

**NIS/CpE 691CE**

**Information System Security**

**Stevens Institute of Technology  
Spring 2006**

**Class 1 – 1/18/06**

# Course Introduction

- Logistics:
  - Instructor: Prof. Bruce McNair
    - Office: Burchard 206
    - Phone: 201-216-5549
    - Email: [bmcnair@stevens-tech.edu](mailto:bmcnair@stevens-tech.edu)
    - Web site: [koala.ece.stevens-tech.edu/~bmcnair](http://koala.ece.stevens-tech.edu/~bmcnair)
      - Class notes will be posted on this site
    - Office hours:
      - Monday – Thursday ~9:30 - ~4
    - Email almost always works – I try to read all email within minutes and respond within an hour. Leave a call-back number and time to reach you if you need to talk.
  - Assignments:
    - Electronic submissions are preferred
    - email is OK with MS/Office (2000 or previous) or .pdf

# Course Introduction (continued)

- Grading
  - Two research papers: 35% each (individual effort)
  - Final project: 20% (individual or joint effort, small group efforts encouraged)
  - Final project presentation: 10% (individual or joint effort)
  
- Recommended references
  - Bruce Schneier, “Secrets and Lies: Digital Security in a Networked World,” Wiley, ISBN 0-471-25311-1
  - ---, *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, Wiley, ISBN 0-471-11709-9.
  
- Other resources/suggested readings
  - CRYPTOGRAM: <http://www.counterpane.com/crypto-gram.html>
  - RISKS Digest: <http://www.csl.sri.com/users/risko/risksinfo.html>
  - David Kahn, *The Codebreakers-The Story of Secret Writing*, Scribner; ISBN 0-684-83130-9
  - Cliff Stoll, *The Cuckoo’s Egg*, Pocket Books; ISBN: 0-743-41146-3
  - James Bamford, *The Puzzle Palace: Inside America’s Most Secret Intelligence Organization*, Viking Press, ISBN 0-140-23116-1.

# Your instructor's background

- BE (EE) Stevens, 1971, MEE Stevens, 1974, countless graduate courses at Stevens
- 1971 – 1973 Fort Monmouth – Production and Procurement, COMSEC Branch
- 1973 – 1973 ITT Defense Communications Division, Nutley, NJ (digital hardware design, low data rate speech coding for secure voice applications)
- 1974 – 1978 Fort Monmouth – Communications R&D Command (VHF-FM tactical radio – modulation techniques, COMSEC, ECCM capabilities)
- 1978 – 2002 Bell Labs/AT&T Labs – Research (Public data networks, analog modems, secure voice, encryption hardware, speaker verification, computer and network security, next generation wireless data networks, Wireless LAN extensions)
- March 2002 – present – Novidesic Communications
- August 2002 – Present – Stevens Electrical and Computer Engineering Department (wireless, security, signal processing)

Three career threads:

1. Security/Cryptography – It kept following me, besides it's interesting
2. Wireless Communications – A lifelong interest
3. Signal Processing – The infrastructure that makes 1&2 work

# Course Topics

- Introduction
  - Definition of security
  - Assessing security
  - Security terminology
  - Historical developments
  - Structure of security
- Cryptography
  - Applications of cryptography
  - Terminology
  - Evolution of cryptography, Caesar ciphers, one-time pads
  - Operation of DES, AES
  - Public-key cryptosystems
- Topics in Information Systems Security
  - Minimum privilege
  - Compartmentalization
  - Dual controls
  - Security perimeters
  - Trustworthy software, proof of design correctness
  - Single-points-of-failure
  - Covert channels
  - Inference

# Course Topics

- More topics in Information Systems Security
  - Security models
    - Requirements
    - Types
    - State-machine models
    - Mandatory/Discretionary controls
    - Information-flow models
    - Informal models
- Kerberos Authentication
- Authentication in centralized systems
- Distributed Authentication
- Denial of Service attacks
- Security vs. ATM, IP, wireless mobile networks
  - QoS
  - Traffic modeling
  - Network topology

# Course Topics

- Intrusion Detection Systems
- Security Protocols
  - Zero-knowledge proofs
  - Subliminal channels
  - Oblivious transfer
  - Digital signature schemes
  - Bit commitment
  - Digital cash
  - Secure contract signing
  - Secure voting
  - Digital certified mail
  - Anonymous message broadcast
- TEMPEST and related topics

# Course Structure

- Weeks 1&2: Lecture format
- Weeks 3 – 12: Seminar/Lecture format
  - Two or three presentations related to current week's topics (research papers that convey state-of-the-art topics)
  - lecture
  - One or two presentations introducing following week's topics (research papers that present broad overviews or surveys of the topics)
  
  - Reference papers will be provided on WebCT for presenters to use and other students to review
  - Presentations will be scheduled at least 1-2 weeks in advance.
- Weeks 13&14: Project presentations

# What is “Security”

- Quality has been defined to be “Meeting (or exceeding) customer’s expectations”

# 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

# 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.”

# 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.

# 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

# 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:

# 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

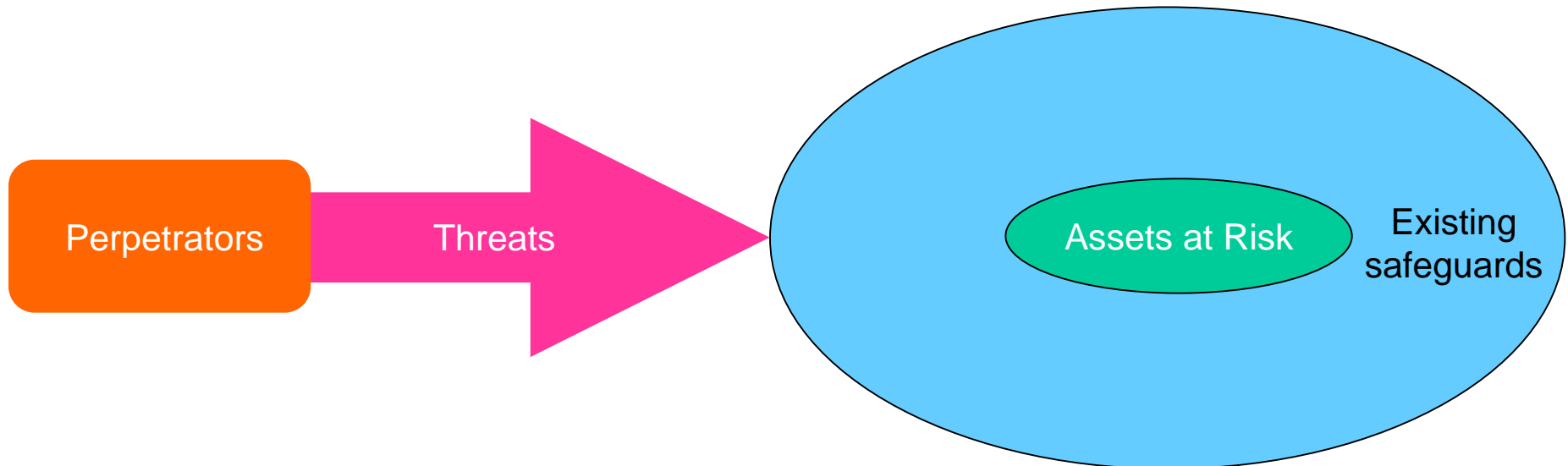
What might be worth stealing?

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

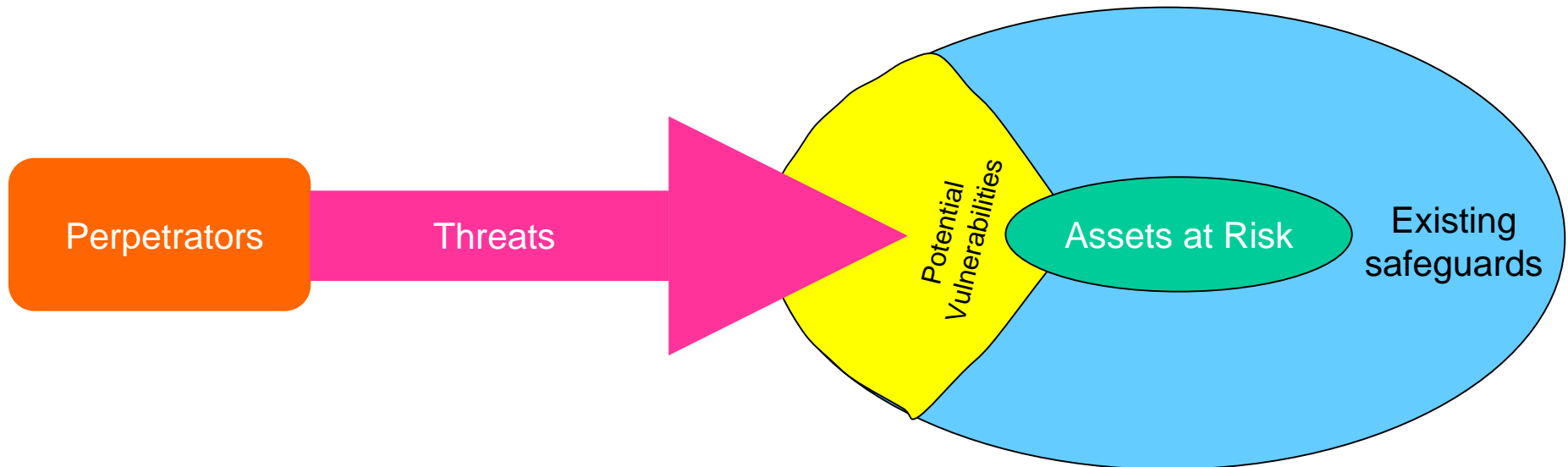


What are potential means of attack?

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

# How Much Security Is Enough?

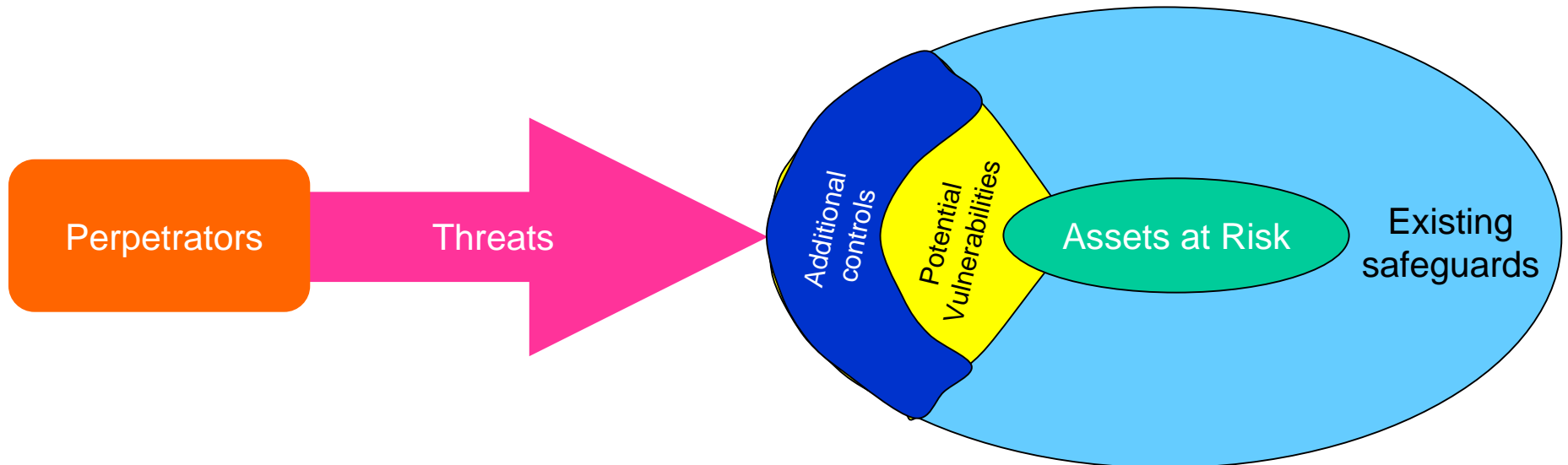
A security assessment model



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!**

# Some Historical Developments in Security

- ~4000 B.C – early human written communications developed
- ~3999 B.C. – first attempts to hide written messages
- ~0 B.C. – Latin alphabet in widespread use
- ~0 A.D. – early use of substitution cipher (Caesar cipher)  
(about same time frame and same technology as Hebrew at-bash cipher)
- ~100 A.D?? – Ali Baba invents “passwords”
- ~101 A.D.?? – Password scheme compromised
- ~800-1200 A.D. – Dark Ages set back most technologies, including security
- ~1760 A.D. – Thomas Jefferson invents cryptographic “rotor” machine, later suggests creation of patent office. (Rotor based cryptography used beyond 1950’s)
- 1800’s - early 1900’s, invention of electrical devices, telegraph, programmable computer, wireless communications, vacuum tube, etc. lay foundation for technology revolution of 1900’s. Ciphers are invented and broken few years later
- ~1920 – discovery of “One time pad” – the only provably secure method of encryption
- ~1960’s – Creation of ARPAnet – highly survivable packet switching data network, ancestor of Internet
- 1988 – Cornell graduate student brings down Internet accidentally
- ~1992 – World Wide Web born, graphical Web browsers follow ~1994
- ~1997-present – ongoing denial of service, web page modification, compromise of private user information attacks

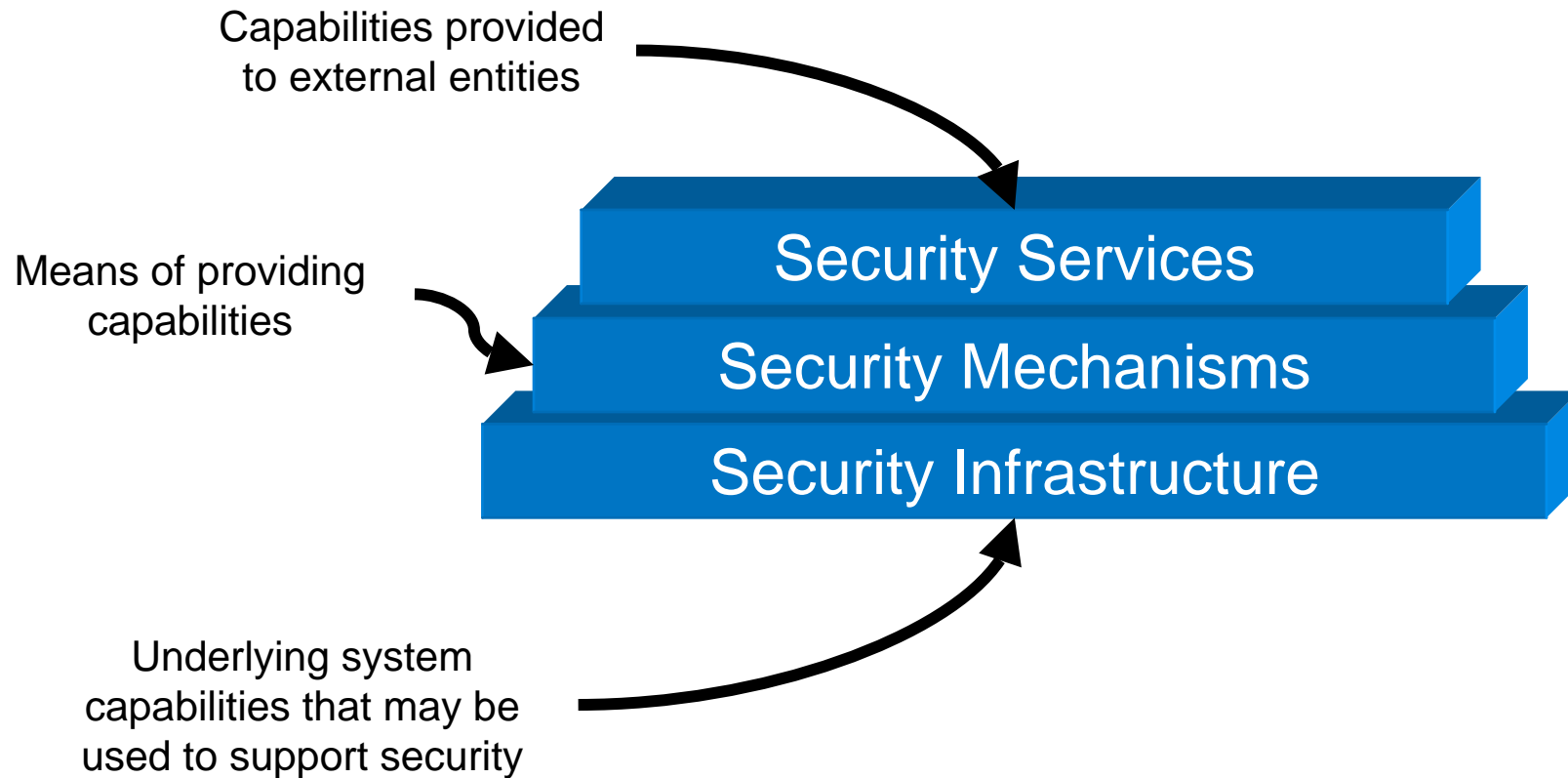
# Approaching a Discussion of Security for a System

- 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

# Categories of Security Mechanisms

- *Prevent* occurrence of compromise ← In the future
- *Detect* occurrence compromise ← In the present
- *Correct* after-effects of compromise ← In the past

# Some Security Mechanisms and the Security Services They Could Enable

Mechanisms: \ Service:	ID	Auth	AC	Conf	Integ	Avail	NR
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

Prevent unauthorized persons/processes  
from reading sensitive information



The basis of the military classification system  
(CONFIDENTIAL, SECRET, TOP SECRET)

**Security Services**

# One Structured Way of Viewing Security



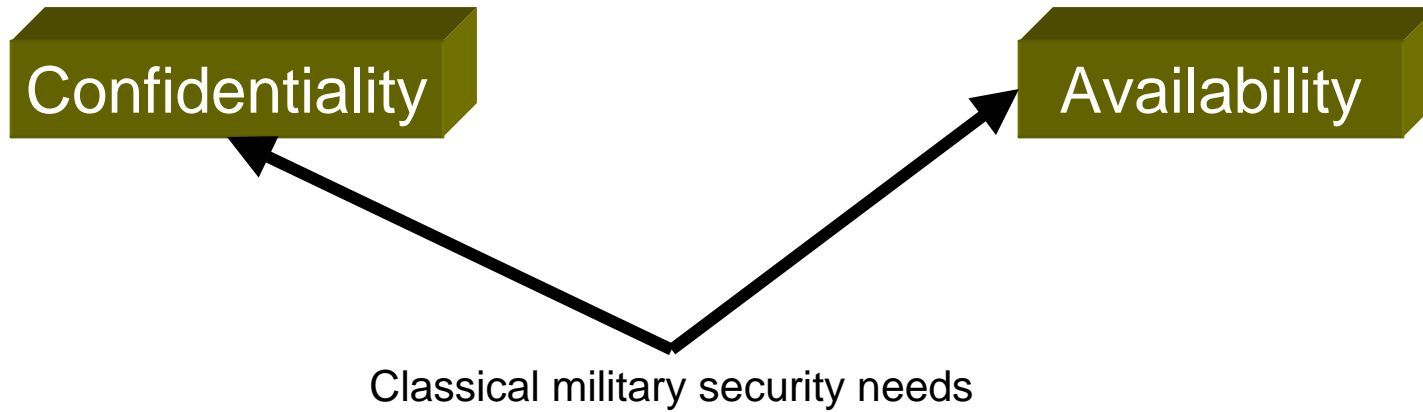
Insure that operational capabilities are available when required.

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**

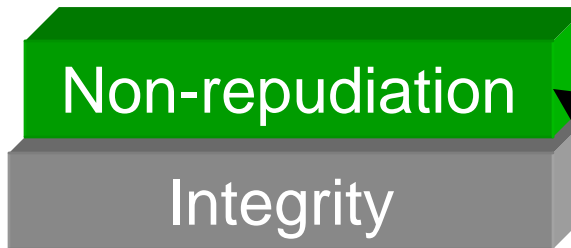
# One Structured Way of Viewing Security



Control against a posteriori  
modification of a transaction

**Security Services**

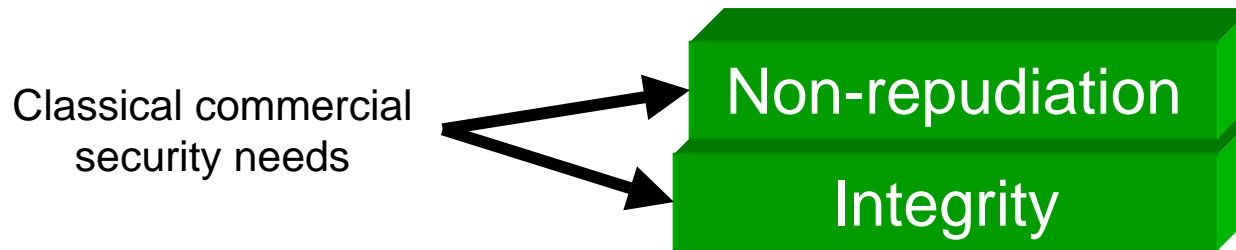
# One Structured Way of Viewing Security



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

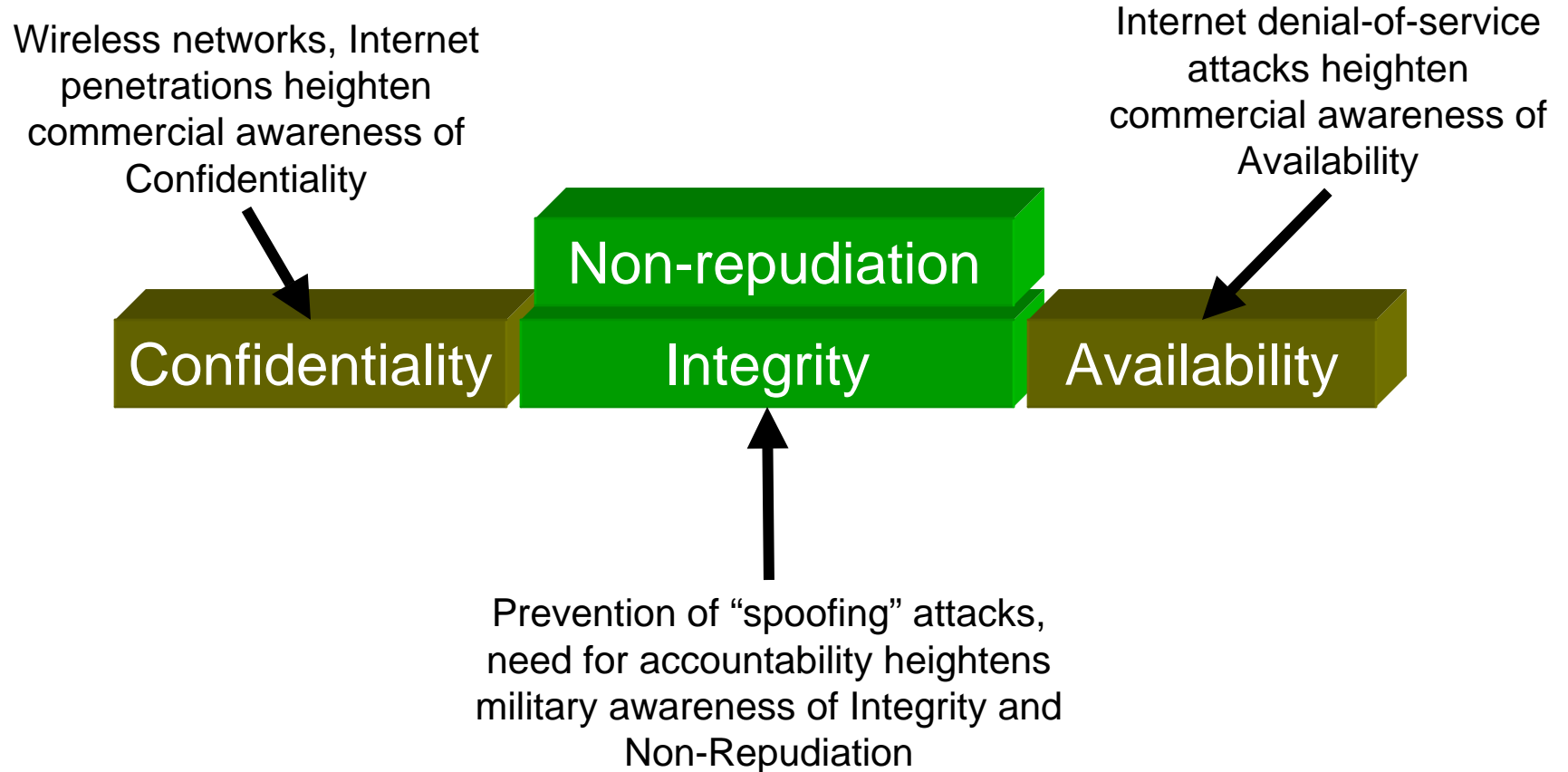
**Security Services**

# One Structured Way of Viewing Security



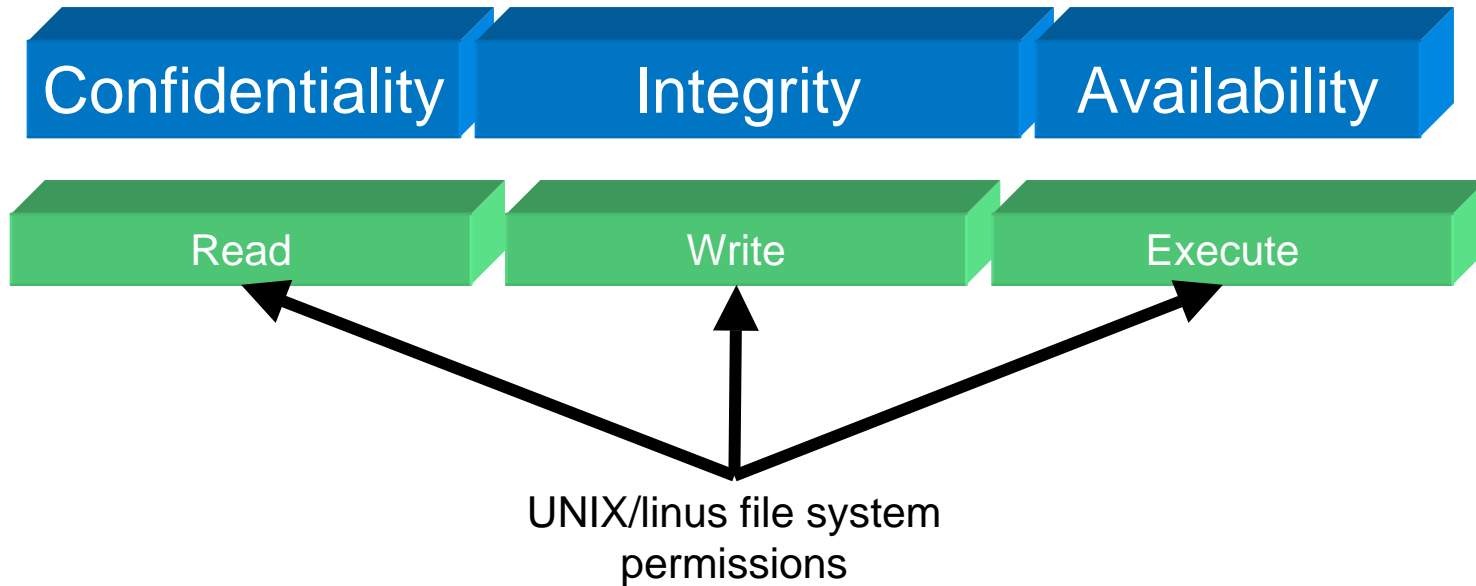
**Security Services**

# One Structured Way of Viewing Security



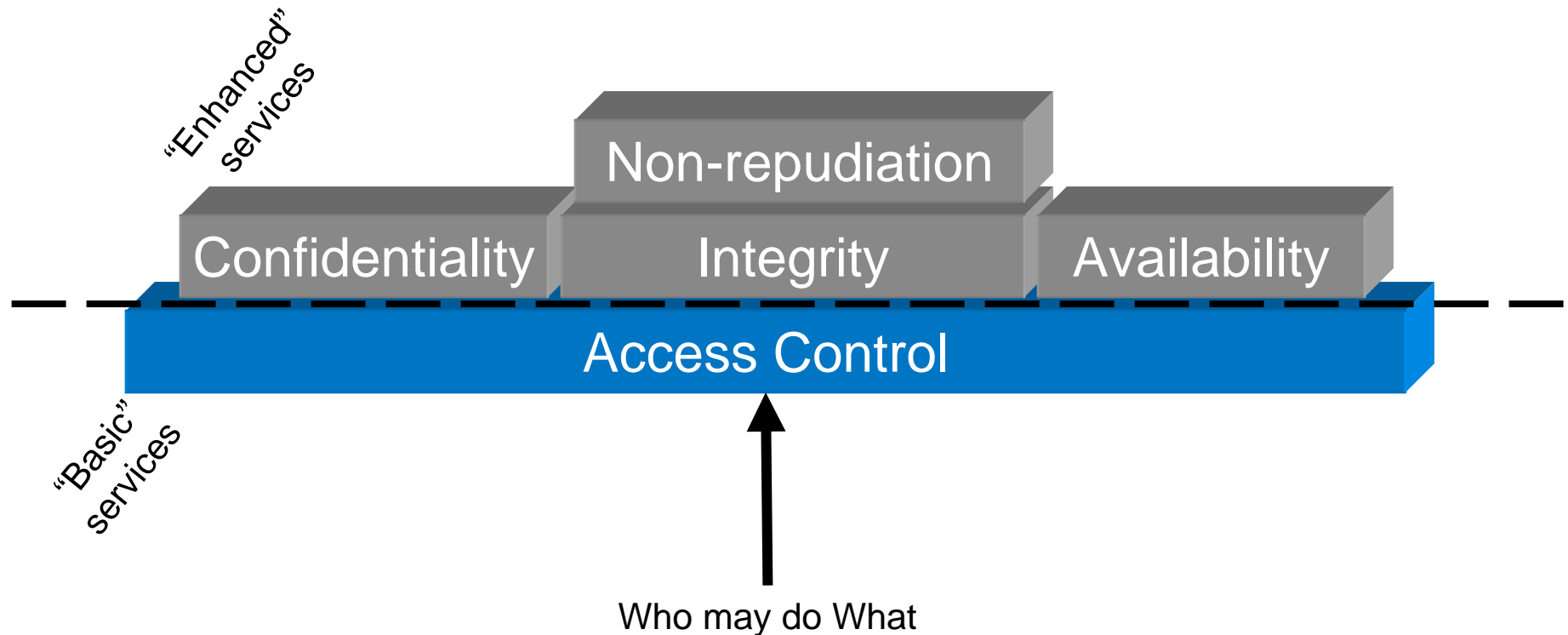
**Security Services**

# One Structured Way of Viewing Security



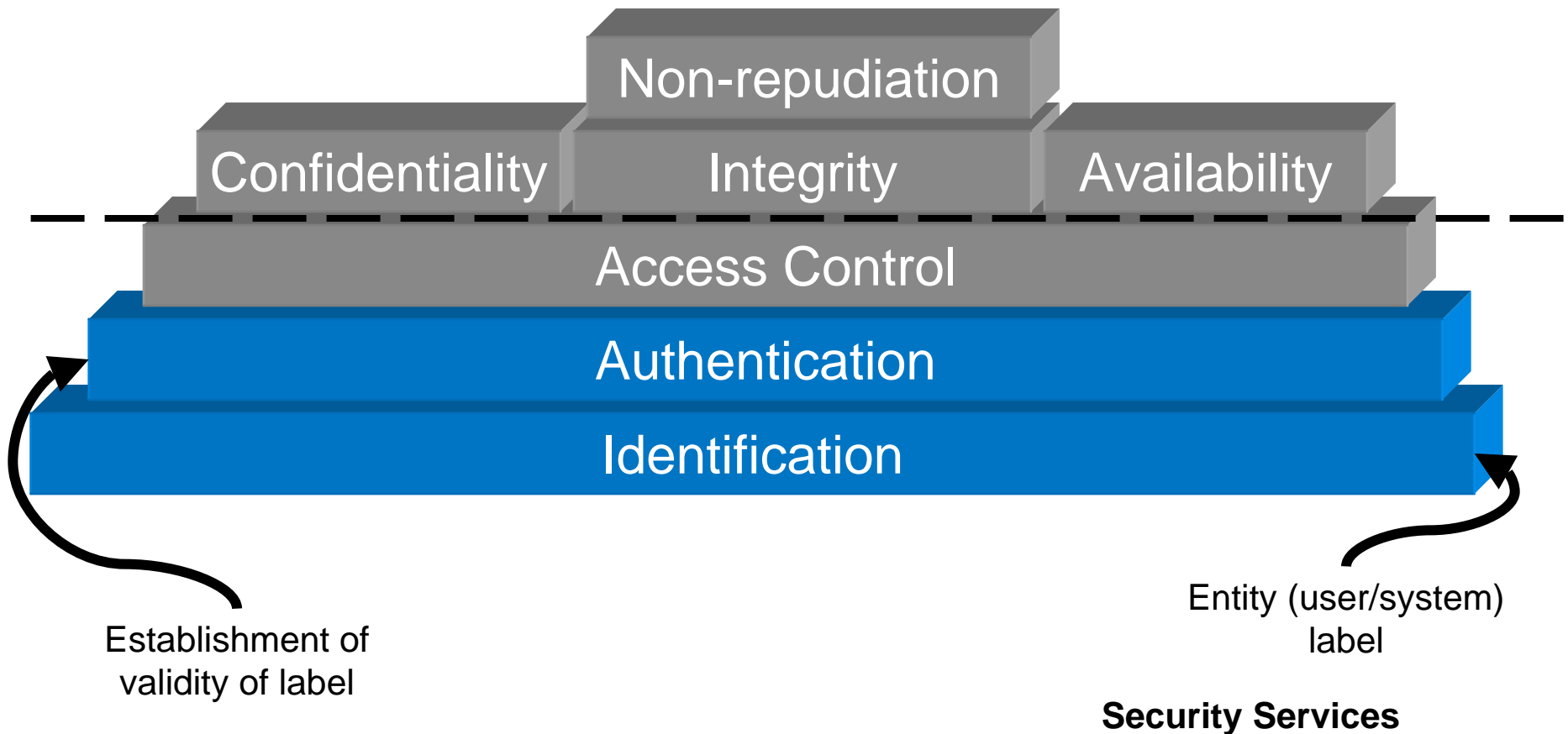
**Security Services**

# One Structured Way of Viewing Security

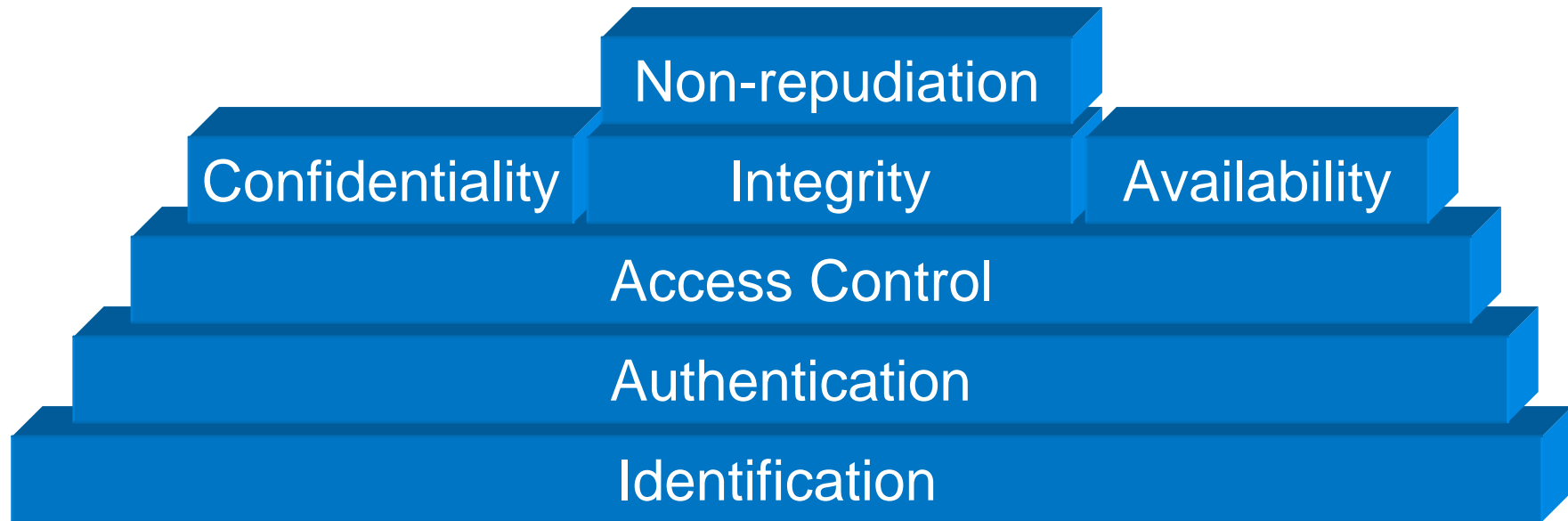


**Security Services**

# One Structured Way of Viewing Security



# One Structured Way of Viewing Security



## Security Services