Prolog to Lecture 8
CS 236
On-Line MS Program
Networks and Systems Security
Peter Reiher

Smart Cards in Trouble

- Smart cards are used for authentication
- But they're also used for other things
  - Like electronic cash
  - Or public transit payments
- These uses are problematic
- Why?

A Problem With Smart Cards

- Smart cards are in the physical possession of users
- If it’s in the user’s interest to alter the smart card’s behavior, he might
  - E.g., free rides on the subway
- Preventing this is one of the hard problems in security

What’s the Real Problem?

- Ultimately, the smart card’s security is based on keeping a secret
- But the secret is on the card
- And the card is in the user’s wallet
- How do you keep the secret from the user?
- Similar problem to DRM technologies

An Example of the Problem

- The Mifare card
- Used by Netherlands, Britain, Boston for public transport
- Reverse engineering of the card uncovered the crypto algorithm
- Weaknesses in that algorithm allow attackers to guess the key
  - They can then clone the card

Effect of the Attack

- Attackers can create cards that were never paid for
  - So you ride the Tube or the MTA for free
- Same cards can also be used for building access
  - Cloning allows you to pretend to be someone else

What the Attack Does and Doesn’t Mean

- These cards are too weak for public transit systems
- But if attacker can’t get hold of your card, he can’t clone it
  - So maybe OK for authenticating you
  - Unless other mechanism gives attacker access to your card