Computer Security: Problem

- The Problem: Billions in Losses
  - Outright theft
  - Online scams
  - Viruses / Worms
    - Actual damage
    - Actions to avoid damage
  - Denial of Service
  - Etc.
- Possible Traps (Public System)
  - Trojan Horse
  - Onlooker
  - Cameras

Computer Security: Defenses

- Passwords
  - Using Secure Passwords
  - Keeping them Secure
- Encryption
  - Simple (Classical Encryption – Pre-Computer)
  - Strong (Modern – Computer Based)
- Good Practices
  - Like all fields, doing something stupid ...
- Tradeoffs
  - Is the cure worse than the disease?
- Long Live Common Sense!

Good Passwords and Cracking

- Briefcase (style) Combination Locks
  - Brute force methods: Try all combinations
    1. Number of wheels
    2. Number of position per wheel
    3. Time per trial
    4. How long does it take?
- Contrast to BRUTE brute force method (Always Consider!)
- Password on a computer
  - More possibilities per “wheel”
  - More “wheels” (often up to user)
  - Computer based cracking faster!
  - Dictionary attacks
- Picking a good UNIX password

Classical Encryption

- When passwords fail, encryption can be fallback
  - Also provides extra level of difficulty
- Security vs. Privacy
- Many levels of encryption sophistication:
  - Go through some of them
- Single Alphabetic Substitution
  - Caesar: LFDPH, LVDJ, LFQTXHUHG
  - Magic decoder ring?
  - Cryptoquote
- Cracking single alphabetic substitution
  - Character frequency -- ETAONIRSH
  - (Length of text)
Classical Encryption: Single Alphabet

Classical Encryption

Polyalphabetic Substitution
- The Vignere Cypher
- The Babbit Solution
  - How many alphabets used?
  - Digraph frequency “th”
  - Several Single-Alphabet problems
- Cypher Reuse!
  - Bigger pool of data
  - Patterns become obvious
- One Time Pads
  - Can be Absolutely Secure
  - Computers and Random Number Generators ?!

The Key Exchange Problem
- Threats
- Using your “secure” channel
- A padlock analogy
- Diffie, Hellman, and Merkle solution