NISTIR 8103

Advanced Identity Workshop on Applying Measurement Science in the Identity Ecosystem:

Summary and Next Steps

Michael E. Garcia
Paul A. Grassi

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.IR.8103

National Institute of Standards and Technology
U.S. Department of Commerce

NISTIR 8103

Advanced Identity Workshop on Applying Measurement Science in the Identity Ecosystem:

Summary and Next Steps

Michael E. Garcia
Paul A. Grassi
Applied Cybersecurity Division
Information Technology Laboratory

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.IR.8103

September 2016

U.S. Department of Commerce
Penny Pritzker, Secretary

National Institute of Standards and Technology
Willie May, Under Secretary of Commerce for Standards and Technology and Director

National Institute of Standards and Technology Internal Report 8103
14 pages (September 2016)

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.IR.8103

Comments on this Publication and the Workshop may be submitted to:

National Institute of Standards and Technology
Attn: Applied Cybersecurity Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 2000) Gaithersburg, MD 20899-2000
Email: NSTICworkshop@nist.gov

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal information systems.

Abstract

On January 12-13, 2016, the Applied Cybersecurity Division (ACD) in the National Institute of Standards and Technology (NIST) Information Technology Laboratory (ITL) hosted "Applying Measurement Science in the Identity Ecosystem"—a workshop to discuss the application of measurement science to digital identity management. This document summarizes the concepts and ideas presented at the workshop and serves as a platform to receive feedback on the major themes discussed at that event.

Keywords

Identity; NSTIC; authentication; biometric authentication; biometrics; identity proofing; attributes; metadata; identity management; cybersecurity; security; information security.

Disclaimer

Any mention of commercial products or reference to commercial organizations is for information only; it does not imply recommendation or endorsement by NIST, nor does it imply that the products mentioned are necessarily the best available for the purpose. Content was derived from workshop participant discussions captured by note takers and aggregated for the purposes of summarizing the event. Any misrepresentation of comments or concepts is unintentional. Corrections or clarifications can be provided through the open comment period.

Acknowledgements

The authors would like to thank Ryan Galluzzo and Walter McLean for their contributions to this NISTIR. In addition, we would like to thank panelists Ian Glazer, Kim Little-Sutherland, David Kelts, Dario Berini, Brent Williams, Julian White, Brett McDowell, Stephanie Schuckers, Vance Bjorn, Cathy Tilton, Liz Votaw, LaChelle LeVan, Darran Rolls, Gerry Gebel, Ryan Disraeli, and Robin Wilton and facilitators Kirk Brafford, Mike Wyatt, Roger Cressey, Kiersten Todt, JR Reagan, and Colin Soutar, as well as the workshop participants who provided valuable input to this report. Finally, we would like to thank and acknowledge the efforts of those that developed the workshop white papers, to include Elaine Newton, Kevin Mangold, Mike Garris, Colin Soutar, Ryan Galluzzo, Jim Fenton, Kat Megas, and Justin Richer.

Table of Contents

Introduction

On January 12 and 13, 2016, the Applied Cybersecurity Division (ACD) in the National Institute of Standards and Technology's (NIST) Information Technology Laboratory hosted the "Applying Measurement Science in the Identity Ecosystem" workshop in Gaithersburg, Maryland.[1] The two-day workshop brought together security practitioners, identity solution providers, subject matter experts, and policy makers from across the public and private sectors to discuss the application of metrics and measurement science to common identity management practices.

The Identity Ecosystem has matured to the point where it is appropriate to undertake the work of building measurement science for application in the market—a critical step in further aiding expansion and innovation of the Identity Ecosystem. This workshop was held to obtain feedback from stakeholders on the feasibility of, and approaches necessary to, measure and compare three disciplines of digital identity management:

1. Strength of identity proofing;
2. Strength of authentication; and
3. Attribute metadata and confidence scoring.

NIST's ultimate goal is to establish frameworks that enable objective measurement of identity solutions, so that their ability to mitigate risk is more quantitatively measurable, they can more easily be compared, and, ultimately, measured when combined. NIST believes making progress in this space will achieve greater alignment of identity solutions and technology with risk assessment and management practices. This document provides a summary of the proceedings to ensure NIST captured stakeholder feedback accurately as it executes the next steps in its broad effort towards improved digital identity.

Workshop Summary and Key Takeaways

Workshop attendees represented diverse public and private sector stakeholders. In total, 224 people attended the event: 67 % from the private sector, 26 % from government organizations, and 7 % from academia and non-profits. The workshop included moderated panels and facilitated working sessions for each workshop topic. Throughout the event, participants shared risk management practices, security evaluation approaches, and testing processes that they utilized within their organizations. Additionally, participants identified barriers, evaluated solutions, and specified implementation considerations to enable greater quantification of strength within each digital identity management discipline the workshop covered.

The summary below identifies takeaways and observations from the event. These do not necessarily indicate items that were unanimously supported by those in attendance, but rather frequently voiced ideas and input among panelists, audience questions, and the breakout teams during the course of workshop.

[1] Information about the workshop is available at: https://www.nist.gov/itl/nstic/projects-events.

Overall Observations

NIST heard several recurring themes that transcended the individual workshop topics. These typically involved NIST's overall effort to apply measurement science to digital identity, the efficacy of measurement within each topic, and how the relationships, or lack thereof, between topics could influence a future direction.

- **Application of Metrology to Digital Identity and Access Management.** Many participants saw value in NIST's effort to establish measurement science to communicating the strength, and ability to mitigate risk, of identity management practices and solutions. Furthermore, most expressed willingness to remain engaged as those efforts develop and mature. Some attendees expressed a view that mandatory metrics and measurements may place an undue burden on vendors. Overall, attendees felt the three focal areas of the workshop were appropriate to evolve and enhance the Identity Ecosystem, and supported NIST's efforts to produce measurement-based guidance associated with each.

  While the idea of producing additional guidance regarding measurements and metrics was generally well received, there was no consensus on any specific approach to apply measurement science to digital identity, nor how to develop such approaches. Likewise, there was no consensus on the metrics that should be measured and reported within systems and federations. A few participants felt scoring digital identity processes and technologies was neither feasible nor appropriate.

- **Improved Transparency and Standardization.** Most participants expressed a desire to see increased transparency and standardization across identity practices—particularly in the realm of remote identity proofing practices. Many attendees expressed a desire to better understand the way identity solutions operate and to overcome a lack of visibility, whether real or perceived, into how proprietary scoring works within existing remote identity proofing solutions. Many participants also saw a need to better understand the processes that contribute to data they leverage and trust to remotely proof identities. Many felt that standardized processes for evaluating solutions and communicating the efficacy of these solutions would provide greater interoperability and trust on a broad scale.

- **Flexibility and Extensibility.** Participants broadly encouraged NIST to ensure that any future guidance is both flexible and extensible to support the diverse needs of different communities, trust frameworks, and sectors. Notably, most participants wished to ensure that any guidance was reflective of the need to address risks to federal agencies—while also acknowledging the needs and concerns of the private sector. This reflected the view that many, if not all, digital identity solutions will come from the private sector vendor community, so NIST

must attempt to develop guidance that does not create an environment where cross-sector solutions will no longer be viable within the Federal Enterprise. Many expressed a strong desire for NIST to craft documentation in a manner that could subsequently be submitted as a work product in open, consensus-based standards development organizations.

- **Topic Area Relationships:** Participants acknowledged the pre-event whitepapers as thoughtful starting points for much of the workshop discussion, but sought greater insight on how the measurement of authenticator strength, remote and in-person identity proofing, and attribute confidence would or could impact each other in future NIST deliverables. Many suggested NIST should explore an overarching model of identity measurement to help clarify the role of measurement science in digital identity and the interplay between these, and potentially other, components.

- **Existing Work and Fora:** The digital identity community is one of constant innovation and many complementary efforts. Participants repeatedly sought to ensure that NIST recognize and collaborate with existing initiatives focused on similar outcomes. Participants identified multiple existing efforts as places where NIST could leverage synergies to advance the community's collective interests. Efforts mentioned include:

    - UK Cabinet Office and the Good Practices Guides (GPGs) : https://www.gov.uk/government/collections/identity-assurance-enabling-trusted-transactions
    - The Kantara Initiative Identity Assurance Working Group: https://kantarainitiative.org/confluence/display/idassurance/Home
    - The IETF Vectors of Trust internet draft: https://tools.ietf.org/html/draft-richer-vectors-of-trust-00
    - OASIS Trust Elevation Group: https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=trust-el
    - ISO/IEC SC 27 Working Group 5: http://www.iso.org/iso/iso_technical_committee?commid=45306
    - ISO/IEC SC 37 biometric activities: http://www.iso.org/iso/home/standards_development/list_of_iso_technical_committees/iso_technical_committee.htm?commid=313770
    - FIDO Certification Working Group: https://fidoalliance.org/working-groups/
    - FIDO Biometric Assurance Sub-working Group

Strength of Identity Proofing

Strength of identity proofing was the first topic of the workshop. Participants discussed existing and potential identity proofing methods and ways to measure strength of each

individual process, as well as the establishment of a scoring framework to communicate common results of digital identity proofing for the purposes of risk management. Across the discussion groups, several major themes emerged.

- **Develop a common lexicon**. Many participants identified a lack of standardized terminology regarding identity proofing processes and functions. For example, some attendees used the term "verification" while others preferred "validation" for the same process. For the purposes of NIST's work, attendees suggested a common vocabulary should be developed to help ensure consistency in the framework and across communities, and that the taxonomy be aligned to the best extent possible with existing schemes.

- **Identify functional components of proofing.** Attendees in most sessions came to the conclusion that proofing could be broken down into a set of component functions or actions that could potentially be evaluated to provide a greater understanding of the processes and the results associated with verifying a claimed identity. Each component could potentially serve as the basis for a scoring structure.

    - Participants suggested additional functional components that could be added to those currently explored in the whitepapers. Specific suggestions included: ongoing maintenance of an identity (i.e., how a provider manages the identity, updates it, and supports necessary modifications when needed); fraud and compromise detection; document authentication; activity history of an identity; biometric collection to support the binding of proofing to a credential; and processes for binding proofing data to an identity.

- **Avoid a single score**. Many participants expressed the belief that any scoring of the processes associated with identity proofing should not be aggregated into a single score. Instead, many felt it more appropriate to provide individual scores for the processes that could be considered and weighted by relying parties (RPs) to meet their needs. In some instances, more fine-grained knowledge of the processes an individual underwent to confirm a claim of identity would be just as valuable as a score.

- **Consider existing standards and practices**. Several participants referenced UK GPG 45 as an example of combining high-level scoring with desired outcomes. Participants discussed the potential to draw lessons from the UK GPGs and apply them to a US based identity proofing framework.

- **Define scope of proofing**. Participants also discussed the scope of identity proofing, specifically that the goal of identity proofing guidelines should be scoped to proving a valid identity exists. Proofing should not, for example, validate an individual's rights and privilege to obtain specific entitlements.

Determining entitlements and eligibility is an RP decision that goes beyond confirming that and identity is associated with a specific individual.

Strength of Authentication

The second workshop session addressed the strength underlying various authentication methods. The session explored measuring mitigation methods of known vulnerabilities to an authentication system as a method to determine an overall score for authenticator performance as well as an overall construct that would enable the assessment and comparison of distinct authentication mechanisms. While the strength of authentication whitepaper identified biometric authentication as a starting point for an overall authentication framework, several of the workshop sessions ended up extensively discussing the broader concept of evaluating various authenticator technologies. While biometrics was selected first due to its increasing consumer and commercial adoption rates, the framework envisioned by NIST would support the evaluation of authentication strength regardless of form or factor, making these broader discussions extremely valuable. Across the groups, several major themes of discussion emerged.

- **Consider user experience—or a poor user experience—as a vulnerability** . Most participants felt that user experience with a chosen authentication method is one of the most important factors in selecting technologies that are not only secure, but also likely to be successfully adopted. Many pointed out that the largest driver behind the adoption of mobile biometric solutions is market demand and the ease with which users are able to access services. As a result of this ease-of-use focus by consumers, many participants noted that security may not be the primary objective of many RPs when instituting authentication solutions. Therefore, inclusion of user experience in any evaluation scheme may have a benefit to both security personnel required to assist in risk management and mitigation, and to business decision makers.

  This led some participants to suggest incorporating a usability score into the framework. Participants also considered the possibility that a poor user experience could be considered a system “vulnerability” and weighted, evaluated, and scored much as the other components of the score. However, poor user experience should not be the only metric. Rather, the result of poor user experience will be the users themselves trying to exploit workarounds to improve their individual experience with the technology. These workarounds would be considered the vulnerability.

- **Consider framework utility to RPs and its long-term applicability**. In addition to the importance of usability with respect to authentication solutions, many identified a need for any scoring or evaluation framework to be usable as well. Attendees indicated that some RPs struggle to balance the need to deliver cutting edge solutions to the market with the needs of security and privacy. For a measurement based framework to have broad adoption it must enable rapid evaluation of solutions to allow users to maintain pace with markets and customer demands.