Social Engineering

Humans: The Good and the Bad

All Security is About People

"Trusted people—people who must be trusted in order for the system to function—are part of any security system. They are a critical element, perhaps the critical element, because they're the most resilient part of the system, the most able to improvise, the best equipped to make on-the-spot decisions, and the most skilled at detecting the presence of attackers. But of course human beings, when considered as components of a security system, are a double-edged sword. They can fall asleep, get distracted, and be tricked. They can turn against a security system. **A good security system leverages the benefits of trusted people, while building counter-measures to prevent them from abusing that trust.**"

- Bruce Schneier, *Beyond Fear* (emphasis added)

Lecture Overview

- Core idea: humans are complex and less rigid than computers
- This can be either a good thing or a bad thing, depending on the circumstances

Human Security is Hard

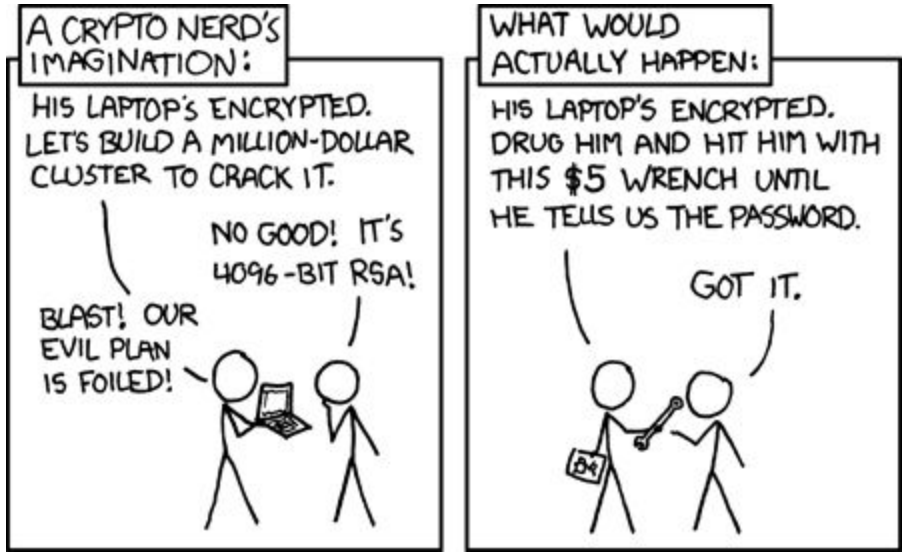
- Humans are tasked with making decisions...
  - That are subtler
  - That are more novel
- ...than those faced by computers
- Examples?

Human Security is Hard

- Humans are tasked with making decisions...
  - That are subtler
  - That are more novel
- ...than those faced by computers
- Examples
  - Should this person be let into the CIT?
  - Should I trust this person to sleep on my couch?
  - Should I trust this email claiming it's from my bank?

Part 1: The Bad

Why Target Humans?



Why Target Humans?

- Computer security is getting better
- Humans aren’t getting better
- Humans are often the weakest link

Psychology

- “Disease to Please”
- Social proof (reflect “correct” behavior)
- Greedy
- Trusting
- Easily pressured by time

Social Norms

- Social norms are ingrained
- People are very uncomfortable breaking them
- Examples?

Social Norms

- Social norms are ingrained
- People are very uncomfortable breaking them
- Examples
  - Cell phones
  - Door piggybacking

Deference to Authority

- People are deferential to authority
- It’s often easy to appear to have authority
- Examples?

Deference to Authority

- People are deferential to authority
- It's often easy to appear to have authority
- Examples
  - Just sound like you know what you're doing
  - Wear official uniforms (bank vault case)

Computers Obey Humans

- Computers obey humans
- Humans don’t understand computer security
- Example: DHS drops USB keys in parking lots
- 60% of people who picked them up plugged them into a computer
- 90% for drives with “official government logos”

Insider Threats

- If humans are trusted, they are a weak point
- They can be compromised
- They can also be malicious themselves
- Examples?

Insider Threats

- If humans are trusted, they are a weak point
- They can be compromised
- They can also be malicious themselves
- Examples
  - Edward Snowden

Video Time

https://www.youtube.com/watch?v=bjYhmX_OUQQ&feature=youtu.be&t=1m51s

Seriousness of Social Engineering

- “The Reason for the Growth in Spear Phishing: It Works” - FireEye report
- 91% of APT attacks start with spear phishing - Trend Micro report

Seriousness of Social Engineering

- Key Point: Many systems are built to keep *unauthorized* users out
- Fail in the face of malicious authorized users
  - Users compromised through phishing
  - Malicious insiders

Defense

- Lesson from the last decade…
- Education isn't enough
- Build systems resilient to insider threats
- Use the principle of least privilege

Part 2: The Good

Security Fails

- We try to design security to be perfect
- Despite this, it *will fail*
  - Fail open (ie, let an attacker in)
  - Fail closed (ie, keep out an authorized party)
- Question: How do you cope with that failure?
- Examples?

Security Fails

- Examples
  - Fail open
    - Metal detectors
    - Power out, security cameras turn off, doors open
  - Fail closed
    - I forgot my password
    - I forgot my key

Security Fails

- Systems can be *brittle* or *resilient*
- Brittle - a small failure can be very bad
- Resilient - a small failure can be coped with
- Examples?

Security Fails

- Systems can be *brittle* or *resilient*
- Brittle - a small failure can be very bad
- Resilient - a small failure can be coped with
- Examples
  - Brittle - Airport security after 9/11
  - Resilient - Credit card security
  - Brittle - Biometric authentication
  - Resilient - A guard desk in the lobby

People are Resilient

- Ahmed Ressam and Diana Dean
- Other examples?

People are Resilient

- Ahmed Ressam and Diana Dean
- Other examples
  - I forgot my CS department password
  - We've been hacked!
  - Natural disasters