Applying the Eightfold Path to NIST SP 800-63B

This analysis examines NIST Special Publication (SP) 800-63B, focusing on digital identity authentication and lifecycle management for public and private users, using the Eightfold Path framework by Bardach (2012).

1. Define the Problem

SP 800-63B addresses challenges in digital identity by establishing new authentication models and techniques that prioritize usability. It also tackles issues surrounding session management, reauthentication requirements, and implementing biometric technologies. (NIST 2022)

2. Diagnose the Problem

The document acknowledges concerns regarding:

- **Clarity:** More detailed information on phishing resistance guidelines, emerging authentication methods, session management thresholds, and reauthentication implementation for organizations is needed.

- **Biometrics:** The impact of proposed biometric performance requirements needs detailed analysis. (NIST 2022)

3. Assemble Evidence

The guidelines were developed using:

- **Expert Feedback:** Contributions from stakeholders and experts informed the document's content.

- **Research:** Extensive research and existing standards were incorporated.

- **NIST Direction:** Existing NIST guidelines provided a foundation.

These diverse sources aimed to establish best practices for authentication and lifecycle management. (NIST 2022)

4. Analyze Evidence

The analysis focused on standardizing authentication and lifecycle management procedures. NIST prioritizes mitigating identification and authentication risks while promoting flexibility for various users. (NIST 2022)

5. Evaluate Alternatives

The policy evaluates different authentication methods, ensuring they utilize valid licenses, credentials, FIDO passkeys, and consider potential security, privacy, and usability benefits. The document compares methods to identify the most suitable approach for standardized procedures. (NIST 2022)

6. Select Criteria

Evaluation criteria include emerging authentication models and techniques, associated security and privacy risks, biometric performance impacts, and usability benefits for organizations. (NIST 2022)

7. Project Outcome

NIST established a model that considers user response to new methods and incorporates current security challenges. This makes the guidelines reliable for diverse institutions and agencies. (NIST 2022)

8. Confront the Trade-Offs

While NIST addresses current security challenges, affordability remains an issue for small businesses. The document prioritizes usability, but can small enterprises implement it effectively considering the cost implications? (NIST 2022)

9. Decide

This development by NIST is a positive step towards addressing security concerns for organizations. However, concerns remain regarding how implementation will affect smaller businesses, as cyberattacks can target any size organization. (NIST 2022)

10. Tell Your Story

NIST's digital identity guidelines address a major security challenge for organizations. The documents on identity management, online risks, and stakeholder involvement can help organizations develop frameworks for their identity policies.

Overall Strengths

- Addresses current needs in online services for reliable, secure, and privacy-protective digital identity solutions.

- Widely accepted guidelines meeting technical requirements for public and private agencies in implementing digital identity services.

- Defines technical requirements for authentication assurance levels.

- Mitigates risk by considering the real-world impact of biometric performance.

- Updates risk and threat models to counter advanced threats and fraud. (NIST 2022)

Weaknesses

- Implementation challenges for small businesses due to complexity and cost of setting up authentication and lifecycle management.

- Limited discussion on data privacy and equity issues. (NIST 2022)

Conclusion

NIST SP 800-63B provides valuable guidelines for digital identity authentication and lifecycle management. While some weaknesses exist, it's a significant step towards strengthening online security for organizations of all sizes.

References

- National Institute of Standards and Technology. (n.d.). Digital Identity Guidelines (SP 800-63-3). Retrieved from https://pages.nist.gov/800-63-3/

- Bardach, E. (2012). A Practical Guide for Policy Analysis: The Eightfold Path to More Effective Problem Solving. CQ Press, Part 1, Pg 1-96.