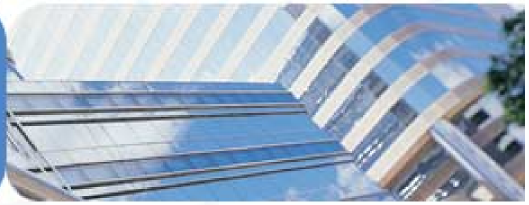
SECURITY PS

STRATEGIC INFORMATION SECURITY

Avoiding Poor Challenge Question Authentication

Bruce K. Marshall, CISSP
Senior Security Consultant
bmarshall@securityps.com

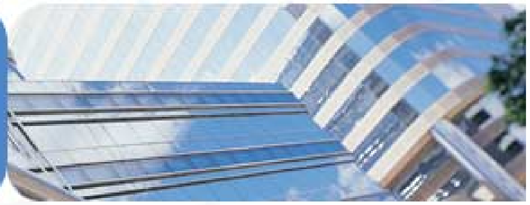
Intro to Challenge Question Authentication



- What are challenge questions?
  - Authentication challenges that attempt to verify a person’s identity by asking them one or more personal questions.
  - Example: *What is your mother’s maiden name?*

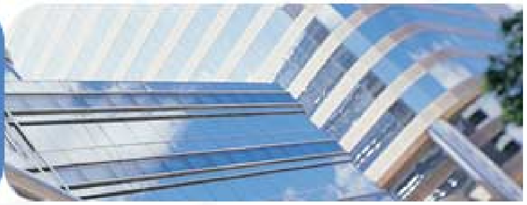
- Why are challenge questions becoming more popular?
  - FFIEC guidance to financial institutions on strengthening online application authentication
  - Growing overall Internet fraud

Challenge Question User Enrollment



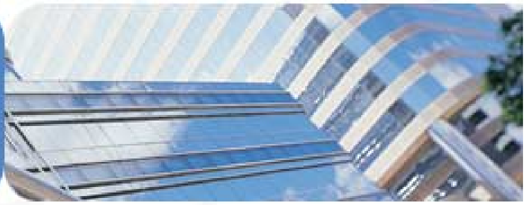
- How users enroll for challenge questions
  - Answer a series of pre-defined questions
  - Create and answer a series of questions
  - Do nothing – challenge questions gathered from private information databases
- How many challenge questions to ask during enrollment
  - Usually 6-8 if asking 3-4 questions during authentication
  - At least 3

Challenge Question Implementation



- How challenge questions are implemented
  - Either asked during every authentication or only when certain situations occur (e.g. RBA)
  - Users are prompted to
    - Answer by filling in the blank
    - Answer by selecting one of multiple choices
  - The number of questions asked typically range from 1 – 4
  - Questions should be randomly pulled from the pool created during enrollment

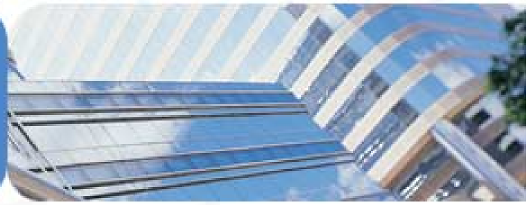
Creating Appropriate Challenge Questions



- Five characteristics of authenticators
  - Usability
  - Uniqueness
  - Integrity
  - Affordability
  - Accuracy

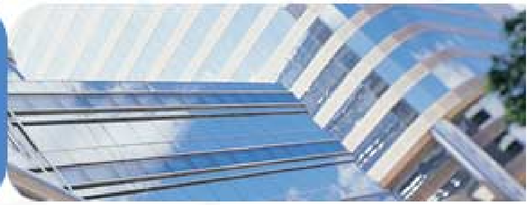
Every challenge question should be evaluated for these characteristics prior to their use.

Challenge Question Usability



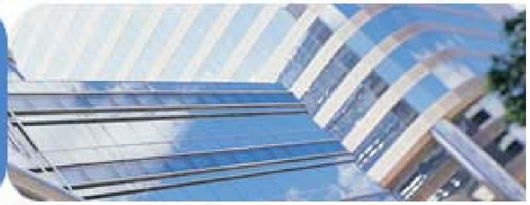
- Usability
  - How effectively people can utilize a challenge question to successfully authenticate
- Advantages
  - Based on personal information, so should be easier to remember
  - Require little training to use
- Disadvantages
  - Question may not be answerable by all users
  - May raise privacy concerns

Challenge Question Uniqueness



- Uniqueness
  - The distinctness of proof used to confirm an identity
- Advantages
  - Question asked directly affects uniqueness
  - A specific type of answer is expected
- Disadvantages
  - Some answers will be more popular than others
  - Can only place limited controls on answers

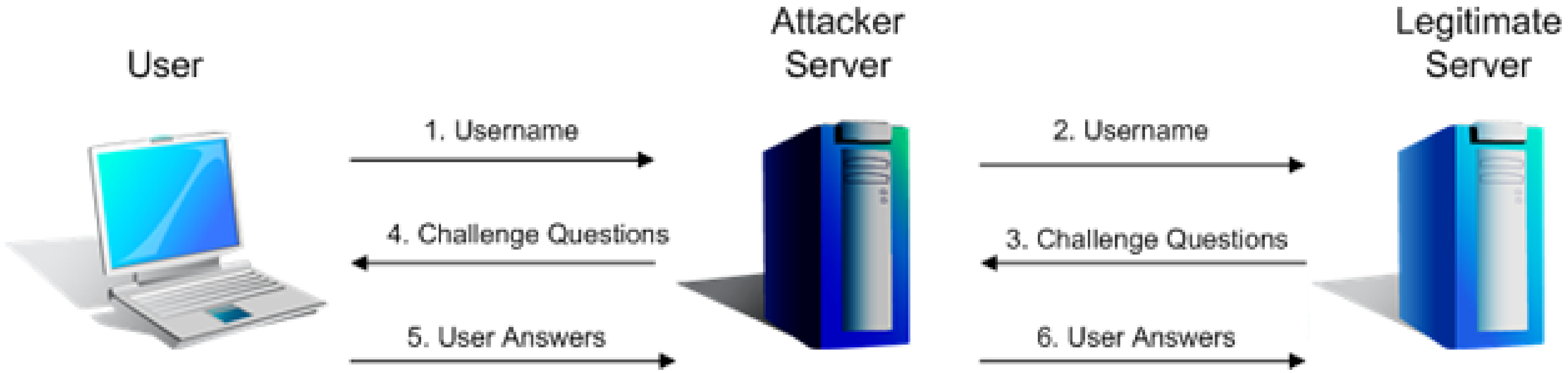
Challenge Question Integrity



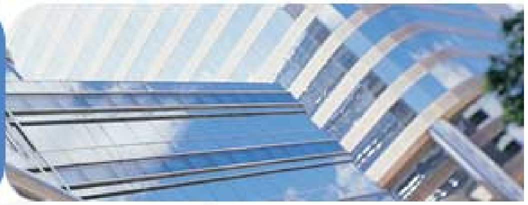
- Integrity
  - How well the authenticator resists duplication attempts over time
- Advantages
  - N/A
- Disadvantages
  - Some types of personal information are regularly shared with others
  - Users don’t know who knows this info
  - Certain answers may be valid forever

Challenge Question MITM Attack

- Man-in-the-middle attack

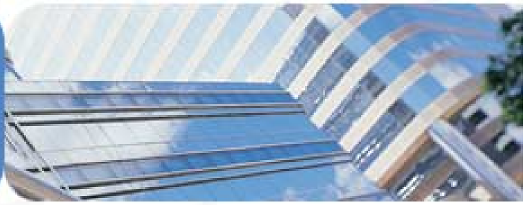


Challenge Question Affordability



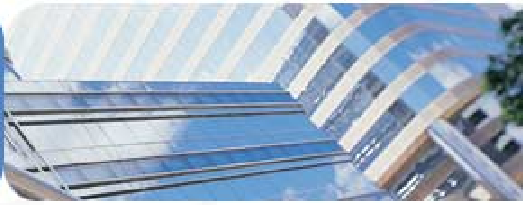
- Affordability
  - The cost to buy and maintain
- Advantages
  - Implementation costs are cheap
- Disadvantages
  - Support costs may be similar to passwords

Challenge Question Accuracy



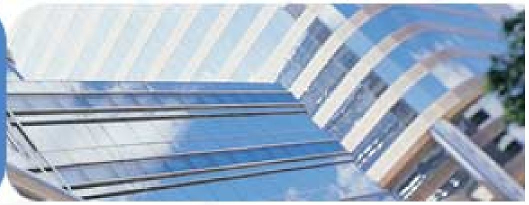
- Accuracy
  - The frequency of authentication mistakes that limit use by legitimate users
- Advantages
  - Asking for personal information tends to be more memorable
- Disadvantages
  - Users will sometimes forget answers
  - The application expects the exact same answer every time

Evaluating Sample Questions



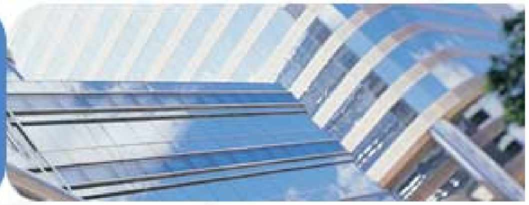
- Evaluate the five characteristics of the following challenge questions:
  - “How many pets do you have?”
  - “What is the location of your dream holiday?”
  - “Who is your favorite actor?”
  - “What do you enjoy doing the most?”

Presentation Summary



- In summary
  - Challenge questions offer an affordable and usable alternative to multi-factor authentication
  - They also include some serious uniqueness and integrity disadvantages
  - Should only be used, in groups, to supplement stronger authenticators

Challenge Question Resources



- Challenge question resources
  - blog.securityps.com
  - blog.passwordresearch.com
  - securityps.infosecmedia.com/whitepapers/TipsforAvoidingBadQuestions.pdf
  - www.owasp.org/index.php/Using_Secret_Questions

Questions?