Introduction to Computer Security II
Administrative Stuff

- **CS166** and **CS162** override request forms close at midnight tonight
  - We will make decisions this weekend
- **Introductory Survey** is out (due next Thursday)
- Homework 01 will be released today
- Questions?

Brown University CS166 © 2016 J. Liebow-Feeser, B. Palazzi, R. Tamassia, CC BY-SA 2.5
Model
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.

Extending the Model

- Threats occur with different probabilities
- *Risk* takes into account the likelihood of a threat
  \[
  \text{risk} = \text{threats} \times \text{probability}
  \]
- *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

<table>
<thead>
<tr>
<th>Low Probability</th>
<th>Low Threat</th>
<th>Low Risk</th>
<th>Medium Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>High Probability</td>
<td>Medium Risk</td>
<td>High Risk</td>
<td></td>
</tr>
</tbody>
</table>
## Risk Matrix

<table>
<thead>
<tr>
<th>Low Probability</th>
<th>Low Threat</th>
<th>High Threat</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lunch stolen from the fridge</td>
<td>Shark Attack² Murder by Stranger Plane Crash</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>High Probability</th>
<th>Low Threat</th>
<th>High Threat</th>
</tr>
</thead>
<tbody>
<tr>
<td>Common Cold¹ Minor Shoplifting Stubbing your Toe</td>
<td>Heart Disease Car Accident</td>
<td></td>
</tr>
</tbody>
</table>

Countermeasures

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

Book Recommendation

To learn more about the fundamentals of security…

Beyond Fear: Thinking Sensibly about Security in an Uncertain World by Bruce Schneier

Aviation Security
Aviation Safety and Security

- Major economic, social, and political importance of aviation
- Safety well understood and with strong record
  - Air travel is much safer than car travel ...
  - 100 times safer!
- Security less understood
  - Many improvement post 9/11
  - Still lacking in various dimensions
Aviation Assets

- Passengers, crews, and ground personnel
- Airport runways, buildings and facilities
- Planes
- Luggage and cargo
- Economic impact
- Social impact
Safety Measures

● Examples
  ○ Aircraft maintenance
  ○ Personnel training and rest
  ○ Airport facilities maintenance
  ○ Air traffic control (ATC)
  ○ Pilot-ATC communication protocol
  ○ Weather monitoring
Challenges to Securing Aviation

● Vast attack surface
  ○ Huge airport surface and facilities
  ○ Millions of passengers and employees
  ○ Massive cargo loads

● Tradeoffs
  ○ Cost vs. security benefit
  ○ Convenience vs. security
  ○ Reality vs. perception of security
Bad People and Things on Planes

● What normally goes into a plane
  ○ People: passengers, crew, ground personnel
  ○ Things:
    ■ luggage, packages, containers, ...
    ■ catered food and beverages
    ■ aircraft supplies
    ■ fuel

● Can we effectively screen all of the above?
Screening Passengers

● Current approach: three checkpoints
  ○ **Reservation**: check if passenger on no-fly list
  ○ **Entering airport**: check boarding pass and ID, screen passenger and carry-on luggage
  ○ **Boarding pane**: check boarding pass and, maybe, ID

● Some issues with current approach
  ○ Different checks at each checkpoint
  ○ Hasty check of ID

● Can one fly under someone else's name?

Source: tsa.gov
Screening Things

- Checked luggage: scanned
  - Various forbidden items
  - “3-1-1” liquids rule
- Carry-on luggage: scanned
  - Various forbidden items
- Cargo: “intelligence-based” scanning
- Is the “3-1-1” liquids rule effective?
Guarding the Airport Perimeter

- Physical access control to the airport
  - Long perimeter at major airports
  - Roads and buildings bordering the airport
  - Garages, hotels, businesses within or near airport
  - Walls, barbed wire, cameras, sensors, patrolling
  - How well guarded is the perimeter?

- Beyond the 2D perimeter
  - 3D surface?
Computer Security
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 remember 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