SECURITY IN COMPUTING, FIFTH EDITION

Chapter 1: Introduction

Objectives for Chapter 1

- Define *computer security* as well as basic computer security terms
- Introduce the C-I-A Triad
- Introduce basic access control terminology
- Explain basic threats, vulnerabilities, and attacks
- Show how controls map to threats

What Is Computer Security?

- The protection of the assets of a computer system
  - Hardware
  - Software
  - Data

Assets

Hardware:

- Computer
- Devices (disk drives, memory, printer)
- Network gear

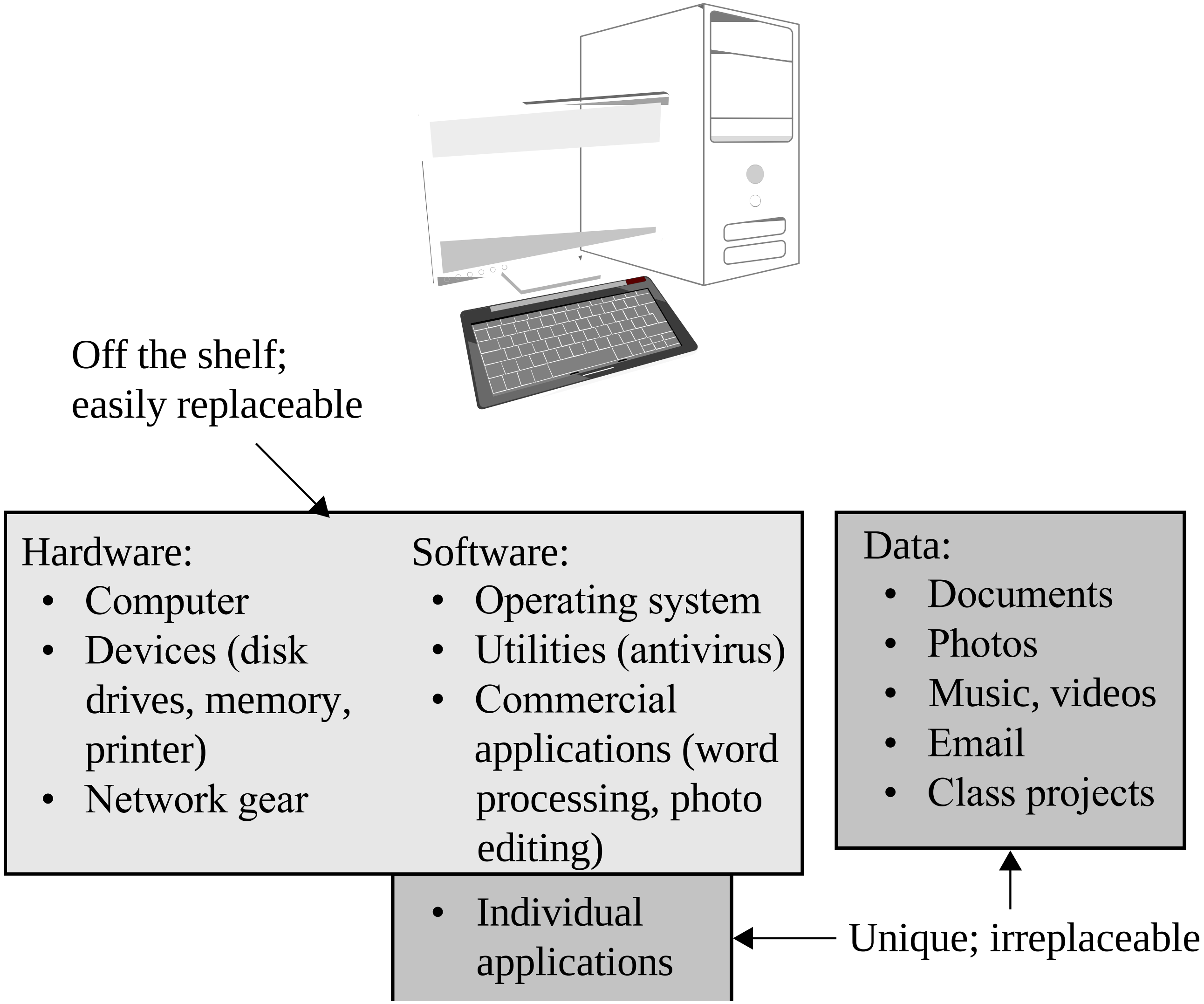
Software:

- Operating system
- Utilities (antivirus)
- Commercial applications (word processing, photo editing)
- Individual applications

Data:

- Documents
- Photos
- Music, videos
- Email
- Class projects

Values of Assets



Off the shelf; easily replaceable

Hardware:

- Computer
- Devices (disk drives, memory, printer)
- Network gear

Software:

- Operating system
- Utilities (antivirus)
- Commercial applications (word processing, photo editing)
- Individual applications

Data:

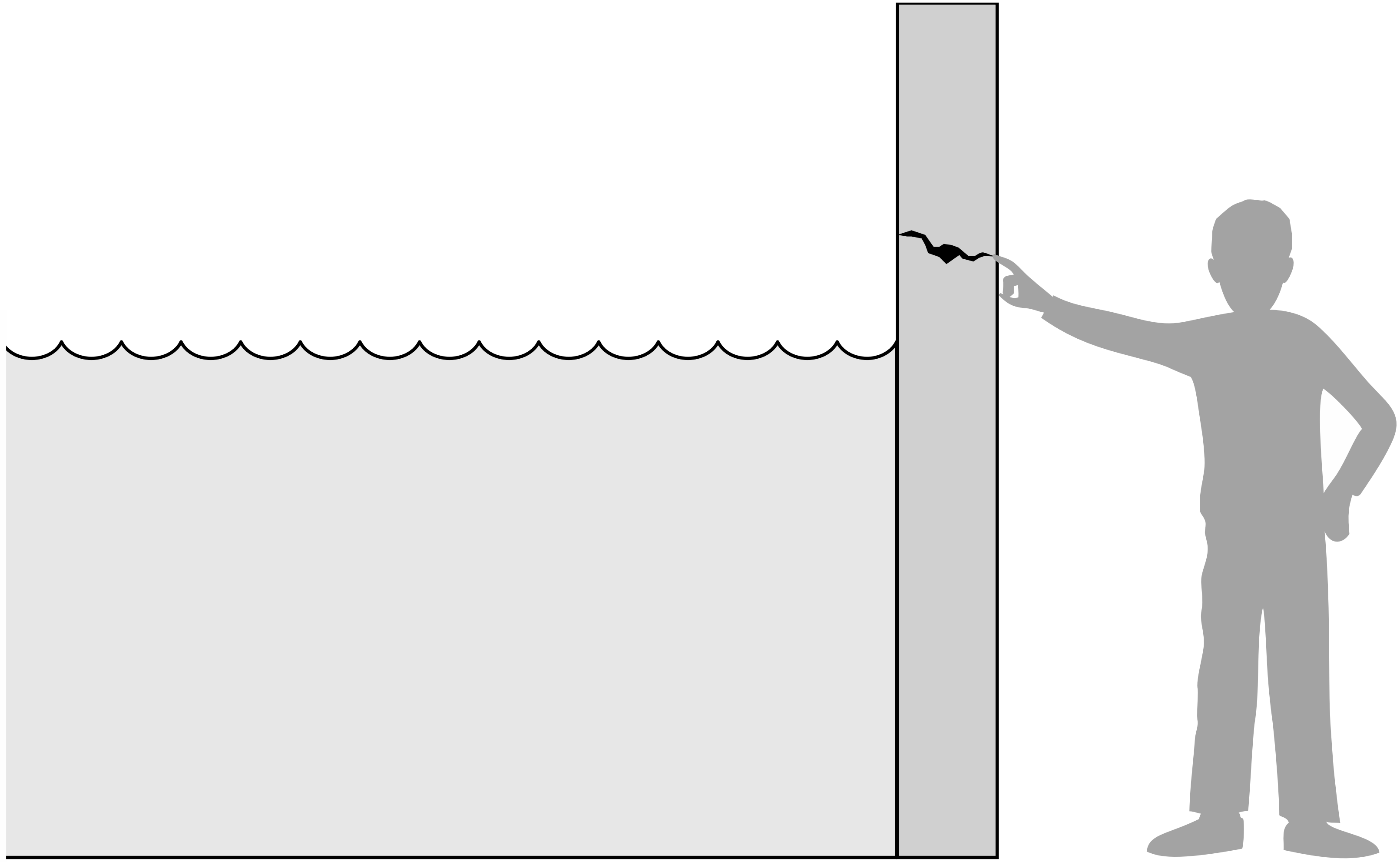
- Documents
- Photos
- Music, videos
- Email
- Class projects

Unique; irreplaceable

Basic Terms

- Vulnerability
- Threat
- Attack
- Countermeasure or control

Threat and Vulnerability

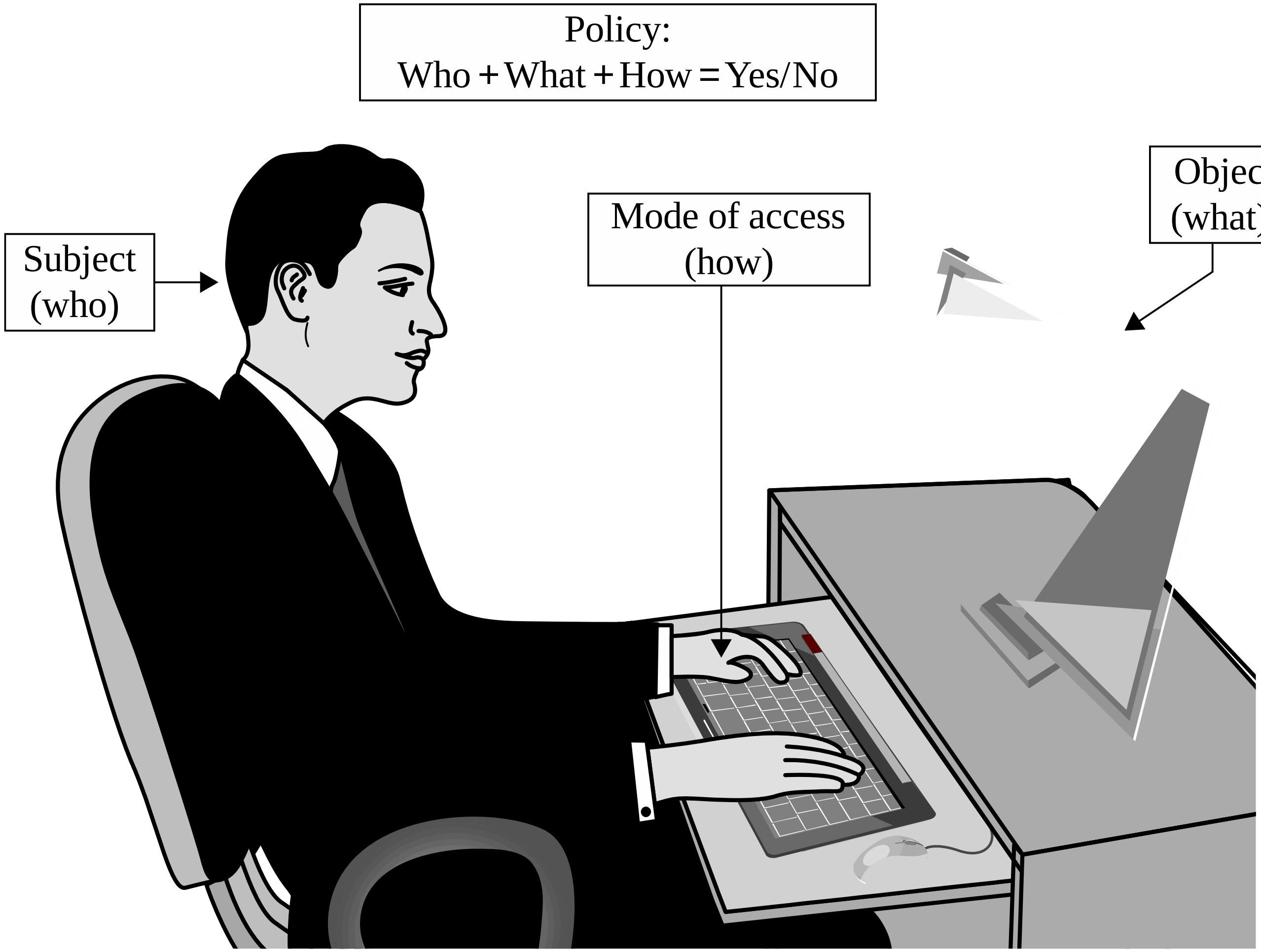


From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

C-I-A Triad

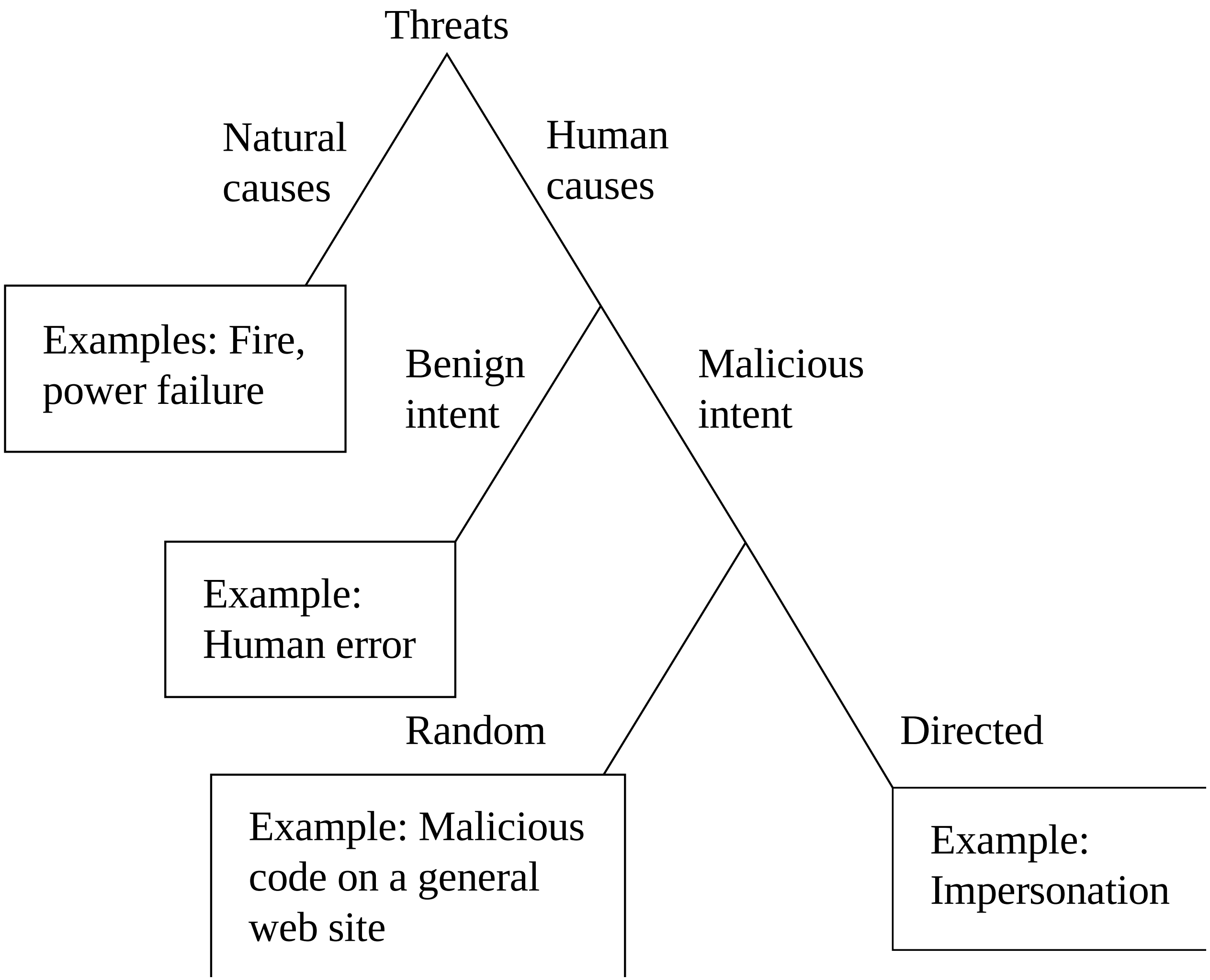
- Confidentiality
- Integrity
- Availability
- Sometimes two other desirable characteristics:
  - Authentication
  - Nonrepudiation

Access Control



From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

Types of Threats

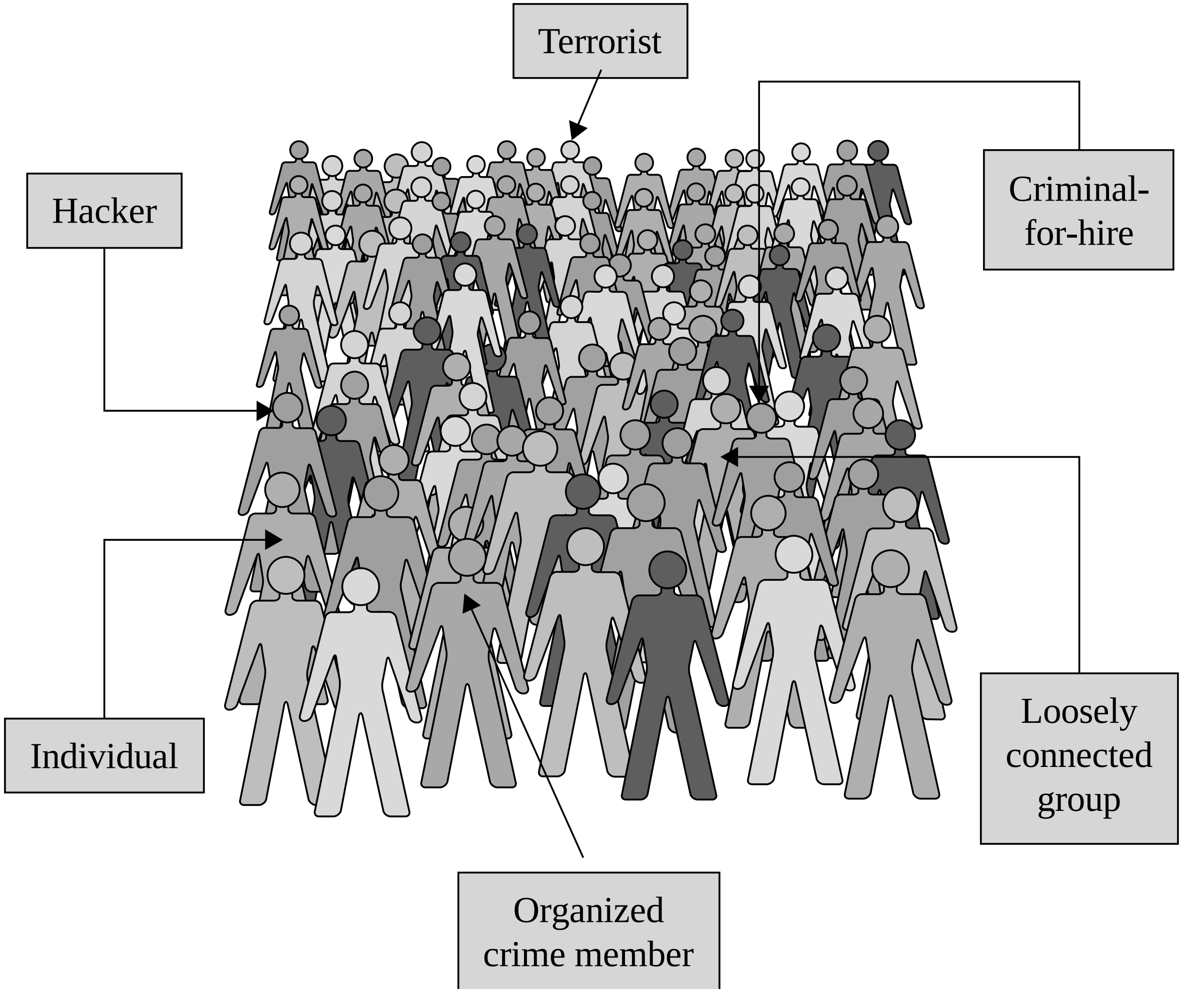


From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

Advanced Persistent Threat (APT)

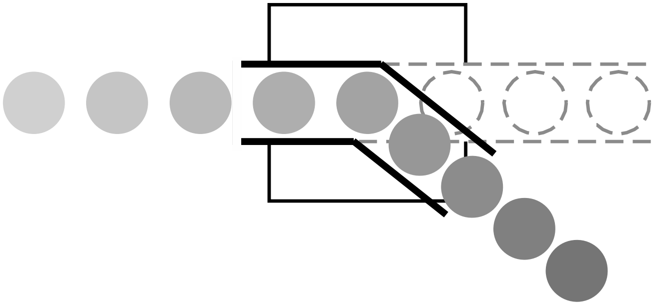
- Organized
- Directed
- Well financed
- Patient
- Silent

Types of Attackers

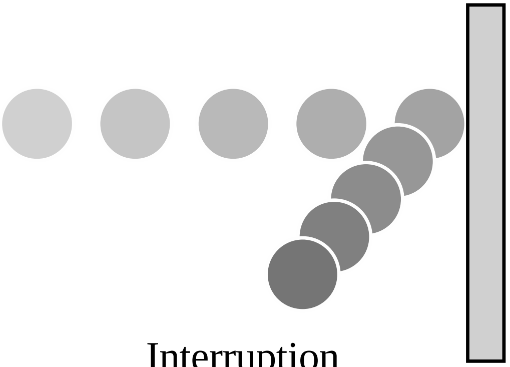


From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043).

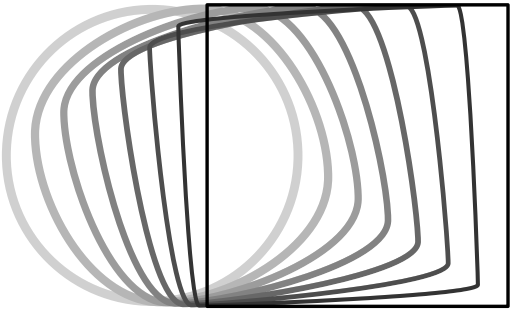
Types of Harm



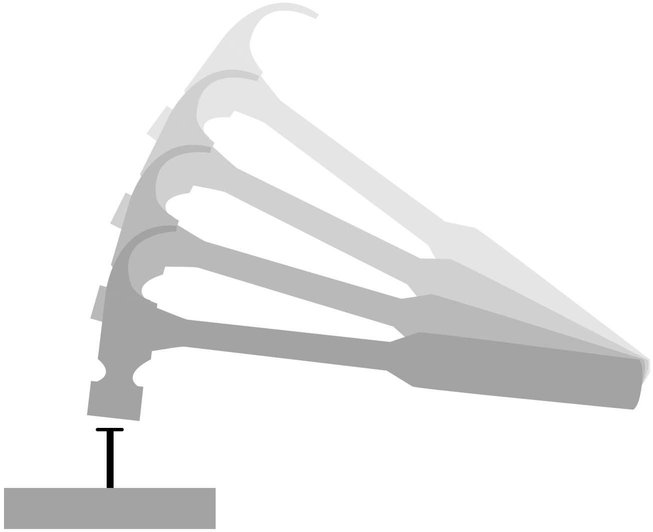
Interception



Interruption



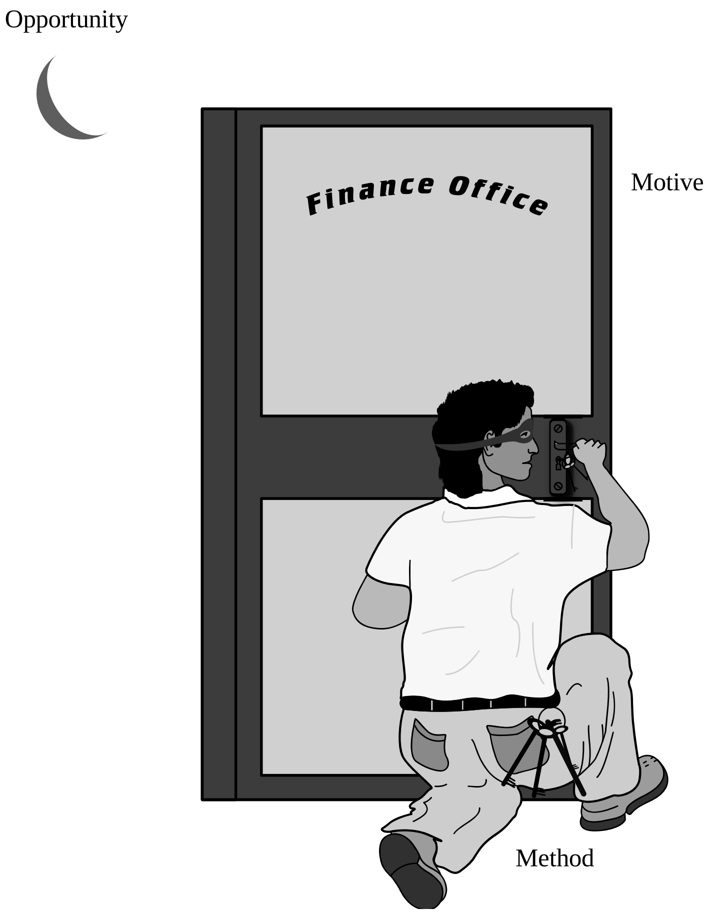
Modification



Fabrication

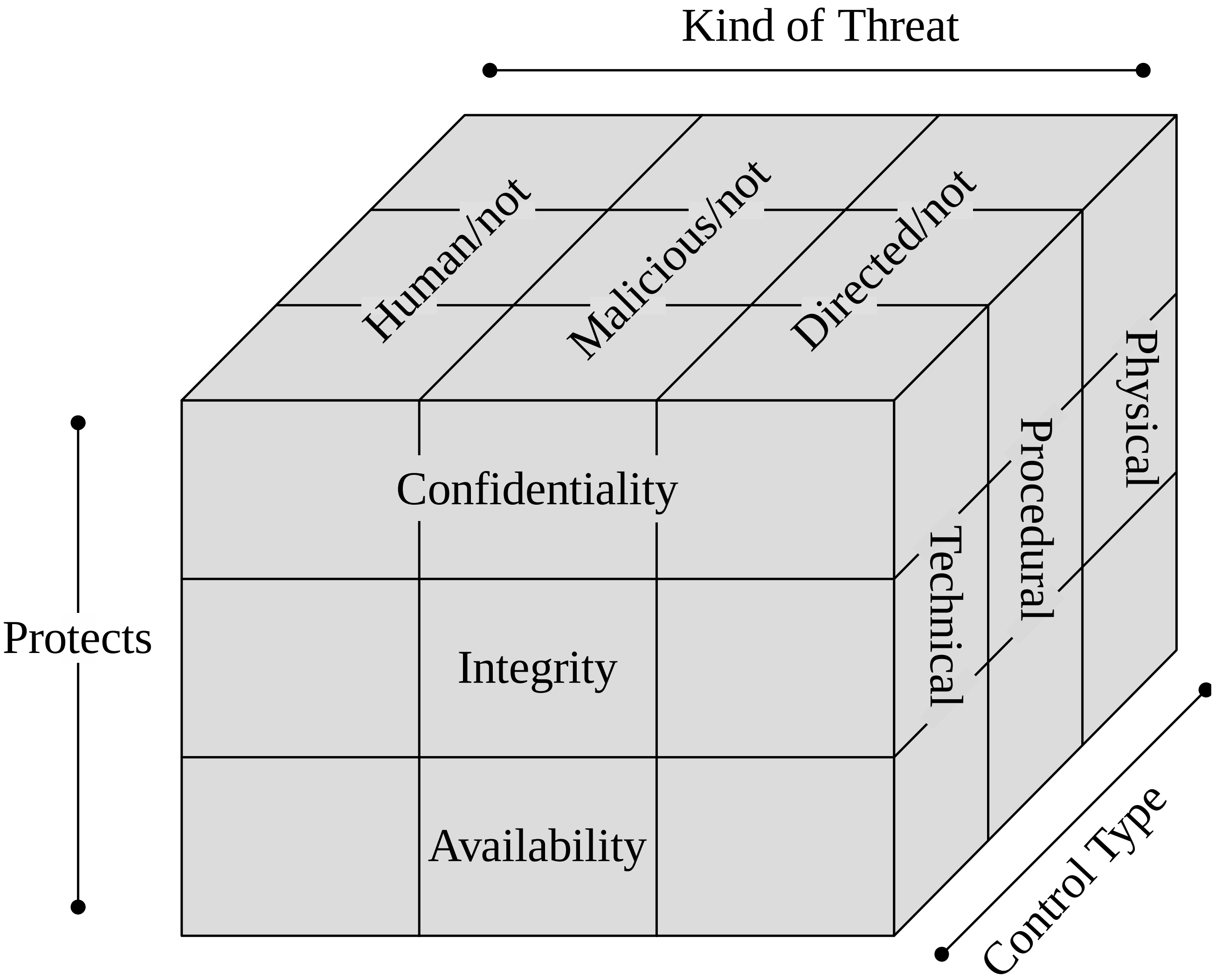
From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

Method—Opportunity--Motive



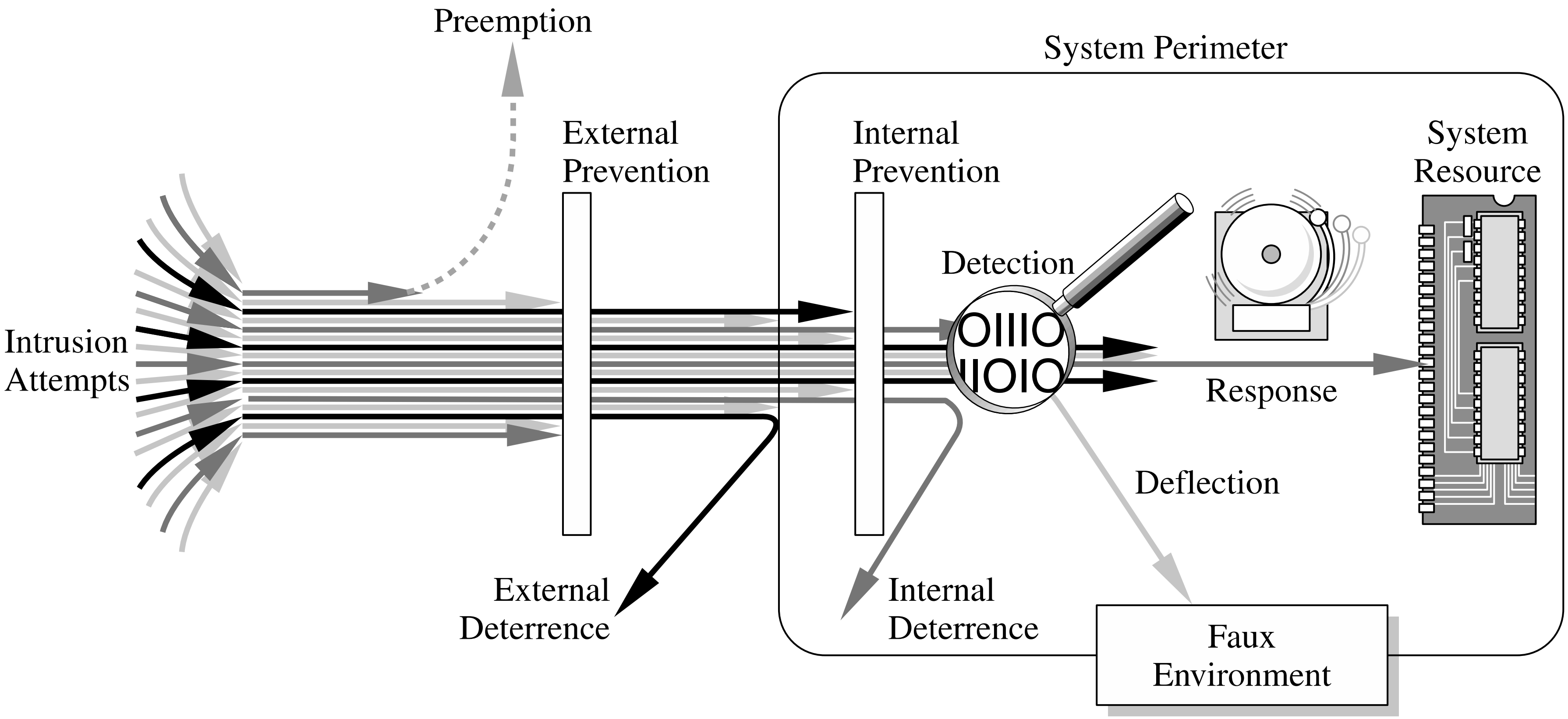
From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

Controls/Countermeasures



From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

Different Types of Controls



From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043).

Summary

- Vulnerabilities are weaknesses in a system; threats exploit those weaknesses; controls protect those weaknesses from exploitation
- Confidentiality, integrity, and availability are the three basic security primitives
- Different attackers pose different kinds of threats based on their capabilities and motivations
- Different controls address different threats; controls come in many flavors and can exist at various points in the system