Multi-Factor Authentication Solution Evaluation Criteria

Multi-Factor Authentication Solution Evaluation Criteria

This document outlines criteria that should be considered when evaluating multi-factor authentication products and services. It can also serve as "raw material" for RFPs, technical requirements, and other more formal specifications.

Much of the content in this document is based on material from The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes by Joseph Bonneau, Cormac Herley, Paul C. van Oorschot, and Frank Stajano, March, 2012.

Deployment Environment

1. Is the solution compatible with existing server and client platforms? Examples for higher education include:
    - Operating Systems
        - Windows
        - Macintosh
        - Linux
    - Mobile Operating Systems
        - Android
        - iOS
        - Windows Mobile
        - Blackberry
    - Browsers
        - Firefox
        - Chrome
        - Safari
        - Internet Explorer
    - Web application platforms
        - PHP
        - .NET
        - Java
        - Ruby
        - Python
        - Node.js
    - Microsoft AD
    - Globus
    - Unix shell
    - VPN
    - Mobile
    - Radius
2. How easily is the solution integrated into existing SSO middleware?
    - CAS
    - Shibboleth
    - Microsoft AD FS
3. What features does the solution have to facilitate broad deployment throughout a community?
    - automated enrollment
    - administration tools
    - user support tools
    - ability to delegate admin rights
4. What features does the solution have to accommodate a BYOD environment?
5. Does the solution support capabilities other than authentication, such as encryption and/or digital signature?
6. Is the solution cloud-based or on-premise? What are the potential points of failure?
7. Is the solution scalable and flexible enough to be adapted to potential future applications? Are capabilities provided that can assist in the migration to another solution at some time in the future?

Usability and Accessibility

1. Are users required to remember additional secrets? How many? What is the required complexity of those secrets?
2. Does adding more accounts for the user increase the burden on the user?
3. Are users required to carry an additional object (to be used as an authentication token)?
4. What physical effort is required of the user?
5. How easy is the solution to learn?
6. How much time is required to perform an authentication? To associate a new account?
7. How reliable is the authentication process (*i.e.*, are false negatives common)?
8. How easy is it to recover from a lost token or forgotten credentials?
9. How accessible is the solution?
    - Do certain disabilities preclude its use?
    - Are multiple technologies supported to accommodate to specific disabilities?
    - Overall, what strategies are employed to address accessibility issues?

Security and Privacy

1. Is the solution resistant to physical observation?

2. Is the solution resistant to targeted impersonation (*e.g.*, by an acquaintance)?
3. Is the solution resistant to throttled guessing?
4. Is the solution resistant to unthrottled guessing?
5. Is the solution resistant to internal observation (*e.g.*, by intercepting traffic across a network or within an endpoint device?
6. Is the solution resistant to leaks from other verifiers?
7. Is the solution resistant to phishing?
8. Is the solution resistant to theft?
9. Does the solution require a trusted third party?
10. Is explicit user consent required to complete authentication?
11. Can authentication with one verifier be linked with another?
12. Does the solution require secrets to be stored on a server?
13. Is the technology mature? Has it been reviewed by a sufficiently large community?
14. Is the solution proprietary? Can the implementation be assessed independently by users?
15. Is the software open source?

User Support

1. What documentation is provided? Is there an FAQ?
2. Are tools available to assist help desk personnel?
3. Are training materials and/or classes available?

Product Support

1. What support services are a provided by the vendor? By third parties?
2. What management tools are available?
3. Are add-ons available from third parties? What other vendors have integrated the solution with their products?
4. What are the communication channels with the provider?
5. Is there a viable user community?

Compliance

1. Does the solution satisfy the authentication criteria for well-known assurance profiles?
2. Does the solution satisfy the authentication criteria for compliance with FERPA, HIPAA, PCI, and other requirements for higher education?
    - Does the service agreement share liability appropriately?
3. Does the solution conform with applicable standards, particularly FIPS 140-2 and NIST 800-63-2? Are there plans for alignment with the Fido Alliance?

Costs

1. Pricing
    - What is the purchase cost of the solution?
    - What are the support costs of the solution?
    - Which portions of the cost are incremental (per user), which grow as the number of users grow (although perhaps for each user), and which are fixed?
2. Life-cycle costs
    - What is the startup cost?
    - What are the ongoing operational costs? What are the staffing requirements?
    - What is the fixed cost per user?
    - Are there variable "per user" costs?
    - What is the potential cost of migration to a new solution in the future?
3. Costs that must be born by end users
    a. Does the solution require telephony services that may have associated costs?