Details on the Multi-factor Authentication Cohortium effort

Details on the Multi-factor Authentication Cohortium effort

The National Strategy for Trusted Identities in Cyberspace (NSTIC) initiative is a "White House initiative to work collaboratively with the private sector, advocacy groups and public-sector agencies" with the goal of advancing the "NSTIC vision that individuals and organizations adopt secure, efficient, easy-to-use, and interoperable identity credentials to access online services in a way that promotes confidence, privacy, choice and innovation." The Internet2 Scalable Privacy Project (ScalePriv) is one of five pilot projects to receive funding from the first round of pilot funding in September 2012. The ScalePriv Project contains several major thrusts around identity and privacy, including a focus on promoting the adoption of Multi-factor Authentication (MFA) across Higher Education institutions. The ScalePriv Project includes three partially supported leadership deployments of MFA at the Massachusetts Institute of Technology (MIT), the University of Texas System, and the University of Utah, as well as the commitment of building the MFA Cohortium described in this Call for Participation.

Promoting the adoption of MFA fits into the overall ScalePriv Project in multiple ways:

- *Good privacy begins with good security*, with several examples being:
  - better assurance that individuals with privileges to see and/or manage other's personal data are indeed the individuals intended to have such access,
  - a more secure account makes phishing harder,
  - privacy managers can leverage higher levels of assurance (i.e., ones requiring MFA) before authorizing the release of sensitive identity attributes.
- A number of approaches to MFA involve biometric or other data (e.g. geolocation from an SMS 2nd factor activity) that has the potential of "privacy spillage". Having MFA behind a campus' Identity Provider (IdP), and then using federation to leverage that MFA for a broad spectrum of services, allows the advantages of MFA while gaining a potential "privacy firewall" in the form of the IdP.
- It helps to minimize the number of Service Providers that might otherwise feel compelled to offer their own MFA implementations that don't have the advantage of the "IdP privacy firewall", and have the potential to confuse users with the multitude of approaches, devices, etc.

One way to frame what this MFA Cohortium is intended to accomplish is to consider an answer to the following question: "Why doesn't Multi-factor Authentication have higher adoption today by Higher Education institutions?" After all, it has been recognized for quite some time that relying on passwords for secure authentication has many problems, including phishing attacks, guessing attacks, compromising password recovery approaches (e.g. answer a few questions), obtaining files of passwords and decrypting them, key loggers, and capturing on the wire. Institutions pursue a variety of strategies to attempt to strengthen the use of passwords, such as increasing password complexity rules, shortening the lifetime of passwords, ensuring encrypted transmission of passwords, minimizing the number of times it is entered and the number of systems handling it (e.g. SSO systems), and password throttling. Those approaches can help, but don't change the underlying reality that a password is a "single-factor" (something you know), and thus has inherent limitations to its level of security. All someone else has to do is to learn what a person's password is (no matter what approach is used to do so), and they can impersonate that person on-line.

It has also been recognized for quite some time that various multi-factor authentication (MFA) approaches could strengthen authentication significantly. But the use of MFA in Higher Education is quite minimal, and has not been growing at any significant rate. According to the Educause ECAR Research Study, Identity Management in Higher Education, 2011 report, adoption of MFA is not significantly increasing, was used in some way by less than 20% of institutions, and about 50% of institutions had no plans to use it. Why is this? We believe two key reasons are cost, and "fear, uncertainty, doubt" (FUD) around questions like the following:

- What will it cost to deploy, to operate, and to support?
- What use cases involve sufficient risk to justify its use? Do we really need it?
- How can we calculate and document the ROI and get the necessary funding?
- What MFA approach/technology should I use?
- Can it be integrated into our applications, our SSO systems, etc.?
- What applications or services should we use it for first? Which users?
- How do we even begin to plan for it?
- At what scale should we start?
- How can we support it?
- What training will be required?
- How do we explain the need to our users and earn their acceptance and support?
- How do we track and manage which MFA device is registered to each user, and what do we do if the user loses it?
- How will users authenticate if they forget one of their factors (if token, smart card, phone, any physical device involved) at home or at their office?

The intent of building the Cohortium is to provide institutions an easier way to remove the veil of FUD and answer all (or at least many) of those questions, by relying on the knowledge, experience, support, and expertise of their sister institutions and colleagues. The MFA Cohortium will build a lasting and living resource that will serve as both a knowledge-bank and a way to tap expertise from a broad spectrum of educational institutions around all topics related to utilizing MFA. And the MFA Cohortium can serve as a source of input to the efforts of Internet2, InCommon and the NET+ program to provide MFA technology options at as cheap a rate per user (or per institution) as possible.

What will participating as a member of the MFA Cohortium gain my institution?

- Increased capability to deploy stronger authentication within your institution, with well-informed and tested "MFA roadmaps" and a clear understanding of costs.
- Best practices for leveraging the use of MFA with federated services, while retaining options for privacy.
- Access to expertise from institutions on the forefront of deploying MFA for varied and broad use, including the three MFA pilot institutions that are core ScalePriv partners – Massachusetts Institute of Technology (MIT), University of Texas System, University of Utah.
- Learn about and from the experiences of early adopters.
- First to see any and all sample artifacts from other institutions involved. Range of materials could include: use cases, requirements, MFA technologies and integration strategies, costs and ROI, planning documents (project plans, business plans, financial models), implementation and deployment strategies, training and support plans and materials, and outreach examples (e.g. news releases, ads, videos, social marketing strategies)

- Understand and potentially influence how to effectively integrate MFA into Web Single-Signon (e.g. Shibboleth, CAS) systems, including options for identifying which individuals need to use MFA for which services, step-up authentication, and tracking which MFA device is associated with which individual.
- Influence the development of best practices for the use of MFA that both enhances security while striving to preserve appropriate privacy.
- Understand the links between privacy management, assurance levels, and MFA.
- Understand how deploying MFA can be a key component in helping your institution achieve certification for asserting higher levels of assurance.

How will the Cohortium operate?

The MFA Cohortium will serve as a hub, the "central nervous system", for campus efforts to deploy MFA for use cases of value to that institution. It will have bi-weekly meetings which will include facilitated discussions, regular presentations from early adopters and experts on their experiences and new and interesting things they are learning, and the opportunity to ask questions of all the other participants. The ScalePriv project support for the Cohortium will include supplying:

- Coordination for the overall MFA Cohortium effort, including organizing and facilitating the meetings, oversight over the web site, help with review, editing, and ingestion of documents and artifacts for the Cohortium web site as needed, meeting notes, etc.
- Private MFA Cohortium web site in which all the resources, documents, artifacts, meeting notes, and presentations will be organized and made available to all participants.
- Mailing list and calendar for supporting the MFA Cohortium work.
- Potential for arranging presentations or facilitated discussions targeted at specific audiences within one or more of the participating institutions (e. g. campus events).
- Facilitation for identifying and establishing, as needed or desired, "sub-cohorts"/working groups within the Cohortium that focus on specific MFA planning/deployment topics.

Finally, by the end of the 15-month lifetime for the MFA Cohortium, the hope and expectation is that each participating institution will have contributed to, and learned from, all of their fellow MFA Cohortium participants. That all, or at least many, of the participating institutions will be in some stage of deploying MFA. And that the Cohortium will have created a public "Higher Education MFA web site" that will become "the go-to resource" for understanding why and how to deploy MFA within one's institution.

The "Higher Education MFA web site"

During the course of the MFA Cohortium activities, a process for "promotion/release" of various documents and project artifacts to a public MFA web site will be established and followed. By the time the formal lifetime of the Cohortium ends, the intent is that this "Higher Education MFA web site" will contain answers, samples and examples for "all questions and things of interest related to the use of MFA in Higher Education". See the The "Higher Education MFA website" page for a detailed list of the intended content for this new resource.