fido alliance | simpler stronger authentication

February 23, 2015

National Institute of Standards and Technology
100 Bureau Drive, Stop 1070
Gaithersburg, MD 20899-1070

Response to NIST RFI on the Framework for Improving Critical Infrastructure Cybersecurity

The Fast Identity Online (FIDO) Alliance welcomes the opportunity to comment on the National Institute of Standards and Technology (NIST) Request for Information (RFI) on the Framework for Improving Critical Infrastructure Cybersecurity.

Two years ago, NIST laid out a number of challenges in the "Roadmap for Improving Critical Infrastructure Cybersecurity" that accompanied the release of the Framework. The roadmap flagged Authentication as the first "high priority" area for Development, Alignment, and Collaboration -- noting that while "*poor authentication mechanisms are a commonly exploited vector of attack by adversaries*" and that "*Multi-Factor Authentication (MFA) can assist in closing these attack vectors*," NIST did not include recommendations on MFA in the Framework because:

> *"There is only a partial framework of standards to promote security and interoperability. The usability of authentication approaches remains a significant challenge for many control systems, as many existing authentication tools are for standard computing platforms. Moreover, many solutions are geared only toward identification of individuals; there are fewer standards-based approaches for automated device authentication."*

The 250+ members of the FIDO Alliance's took this statement quite seriously, and we are pleased to report that in 2016 -- two years after the Framework was first issued -- significant progress has been made in addressing the challenges outlined. Our efforts have focused on improving online authentication by developing open, interoperable industry specifications that leverage proven public key cryptography for stronger security and device-based user verification for better usability.

The results of these efforts are the FIDO 2.0 Technical Specifications, now going through a formal standards approval process at the World Wide Web Consortium (W3C) (see https://www.w3.org/blog/2015/11/w3c-fido/), and numerous deployments of FIDO Technical Specifications protecting tens of millions of users today, as detailed below.

Beyond this standardization process, we draw attention to the wide array of firms who are leading the development of the FIDO ecosystem by being early adopters of the technology and deploying FIDO solutions to their customers at scale. Since the NIST Framework was released two years ago:

- Google launched support for FIDO 2-factor authentication in 2014 and extended this to its Google for Work customers in 2015
- Microsoft has pledged to build support for FIDO into Windows 10
- PayPal in 2014 launched a partnership with Samsung allowing PayPal customers to use FIDO specifications to securely and easily authenticate for payments with the swipe of a finger wherever PayPal is accepted
- Bank of America deployed FIDO-enabled fingerprint authentication for its mobile banking app across both iOS and Android, enabling millions of customers to add a very secure, easy-to-use authentication capability to improve the security of payments and mobile banking transactions
- In Japan, NTT DOCOMO -- Japan's largest Mobile Network Operator (MNO) -- deployed FIDO-compliant strong authentication across its network by introducing 10 FIDO(R) Certified mobile phones, enabling millions of customer to have a streamlined, secure local-match biometric log-in solution for a variety of NTT DOCOMO applications, including banking and payment applications, leveraging both fingerprint and iris biometric technologies from phone manufacturers Samsung, LG, Fujitsu, and Sony.

Additional implementations and deployments of FIDO specifications were launched in 2015 by firms such as Qualcomm, Dropbox and Github; 2016 is on track to produce an even wider array of deployments.

FIDO was founded on a simple premise: to challenge the common but flawed assumption that easy-to-use authentication must be weak, and strong authentication must be difficult to use, by producing a new open industry standard that enables the best of both. For years, the uptake of strong authentication solutions has been inhibited by this assumption (as noted in Figure 1), with solutions in the marketplace falling on one end of the curve or the other.

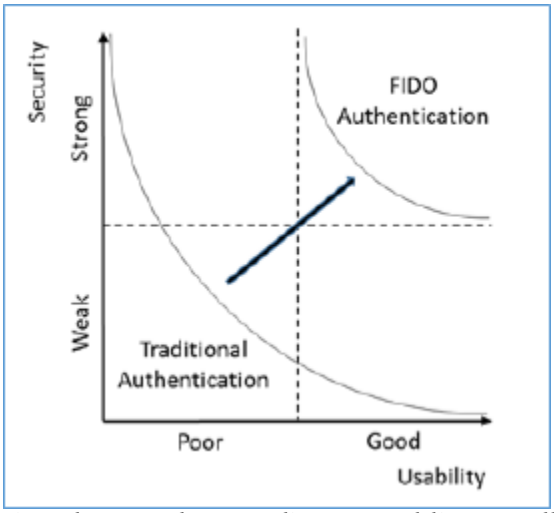

Figure 1: FIDO Authentication changes the paradigm -- enabling excellent security and usability

Too many times, products have been engineered to prioritize security over usability, with the assumption that individuals would use the solution; the reality, however, has been that consumers have rejected using solutions that are hard to use -- leading to a growing number of data breaches and other security exploits. In order for authentication to be broadly accepted by both online service providers and their users, it must be affordable to deploy and easy to use while providing improved security.

As we note in our response, FIDO Alliance members include companies and organizations from many critical infrastructure sectors, including: Communications, Financial Services, Government Facilities, Information Technology, Healthcare and Public Health, Commercial Facilities and Defense Industrial Base. Our board members, listed below, comprise key players across services, apps, devices, platforms, and vendors from across the globe.

As our response details, the problems in cybersecurity caused by weak authentication solutions have gotten worse in the two years since the Framework was published. But through the efforts of the FIDO Alliance and other industry efforts, the standards to address authentication challenges have gotten much better. We believe it is time to update the

Framework to include a new PR.AC Subcategory around Authentication, reading "Authentication of authorized users is protected by multiple factors."

As the President's FY17 Budget stated, "*The President is calling on Americans to move beyond just the password to leverage multiple factors of authentication when logging-in to online accounts....Empower Americans to secure their online accounts by moving beyond just passwords and adding an extra layer of security. By judiciously combining a strong password with additional factors, such as a fingerprint or a single use code delivered in a text message, Americans can make their accounts even more secure.*"

We would welcome the opportunity to engage further with NIST on this topic. Our executive director, Brett McDowell, can be reached at brett@fidoalliance.org.

401 Edgewater Place, Suite 600, Wakefield, MA 01880 USA
Phone +1 408 657 3436 • www.fidoalliance.org

Organizational Information
Organization Name
Organization Sector
Organization Size
Organization Website
Organization Background
Point of Contact Information
POC Name
POC E-mail
POC Phone

Response
The FIDO Alliance
Non-profit with members from sectors including: Communications, Financial Services, Government Facilities, Information Technology, Healthcare and Public Health, Commerical Facilities and Defense Industrial Base
More than 250 members
www.fidoalliance.org
Industry Association
Response
Brett McDowell, Executive Director
brett@fidoalliance.org
413-404-5593

#	Question Text
1	Describe your organization and its interest in the Framework.
2	Indicate whether you are responding as a Framework user/non-user, subject matter expert, or whether you represent multiple organizations that are or are not using the Framework.
3	If your organization uses the Framework, how do you use it? (e.g., internal management and communications, vendor management, C-suite communication).
4	What has been your organization's experience utilizing specific portions of the Framework (e.g., Core, Profile, Implementation Tiers, Privacy Methodology)?
5	What portions of the Framework are most useful?
6	What portions of the Framework are least useful?
7	Has your organization's use of the Framework been limited in any way? If so, what is limiting your use of the Framework (e.g., sector circumstance, organizational factors, Framework features, lack of awareness)?
8	To what extent do you believe the Framework has helped reduce your cybersecurity risk? Please cite the metrics you use to track such reductions, if any.
9	What steps should be taken to "prevent duplication of regulatory processes and prevent conflict with or superseding of regulatory requirements, mandatory standards, and related processes" as required by the Cybersecurity Enhancement Act of 2014?

10	Should the Framework be updated? Why or why not?
11	What portions of the Framework (if any) should be changed, or removed? What elements (if any) should be added to the Framework? Please be as specific as possible.

12	Are there additions, updates or changes to the Framework's references to cybersecurity standards, guidelines, and practices that should be considered for the update to the Framework?
13	Are there approaches undertaken by organizations – including those documented in sector-wide implementation guides – that could help other sectors or organizations if they were incorporated into the Framework?
14	Should developments made in the nine areas identified by NIST in its Framework-related "Roadmap" be used to inform any updates to the Framework? If so, how?
15	What is the best way to update the Framework while minimizing disruption for those currently using the Framework?
16	Has information that has been shared by NIST or others affected your use the Framework? If so, please describe briefly what those resources are and what the effect has been on your use of the Framework. What resources, if any, have been most useful?
17	What, if anything, is inhibiting the sharing of best practices?
18	What steps could the U.S. government take to increase sharing of best practices?
19	What kind of program would help increase the likelihood that organizations would share information about their experiences, or the depth and breadth of information sharing (e.g., peer-recognition, trade association, consortia, federal agency)?
20	What should be the private sector's involvement in the future governance of the Framework?
21	Should NIST consider transitioning some or even all of the Framework's coordination to another organization?
22	If so, what might be transitioned (e.g., all, Core, Profile, Implementation Tiers, Informative References, methodologies)?
23	If so, to what kind of organization (e.g., not-for-profit, for-profit; U.S. organization, multinational organization) could it be transitioned, and could it be self-sustaining?
24	How might any potential transition affect those currently using the Framework? In the event of a transition, what steps might be taken to minimize or prevent disruption for those currently using the Framework?
25	What factors should be used to evaluate whether the transition partner (or partners) has the capacity to work closely and effectively with domestic and international organizations and governments, in light of the importance of aligning cybersecurity standards, guidelines, and practices within the United States and globally?

Response Text
The FIDO Alliance’s mission is to change the nature of online strong authentication by: -Developing technical specifications which define open, scalable, interoperable mechanisms that supplant reliance on passwords to securely authenticate users of online services; -Operating industry programs to help ensure successful worldwide adoption of the specifications, and; -Submitting mature technical specifications to recognized standards development organization(s) for formal standardization. The FIDO Alliance was launched in 2013 to improve online authentication by developing open, interoperable industry specifications that leverage proven public key cryptography for stronger security and device-based user verification for better usability. Today, more than 250 members from across the globe -- representing leaders in enterprise software, banking, payment systems, mobile devices, chip manufacturers, hardware and software manufacturers and others -- have come together to drive the adoption of FIDO standards. FIDO Alliance was created to specifically solve the authentication problem in the larger context of identity and access management, without duplicating effort or reinventing the wheel. FIDO specifications are therefore complementary to other industry efforts in this area. The core ideas driving the FIDO Alliance's efforts are ease of use, privacy and security, and interoperability. The primary objective is to enable online services and websites, whether on the open Internet or within enterprises, to leverage native security features of end-user computing devices for strong user authentication, and to reduce the problems associated with creating and remembering passwords. FIDO Alliance was founded on a simple premise: to address the common but flawed assumption that easy-to-use authentication must be weak, and strong authentication must be difficult to use. With strong authentication such an important element of protecting people and assets online, the FIDO Alliance is keenly focused on standards efforts that make it as easy possible for strong authentication technology to be widely deployed.
We are subject matter experts.
n/a
n/a
n/a
n/a
n/a
n/a
n/a

As detailed below, we believe the Framework should be updated to reflect significant progress in the Identity and Authentication industry since the Framework was first published.

Two years ago, the Roadmap identfied Authentication as a "high-priority area for development, alignement and collaboration," stating: "While new authentication solutions continue to emerge, there is only a partial framework of standards to promote security and interoperability. The usability of authentication approaches remains a significant challenge for many control systems, as many existing authentication tools are for standard computing platforms. Moreover, many solutions are geared only toward identification of individuals; there are fewer standards-based approaches for automated device authentication."

Significant progress has been made on this issue in the last two years -- inspired in large part by the language in the Roadmap. Today, the standards framework for authentication has improved, as has the usability of authentication approaches. The FIDO standards currently going through approval at the W3C are designed with usability as a guiding principle -- breaking the old paradigm that security is at odds with usability.

The emergence of the FIDO standards is notable; more notable is who has pledged to adopt them in the two years since NIST published the Framework:
● Google launched support for FIDO 2-factor authentication in 2014 and extended this to its Google for Work customers in 2015
● Microsoft has pledged to build support for FIDO into Windows 10
● PayPal in 2014 launched a partnership with Samsung allowing PayPal customers to use FIDO specifications to securely and easily authenticate for payments with the swipe of a finger wherever PayPal is accepted
● Bank of America deployed FIDO-enabled fingerprint authentication for its mobile banking app across both iOS and Android, enabling millions of customers to add a very secure, easy-to-use authentication capability to improve the security of payments and mobile banking transactions
● In Japan, NTT DOCOMO -- Japan’s largest Mobile Network Operator (MNO) -- deployed FIDO-enabled strong authentication across its network by introducing 10 FIDO(R) Certified mobile phones, enabling millions of customer to have a streamlined, secure log-in solution for a variety of NTT DOCOMO applications, including banking and payment applications.

Additional implementations and deployments of FIDO specifications were launched in 2015 by firms such as Qualcomm, Dropbox and Github; 2016 should produce an even wider array of deployments. The authentication landscape has changed significantly in two years; the Framework should reflect these changes.

The Protect/Access Control (PR.AC) section should be updated to make clear that use of passwords alone to manage access for authorized users is not sufficient. This fact was noted in the Framework Roadmap published two years ago; the progress in development of better standards and practices to address the challenges noted in the Roadmap now suggests that the Framework itself should be updated to discuss Authentication.

We suggest the addition of a new PR.AC Subcategory around Authentication, reading "Authentication of authorized users is protected by multiple factors."

As the President's FY17 Budget stated, "The President is calling on Americans to move beyond just the password to leverage multiple factors of authentication when logging-in to online accounts....Empower Americans to secure their online accounts by moving beyond just passwords and adding an extra layer of security. By judiciously combining a strong password with additional factors, such as a fingerprint or a single use code delivered in a text message, Americans can make their accounts even more secure."

As noted above, the FIDO standards currently being reviewed for formal approval by the W3C represent a significant leap forward in the standards for authentication. At its core, the FIDO standards enable the old "shared secrets" model of passwords to be replaced with long-proven asymmetric Public Key Cryptography, where the private key is the only “secret,” and it is securely stored on the user’s device. Only the public key is ever shared with the online service, resulting in no credential secrets ever being shared with servers; this renders the threat of credential theft from a data breach moot. These new W3C standards should be included in the Framework's references to cyberseecurity standards.
While some sectors -- or regulators covering those sectors -- have developed guidance calling for multi-factor authentication, we have not seen any sector develop specfic language that seems suited for the tone and langauge of the Framework. As such, we have suggested language above in Section 11 that we believe is well-suited.
As noted above, there has been significant progress by industry in addressing the challenges laid out in the Authentication section of the Roadmap. FIDO Alliance members took the challenges laid out in the roadmap quite seriously; much of the progress made in the last 24 months has been driven by a need to address these challenges.
We do not have an opinion here; we do believe an update that includes a reference to use of stronger authentication would not be disruptive to those currently using the Framework.
n/a
n/a
n/a
n/a
n/a
n/a
n/a
n/a
n/a
n/a

References

https://www.w3.org/blog/2015/11/w3c-fido/ https://www.w3.org/Submission/2015/SUBM-fido-web-api-20151120/	
	CIS CSC Controls 5.6, 11.4, 12.6, 16.11 https://www.w3.org/Submission/2015/SUBM-fido-web-api-20151120/

CIS CSC Controls 5.6, 11.4, 12.6, 16.11 https://www.w3.org/Submission/2015/SUBM-fido-web-api-20151120/
