Introduction to Cyber Security

Prof. Ravi Sandhu
Executive Director and Endowed Chair

Lecture 1

ravi.utsa@gmail.com
www.profsandhu.com
The cyber-elephant problem requires Applied and Basic research Combined (ABC)

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

Control of read and write is fundamental to all three

INTEGRITY modification

CONFIDENTIALITY disclosure

AVAILABILITY access

© Ravi Sandhu

World-Leading Research with Real-World Impact!
Security Objectives

INTEGRITY
modification

CONFIDENTIALITY
disclosure

AVAILABILITY
access

Cannot have it all
Need to compromise

World-Leading Research with Real-World Impact!
Security is Secondary

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

CIA

Cost
Convenience
Growth
Safety
Security Objectives

INTEGRITY
modification

AVAILABILITY
access

CONFIDENTIALITY
disclosure

USAGE
purpose
Security Objectives

INTEGRITY
modification

AVAILABILITY
access

CONFIDENTIALITY
disclosure

USAGE
purpose

Covers privacy and intellectual property protection
Security Objectives

INTEGRITY
modificaton

AVAILABILITY
access

CONFIDENTIALITY
disclosure

USAGE
purpose

USAGE

PROCESS

ABILITY

© Ravi Sandhu

World-Leading Research with Real-World Impact!
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
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

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

Many successful examples
“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
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
- ...

© Ravi Sandhu

World-Leading Research with Real-World Impact!
Cyber Security Landscape

Security Objectives

Enable
Enforce

Security Mechanisms

PROTECT

POLICY

ATTACKS

What?
Why?

How?
Complement

Defend
Respond

© Ravi Sandhu

World-Leading Research with Real-World Impact!
Cyber Security Landscape

Security Objectives

Enable

Enforce

Security Mechanisms

POLICY

ATTACKS

What?
Why?

Technology Domain

Complement

How?

Protect

Detect

World-Leading Research with Real-World Impact!