Workload Authentication Maturity Levels

Draft Submission for IETF Review

Ryan Hurst @ SPIRL, Jeff Lombardo @AWS

Purpose and Goals

- **Establish a Framework**: Create a structured approach for workload authentication, inspired by NIST SP 800-63B
- **Guide Organizations**: Help organizations improve their security posture through consistent workload authentication practices
- **Facilitate Discussion**: Provide a common language to assess security properties and make informed decisions

Background and Status

- **Initial Draft**: Developed from initial notes and formatted according to RFC standards
- **Community Consensus**: Prior discussions indicated support for a document aligned with these goals
- **Preliminary Feedback**: Initial input gathered on potential structure and content
- **Co-Author Update**: Jeff Lombardo has joined to support further progress

Summary of Key Feedback

- **Clear Objectives**: Abstract refined to outline goals, best practices, and assurance levels
- **Structured Approach**: Sections aligned with NIST SP 800-63 standards to establish consistency
- **Threat Mitigation**: Dedicated security section addressing threats and mitigations
- **Granularity**: Levels reduced to 3-4, aligning with xAL standards for simplicity
- **Defined Boundaries**: Clear distinction between workload and human identity requirements
- **Standardized Terminology**: Consistent definitions for authenticators, including enrollment, management, and usage
- **Supporting Components**: Defined requirements for supporting authentication elements

Next Steps and Community Involvement

- **Please Review the Draft**: https://github.com/rmhrisk/WorkloadIdentityAuthenticationLevels/
- **Request for Contributions and Feedback**:
  - The proposed next steps
  - Other topics and goals
- Lets work together to create a practical framework that helps consumers and implementers communicate effectively about workload authentication maturity.