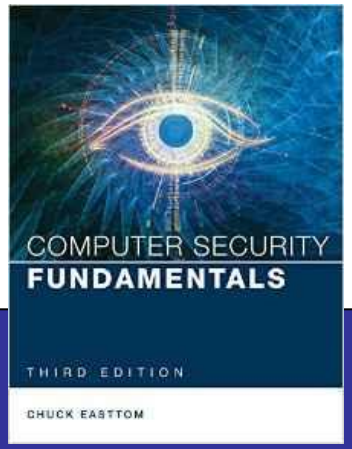
Computer Security Fundamentals

by Chuck Easttom



Chapter 7 Industrial Espionage in Cyberspace

Chapter 7 Objectives

- Know what is meant by industrial espionage
- Understand the low-technology methods used
- Understand how spyware is used
- Know how to protect a system

Introduction

- Espionage
  - Is NOT:
    - Sophisticated glamour
    - Exciting adventure
  - Its ultimate goal:
    - Collecting information
    - Without fanfare
    - Without knowledge of target

Introduction (cont.)

- Espionage
  - NOT done only by governments and terrorists
    - Spies for political and military goals
  - Also done by private companies
    - Industrial espionage.
    - Billions of dollars.
    - Companies fear to reveal they are targets.

What Is Industrial Espionage?

- Industrial Espionage
  - Spying to find out valuable information:
    - Competitor's projects, client list, research data
  - While the goal is different than military espionage, the means are the same:
    - Electronic monitoring, photocopying files

Information as an Asset

- Information can be a real asset.
- Billions are spent on research and development.
- How to value your information:
  - VI = C + VG

Information as an Asset (cont.)

- Information is as much an asset as anything else.
- Worth more than the hardware and software that houses it.
- Much more difficult to replace.

Information as an Asset (cont.)

- Data has value for two reasons:
  - Time and effort spent to create and analyze it.
  - Data often has intrinsic value.
    - A proprietary process, invention, or algorithm
    - A competitive edge

Information as an Asset (cont.)

- Asset identification
  - Listing the organization's assets
  - www.cert.org/archive/pdf/tutorial-workbook.pdf
    - Tutorial covering information security considerations

How Does Espionage Occur?

- Espionage can occur in two ways
  - Easy low-tech way
    - Employees simply take the data.
    - Social engineering.
  - Technology-oriented method
    - Spyware
      - Cookies and key loggers

How Does Espionage Occur? (cont.)

- Espionage can occur in two ways:
  - Easy low-tech way
    - Employees divulge sensitive data.
    - Disgruntled employees.
    - Motives vary.

How Does Espionage Occur? (cont.)

- Espionage can occur in two ways:
  - Easy low-tech way
    - Information is portable.
      - CDs, flash drives
    - Social engineering.
    - E-mail.

How Does Espionage Occur? (cont.)

- Espionage can occur in two ways
  - Technology-oriented method.
  - Any monitoring software can be used.
    - Spyware
    - Keystroke loggers
    - Capturing screenshots

Protecting Against Industrial Espionage

- Cannot make system totally secure
  - Employ antispyware software.
  - Use firewalls and intrusion-detection systems.
  - Implement security policies.
  - Encrypt all transmissions.
- Of no use against internal sabotage

Protecting Against Industrial Espionage (cont.)

- How to lessen risk of internal espionage
  - Give out data on a “need-to-know” basis.
  - Ensure no one person has control over all critical data at one time.
  - Limit portable storage media and cell phones.

Protecting Against Industrial Espionage (cont.)

- How to lessen risk of internal espionage:
  - No documents/media leave the building.
  - Do employee background checks.
  - Scan PCs of departing employees.
  - Lock up tape backups, documents, and other media.
  - Encrypt hard drives of portable computers.

Protecting Against Industrial Espionage (cont.)

- How to lessen risks of internal espionage
  - Encryption software
    - www.navastream.com
    - www.secure-messaging.com/products/cgfolder/index.htm
    - www.smart-cardsys.com/security/

Real-World Examples of Industrial Espionage

- Professor Hao Zhang
  - Stealing trade secrets from universities
  - Giving secrets to Chinese government

Real-World Examples of Industrial Espionage (cont.)

- Houston Astros
  - Team and scouting information
  - Allegedly stolen by competitor

Real-World Examples of Industrial Espionage (cont.)

- General Motors
  - GM alleges that eight former employees transferred proprietary information to Volkswagen.
  - GM sued in criminal court under RICO.
  - GM sued in civil court for damages.
  - Industrial espionage not restricted to technology companies.

Real-World Examples of Industrial Espionage (cont.)

- Interactive Television Technologies, Inc.
  - A break-in resulted in theft of data.
    - Years of research and substantial financial investment
  - Other companies shortly came out with competing products.

Real-World Examples of Industrial Espionage (cont.)

- Bloomberg, Inc.
  - BI provided services to a Kazakhstan. company; gave them software needed to use BI's services.
  - A KS employee, Oleg Zezev, illegally entered BI's computer system.
  - He sent an e-mail to Michael Bloomberg threatening extortion.

Real-World Examples of Industrial Espionage (cont.)

- Avant Software
  - Charged with attempting to steal secrets from a competitor.
  - A former consultant for Avant took a job with Cadence.
  - There were allegations on both sides.
  - The criminal case was pled out.

Industrial Espionage and You

- Most companies decline to discuss the issue.
- Larry Ellison, CEO of Oracle Corporation, has openly defended his hiring of a private detective to dumpster-dive at Microsoft.

Summary

- Industrial espionage exists and will grow into an even larger problem.
- There are a variety of methods by which espionage can take place.
- An employee revealing information is the most common.
- Compromising information systems is an increasingly popular method of espionage.