Prolog to Lecture 4
CS 236
On-Line MS Program
Networks and Systems Security
Peter Reiher

Brute Force Attacks, the iPhone, and the FBI

- Recently lots of news about the FBI needing to crack an iPhone
- It was used by dead terrorists
- The FBI wanted to examine it
- But it was locked
- The FBI wanted to crack it
- Using brute force

What Does That Mean?

- Brute force attacks are trying every possible key
- Almost (not quite) what the FBI wanted to do
- The iPhone’s data was encrypted by AES
- Using a key based (in part) on a password

The Desired Brute Force Attack

- The FBI wanted to:
  - Keep guessing passwords till it found the right one
  - As quickly as possible
  - Despite iPhone features to prevent that

So What Was Stopping Them?

1. Passwords could only be entered via the keyboard
2. After each incorrect guess, the iPhone injected delay before accepting another guess
3. After some number of consecutive wrong guess, it locked up
   - Permanently, “destroying” the data

What Did the FBI Want?

- A new version of the OS that:
  1. Allowed guess to be sent over a wire
  2. Didn’t inject delays after wrong guesses
  3. Never locked up after too many wrong guesses

Why Couldn't the FBI Do It Themselves?

- Because of other iPhone security features
- Essentially related to *digital signatures*
- Which we'll talk about in more detail in today's lecture
- Also issues related to hardware security
  - Which we'll get to when we talk about OS security

How Did They Do It?

- Well, the FBI didn’t do it themselves
- Whoever did it isn’t talking
  - About who they are
  - Or what they did
- We’ll discuss some possibilities in later classes