More Authentication

General Attacks on Protocols continued

Attack the System
find a weakness in another part of system
exploit that to bypass auth and/or to steal
the user database
caused by bugs in programs
better programming minimizes these
Buffer Overflow is a classic example
program has a variable to store data the
user has typed
variable can only store \( x \) characters
overflow happen when program doesn't check
if user has typed \( \leq x \) chars

\[ x \text{ chars} \]

overflow
not exploit
exploit

C++ Example

```cpp
int main() {
    char input[16];

    cin >> input;    // bad - no boundaries

    cin >> setw(15) >> input;    // good - boundary
}
```

"Live" scan/attack against Password Logins
Attacker doesn't want a specific account, just
wants in to any account
Use a list of really common passwords
Try list against a range of usernames

Best Practices for Passwords
Always gauge your risk tolerance for live scans vs. user
database compromises (GPU cracking of hashes)
Universal Best Practice (from Tuesday):
Use a different password for each site
Guard against Live Scans:
1) Don’t use a dictionary word, particularly one of the common passwords or one related to personal info or website
2) Do use mix of upper case, lower case, numbers & symbols for password (if allowed by site)
3) 8-10 chars should be okay for live scans (would fall quickly for GPU cracking)

Guard against GPU cracking
1) Don’t use dictionary words OR phrases directly
2) Same as above, use mix of upper, lower, numbers & symbols as allowed by website
3) Long passwords are best
4) Change passwords periodically

“Best Pratice” that Aren’t Best Practices
1) Forcing users to change passwords when logging in
   Better: talk to the user if they haven’t changed passwords recently
2) Completely locking out account when too many bad passwords given
   Better ways:
   Block the address(es) that failed, but not others
   Use a captche or other mechanism that blocks bots from trying to log in

System Admins & Managing User Passwords
Sys admins are responsible for the security & well-being of the servers & networks
Want users to use good passwords to help w/ this
Avoid “bad” passwords (easy to guess or crack)
Dictionary words
Personally related to user (family/pet names, dates, etc)
Passwords that match cracking profiles:
≤4 chars
  - lower case
  - lower case + numbers
  - also upper case & mixed numbers
  - charset space for each:
    - lower or upper: 26
    - numbers: 10
    - lower (or upper) + numbers: 36
    - mixed (lower & upper): 52
    - mixed + numbers: 62
    - mixed + num + symbols: 96

8 char password at 2.5 billion guesses/sec
  - lower or upper: $26^8/2.5$ billion, 84 seconds
  - numbers: $10^8/2.5$ billion, 1 second
  - lower (or upper) + num: $36^8/2.5$ billion, 19 minutes
  - mixed: $52^8/2.5$ billion, 6 hours
  - mixed + num: $62^8/2.5$ billion, 24 hours
  - mixed + num + symbol: $96^8/2.5$ billion, 1 month

Want users to choose passwords that resist dictionary attacks & also make brute force attacks take longer.

How to "Make" Users Do This?
  - Educate users about how to make more complex passwords
  - Dice words + numbers & symbols
    - Correct S3 horse # battery [4 staple]
    - Correct S3 horse # battery [4 staple]
  - Pronounceable passwords
  - Algorithms to create passwords
  - Check password database for "bad" passwords
  - Check passwords as they are chosen
  - Suspend accounts of chronic offenders