What Deploying MFA Taught Us About Changing Infrastructure

Abe Singer
National Energy Research Scientific Computing Center (NERSC)
abe@lbl.gov

Shane Canon
National Energy Research Scientific Computing Center (NERSC)
scanon@lbl.gov

Rebecca Hartman-Baker
National Energy Research Scientific Computing Center (NERSC)
rjhartmanbaker@lbl.gov

Kelly L. Rowland
National Energy Research Scientific Computing Center (NERSC)
kellyrowland@lbl.gov

David Skinner
National Energy Research Scientific Computing Center (NERSC)
deskinner@lbl.gov

Craig Lant
National Energy Research Scientific Computing Center (NERSC)
clant@lbl.gov

ABSTRACT

NERSC is not the first organization to implement multi-factor authentication (MFA) for its users. We had seen multiple talks by other supercomputing facilities who had deployed MFA, but as we planned and deployed our MFA implementation, we found that nobody had talked about the more interesting and difficult challenges, which were largely social rather than technical. Our MFA deployment was a success, but, more importantly, much of what we learned could apply to any infrastructure change. Additionally, we developed the sshproxy service, a key piece of infrastructure technology that lessens user and staff burden and has made our MFA implementation more amenable to scientific workflows. We found great value in using robust open-source components where we could and developing tailored solutions where necessary.

CCS CONCEPTS

• **Security and privacy** → **Social aspects of security and privacy**; **Usability in security and privacy**; • **General and reference** → General conference proceedings.

KEYWORDS

multi-factor authentication, MFA, infrastructure

ACM Reference Format:
Abe Singer, Shane Canon, Rebecca Hartman-Baker, Kelly L. Rowland, David Skinner, and Craig Lant. 2019. What Deploying MFA Taught Us About Changing Infrastructure. In *Proceedings of The International Conference for High Performance Computing, Networking, Storage, and Analysis (SC19).* ACM, New York, NY, USA, 8 pages. https://doi.org/10.1145/xxxxxxx.yyyyyyy

1 INTRODUCTION

The National Energy Research Scientific Computing Center (NERSC) is the primary scientific computing facility for the Office of Science in the U.S. Department of Energy, located at Lawrence Berkeley National Laboratory (LBNL). More than 7,000 scientists use NERSC to perform basic scientific research across a wide range of disciplines, including climate modeling, research into new materials, simulations of the early universe, analysis of data from high energy physics experiments, investigations of protein structure, and a host of other scientific endeavors. In 2018, NERSC introduced multi-factor authentication (MFA) to users; use of MFA at NERSC became mandatory in early 2019. In this paper, we describe the constraints under which we chose to implement MFA, the challenges encountered in the process, solutions we found to those challenges, and other technical points of interest generated along the way. Detailing this transition may be useful to other facilities where planned changes in digital infrastructure must be implemented while minimizing impact on user productivity.

The most interesting part of implementing and deploying MFA was not the technical aspects (though we did develop some innovative technology), but the social factor of getting users enrolled and using MFA. Not unlike the transition from Telnet to SSH or from one batch system to another, this digital transition is complicated by the scale and diversity of our user workloads, software and services, as well as user needs for workflow automation. The MFA transition at NERSC is useful as a point of reference in similar large-scale changes in scientific computing infrastructures.

As we were not under a formal mandate for MFA, we were not constrained by prescriptive standards, so we had the freedom to implement our solution in a manner that best supports our users' scientific needs. In the remainder of this paper, we describe the goals of the MFA project at NERSC, detail specific requirements imposed on the project by the communities supported at NERSC, present technical and social solutions that were developed through the course of the project, and conclude with a summary.

2 GOAL

The overall goal of the work described in this paper was to enhance security in how users authenticate to NERSC systems and services by requiring multiple factors while minimizing the impact on users' ability to get science done. Doing so in a scalable and supportable way across a diverse scientific workload presents challenges of a technical and social nature. MFA is not new to most of the NERSC user community in their daily lives, but its role in scientific workflows comes with requirements in need of unique solutions described below.

SC19, November 17–22, 2019, Denver, CO, USA

ACM ISBN 978-x-xxxx-xxxx-x/YY/MM…$15.00
https://doi.org/10.1145/xxxxxxx.yyyyyyy

3 REQUIREMENTS

NERSC's unique position as the primary scientific computing facility for the Office of Science means that NERSC's diverse user base performs a wide variety of different computational workflows using NERSC resources. This includes anything from simple SSH sessions where a user submits jobs by hand to elaborate, multistep, automated workflows. Because of this, first and foremost special consideration needed to be given to minimize the impact of the new MFA requirement across the spectrum of use cases. NERSC has maintained a reputation with its users for being a productive computing facility where the cybersecurity requirements are largely hidden from the users, so we could not afford to create a cumbersome process that would not accommodate automation in these special workflows.

Unlike many other HPC sites, NERSC does not require users to hop through a gateway system or connect to a VPN to access resources. This direct access model is critical for many complex workflows and users have applauded this ease of access in the past. Because of this direct access model, NERSC could not simply implement MFA on some perimeter system instead it needed to be integrated throughout the center.

Another important factor in the technologies we chose to use in the MFA project was flexibility. Any particular authentication technology could eventually have fundamental vulnerabilities discovered, or weaknesses in the underlying cryptographic algorithms (e.g., MD5, DES, etc. [2, 9]). Thus, it should be possible to change out the authentication technology, should vulnerabilities be discovered, without having to rebuild our entire authentication infrastructure; being too tightly wedded to any particular solution could leave us at the risk of having a vulnerable system that we could not change.

Further, a token is supposed to be "something that you have". As such, it is also something that you can lose. Soft-tokens, in particular, are vulnerable to the loss or destruction of data (e.g., reformatting) on the device upon which they are stored. Thus we wanted to allow users to have multiple active tokens so that they were less impacted should they e.g., lose their phone, keys, laptop.

We faced an additional complexity of supporting multiple platforms. Unlike many commercial services, our users do not log into a single application, nor are the applications all web services. We had to be able to support MFA over multiple command-line and web services, including SSH, Shibboleth/SAML-based authentication, custom web services, data transfer services, and NERSC RESTful API services. Being able to integrate MFA with single-sign-on technologies (e.g., Shibboleth, Kerberos) was also desirable.

Any additional steps users have to take to enroll and use our systems are an increase in complexity. With increased complexity come increased support calls. We wanted to avoid users overloading our support staff just because they couldn't get MFA to work. Additionally, we wanted to keep the overall support costs down, for both staff as well as equipment, licenses, etc.

Finally, as one of the largest American HPC centers, NERSC is a high-profile target for hackers worldwide. NERSC systems are continuously under attack and NERSC already devotes extensive efforts to security. We did not want to entrust third-party vendors with secrets such as OTP seeds or depend on a third party for a trusted path to authentication as this would increase the risk of third-party hacks compromising our systems.

4 SOLUTION AND APPROACH

4.1 Design of MFA Implementation

When designing the MFA implementation, NERSC carefully considered measures to increase the ease of use and minimize impact on users. Of particular interest were means that could also minimize additional burden to NERSC staff.

4.1.1 Early Implementation Design and User Testing. As NERSC embarked on the process of implementing and deploying MFA for its users, we first evaluated different options and performed user testing with early prototypes. NERSC reviewed the solutions at other large HPC centers and spoke to staff from those centers to hear about their experiences. NERSC also spoke to users who had experience with using these other facilities. This helped us identify a few candidate solutions to consider. Some of these solutions were then tested by NERSC staff and evaluated on ease of use, ease of integration, cost, and support overhead.

NERSC conducted a series of user testing exercises prior to finalizing the implementation choices. NERSC had approximately 60 users, consisting of both staff and user volunteers, work through the process of registering a token and using MFA in their regular routine. This prototype was not fully integrated with the account management system so didn't cover the full user experience, but it gave us feedback that both helped us solidify the technology choices and helped us identify typical issues encountered by users. It also helped in identifying workflows or use cases that were particularly problematic with MFA. For example, we realized that some web logins used the same authentication password to authenticate to multiple backend services, which would break under MFA.

4.1.2 User Experience Implementation Design. Among the design goals of the MFA infrastructure was to make the user experience as positive as possible and to minimize the load on support staff. To this end, instead of requiring a hard token, NERSC chose free, software-based, one-time password authenticators [5] that users can download and install themselves. This method is based on an open standard and is implemented by multiple clients supported on a variety of platforms. NERSC added features to NIM, the NERSC identity management system, to allow users to provision their authenticator. Thus users were able to install and configure MFA for their account without an incremental cost to support staff time.

Most NERSC users have access to a smartphone, so the primary authenticator NERSC selected for users is Google Authenticator [1], which can be installed on most smartphones. Some users were unable to use a smartphone in the secure environment of their workspace, or had a physical disability that prevented them from using a smartphone in this manner. For these users, NERSC added support for the Authy free authenticator [8], which is available for Windows and MacOS and also as a Google Chrome browser plug-in. The majority of users were able to avail themselves of at least one of these options, but some chose other options such as OnePass or Firefox plugins without NERSC support.

The majority of users set up an authentication token on their smartphone. A typical consumer changes devices at least every

couple of years, potentially resulting in the user no longer being able to access NERSC resources. Without an easy way for users to manage their authentication tokens, including a way to recover after losing access to a phone or accidentally removing an active token, users might be unable to work and would require extensive staff assistance. To address circumstances in which a user loses access to all of their active tokens, for whatever reason, NERSC developed a means for users to completely remove all tokens from their account, then log in (without MFA) to NIM to set up a new token.

In addition, NERSC wanted to make it possible for users whose tokens were not immediately available to be able to work. For this purpose, NERSC developed the capability within NIM for users to provision back-up one-time passwords that a user could print and store in a safe place (e.g., wallet, locked drawer) to be used in the event of an emergency.

4.1.3 Infrastructure Design. Figure 1 shows a diagram of the MFA system at NERSC. Because an MFA system is inherently more complex and potentially more fragile than conventional single-password authentication, another design goal of the MFA infrastructure was to ensure that users would not be impacted by authentication failures due to maintenance or outages on the infrastructure itself. NERSC operational staff built in redundancy, monitoring, and emergency controls to mitigate this risk. First, the MFA infrastructure was built with a redundant "shared-nothing" design, enabling components to fail or be taken offline for maintenance non-disruptively. Then, a complete suite of real-time checks were added to NERSC's center-wide monitoring framework that continuously exercise the MFA backend, performing authentication on frequent intervals and producing alerts for Operations to dispatch to staff. As a last resort, the system was designed with a "kill switch" capability that can be quickly activated by Operations to temporarily deactivate the token authentication subsystem during a loss of service. The redundancy, monitoring, and "kill switch" features of the MFA infrastructure have all been used since launch to prevent, detect, and respond to events that would have otherwise impacted users.

The core component of NERSC's MFA design is LinOTP. LinOTP is an open-source, one-time password authentication server [3] with a variety of features that were well-aligned with NERSC's requirements. LinOTP supports numerous simultaneous authentication methods, providing us with flexibility both in options we were able to provide to our users, plus the ability to make changes should a vulnerability be discovered in the method in use. The software also supports token provisioning and management, and an API for integrating those features into existing infrastructure. Those features greatly reduced the effort required for building the token infrastructure. As an added bonus, we were able to leverage an existing LinOTP server run by the central IT department at LBNL.

NERSC was concerned that the external LinOTP server could create a potential risk of disruption in service if there were issues with the LinOTP service or connectivity issues. To address this, NERSC developed an intermediate service, OTPProxy, that sits between the clients and the LinOTP service. This service performs the LDAP authentication portion of MFA and then sends the one-time password portion to the LinOTP service. If the proxy is set in a "fail-open" mode and detects an error in the response, such as a connection error, it can ignore the OTP portion and still permit the login. This approach also helps prevent cases where the user gets locked out of their account because of too many failed attempts due to an issue in the OTP server. This also provides a single place in which we can temporarily disable the OTP check without having to push out any changes to the clients. NERSC has used this feature when the LinOTP service has scheduled maintenance; users continue to authenticate with the password plus one-time password, but are unaware that only the password is being checked. The prompt and user action is the same during the failure event. This is advantageous for the user as they do not need to change their behavior. The OTPProxy service is not currently openly released since it is fairly specialized to our environment, but can be opened if there is interest.

Another infrastructure design goal was to minimize the impact of MFA on users' ability to conduct their research, particularly for users with complex workflows that may require data transfer into or out of NERSC. MFA by its nature impedes automated workflows, as it requires a user to enter a new password with each connection. While the MFA policy allows for exemptions to the requirement in cases where MFA would have a significant impact on a user's scientific work, NERSC wanted to minimize the number of users who had MFA exemptions. A key NERSC innovation, sshproxy, described in detail in Section 4.2.1, was instrumental to achieving this goal. sshproxy allows users to use MFA to obtain time-limited SSH keys that can be used with automated workflows. NERSC sets the time limits based on the needs of the particular user or project, with a default limit of one day.

As the implementation became usable, initial testing was conducted on small groups of NERSC staff, followed by voluntary testing by friendly user teams, and finally extending to a system-wide deployment. During this process NERSC was able to refine the implementation based on user feedback. For example, in addition to the option of scanning a QR code, we added support for manually typing the shared seed into an authentication app.

4.2 Automation and Operations

4.2.1 sshproxy. As noted above in Section 2, a key concern in the move to MFA was minimizing the impact to users and ensuring that automated workflows continued to function. A number of projects rely on NERSC to provide automated analysis of data coming from various instruments and detectors. Many of these use cases are tied to other user facilities that have their own set of users and metrics, and changes in NERSC's policies can impact these facilities. Many of these automated use cases were already using SSH as the underlying method to transfer data and trigger the execution of analysis pipelines. Clearly, requiring a user to enter a one-time password for each of these operations was not feasible. Additionally, many users will log into NERSC system many times a day and requiring them to enter their one-time password each time impacts their productivity.

NERSC required a solution that would allow users and robot accounts to access systems via SSH but with strict controls on the lifetime of the access and other limits. NERSC developed a RESTful-based service called sshproxy to generate and maintain SSH keys

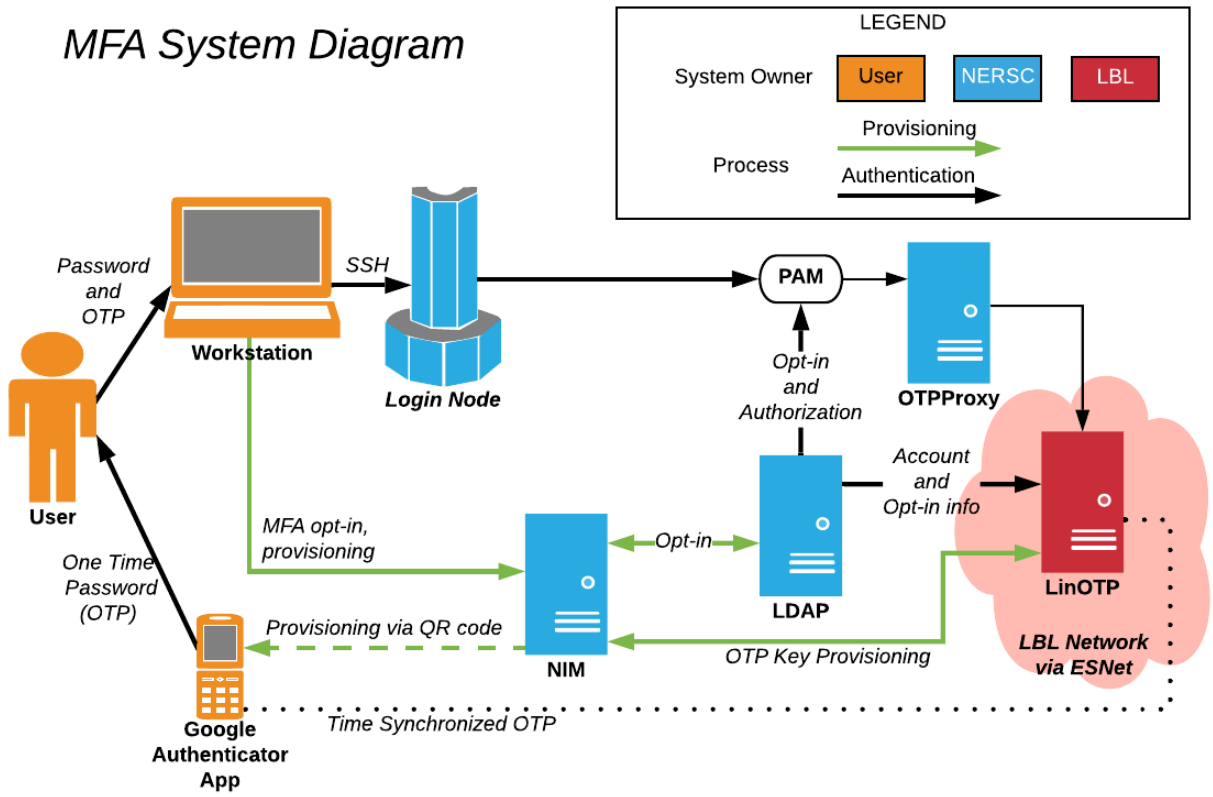

Figure 1: NERSC MFA system architecture.

to help meet these requirements. This allows a user to generate a long-lived key that can be used in automated workflow for an extended period of time (potentially up to a year). The user only needs to authenticate with their password and token when they generate the key. The sshproxy architecture is shown in Figure 2. Workflows that already relied on SSH were able to easily convert over to using the long-lived keys without any changes to their process or workflows.

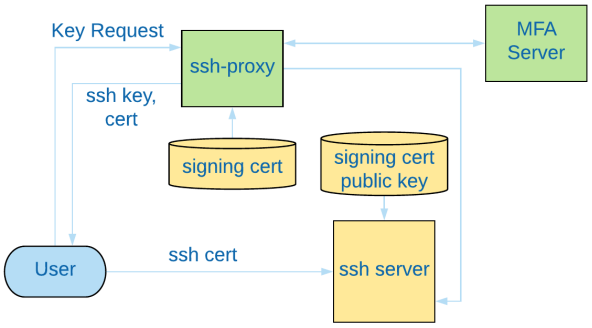

Figure 2: sshproxy architecture.

The sshproxy service works by allowing the user to authenticate using MFA to the service and generate an SSH private key and certificate [4] that can then be used to connect to NERSC systems using standard SSH clients. This request is done with a simple shell script that the user can run on their remote system. The generated key has a default lifetime of 24 hours. This lifetime is typically sufficient for most daily interactive work. For use cases that require longer lifetimes such as automated workflows, users can request the ability to generate extended life-time keys that can span from weeks to a year. In general, these longer lifetime keys require stricter limits on where the keys can be used. For example, the keys would be limited to the IP addresses of the instrument system in a given scientific workflow.

Since sshproxy greatly enhances the usability of the MFA system, it was important that it could be used on various OS platforms and SSH clients. The service can generate keys that can be used by OpenSSH clients, SSH client libraries and many Windows-based SSH clients such as PuTTY. It has been tested with Windows, OSX, and Linux. While the service can generate signed certificates that are honored by NERSC systems, the service also supports a fallback mechanism for older clients that may not support these certificates. This fallback mechanism makes use of OpenSSH's *AuthorizedKeysCommand* which allows the server to run an executable to get the list of valid authorized keys. In our case, this script makes

a request to the sshproxy service to get the list of currently active keys for the user. The service can also generate keys to access "collaboration accounts" which are shared accounts primarily used by large collaborations and projects. In this case, the user authenticates using their personal account and MFA credentials, but the generated key maps to the collaboration account.

An alternative to sshproxy is to use OpenSSH's built-in *ControlMaster* functionality [6], which allows multiple sessions to reuse a connection. The main disadvantage of this approach is that once the control connection is severed (e.g., a network issue, login node reboot, etc.), the session must be reauthenticated. So, this is less useful for automated workflows or even laptop access where the network connection may change.

The sshproxy service has become a key component of the overall NERSC MFA architecture. The software has been approved for public release and NERSC is planning to make it public in the near future, hopefully by the end of 2019.

4.2.2 Host-based Authentication. Another important usability component is making sure NERSC users are not required to re-authenticate once they are inside the NERSC domain (e.g., SSH from one NERSC system to another). NERSC implemented host-based access to address this. However, one challenge in using SSH host-based authentication is managing and propagating keys. NERSC utilized another feature of SSH certificates [7] which allows the target system to be configured with a signing authority that can be used to validate a signed host key. NERSC maintains a well-protected signing host that is used to generate certificates for the various NERSC systems. The client systems are then configured to present this certificate as part of the host-based authentication exchange. The key advantage of this approach is that if new hosts are added or host keys need to be regenerated, the new keys can be signed and configured on the client system and no additional changes are required on the target systems.

4.2.3 Exemptions and Edge Cases. While the combination of the sshproxy service and host-based authentication has addressed most use cases, some examples have emerged that still require further work. For example, one project has a series of remote sensing devices that are extremely difficult to access and update. NERSC has an MFA exemption process to ensure these projects can continue to function and is working to further enhance the sshproxy tool to address these edge cases.

4.3 Social Aspects

With a point-in-time deadline for users to switch to using MFA, NERSC was concerned about the impact on support staff should the thousands of NERSC users wait until the deadline and then enroll in MFA all at once. To minimize this impact, NERSC set a goal of having 1,000 existing users enrolled by the end of December 2018. This goal not only served to reduce the number of users enrolling at once, but to help NERSC identify and correct any issues with the enrollment process ahead of the deadline.

Figure 3 shows the number of NERSC users enrolled in MFA over 2018; key points spurring MFA uptake are annotated on the plot. To meet and eventually exceed our goal of 1,000 users enrolled in MFA by January 2019, we took a multi-pronged approach to user communications which included personalized messages, targeted engagements, and open office hours. Appendix A provides detail regarding the various user communications, including the texts of emails sent out to NERSC users and links to NERSC publications promoting early adoption of MFA.

NERSC conducted an extensive communications campaign along several fronts. The User Engagement Group (UEG) developed thorough, clear documentation for users on how to enroll and use MFA. The campaign to inform users of the plan kicked off in August 2018 with an announcement by the NERSC Director that MFA would become mandatory in the new allocation year. Over the following months, department heads sent memos to users encouraging enrollment and testifying to the ease of use (see Section A.1), and NERSC published profiles on the NERSC website of users who had successfully transitioned to using MFA, which included a discussion of their research and the minimal impact of MFA on their workflows (see Section A.4). In November and December 2018, UEG reached out to projects with high usage and low MFA enrollment, encouraging them to enroll before the deadline and offering help if there were any questions. UEG included reminders and announcements of new features in the NERSC weekly newsletter, and MFA was the topic for three of the weekly podcasts. Finally, UEG held several rounds of virtual "office hours" where support staff spent the day online in a video conference room, and users could dial in and ask questions.

Emails from NERSC management resulted in upticks in adoption of MFA, and as the deadline approached, many users embraced the inevitable and signed up. Most users were able to transition to MFA without NERSC assistance, but we helped more than 100 users during the office hours in the final days before and immediately following the deadline. Many of these users experienced minor difficulties with creating and installing an MFA token; staff who were familiar with the process were able to successfully guide users through the initial setup process. In some individual cases where a user was not able to use a smartphone for MFA, NERSC staff assisted the users in finding solutions that were suited to their environment.

5 SUMMARY

NERSC successfully deployed a new MFA system over a 12-month period, converting the majority of its users to using MFA for authentication by the beginning of the new allocation year. Through the process of implementing and deploying MFA, NERSC staff took home a variety of lessons from the project. First, the social factors of the technologies are just as important as their technical merits. To implement a change of this magnitude, high-quality, frequent communication with users is crucial. Second, technology choices that minimize the additional load on staff and users alike are essential. We found great value in using robust open-source components, such as LinOTP, where we could and developing tailored solutions like sshproxy where necessary. Finally, implementing a new technology should minimize changes in users' daily routines. If the burden of a new requirement is too high, users will look for ways to circumvent it. Thus, we introduced the NERSC sshproxy service to lessen both user and staff burden and better enable scientific computing workflows.

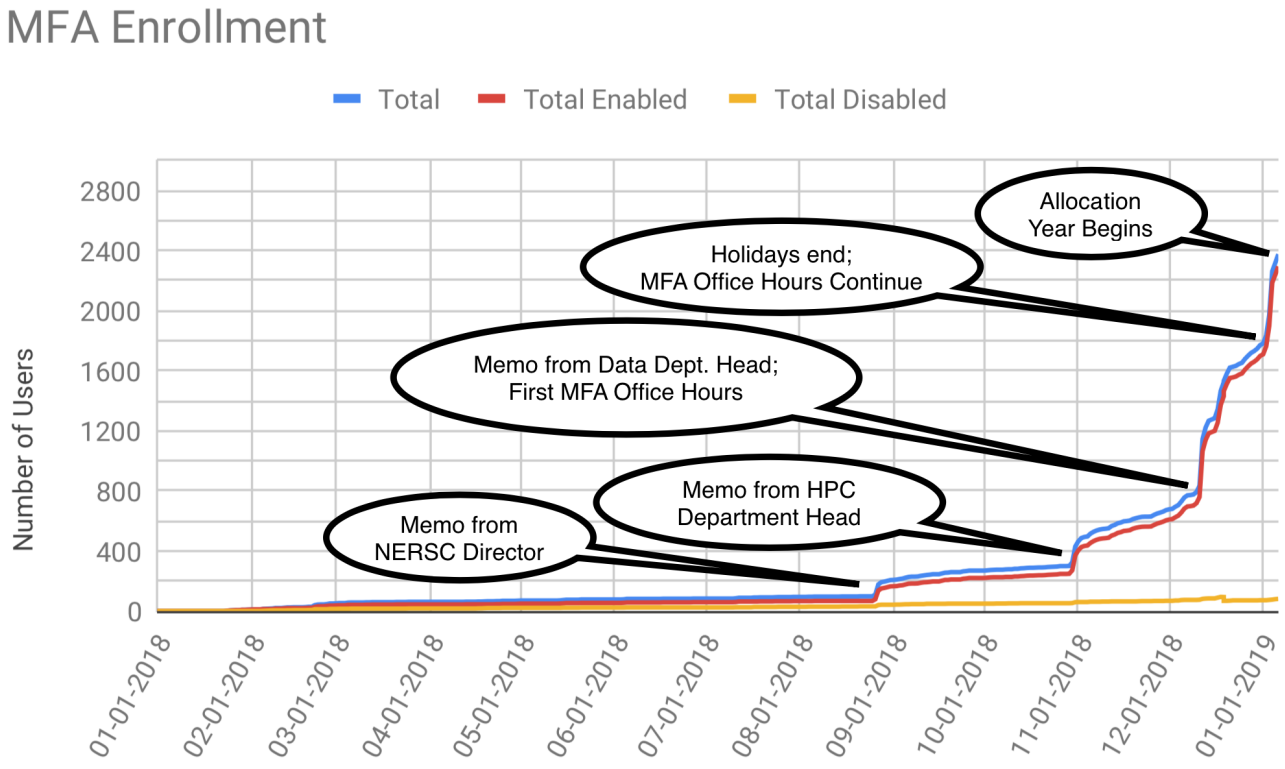

Figure 3: User enrollment in MFA in 2018, from initial rollout to mandatory requirement.

REFERENCES

[1] Wikipedia contributors. 2019. Google Authenticator. https://en.wikipedia.org/wiki/Google_Authenticator

[2] Whitfield Diffie and Martin E Hellman. 1977. Special feature exhaustive cryptanalysis of the NBS data encryption standard. *Computer* 10, 6 (1977), 74–84.

[3] KeyIdentity GmbH. 2019. LinOTP. https://www.linotp.org/

[4] Thomas Habets. 2011. OpenSSH certificates. https://blog.habets.se/2011/07/OpenSSH-certificates.html

[5] David M'Raihi, Salah Machani, Mingliang Pei, and Johan Rydell. 2011. Totp: Time-based one-time password algorithm. *Internet Request for Comments* (2011).

[6] OpenSSH. 2004. OpenSSH 3.9 Release Notes. https://www.openssh.com/txt/release-3.9

[7] Inc. Red Hat. 2019. *Creating SSH CA Certificate Signing Keys.* https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/6/html/deployment_guide/sec-creating_ssh_ca_certificate_signing-keys

[8] Inc. Twilio. 2019. Authy. https://authy.com/

[9] Tao Xie, Fanbao Liu, and Dengguo Feng. 2013. Fast Collision Attack on MD5. *IACR Cryptology ePrint Archive* 2013 (2013), 170.

A COMMUNICATIONS TO USERS ABOUT MFA

NERSC used many different avenues of communication to reach out to users about the impending transition to MFA. In this appendix, we detail some of those communications.

A.1 Email Communications

NERSC launched an aggressive communications campaign over email to encourage users to adopt MFA. Regular communication about MFA was included in the NERSC weekly email, and NERSC user engagement staff also enlisted the help of upper management in communicating the importance of the transition to MFA. Staff wrote memos that leadership adapted to their writing style and sent to users.

A.1.1 Email from NERSC Director. NERSC director Sudip Dosanjh kicked off the MFA campaign on August 26, 2018 with this email to users letting them know that MFA would become mandatory in the new allocation year.

Dear NERSC Users,

I'm writing to communicate an upcoming change in how user accounts will be authenticated at NERSC. As you may know, NERSC currently supports multi-factor authentication (MFA) for user accounts on a voluntary basis. Starting in the 2019 allocation year, NERSC will require MFA for accessing NERSC systems in the majority of cases. To prepare for this change, we encourage you to start testing MFA now (see this help page to see how to use MFA).

I have authorized this policy change to protect the integrity of your data, accounts, and allocations and to align NERSC with best practices in HPC and the online world in general. MFA provides greater protection against phishing and other modern threats to your digital security. NERSC makes security largely transparent to users, but we need your help to ensure there is not unauthorized access to your account and data.

NERSC experts have been working hard to implement MFA in ways that minimally impacts how you work at NERSC. For example, we've created technologies that allow you to authenticate with

MFA only once per day as well as incorporate MFA into automated workflows. The policy also allows for longer periods of single sign-on access, or opting-out of MFA where reasonably justified. You can read more about how this works here.

In the next few weeks you will receive communications from our Security and User Engagement staff with pointers to additional information about transitioning to MFA across all NERSC resources. I encourage you to pay attention to these communications and try MFA well before the new allocation year begins. And of course, NERSC staff are always happy to answer any questions or help troubleshoot issues at https://help.nersc.gov .

Thanks for your help as we build a more secure infrastructure for you!

Best regards,
Sudip

A.1.2 HPC Department Head Email. HPC Department Head Richard Gerber sent the following message to users on October 30, 2018.

Dear NERSC users,

I'm writing to encourage you to start using Multi-Factor Authentication (MFA) on your NERSC account now, ahead of January 8, 2019 when MFA will be required for most accounts. MFA helps protect your account and your data from unauthorized access and also enhances the security environment on NERSC systems for everybody.

MFA is pretty easy to set up and use as documented on the NERSC MFA web page. I was able to enable it quickly for my account and then I used NERSC's innovative sshproxy service that allows me to enter my token only once per day. This works great for interactive SSH connections, but if your workflow involves other ways of accessing NERSC you may need to make additional changes. We believe we have solutions for most use cases, but we want to work with you now to make sure you're set before January. Please contact us with your questions via help.nersc.gov.

Please consider joining the NERSC User Group webinar this Thursday at 11 a.m. Pacific Time. The meeting will will include a presentation on how to use MFA at NERSC.

Thank you for your assistance in helping keep your data and NERSC secure.

Regards,
Richard Gerber

A.1.3 Email from Data Department Head. Data Department Head Katie Antypas sent the following note to NERSC users on December 12, 2018.

Dear NERSC Users,

Perhaps, like me, you've put off enabling Multi-Factor Authentication (MFA) for your NERSC account until the last possible moment. Well that time is approaching, and yesterday I decided that I too should bite the bullet and enable MFA. And it really wasn't hard!! I strongly encourage you to enable MFA now, so that if you do have any issues you will have time to get your questions answered before MFA becomes required on January 8, 2019.

To provide some hard data to the NERSC user community I timed myself while setting it up. I'm not super fast at these things and even including a few urgent Slack messages and an inbound photo text of my cute nieces, I still managed to set up MFA in 13 minutes. I wanted to set up sshproxy keys so I would only have to enter my one-time-password one time per day, and I managed to get that enabled in an additional 7 minutes.

If you'd like to have some help, the NERSC consultants will be holding MFA "office hours" each week through January 8 (excepting the holidays). During those times you can join a zoom session where several people will be available in real-time to help you get set up. The dates for the office hours are December 17th, January 4, and January 7, 8, and 9. For more information on office hours please see https://www.nersc.gov/users/announcements/featured-announcements/mfa-office-hours-in-december-and-january/

On January 8th, if you have not enabled MFA, you will not be able to login into NERSC resources until you log into NIM and set up at least one MFA token.

NERSC is committed to making MFA work with the many diverse use cases and workflows of our users. We have enabled and developed several technologies to minimize how often you need to use MFA. And for those who have long-lived workflows, we can give you the ability to get sshproxy keys that last longer than a day.

As noted above, setting up MFA is pretty easy. The basic steps are:

(1) Install the Google Authenticator app on your mobile device.
(2) Login to NIM enable MFA
(3) Create your One-Time Password token in NIM.
(4) Scan the QR code presented using the Google Authenticator App.
(5) You're done!

For detail instructions, example, and more, please see our MFA documentation at https://www.nersc.gov/users/connecting-to-nersc/mfa

A.2 Outreach through the NERSC User Group

The NERSC User Group (NUG) monthly webinar was another venue where we exposed users to MFA. The September 20, 2018 webinar included a discussion of NERSC's plans for the new allocation year and how to use sshproxy. (URL: https://www.nersc.gov/assets/Uploads/NUG-Webinar-20180920.pdf) The November 1, 2018 webinar drew more participants than usual because it included the announcement of NERSC's new Perlmutter system, so we took advantage of the extra attention to also include a section about using MFA for web and SSH clients (including using sshproxy). (URL: https://www.nersc.gov/assets/Uploads/2018-11-01-NUG-MFA-Presentation.pdf)

A.3 "NERSC User News" Podcasts

The weekly "NERSC User News" podcast (URL: https://anchor.fm/nersc-news) featured three episodes with NERSC security engineer Abe Singer:

- MFA (May 2018) An overview of what MFA is and what we're doing at NERSC (URL: https://anchor.fm/nersc-news/episodes/MFA--Abe-Singer-Interview-e1fied/a-a3g5ba)
- Latest MFA Developments (September 2018) Introducing sshproxy and answering common user questions about MFA (URL: https://anchor.fm/nersc-news/episodes/Latest-MFA-Developments-at-NERSC--Abe-Singer-Interview-e288uq)
- Multi-Factor Authentication at NERSC (November 2018) Plans for further MFA developments and what happens

in the new allocation year when MFA becomes mandatory (URL: https://anchor.fm/nersc-news/episodes/Multi-Factor-Authentication-at-NERSC--Aber-Interview-e2kmad)

A.4 NERSC Center News Publications

In December 2018 and January 2019, NERSC published interviews with two users about their experiences incorporating MFA into their workflows. The December 2018 posting featured a testimonial from a user who voluntarily enrolled in MFA at NERSC before it was made mandatory (URL: https://www.nersc.gov/news-publications/nersc-news/nersc-center-news/2018/nersc-users-begin-implementing-mfa-for-higher-security-access-to-cori/) and how their use of the sshproxy service made the MFA transition minimally disruptive. The post from January 2019 (URL: https://www.nersc.gov/news-publications/nersc-news/nersc-center-news/2019/nersc-adds-new-layer-of-security-with-mfa-authentication/) discusses a data analysis workflow and how introducing MFA did not interrupt the process. The two users interviewed have different workflows but were both able to successfully incorporate MFA into their scientific processes; the publications were intended to demonstrate to the larger user community the ease of use of MFA.