Core Characteristics for Evaluating Authenticators

By Bruce K. Marshall, CISSP
bkmarshall@passwordresearch.com

Date: August 12, 2004 *Revision:* v1.11

"Your secrets are your business, but your password is ours."

Introduction

When looking at the basic authentication system model, we see that a system is separated into four main components: the authenticator, the input, the transport, and the verification. While all four parts must work together effectively for secure authentication, the authenticator component deserves special attention.

Authenticators are the proof offered by an individual to confirm his or her identity. This can be secret knowledge, a physical object, or other unique feature. Authenticators are also called *authentication factors*.

Authenticator Categories

We commonly sort authenticators into three general categories based on their relationship to a person:

- *What you know* – knowledge-based authenticators
- *What you have* – possession-based authenticators
- *What you are* – biometric-based authenticators

These authentication factors provide a wide variety of technologies and products from which to choose. Like any technology, authenticators have characteristics that make them more or less suitable for use in our organizations. Unfortunately, making the right authenticator choice is difficult without a standardized set of characteristics that can be used to judge our options.

While some in the security industry have sought to establish guidelines for authenticator use, these recommendations are usually limited by their lack of detail. Because this advice deals in generalities it may not be appropriate for your business environment. The one-solution-fits-all approach isn't the preferable way to make security decisions. When possible, we should take the time to evaluate the pros and cons of authenticators as they apply to our unique organizations.

As security professionals we tend to focus on the security aspects of authenticators, but there are other important issues that require consideration. The following list details what I consider the five fundamental characteristics of authenticators:

- Usability
- Uniqueness
- Integrity
- Affordability
- Accuracy

The following pages explain each one of these characteristics in more detail and offer some questions you can ask when performing your own authenticator evaluation.

Usability

Usability answers the question of how effectively can people utilize the authenticator. It is concerned with any human or environmental factors that might hinder the use of an authenticator. Every organization has a number of users that will be unable or unwilling to utilize a particular authenticator, or at least use it without a struggle. Exceptions can occur due to physical or mental deficiencies, cultural or medical concerns, unaccommodating work locations, or just the burden of using and maintaining the authenticator.

In turn, we can break usability into a number of distinct sections. When evaluating an authenticator we should answer the questions posed and allow the answers to influence our choice.

Usability within the user population

- Does the authenticator require certain physical features, skills, or mental abilities that would exclude members of the user population?
    - If so, what percentage will be affected?

Usability within the work environment

- Are their environmental or functional factors that would prevent the authenticator from properly functioning? Example: humidity, heat, lighting, dirt, chemical fumes.
    - If so, what locations or departments will be affected?
- Is the authenticator limited to use on certain computers? Example: certificates and private keys.

Burden of use

- Is the user required to carry extra devices, authenticate on specific computers, or do extra work to use the authenticator?
    - Evaluate the form factor of the authenticator: is it bulky, hard to carry, etc?
    - Consider the accumulative burden. Does the burden to the user grow as they are forced to support authenticators from multiple internal or third-party systems?

Skill required to properly use

- How much training or talent does it take to complete a successful authentication?

Speed of using

- How long (both average and maximum time) does it take a user to successfully input the authenticator?

Cultural objections

- Are there any cultural reasons that could cause people to object to using the authenticator?
    - Example: facial recognition may face resistance in areas where religious beliefs compel people to cover their faces.

Health objections

- Are there any health related reasons that could cause people to object to using the authenticator?
  - Example: People might object if everyone has to place their hand on a hand geometry scanner if it is not regularly sanitized.

Ease of enrollment

- Are there requirements for physically visiting an enrollment station or enrolling only while connected to the corporate network?

Skill required to enroll

- How much training or talent does it take to complete a successful enrollment?

Speed of enrollment

- How long does the enrollment process take for each user?

Frequency of enrollment

- How often must the user enroll to change their authenticator?
  - Example: passwords that must be changed every 60 days.

Usability requirements over time

- Do usability requirements change over time?
  - Example: an aging user population may affect the usability

Uniqueness

Uniqueness answers the question of how distinct is the proof used to confirm an identity. We require uniqueness to impede attacks that attempt to guess a legitimate authenticator, and to limit accidental user impersonation.

Combats guessing

- Is the authenticator complex and unique enough that an attacker cannot easily guess the authenticator of a legitimate user?
  - Example: passwords consisting of dictionary words should not be considered sufficiently unique in an environment that needs good authentication.

Limits the false acceptance of illegitimate users

- Is the authenticator, or authenticator input, unique enough that one user can't accidentally or purposely authenticate to another user's account with their own authenticator?
  - Example: a biometric system where it is not tuned well enough to tell certain users from other users in the same population (measured by the false acceptance rate).

Integrity

Integrity answers the question of how difficult is it to guess, forge, or steal the authenticator. Integrity of an authenticator is the key influence of how tightly it can be bound to a user. Good integrity provides resistance to authenticator disclosure, duplication, and theft, thereby ensuring that it is available only to the genuine user. As integrity diminishes, so does user accountability.

Resistance to disclosure

- Is the authenticator reasonably complex so that a user cannot easily convey information that would allow another person to use their authenticator?
    - Example: a user can easily share their password if they think the request is appropriate. But they can't give someone their hand to use for a biometric authentication system.

Resistance to theft

- How hard is it for an attacker to steal the authenticator from the legitimate user?
    - Example: if a user can leave their one-time token card on their keyboard then it may not be difficult for some attackers to steal it. If it is on their key ring, the attacker will probably face more difficulties.

Resistance to duplication

- How difficult is it for an attacker to create a working duplicate of the user's authenticator?
    - Example: Duplicating a password takes no skills or special tools; duplicating a fingerprint requires some skill, special tools, and access to a fingerprint impression.

Detection of theft, duplication, or disclosure

- If theft, duplication, or disclosure of the authenticator occurs how likely is detection by the user or administrators?
    - Example: If a user can't log into their computer they are more likely to detect the theft (or presume loss) and report it.

Affordability

Affordability answers the question of how much does it cost to buy and maintain the authenticator. It involves the cost of the authenticator, supporting software and hardware, user and administrator training, and reoccurring support (replacements, resets, tracking, etc.).

Cost of selection

- What is the cost of purchasing or using the authenticator?
    - Example: starting to use passwords is typically free, starting to use private keys and certificates may not be.

Cost of the deploying hardware and software

- What is the cost of implementing input hardware and software to accommodate the authenticator?
  - Example: again, passwords are typically supported by the existing hardware, but smart card readers are needed for smart card support

Cost of managing

- What are the ongoing management costs related to deploying, resetting, and retiring authenticators?
  - Example: if each user, on average, contacts the helpdesk two times a year to have their password reset, then you should be able to estimate the cost of managing passwords based on the value of help desk personnel time.

Accuracy

Accuracy answers the question of how often do mistakes occur that limit use by legitimate users. Accuracy of authenticators is important to limit the false rejection of legitimate users. A verification component can't link people to their identities unless it is supplied with an accurate authenticator. Inaccuracies may stem from improper user interaction or imprecise system calibration.

Limit false rejection of legitimate users

- Is the authenticator, or authenticator input, predictable enough?

Measuring Core Characteristics

To end up with meaningful results, characteristics must be measured for the exact authenticator type being evaluated. Different biometric-based, possession-based, and knowledge-based authenticators do share some qualities but also have their own unique characteristics.

For instance, passwords and passphrases both share a common integrity risk of user disclosure, but passphrases fare much better against guessing attacks. A secret pattern based authenticator manages the disclosure problem because it is more difficult for one person to describe this knowledge to another.

Conclusion

Different organizations have different needs for authentication. Ultimately, the importance your company gives to authentication should reflect the importance of the data you protect. It doesn't make sense to secure unimportant data or services with an expensive or burdensome authentication solution. Conversely, it generally isn't sensible to protect mission critical services and trade secrets with an ineffective authenticator.

I don’t want to downplay the importance of paying attention to industry authentication trends and guidelines. Combating authentication problems with a methodical, tailored approach just brings greater success. Armed with these tips you have the ammunition to win the authentication battle.

Visit www.PasswordResearch.com for more recommendations on improving the security and effectiveness of your password and authentication practices.