50.042 FCS Summer 2024 Lecture 6 – Authentication Schemes and Passwords

Felix LOH
Singapore University of Technology and Design

Terminology

- Access control:
  - Allow or deny access to resources
  - Delegation may be possible
- Identification:
  - Provision of an identity
  - Identification itself does not include verification
- Authentication:
  - General meaning of ‘authentication’: verification of correctness of data and source
  - In this context, ‘authentication’ means verifying the *identity* of the login request

Identification schemes

- Identification schemes only require the provision of an identity
  - No direct security requirements
  - The identity/identifier should **not** be secret
- Common identification schemes:
  - Email addresses
  - Usernames
  - Phone numbers
  - National ID number
  - Facial recognition

Authentication schemes

- Knowledge-based authentication
  - Passwords
  - Patterns (e.g Android phone unlock screen)
  - Banking PINs
- Token-based authentication
  - Physical keys
  - Cryptographic token devices (e.g. those issued by banks)
  - Certificate-based (e.g. TPM)
- Biometric-based authentication
  - Fingerprint and/or retina scanning
  - Voiceprint
- Multi-factor authentication (MFA)

Password-based authentication

- Passwords are the most common method of authenticating users
- Advantages:
  - Passwords can be changed easily
  - The user has the freedom to choose their own password
- Disadvantages:
  - Passwords can be easily forgotten
  - Password reuse across different services
  - It’s possible for the user to create a weak password

Guessing of passwords

- Guessing passwords is can be easier than one might think, because:
  - Passwords are typically restricted to a limited set of characters
  - Passwords can be somewhat short
  - Some passwords are very frequently used
- This enables “semi-intelligent” brute-force attacks:
  - Use dictionaries or rainbow tables
  - Hybrid attacks

Dictionary attacks

- Typically, users prefer simple passwords
- There are dictionaries that list popular passwords, ranked by popularity, along with their corresponding hashes (for different hash functions)
- Using a dictionary increases the likelihood of successfully cracking a password
- These dictionaries are often based on leaks or theft of password databases from servers (data breaches)

Rank	Password
1	123456
2	password
3	12345678
4	qwerty
5	abc123
6	123456789
7	111111
8	1234567
9	iloveyou
10	adob123

Popular passwords in 2013 (SplashData)

Hybrid attacks

- Many users are now aware of dictionary attacks
- Some of these users might modify their existing passwords to be more difficult to guess
  - E.g. “password” → “p@ssw0Rd”
  - But still quite similar
- Hybrid attacks involve trying combinations and substitutions of the characters/words in popular passwords
  - E.g. try different replacements of the characters in “password”, like “a”→ “@” and “o” → “0” and changing of upper case to lower case and vice versa
  - Password cracking programs, like John the Ripper and Crunch, can perform “word-mangling” operations to try different replacements and even add characters to existing popular passwords

Finding passwords in practice

- Existing dictionaries and word mangling techniques can be used to build long lists of likely passwords
- May be possible to break into a system using an API that can submit unlimited password attempts
  - But in practice, most systems limit the number of password attempts to prevent such an occurrence

Finding passwords in practice

- In many cases, dictionary and hybrid attacks are used to attempt to find preimages of password hashes
  - These password hashes were stolen in a previous attack
  - The attacker has unlimited attempts to find a preimage for each hash
- A helpful website for checking whether your account may have been compromised:

`https://haveibeenpwned.com`

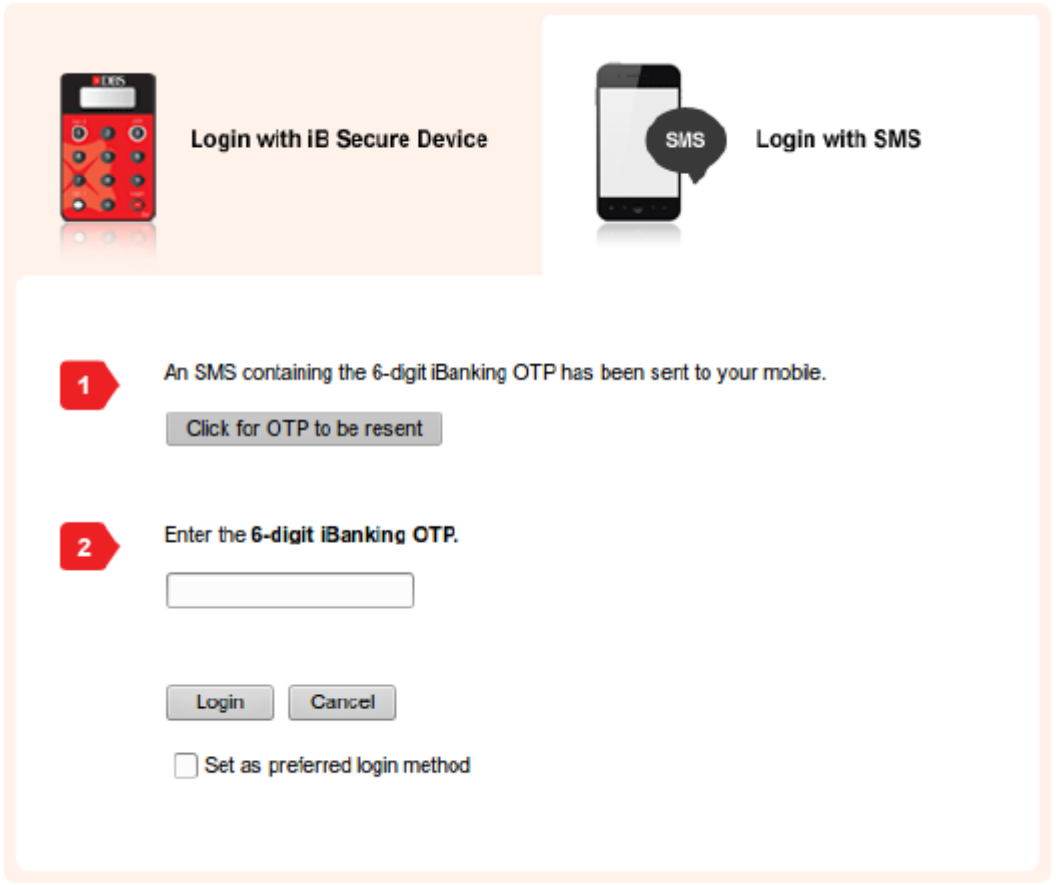
Improving authentication schemes

- Systems can utilize multi-factor authentication (MFA)
  - This is an application of *defence in depth*
  - Comes at a cost to convenience
- Simple and most common form: two-factor authentication (2FA)
- The two factors are chosen from two out of three different categories:
  - Something you know (e.g. passwords, PINs)
  - Something you are (e.g. fingerprint, iris scans)
  - Something you have (e.g. token, RFID card)

- E.g. DBS Internet Banking login procedure

Improving authentication schemes

- E.g. DBS Internet Banking login procedure



Login with first factor
(something you know)

Further authentication with second factor
(something you have)

Passwords: best practices

- Do not reuse the same password across different services
- Change your passwords periodically (but not too often!)
- Do not base your passwords on words in the dictionary
  - Use a dialect or made-up words or a mnemonic
- Use passwords made from random characters
- Utilize a password manager

Detecting system compromise

- If you are a system administrator, it is good to be able to detect whether some attacker is trying to break into your system
- Can create accounts for dummy users with corresponding passwords
  - These fake accounts are isolated from the actual system
  - Trigger an alert if these users attempt to log in
  - Trigger a major alert if such a user logs in with the correct password

- This is basically a honeypot or decoy
  - Lures attackers away from your actual digital assets
  - Can also monitor their behavior in the system