Introduction to Computer Security II

[redacted]

Model

[redacted]

Model

- Recall from last lecture:
    - Assets (what you want to protect)
    - Threats (what could damage your assets)
    - Security is about threats arising from intelligent, motivated attackers

Clarifications and Terminology

- Safety and security are about the prevention of adverse consequences
- Security is concerned with intentional threats against assets
  - Unwarranted from the point of view of the defender
  - The person carrying these out is the attacker

Schneier, Bruce. *Beyond Fear: Thinking Sensibly about Security in an Uncertain World*. New York: Copernicus, 2003.

Extending the Model

- Threats occur with different probabilities
- *Risk* takes into account the likelihood of a threat

risk = threats x probability

- *Countermeasures* we put in place to protect assets from threats

Risk

- Goal of a safety or security system is to reduce *risk*, not to reduce *threat*
- Reducing *threat* could lead us astray:
  - Focus too much on serious but unlikely threats
  - Focus too little on mild but very common threats

Risk Matrix

	Low Threat	High Threat
Low Probability	Low Risk	Medium Risk
High Probability	Medium Risk	High Risk

Risk Matrix

	Low Threat	High Threat
Low Probability	Lunch stolen from the fridge	Shark Attack[2] Murder by Stranger Plane Crash
High Probability	Common Cold[1] Minor Shoplifting Stubbing your Toe	Heart Disease Car Accident

[1] https://www.ncbi.nlm.nih.gov/pubmed/12227674

[2] Schneier, Bruce. *Beyond Fear: Thinking Sensibly about Security in an Uncertain World*. New York: Copernicus, 2003.

Countermeasures

- No countermeasure is perfect
- No countermeasure is free
  - Money
  - Time
  - Convenience
  - Social acceptability
  - Liberty

Trade-Offs

[redacted]

Trade-Offs

- Recall:
    - We care about mitigating risks (not threats)
    - No countermeasure is perfect
    - No countermeasure is free
- The trade-off is balancing:
    - Cost of countermeasures
    - Risk of not employing countermeasures

Trade-Offs

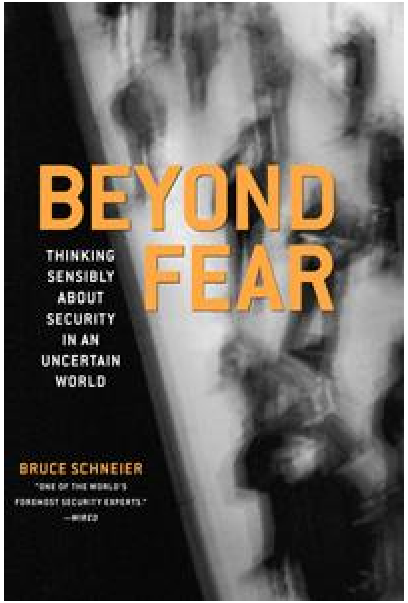
- We do this all the time
  - Clean the dishes
  - Lock your bike
  - Choosing between expiration dates
  - Others?

Trade-Offs: Consequences

- “Absolute security” never worth it
  - Want to stay perfectly safe? Never go outside.
  - Keep airplanes safe? Strip search every passenger.
- Sometimes less security is the better trade-off
  - Most shoplifting occurs in dressing rooms - get rid of the dressing rooms?
  - Hire extra guards at the movie theater to prevent a few people sneaking in?

Schneier, Bruce. *Beyond Fear: Thinking Sensibly about Security in an Uncertain World*. New York: Copernicus, 2003.

Book Recommendation


BEYOND FEAR
THINKING SENSIBLY ABOUT SECURITY IN AN UNCERTAIN WORLD
BRUCE SCHNEIER
"ONE OF THE WORLD'S FOREMOST SECURITY EXPERTS." —WIRED

To learn more about the fundamentals of security…

Beyond Fear:

Thinking Sensibly about Security in an Uncertain World by Bruce Schneier

Schneier, Bruce. *Beyond Fear: Thinking Sensibly about Security in an Uncertain World*. New York: Copernicus, 2003.

Computer Security

[redacted]

Computer Security

- Computer security is a subset of security
    - Same principles apply
- However, it’s useful to make simplifying assumptions (that we couldn’t make in the physical world)
- Such as?

Simplifying Assumptions

- Idealized behavior of systems
  - bug-free implementations
  - vulnerabilities “exist” or “do not exist”
  - tools can achieve perfect security
- Idealized attackers
  - can eavesdrop but not modify network traffic
  - can’t beat users with rubber hoses
- Idealized users
  - can remeber 200-character passwords

Reality

- These simplifying assumptions aren’t true...
    - Formal definitions ≠ reality
        - Reality doesn’t match the model; “perfect” security doesn’t actually exist
        - We can’t know whether a vulnerability has been fixed or not
        - Even if we pretend to strive for perfect security, we’ll never get there

Computer Security

- Consequence:
  - When deploying/designing/building a sufficiently large system, consider *risk* and *imperfect countermeasures*
  - When developing tools/working with cryptography/etc., pretend there's perfect security
- Rest of the course
  - start with the ideal world
  - end with the real world