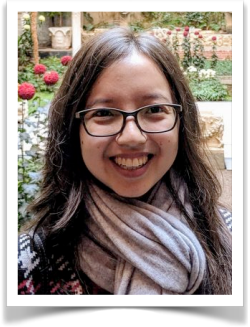
CSCI 331:
Introduction to Computer Security

Lecture 18: Physical security

Instructor: Dan Barowy

Williams

Announcements



- Friday's colloquium: **Su Lin Blodgett** (MSR Montreal) social implications of NLP tech.
- Final project presentations:
  Sat, Dec 18 1:30-3pm
  Sat, Dec 18 3:30-5pm

Topics

Social engineering

Physical security

Your to-dos

1. Reading response (Blaze), **due Wed 11/17**.
2. Lab 7, **due Sunday 11/21**.
3. Last two reading responses:
   a. Reading response (Thompson/Stoll), **due Wed 12/1**.
   b. Reading response (Provos), **due Wed 12/8**.

Social engineering attacks

Social Engineering

Social engineering, in the context of information security, is the **psychological manipulation of people** into **performing actions** or **divulging confidential information**.

- Cognitive biases
- Social/cultural pressures

Heuristics

Heuristics are simple strategies or mental processes that we use to **quickly form judgments**. Heuristic processes are **used to find solutions** that are approximately correct; however, **they are not foolproof**.

Attack: People do not think logically about risk. E.g., hackers reading your emails are far less likely (and possibly less consequential) than your spouse reading your emails.

Example

Linda is 31 years old, single, outspoken, and very bright. She majored in philosophy. As a student, she was deeply concerned with issues of discrimination and social justice, and also participated in anti-nuclear demonstrations.

Which is more probable?

1. Linda is a bank teller.
2. Linda is a bank teller and is active in the feminist movement.

Reciprocity

In cultural anthropology, **reciprocity** refers to the non-market exchange of goods or labor where **a return is eventually expected** as in the exchange of birthday gifts.

Attack: People can be tricked into giving away valuable things. E.g., romance scams, phishing.

Human Vulnerabilities

This list is not exhaustive!

- Cognitive bias
  - Heuristics
  - Consistency
- Social/cultural pressures
  - Conformity
  - Authority
  - Reciprocity

Physical security

"Government security requirements, in general, state: if a vulnerability or a security deficiency is believed to exist, it must be presumed to actually exist until it can be proven, beyond any reasonable doubt, that the vulnerability does not exist, or that a security violation could not possibly have occurred."

—The Inadvertest Adversary to Nuclear Security—Ourselves, Don D. Darling

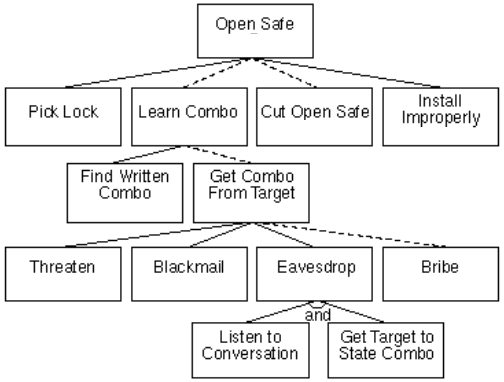
Physical security

Physical security describes analysis **processes** and **countermeasures**, both physical and psychological, whose aim is to deny unauthorized access to facilities, equipment, and resources, and **to protect personnel** and **property** from damage or harm.

Physical security

- Analysis tools
  - Risk-reward analysis
  - Analysis of attacker motivations
  - Checklists / knowledge of common vulnerabilities
  - Wargaming
- Impediments
  - Perception of risk
  - Obstacles to movement
  - Intrusion detection
  - Response

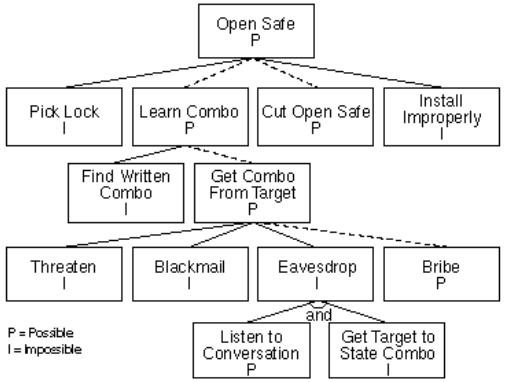
Attack trees



Attack Trees, Bruce Schneier, Dr. Dobb's Journal, December 1999.

https://www.schneier.com/academic/archives/1999/12/attack_trees.html

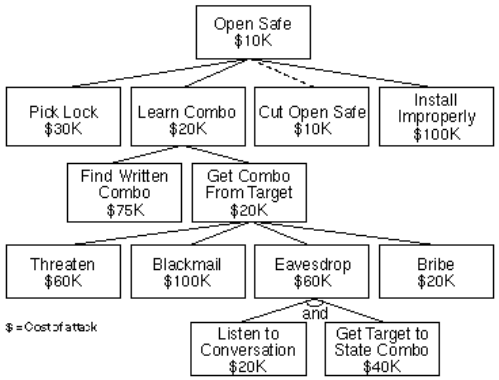
Attack trees



Attack Trees, Bruce Schneier, Dr. Dobb's Journal, December 1999.

https://www.schneier.com/academic/archives/1999/12/attack_trees.html

Attack trees



Attack Trees, Bruce Schneier, Dr. Dobb's Journal, December 1999.

https://www.schneier.com/academic/archives/1999/12/attack_trees.html

Analysis

ATTRIBUTES OF POTENTIAL ADVERSARIES TO U.S. NUCLEAR PROGRAMS[1]

Allan M. Fine

Sandia Laboratories, Albuquerque, NM 87115

Motivations

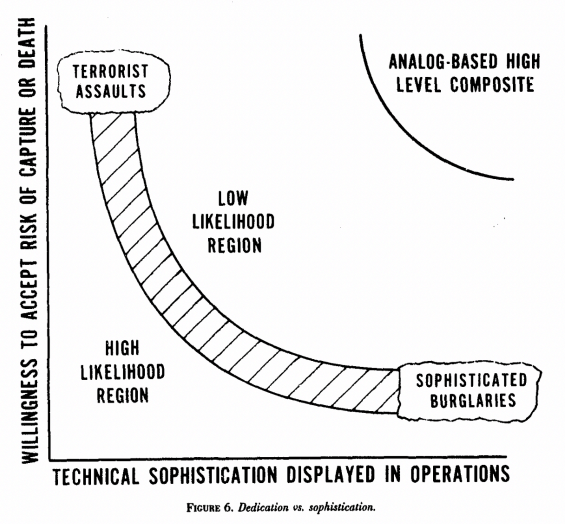
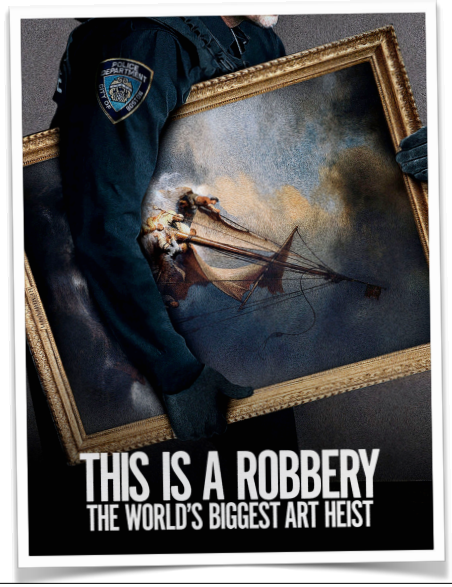


FIGURE 6. *Dedication vs. sophistication.*

Motivations



Motivations

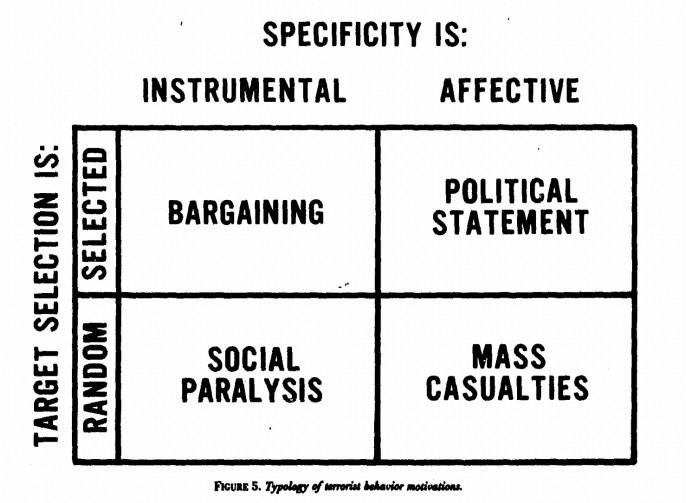
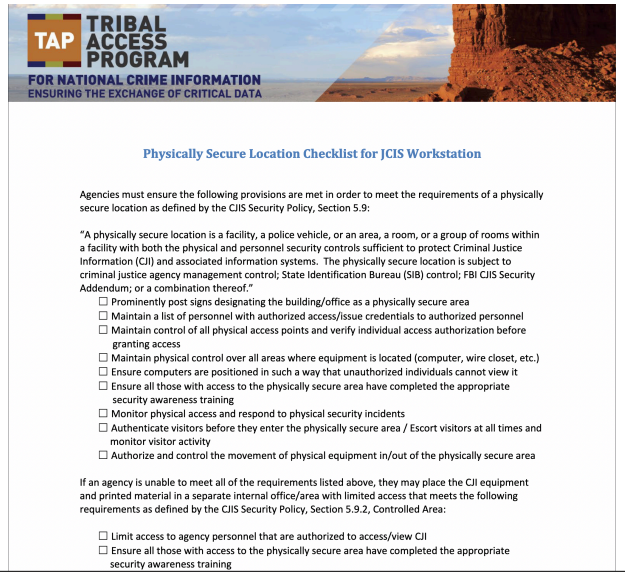


FIGURE 5. *Typology of terrorist behavior motivations.*

Checklists



Checklists

https://www.dm.usda.gov/physicalsecurity/physicalcheck.pdf

Wargaming

Red-teaming is a structured, iterative process executed by trained, educated and practiced team members that provides defenders with an independent capability to **continuously challenge plans**, operations, concepts, organizations and capabilities in the context of the operational environment and from **partner and adversarial perspectives**.

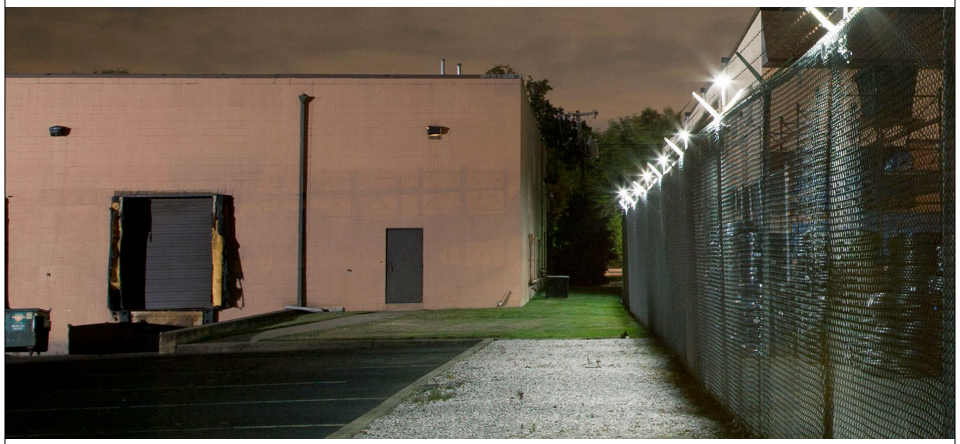
Perception of risk

Nike Missile Site HM-69 (now a part of the Everglades National Park)

Perception of risk

Perimeter warnings

Perception of risk



Security lighting

Perception of risk

(really scary) guards

Movement obstacles

Locking door

Movement obstacles

Gate

Movement obstacles

Retractable bollard

Movement obstacles

Jersey barrier

Movement obstacles

Man trap

Intrusion detection

Video surveillance (CCTV)

Intrusion detection

Alarm system

Intrusion detection (sensors)

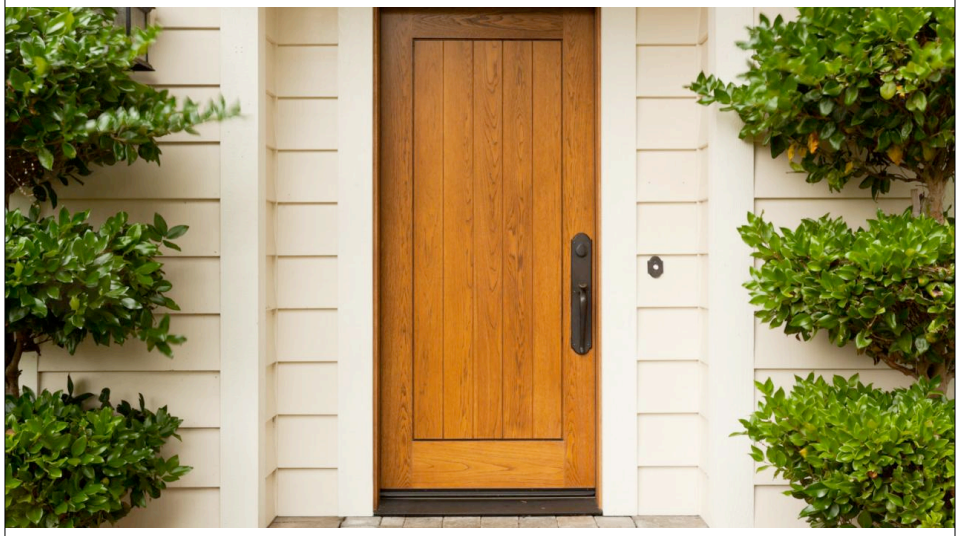
- Reed switch
- Motion detector (using EM, collimated beams, or sound)
- Glass-break/movement detector (accelerometer)

Response

Security responders (Univ. at Buffalo)

Common vulnerabilities

Doors



Mostly “secure” only on one side: the outside

Hinge vulnerability

More on combo attack: https://www.youtube.com/watch?v=mxgbY4wTES0

Recap & Next Class

Today we learned:

- Physical security basics
- Some common physical vulnerabilities

Next class:

- More common physical vulnerabilities
- Locks