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.

Something You Know: Passwords

- A second disadvantage of password security systems is that a user needs to reuse a password each time she logs into a system—that gives an attacker numerous opportunities to "listen in".
  - IMAGINE ONE FINE DAY A KEYLOGGER WAS INSTALLED INTO YOUR PC….

- If the attacker can successfully "listen in" on a password just once, the attacker can then log in as YOU UNTIL U NEXT CHANGE YOUR PASSWORD!

Something You Know: Passwords

- A one-time password (OTP) system, which forces the user to enter a new password each time she logs in, eliminates the risks of using a password multiple times.
- This basic idea to implement this naturally leads us from the topic of "something you know" to the topic of "something you have."
- OTP is sent to your bank token in the past when u try to access your bank account.
- Now banks send OTP your handphone.
- Don't lose your handphone!

Something You Have

Something You Have:

- A second general method of authenticating a user is based on something that the user has.
  - OTP Cards (one-time password)
  - Smart Cards
  - ATM Cards

Something You Have: OTP Cards

- OTP products generate a new password each time a user log in.
- One such product, by RSA Security, is the SecurID card
- The SecurID card is a device that flashes a new password to the user periodically (every 60 seconds or so).
- When the user wants to log into a computer system, he enters the number displayed on the card when prompted by the server.

Something You Have: OTP Cards

- Server knows the algorithm that the SecurID card uses to generate passwords, and can verify the password that the user enters.
- Other variations of OTP systems as well:
- For instance, some OTP systems generate passwords for their users only when a personal identification number (PIN) is entered.
- Also, while OTP systems traditionally required users to carry additional devices, they are sometimes now integrated into personal digital assistants (PDAs) and cell phones.