

# Week 3: Security Topics

# What is “Security”

- Quality has been defined to be “Meeting (or exceeding) customer’s expectations”
  - Assumes no sentient forces to deny the desired outcome
  - natural failures and accidental shortcomings/oversights only
- An operative definition of security for this course:
  - “Meeting (or exceeding) customer’s expectations in the presence of the actions of an adversary.”
  - Parenthetical extension is especially important here – it addresses cases where customer has not thought through implications of system and its potential impact on their operations.
  - Open ended definition implies ongoing need to address evolving threats
- Other quality-derived concepts that are especially pertinent to security:
  - Root cause analysis of faults
  - Continuous process improvement
  - Pareto principle (80/20 rule)
  - “Quality is Free” (refer to Phil Crosby book of same title)

# How Much Security Is Enough?

A security assessment model



Perpetrators

Who might try to steal the assets?

- What resources do they have?
- Where and how might they be able to attack?
- What might they be after?
- What are their motivations?



Assets at Risk

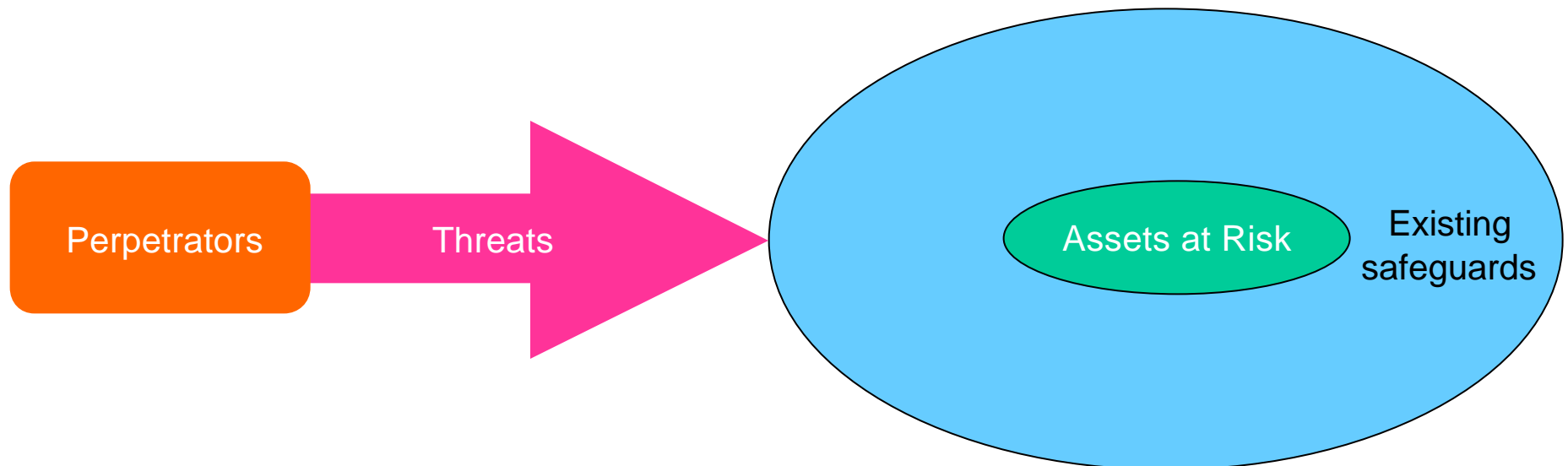
What might be worth stealing?

Assets may be resources, capabilities, etc. that the system has, controls, or influences

- Tangible assets
- Intangible assets

# How Much Security Is Enough?

A security assessment model

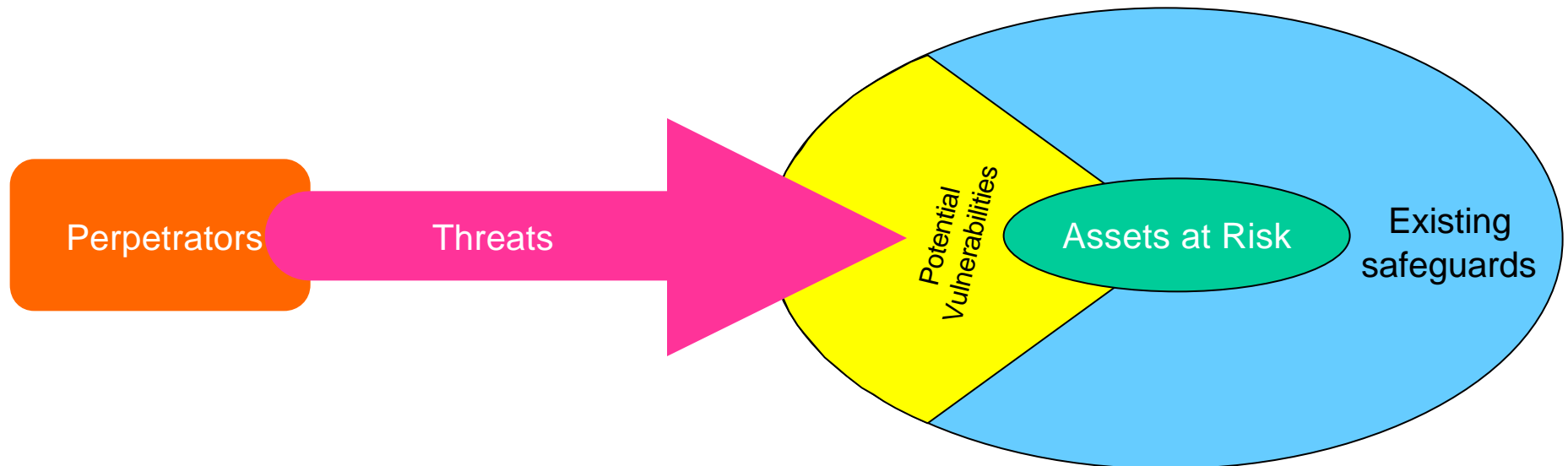


What are potential means of attack?

What inherent or predefined security controls exist for the system under study?

# How Much Security Is Enough?

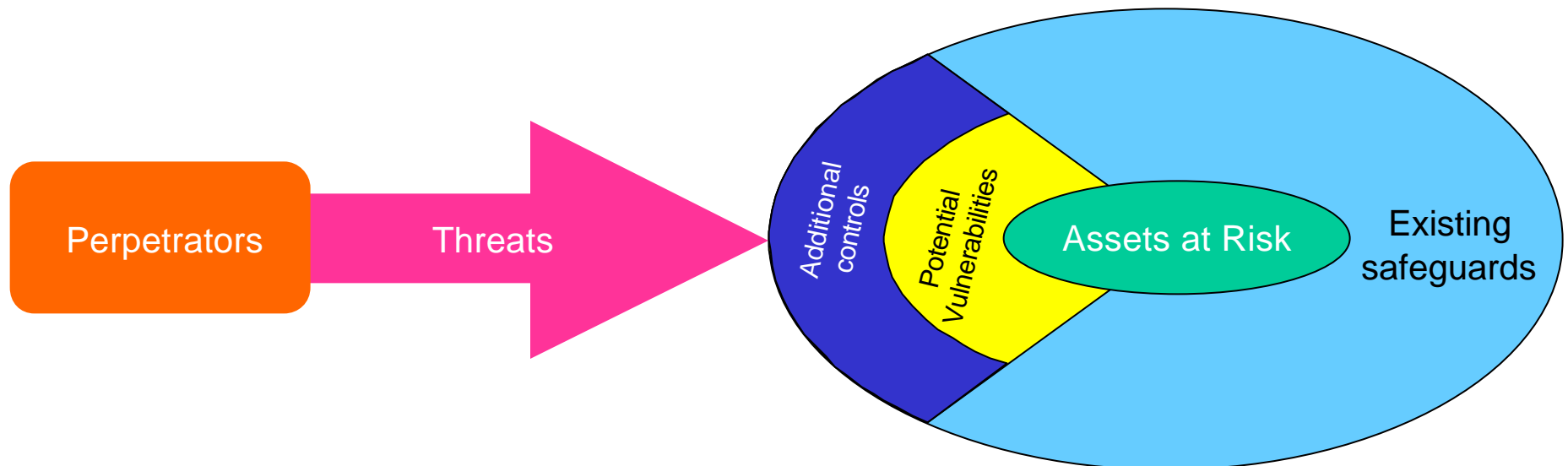
A security assessment model



What problems might exist in the system under study, perhaps due to unanticipated perpetrators or threats?

# How Much Security Is Enough?

A security assessment model



What problems could be averted by adding additional security controls to the system design?

Does the risk of attack justify the cost of defending against it?

# Other Security Terms

- Security policy
  - A concise, high level statement of issues that will be dealt with in security the system under consideration
- Security domain
  - The scope of authority or scope of responsibility for security of the system. Think of this as corresponding to the security perimeter or edges of a physical system.
- Security architecture
  - A high-level description of the system under consideration, including all security-relevant capabilities, features, etc. and security controls, described in a way that is conducive to analysis of the system.
  - **System security cannot be discussed without a view of the system architecture!**

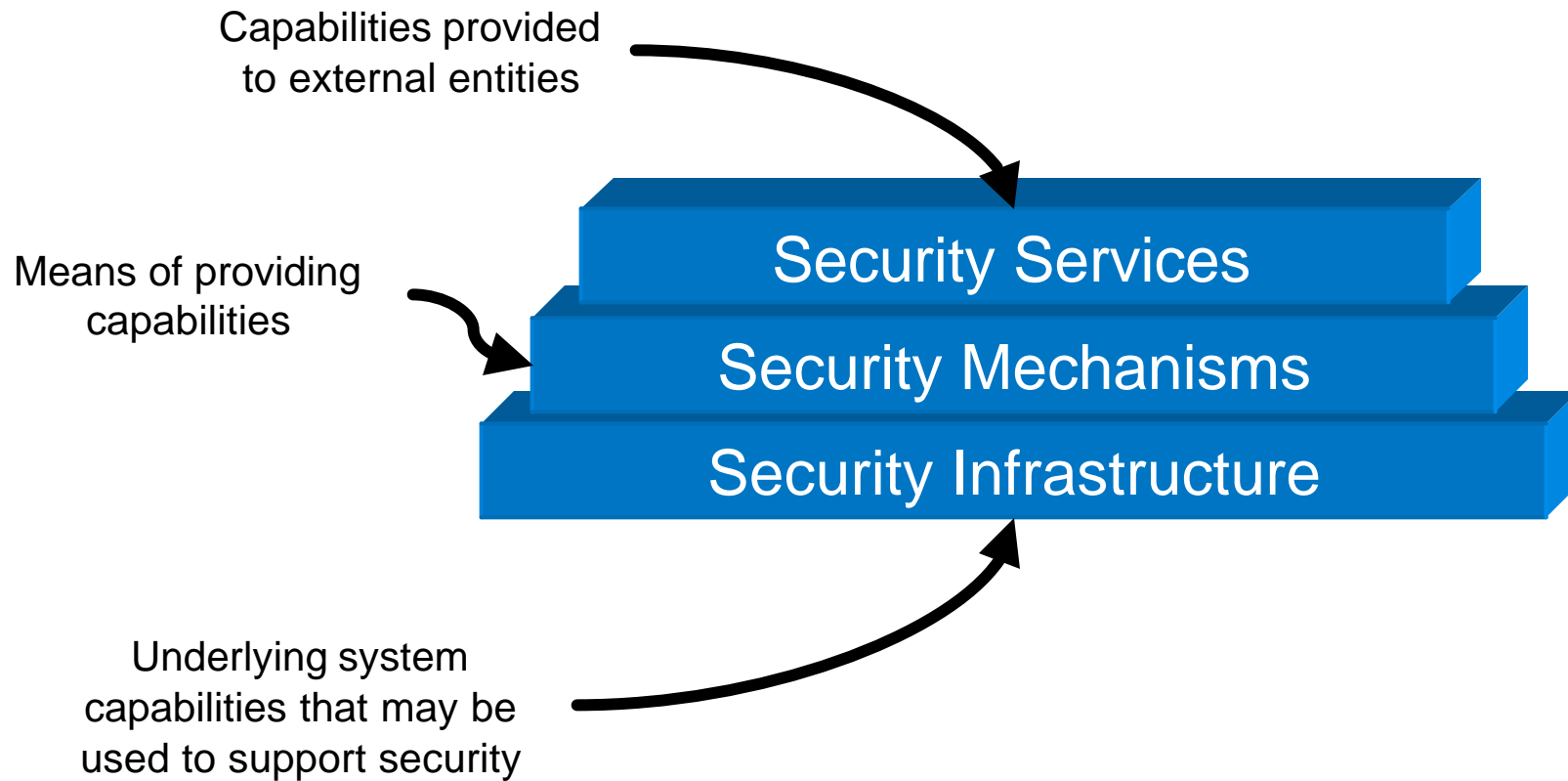
# Approaching a Discussion of Security for a System

- Assume that it is not really needed
  - or –
- Assume that it already exists
- Test it in
- Add it on
- Design it in



Decreasing final  
cost

# One Structured Way of Viewing Security



# Some Security Infrastructure Capabilities

- Time-of-day, time synchronization across network
- Naming infrastructure
- Directory infrastructure
- Registration authority
- Network management

# Categories of Security Mechanisms

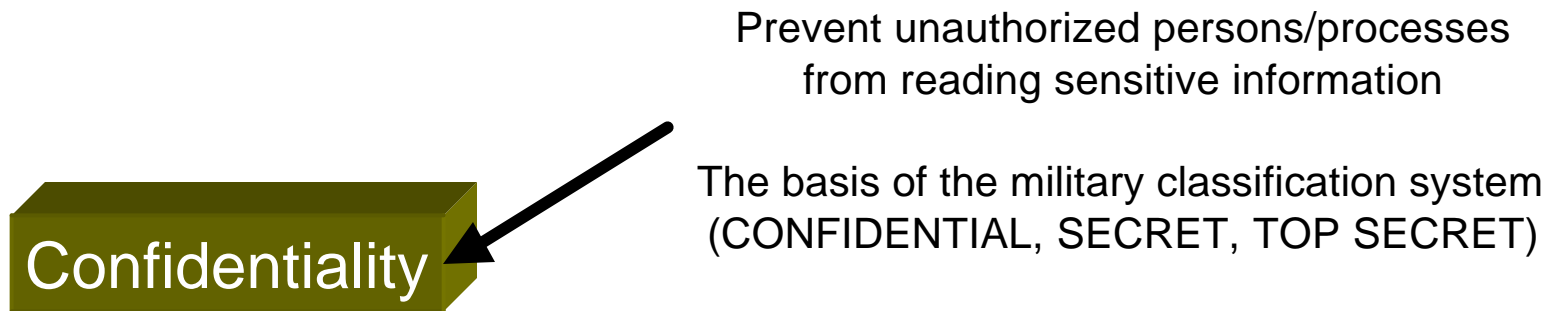
- *Prevent* occurrence of compromise
- *Detect* occurrence compromise
- *Correct* after-effects of compromise

## Some Security Mechanisms and the Security Services They Could Enable

Service:	ID	Auth	AC	Conf	Integ	Avail	NR
Mechanisms:							
Cryptography/Encryption		✓		✓	✓		✓
Quality of Service Controls						✓	
Audit Logs			✓ *	✓ *	✓ *	✓ *	✓
Trusted Software			✓	✓	?	?	?
Security Policies	✓	✓	✓	✓	✓	✓	✓
Biometrics	✓	✓					
Smart Cards	✓	✓	✓	✓	✓		✓
System Backups					✓		✓
Security Assessment	✓	✓	✓	✓	✓	✓	✓

List of mechanisms is not meant to be exhaustive

# One Structured Way of Viewing Security



**Security Services**

# One Structured Way of Viewing Security



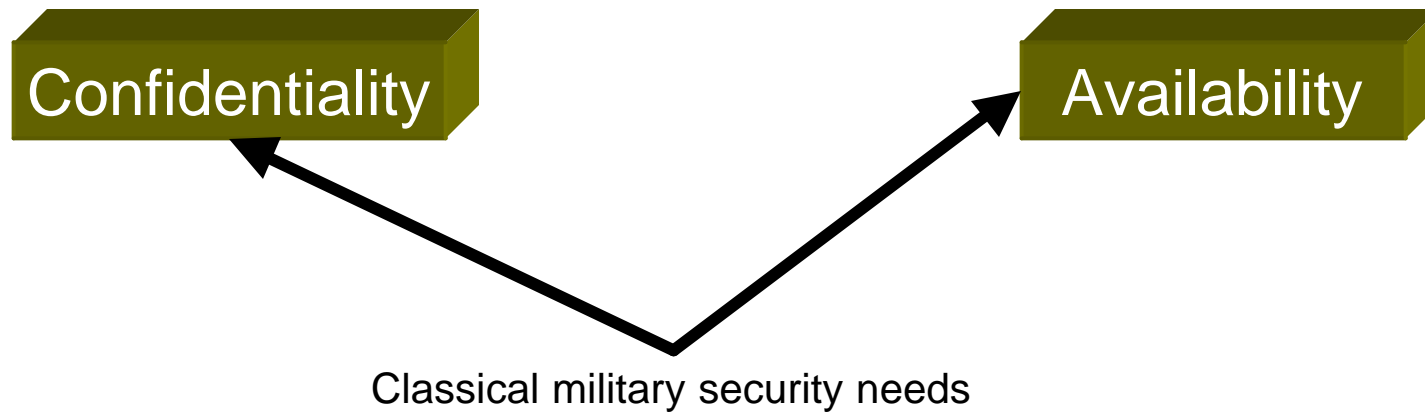
Insure that operational capabilities are available when required.

Counter denial-of-service threats, system outage due to failures/damage.

The essential routing capabilities of the Internet are intended to make it a high-availability network

**Security Services**

# One Structured Way of Viewing Security



**Security Services**

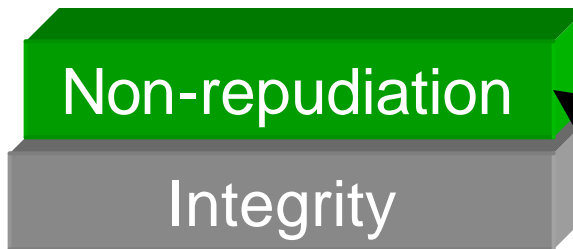
# One Structured Way of Viewing Security



Control against a posteriori  
modification of a transaction

**Security Services**

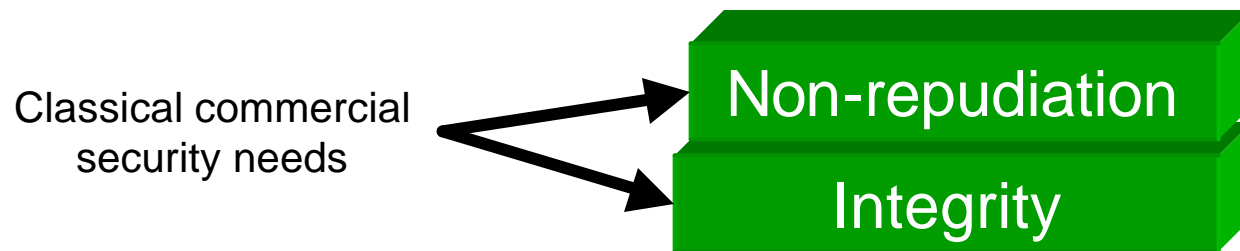
# One Structured Way of Viewing Security



Prevent a posteriori denial of occurrence of details of event/ transaction

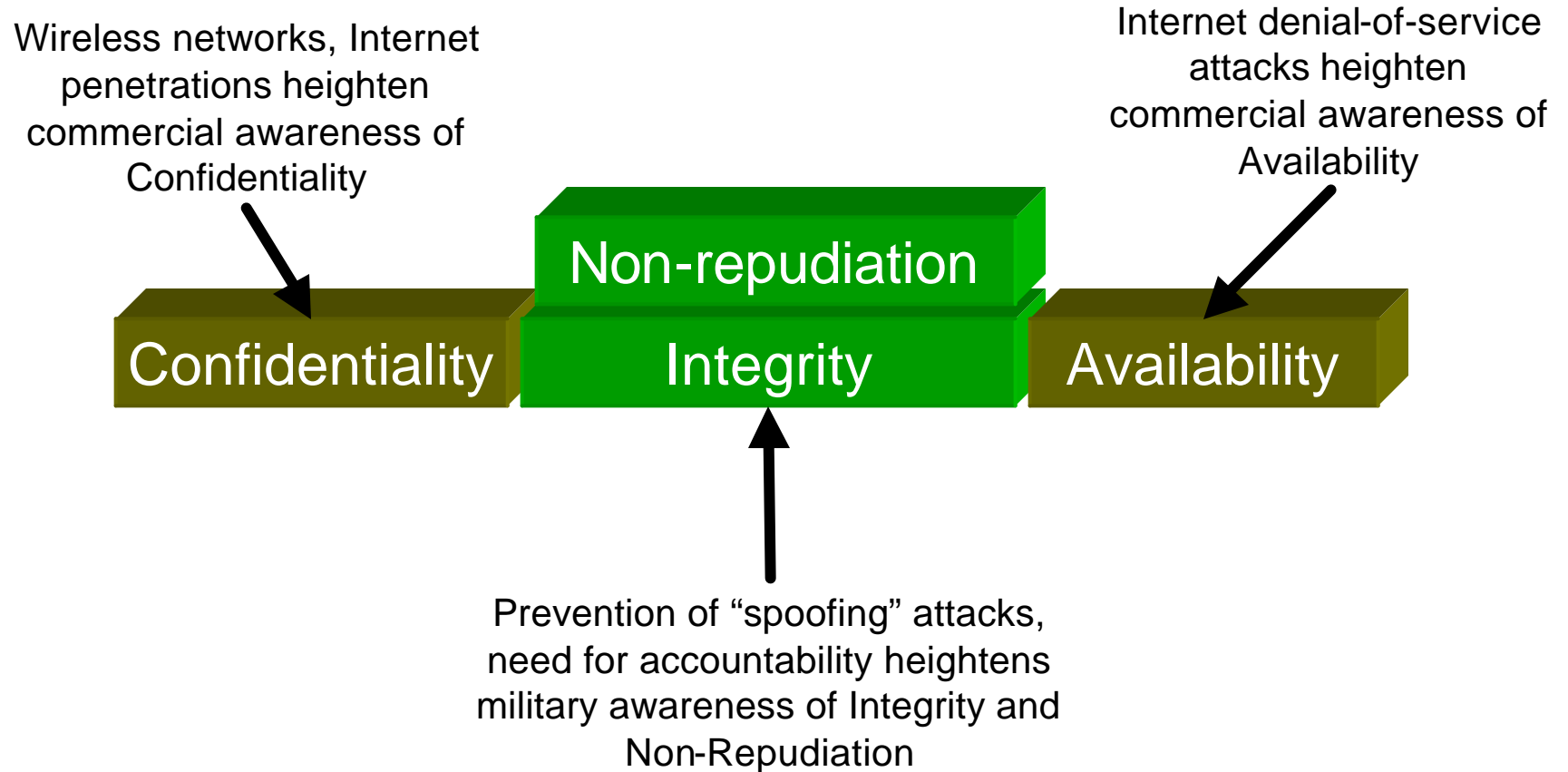
**Security Services**

# One Structured Way of Viewing Security



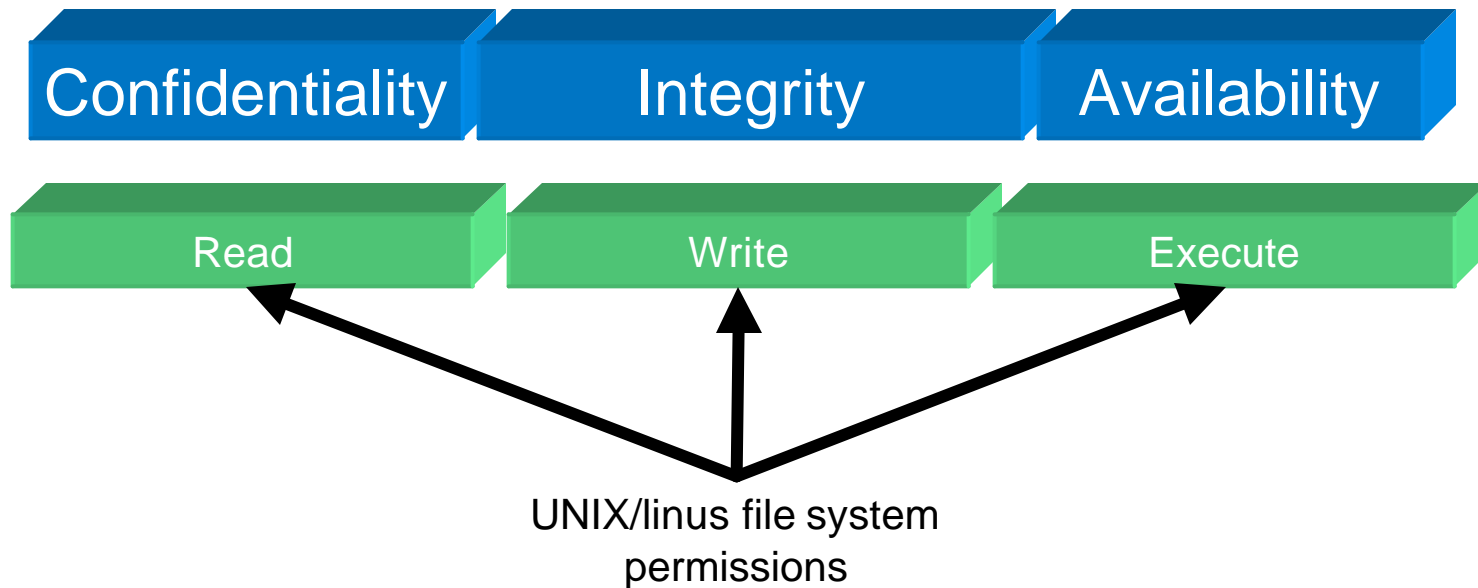
**Security Services**

# One Structured Way of Viewing Security



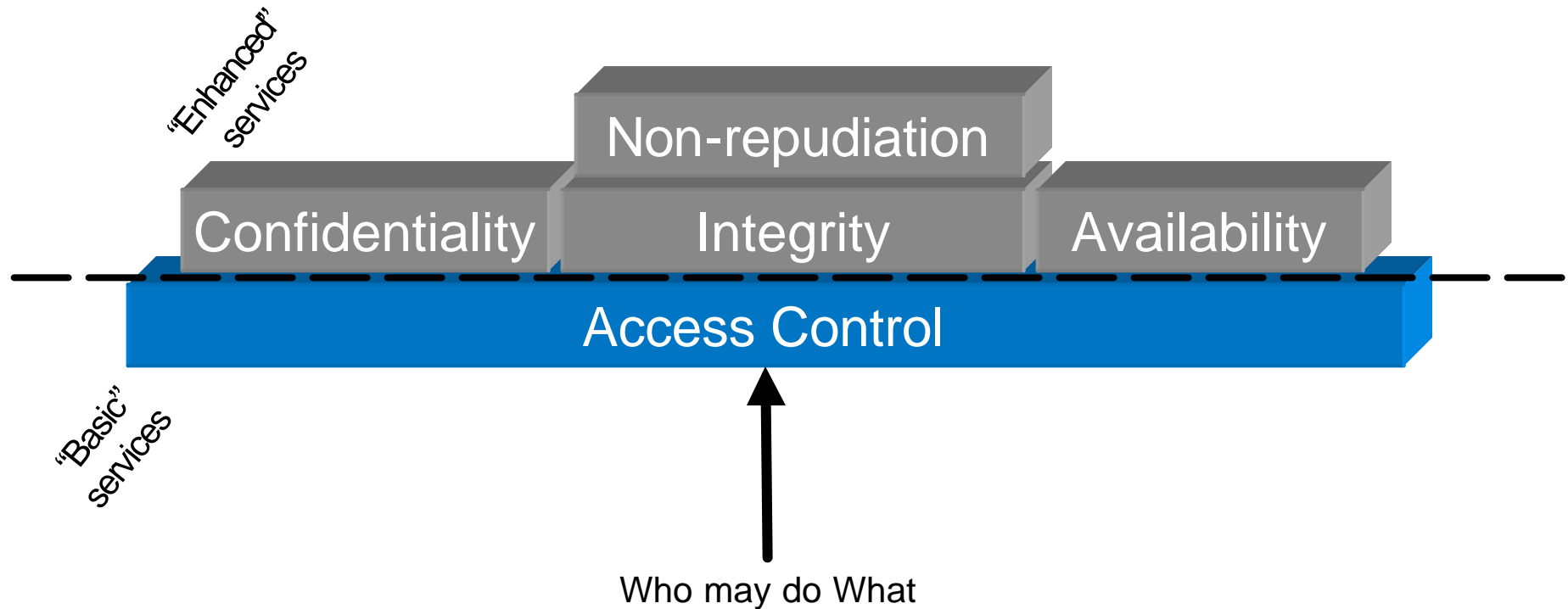
## Security Services

# One Structured Way of Viewing Security



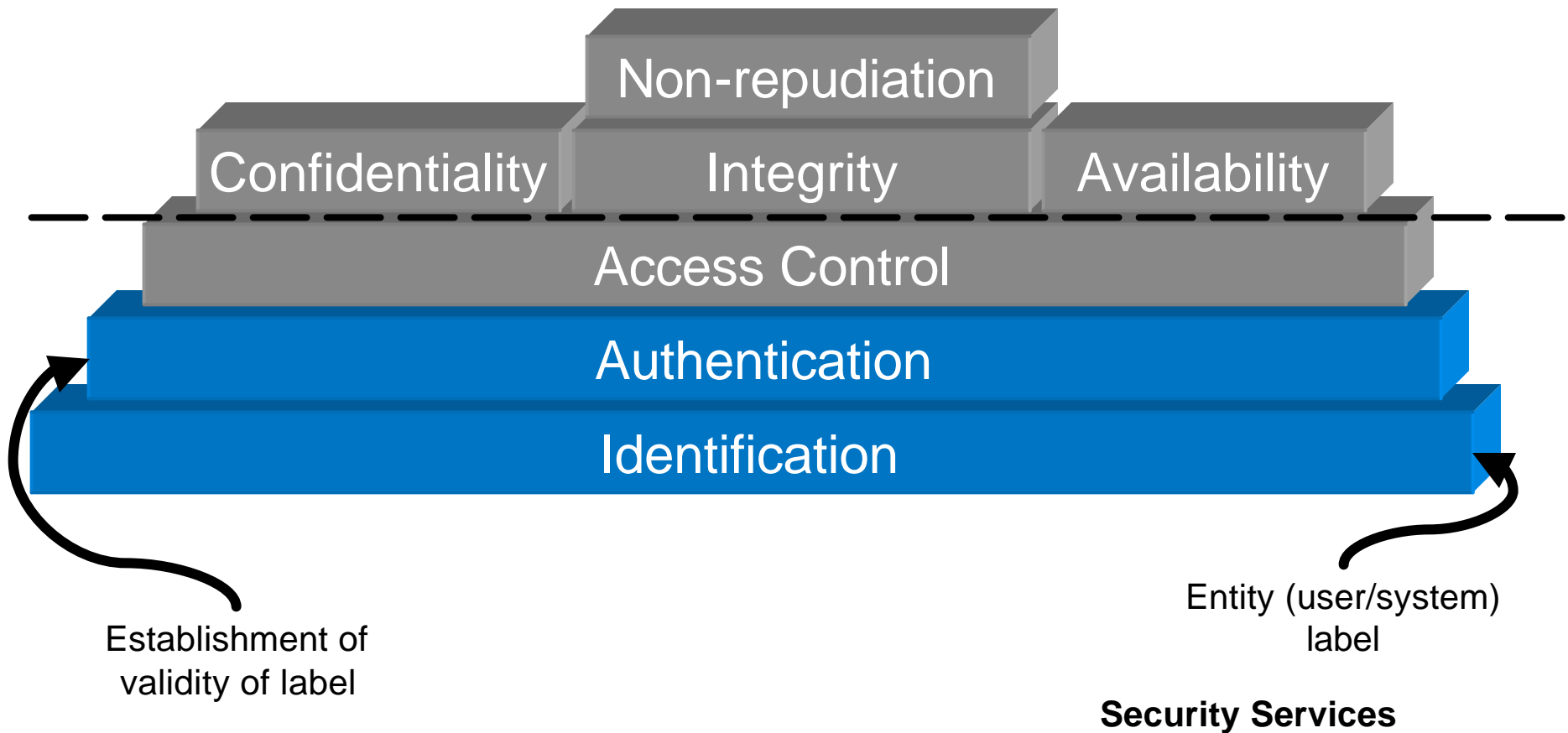
**Security Services**

# One Structured Way of Viewing Security

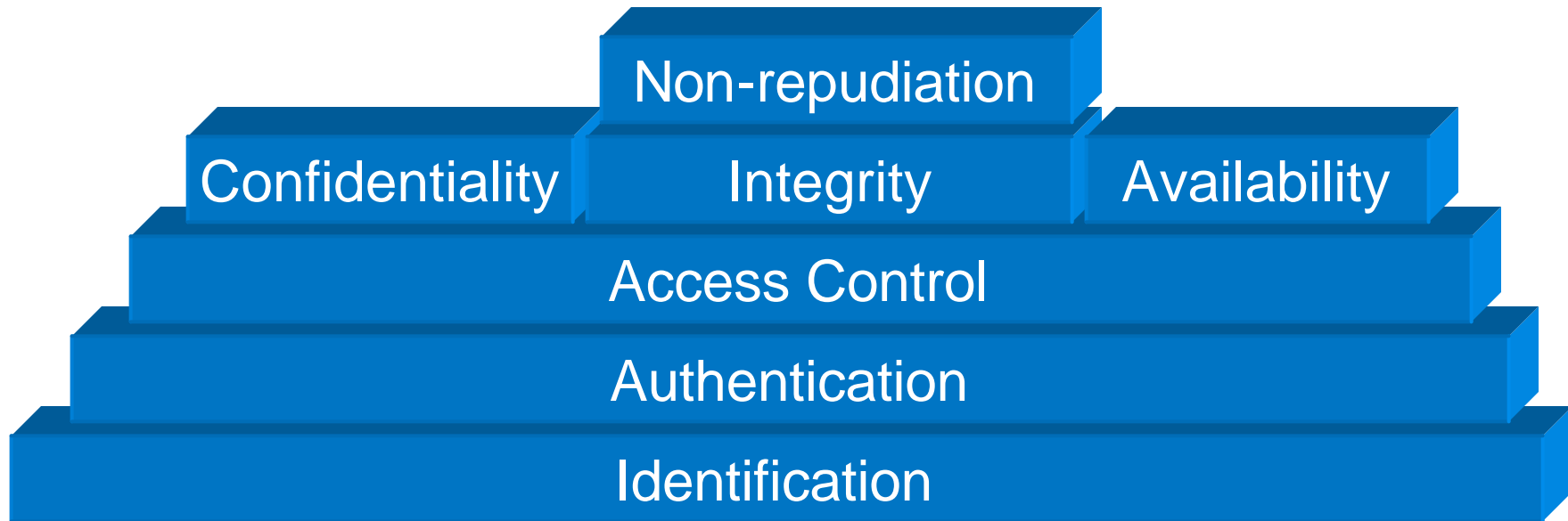


**Security Services**

# One Structured Way of Viewing Security



# One Structured Way of Viewing Security

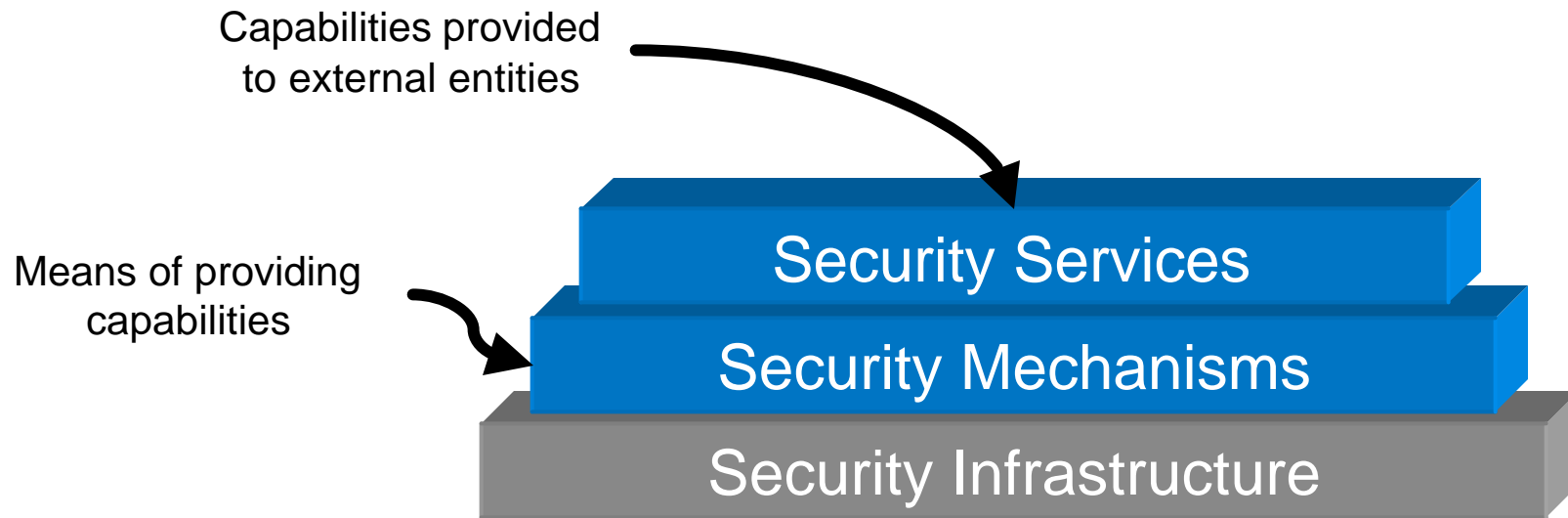


## Security Services

# What Security Issues Can Be Addressed By Cryptography and Related Techniques?

- Cryptography is NOT the solution to all security problems, but
- It does provide an enabling technology for many issues.
- If intelligently applied (balanced against other issues and needs) it can be of substantial value
- It provides a good place to start discussing detailed security technologies in an Information System

# From Last Time: One Structured Way of Viewing Security



# Categories of Security Mechanisms And Those That Can Be Addressed By Cryptography

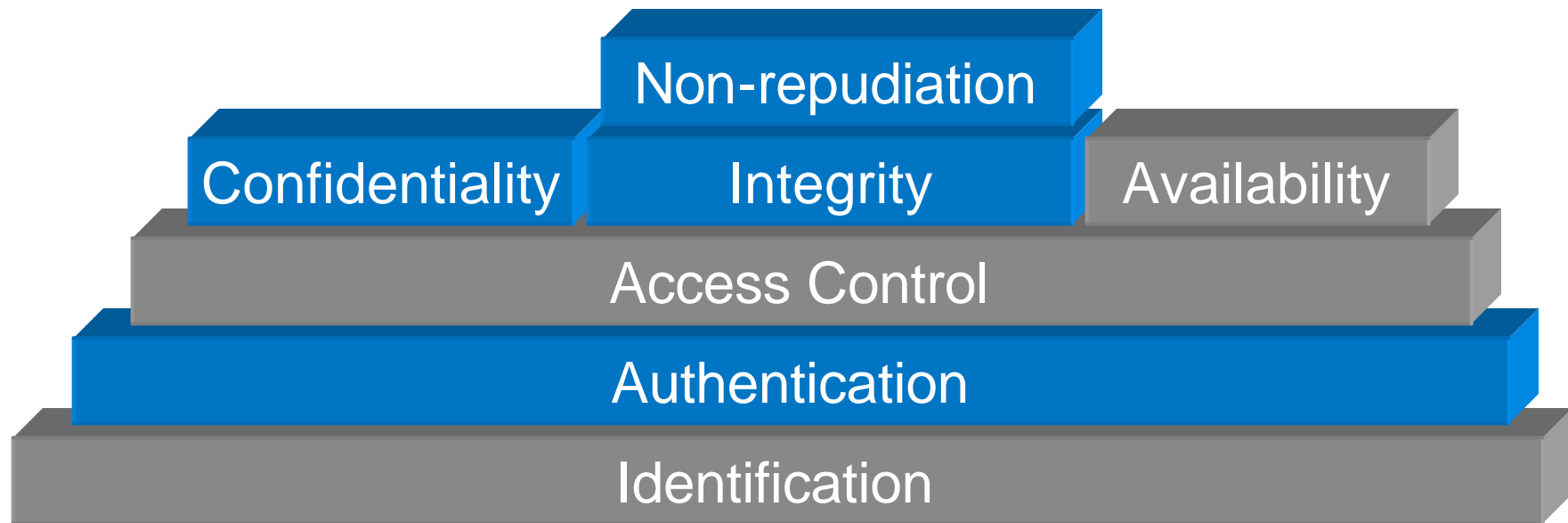
- *Prevent* occurrence of compromise
- *Detect* occurrence compromise
- *Correct* after-effects of compromise

## Some Security Mechanisms and the Security Services They Could Enable

Service:	ID	Auth	AC	Conf	Integ	Avail	NR
Mechanisms:							
Cryptography/Encryption		✓		✓	✓		✓
Quality of Service Controls						✓	
Audit Logs			✓*	✓*	✓*	✓*	✓
Trusted Software			✓	✓	?	?	?
Security Policies	✓	✓	✓	✓	✓	✓	✓
Biometrics	✓	✓					
Smart Cards	✓	✓	✓	✓	✓		✓
System Backups					✓		✓
Security Assessment	✓	✓	✓	✓	✓	✓	✓

List of mechanisms is not meant to be exhaustive

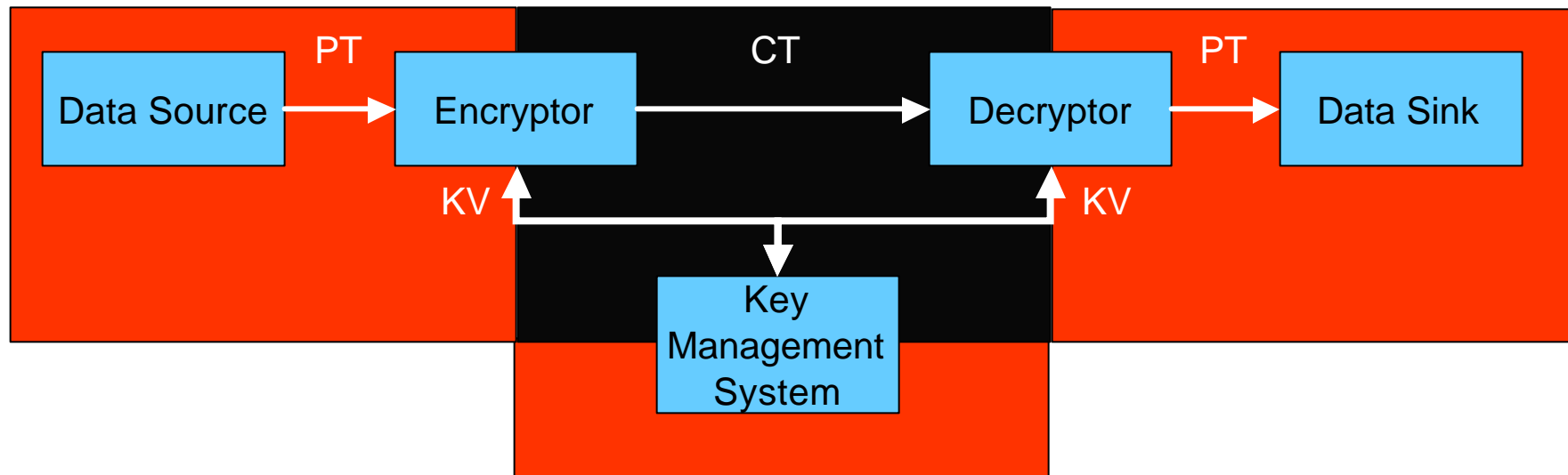
# One Structured Way of Viewing Security And Security Services Addressed By Cryptography



**Security Services**

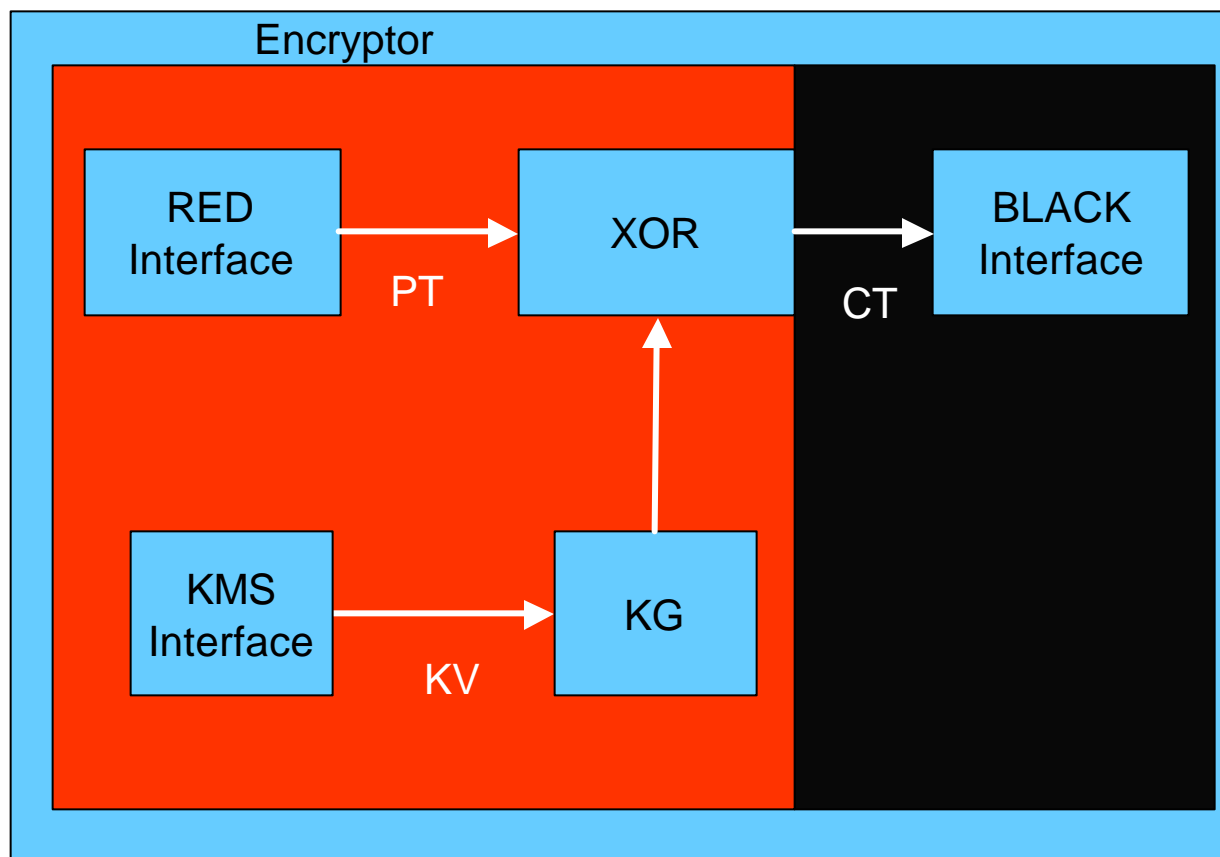
# Cryptography Terminology

- Plaintext (PT) – unprotected source material (images, text, data, etc.)
- Ciphertext (CT) – Plaintext that has been enciphered (encrypted)
- Key Variable (KV) – Parameter of cryptographic system that selects, specifies, or controls key stream
- Key Management – Process for providing corresponding key variable(s) to sender and receiver



## Cryptography Terminology - Continued

- Key Stream (Key Sequence) (KS) – (Pseudo)random string of symbols used to encrypt and/or decrypt plaintext
- Key Generator (KG) – Device that generates the key stream for a stream encipherment device



# Miscellaneous Cryptography Terminology

- Affine:

$$F(x) = \alpha x + \beta$$

- Linear:

$$F(x) = \gamma x$$

$$F(\alpha x + \beta y) = \alpha F(x) + \beta F(y) \quad [\text{superposition}]$$

- Nonlinear:

Superposition does not apply

- Permutation:

Reordering of inputs, e.g.,  $P(\{a,b,c,d\}) = \{c,b,a,d\}$

- Substitution:

Functional mapping, non necessarily 1-1 or onto

# Wireless Technical Paper Assignment

- <http://www.argreenhouse.com/society/J-SAC/past.html> lists the tables of contents of previous issues of the IEEE Journal on Selected Areas of Communications. Tables of Contents and article abstracts are also available through the Stevens library technical journal database (actually IEEE Xplore®)
- Full .pdf copies of J-SAC papers are available from through the Stevens library at <http://www.lib.stevens-tech.edu/research/serials/jnlsIndex.html> by following the link to *IEEE Electronic Library Online -> Journals and Magazines -> S – Selected Areas of Communications, Journal of*  
(you must be at an on-campus computer or connected via the Stevens VPN)
- Pick a J-SAC paper that interests you from either the April or June 2003 editions (the topics for these issues are: MIMO Systems and Applications I & II)
- Write a 3-5 page report on the paper. Report should include:
  - Summary of fundamental ideas presented in the paper
  - Issues paper addresses and how they have been addressed in the past
  - Discussion of 1 or 2 core ideas of paper
  - Identification of any security-related issues brought up in the paper
  - Potential applications of technology presented
  - Future opportunities created by the technology