

Something You Know: Passwords

- The first general method Bob can use to authenticate Alice is to ask her for some **secret only she should know**, such as her secret password.
- If Alice produces the right password, then Bob can assume he is communicating with Alice.
- Passwords are so prevalently used that we will further study how to properly build a password management system.

Something You Know: Passwords

- There are advantages and disadvantages to using passwords.
- One advantage is that password schemes are simple to implement compared to other authentication mechanisms, such as **biometrics**, which we will discuss later.
- Another advantage of password security systems is that they are **simple for users** to understand.

Something You Know: Passwords

- There are, however, disadvantages to using password security systems.
- First, most users do not choose strong passwords, which are hard for attackers to guess.
- Users usually choose passwords that are simple concatenations of
 - common names,
 - common dictionary words,
 - common street names, or
 - other easy-to-guess terms or phrases.

How Hackers Crack Your Passwords

- They don't go to the applications and try various combo of your passwords!
- They will commonly sniff & extract the "password hash" over the internet as you log in.
 - Normally systems uses common standard hash function
- They will write or use a password cracking program with dictionary of common passwords. They will crack Offline!
- They store password hashes in dictionaries.
- If your password hash appear in the dictionary, you are toast!

Something You Know: Passwords

- Attackers interested in hacking into somebody's account can use **password-cracking programs** to try many common login names and concatenations of common words as passwords.
- Such password cracking programs can easily determine 10 to 20 percent of the usernames and passwords in a system.
- Of course, to **gain access to a system**, an **attacker typically needs only one valid username and password**.
- **Passwords are relatively easy to crack**, **unless** users are somehow **forced to choose passwords** that are **hard for such password-cracking programs** to guess.