10 - Challenge questions and secondary authentication

Shing-hon Lau

February 13th, 2014

05-436/05-836/08-534/08-734
Usable Privacy and Security

Today!

- Terminology
- Warmup: what are some secondary authentication methods?
- What desirable properties should secondary authentication have?
- Case study: Attackers exploiting secondary authentication
- Group exercise: create a secondary authentication method
- “It’s no secret” paper

Terminology

- Two types of secondary authentication:
  - Two- (or multi-) factor authentication where secondary authentication is used in conjunction with primary authentication
  - Account reset where secondary authentication is used when the primary authentication is lost/forgotten/invalidated

Secondary authentication methods

- Answer challenge questions (both)
- E-mail with key/link (both)
- SMS with key/link (both)
- Smartphone (both)
- Provide old passwords (reset)
- Trusted 3rd party verification (reset)
- Printed secrets or code book (two-factor)
- USB dongle (two-factor)
- Identify your friends in photos (both)
- Biometrics (voice, fingerprint, palm, iris, keystrokes, mouse, pressure) (two-factor)

Desired properties

- Widely (universally) applicable
- Easy to use
- Easy to remember
- Should be consistent over time
- Hard to guess (large search space)
- Hard to research answers
- More secure than primary authentication (for account reset)
- Should not take too long
- Can be revoked

Revocation: Case study

- Blizzard authenticator
- Time-synchronous token
- When logging in, you press the button on the authenticator and enter the generated number
- The server was synchronized with the token when it was created, so it can confirm if the number is correct

Revocation: Case study

- Why do people pay for this authenticator?
- Game accounts (particularly World of Warcraft) can be worth hundreds to thousands of US dollars
- Many, many vanity-related items that are purchased with USD, limited-time only, or require high skill/luck to obtain
- Strong incentive to steal accounts and then sell them to others OR steal in-game currency to sell to others

Revocation: Case study

- So what’s the problem?
- Thieves steal accounts and then add their own authenticator!
- More time to sell the account or to use the account to obtain more gold via social engineering
- Removing an authenticator currently requires sending in a copy of your government-issued ID
- Several days of delay, assuming you have an ID available

Revocation: Case study

- How can you preserve the effectiveness of secondary authentication without allowing an attacker to use the authentication against you?

Group exercise

- Design a secondary authentication mechanism
  - Could be some good challenge questions
  - Could be an entirely different method
- Keep in mind:
  - Who will be using this?
  - What are the most important attributes for your mechanism?

“It’s no secret” paper

- What recruitment method was used for this study?
- Do you think this method would introduce bias into the study?
- What other method(s) would you have used to recruit subjects for a study like this?