Covers privacy and
intellectual property
protection

INTEGRITY
modification

AVAILABILITY
access

CONFIDENTIALITY
disclosure

World-Leading Research with Real-World Impact!

USAGE
purpose

INTEGRITY
modification

USAGE

ABILITY
cess

World-Leading Research with Real-World Impact!

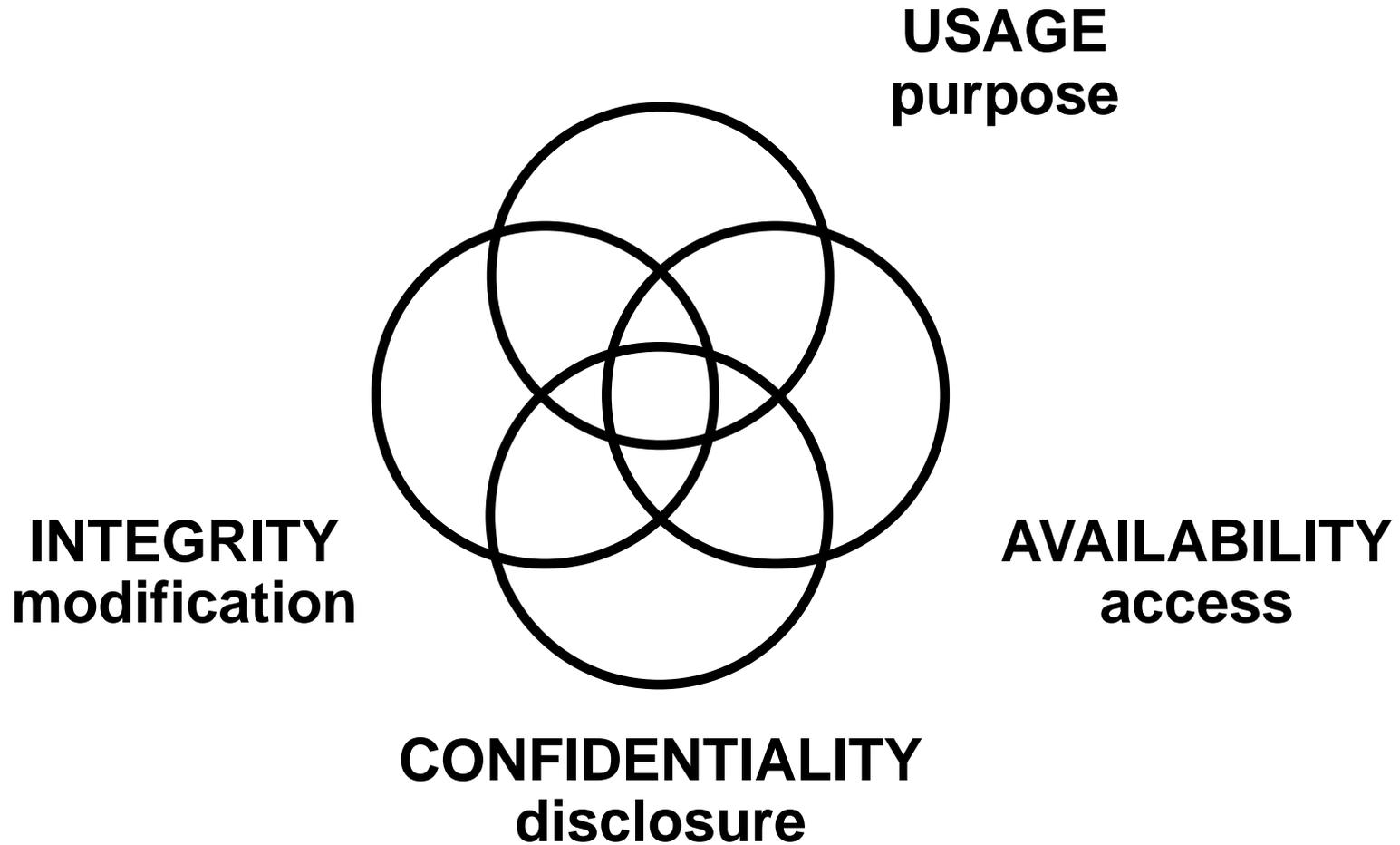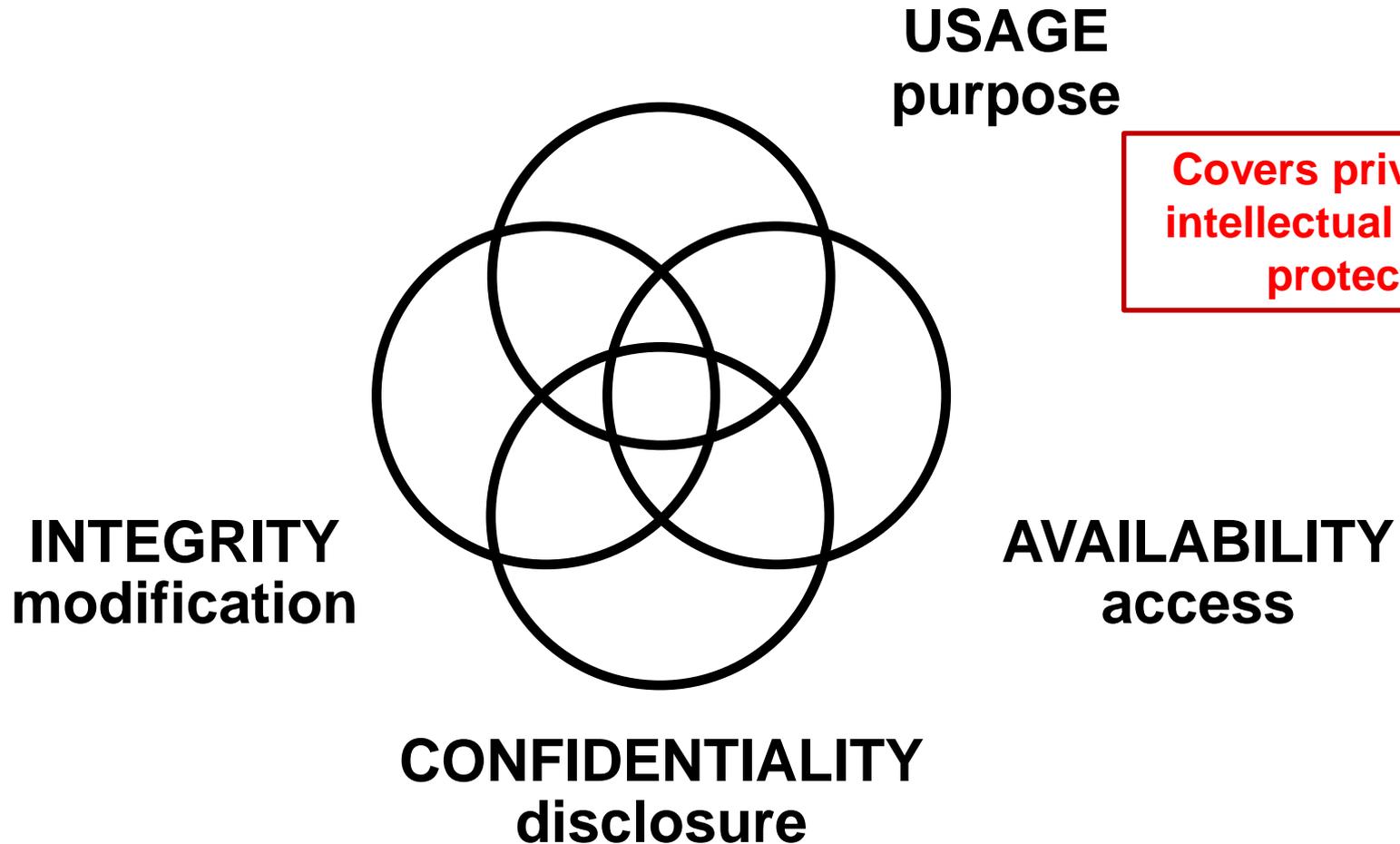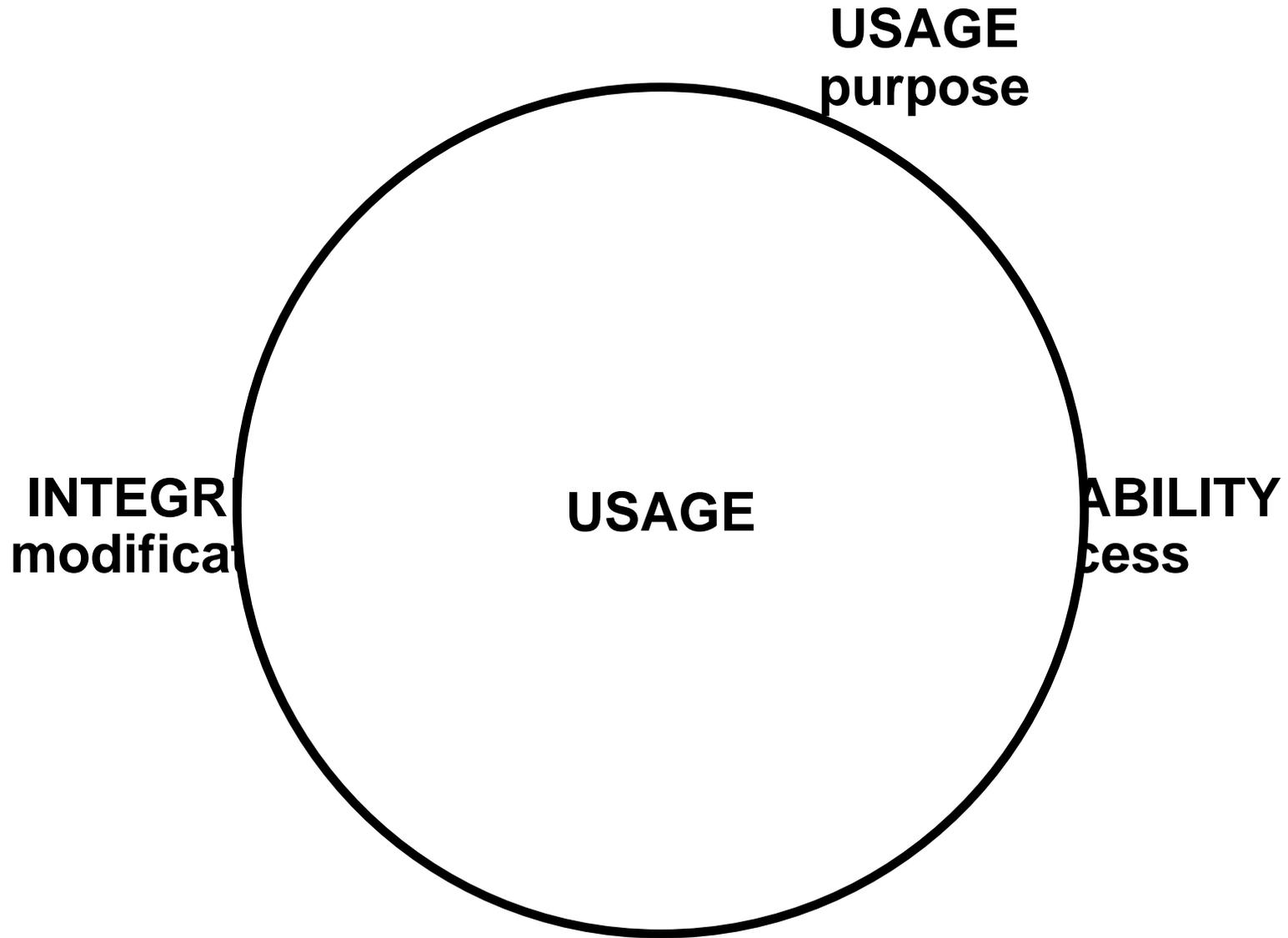**Single Enterprise**
- owns all the information
- employs all the users

Multiple Interacting Parties
- no one owns all the information
- no one can unilaterally impose policy on all the users

World-Leading Research with Real-World Impact!

➢ Computer security

➢ Information security =

  ❖ Computer security + Communications security

➢ Information assurance

➢ Mission assurance

  ❖ Includes cyber physical

➢ Enable system designers and operators to say:

This system is secure

➢ Enable system designers and operators to say:

This system is secure

➢ 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

➢ Enable system designers and operators to say:

This system is secure enough

Many successful examples

World-Leading Research with Real-World Impact!

➢ The ATM (Automatic Teller Machine) system is
  ❖ secure enough
  ❖ global in scope
➢ Not attainable via current cyber security science, engineering, doctrine
  ❖ not studied as a success story
➢ Similar paradoxes apply to
  ❖ on-line banking
  ❖ e-commerce payments

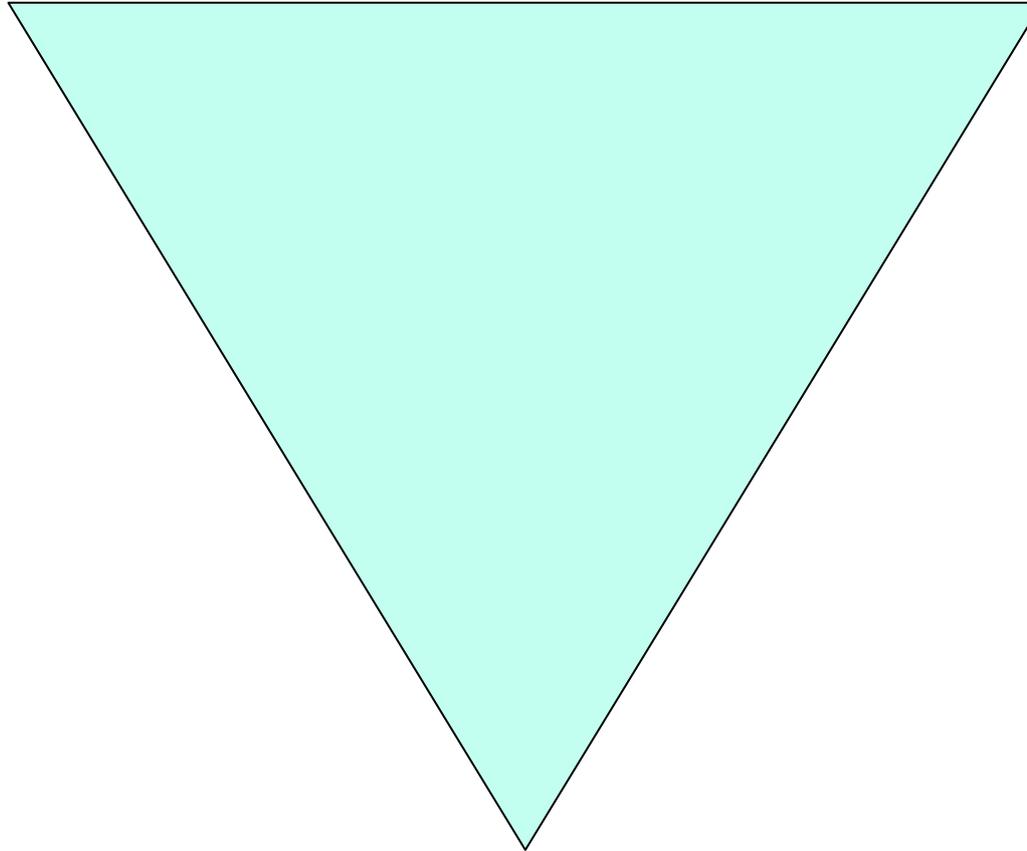- ➢ US President's nuclear football
- ➢ Secret formula for Coca-Cola

"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."
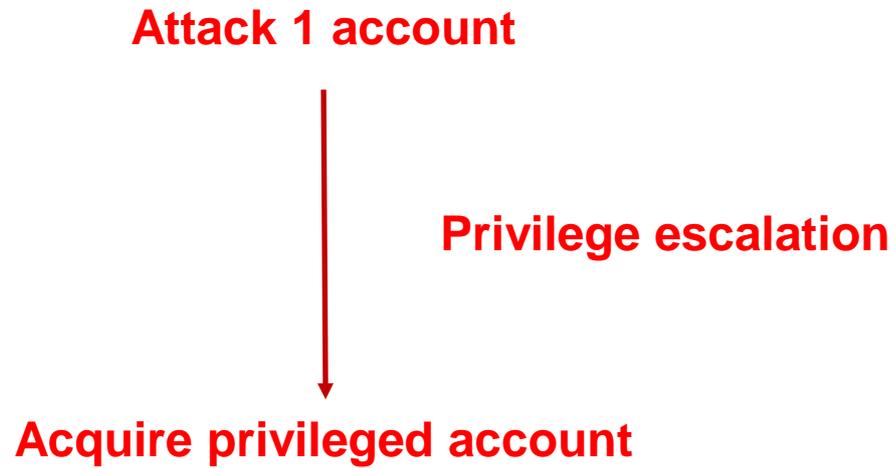
— Lewis Carroll, Alice in Wonderland

World-Leading Research with Real-World Impact!

Protect

Detect
(and Respond)

Accept

World-Leading Research with Real-World Impact!

Attack 1 account

Privilege escalation

Acquire privileged account

World-Leading Research with Real-World Impact!

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