Password Management

- Limit login attempts
- Encrypt your passwords
- Protecting the password file
- Forgotten passwords
- Generating new passwords
- Password transport

Limit Login Attempts

- Don’t allow dictionary attacks “over the wire”
- After some reasonable number of failed login attempts, do something
  - Lock account
  - Slow down
    - iPhone does this, Android doesn’t
  - Watch more closely

Encrypt Your Passwords

- Using the techniques we just covered
- One would think this advice isn't necessary, but . . .
  - Yahoo lost half a million unencrypted passwords in 2012
- Encryption is more expensive and less convenient
  - But a lot more secure

Protecting the Password File

- So it’s OK to leave the encrypted version of the password file around?
- No, it isn’t
- Why make it easy for attackers?
- Dictionary attacks on single accounts still work
- And there are “popular” passwords, leading to easy dictionary attacks even with encryption
- Generally, don’t give access to the encrypted file, either

Other Issues for Proper Handling of Users' Passwords

- Sites should store unencrypted passwords as briefly as possible
  - Partly issue of how they store the file
  - Partly issue of good programming
- Don't leave passwords in temp files or elsewhere
- Should not be possible to print or save someone's unencrypted password
- Use encrypted network transport for passwords
- If your server is compromised, all of this might not help

Wireless Networks and Passwords

- Wireless networks are often unencrypted
- Web sites used to request and transport passwords in the clear
- So eavesdroppers could hear passwords being transported
- Important to encrypt these messages

Handling Forgotten Passwords

- Users frequently forget passwords
- How should your site deal with it?
- Bad idea:
  - Store plaintext passwords and send them on request
- Better idea:
  - Generate new passwords when old ones forgotten
- Example of common security theme:
  - Security often at odds with usability

Generating New Passwords

- Easy enough to generate a random one
- But you need to get it to the user
- If attacker intercepts it, authentication security compromised
- How do you get it to the user?

Transporting New Passwords

- Engineering solution is usually to send it in email
  - To an address the user registered with you earlier
- Often fine for practical purposes
- But there are very serious vulnerabilities
  - E.g., unencrypted wireless networks
- If you really care, use something else
  - E.g., surface mail

User Issues With Passwords

- Password proliferation
- Choosing passwords
- Password lifespan

Password Proliferation

- Practically every web site you visit wants you to enter a password
- Should you use the same password for all of them?
- Or a different password for each?

Using the Same Password

+ Easier to remember
- Much less secure
  - One password guesser gets all your authentication info
  - Do you trust all the sites you visit equally?
  - Compromise in one place compromises you everywhere
  - Real attacks are based on this vulnerability

Using Different Passwords

+ Much more secure
- But how many passwords can you actually remember?
- And you might “solve” this problem by choosing crummy passwords

Other Options

- Use a few passwords
  - Maybe classified by type of site or degree of trust
- Write down your passwords
  - Several disadvantages
  - Could write down hints, instead
- Use algorithm customized to sites
- Password vaults

Choosing Passwords

- Typically a compromise between:
  - Sufficient security
  - Remembering it
- Major issues:
  - Length
  - Complexity

How Long Should Passwords Be?

- Generally a function of how easy it is for attackers to attack them
- Changes as speed of processors increase
- Nowadays, 15 character password are pretty safe
  - If they aren't guessable . . .
- Old sites may demand shorter ones

Some Password Choice Strategies

- Use first letters from a phrase you remember
- Use several randomly chosen words
- Replace letters with numbers and symbols
  - Helps, but less if you use common replacements (e.g., “0” for “o”)
  - Also less useful if you limit it to 1st and last character of password

Password Lifespan

- How long should you use a given password?
- Ideally, change it frequently
- Practically, will you remember the new one?
- Is a good, old password worse than a bad, new one?
  - Many issues of crypto key reuse are relevant here