pennsylvania
OFFICE OF ADMINISTRATION

Title:

Risk Based Multifactor Authentication

Category:

CyberSecurity

State:

Pennsylvania

Contact:

John MacMillan,
Chief Information Officer
Commonwealth of Pennsylvania
jmacmillan@pa.gov

Project Initiation and End Dates:

March 2016 – June 2017

Executive Summary

Many public-sector entities are steadily moving away from providing on-premise based services such as email, data storage, and collaboration and instead moving to a cloud-based X-as-a-Service model. These service transformations look to create efficiencies in government operations and meet business demands through:

- Cost reduction via reduced on-site system footprints, reduced capital expenditures and support costs
- Agility to meet short or long-term capacity changes in line with business needs
- Achievement of economies of scale

The move away from an on-premise service model located in data centers (under the control of Commonwealth staff) to locations outside the network designed to be reachable via the Internet bring with it obvious security concerns. The service or data is now, by nature, available from anywhere around the world and not just from within the Commonwealth's protected network. In turn, the risks related to improper or unauthorized access by hacked or compromised user accounts are elevated. Furthermore, remote access into systems internal to our agencies and data centers to accommodate teleworking and continuity of government efforts is similarly at risk from such improper or unauthorized access. Even within our "protected" networks, administrative-level or privileged access to servers, databases, networking components, etc. is an inherent risk and can/has resulted in large scale data breaches in both the public and private sector.

Early in 2016, the Commonwealth began to move to the Microsoft Azure cloud with One Drive and related services to meet the demands of the business. The Commonwealth of Pennsylvania's Office of Administration, Office for Information Technology (OA/OIT) recognized the need to protect the data being placed there and ensure authentication processes were strengthened. To mitigate the risks related to uncontrolled or unauthorized access to the data being placed there, OA/OIT instituted a Risk Based Multi-Factor Authentication (RBMFA) enterprise service.

The service encompasses a risk profile which considers various factors including the data or application being sought, the geographical location of the request, the nature of the device being used, and number of access attempts in a given time period. Based on this risk assessment, the system controls access with either requiring one-factor (user's ID and password) or multi-factor (user's ID and password plus an additional factor) to further authenticate the user. Various types of the second factor are available to meet various agency use cases and business needs.

The service went live at the end of June 2016. Currently serving 10,000 users, service adoption continues to grow at a feverish pace as the Commonwealth moves to integrate RBMFA into additional enterprise applications and cloud centric services. While currently only available to employees, the RBMFA service was designed with scalability in mind. The underlying architecture provides the foundational backbone to expand. Such expansion will include integration into public facing applications, providing our citizenry with enhanced security and assurance their credentials are secured. The RBMFA solution directly aligns with the governor's priority for a "Government that Works", the CIO's IT strategic plan, the National Governors Association's "Call to Action" for Governors and NASCIO State CIO Priorities for 2017.

Business Problem

The Commonwealth of Pennsylvania is entrusted with a wide variety of citizen, business, and government data, some of which is highly sensitive and/or confidential; including Social Security numbers, as well as education, employment, health, financial, and criminal records, to name a few. It offers services to its constituents which includes routine public information, licensing and registration services, health and medical benefits, financial assistance, and more.

We have a fiscal responsibility to our constituents and, in these days of fiscal restraint, we need to spend their tax dollars wisely. Keeping this in mind, the Commonwealth has begun availing itself of cloud and other X-as-a-Service offerings, both at the enterprise and at the agency level. Such offerings promise efficiencies and cost savings through economies of scale and the reduction of capital expenditures and ongoing support costs. These offerings, however, place these resources outside of the direct control of the Commonwealth, generally routing any access by Commonwealth staff to those resources through the Internet rather than through a dedicated and secured pipeline. As a result, these Commonwealth data and applications have increased the vulnerability of being compromised from improper or unauthorized access by, among other things, compromised user accounts.

Even data and applications which remain within the confines of the Commonwealth network and data centers are vulnerable to attacks by compromised accounts, particularly those workers with administrative-level or privileged user access. Such workers have the keys to the city and are an enticing target for hackers. The South Carolina Department of Revenue data breach in 2012 is a case study. In this incident, one or more workers clicked on a link in a malicious email sent to that agency and had their username and password stolen. Within one month the hackers parlayed this compromise into a breech involving the personal data of nearly 4 million individuals and 700,000 businesses and cost the state tens of millions of dollars.

Other efforts in the Commonwealth and elsewhere to reduce costs and improve workers' productivity is centered around teleworking where the worker can perform their job functions remotely from outside of the office. These efforts run the spectrum from simply being able to read and respond to emails on a Commonwealth-issued or personal smart phone to working from a remote "office" at home or other location using an office laptop or personal PC to connect to Commonwealth systems. Generally, this is through a VPN connection of one form or another which effectively extends the Commonwealth's network to the remote location. Such efforts also factor into continuity of government planning where the worker's primary worksite may not be available. Teleworking is subject to vulnerabilities such as hacked or compromised user accounts as well as compromised devices (particularly BYOD or lost/stolen devices).

In early 2016 as the enterprise and agencies began planning to utilize the Microsoft Azure cloud and its One Drive offering for cloud storage and file sharing, OA/OIT evaluated the security risks involved with this effort and ways to mitigate them. As part of this effort, the OA/OIT looked at the use of multi-factor authentication (MFA) as a way to enhance the traditional login process of username and password. MFA consists of three types of authentication factors:

- Something you know (e.g. username and password)
- Something you have (e.g. a software or physical token)

- Something you are (e.g. fingerprint)

The OA/OIT set out to determine requirements for an enterprise MFA solution including:

- Cost effectiveness
- User acceptance and ease of use
- High availability
- Applicable to multiple types of devices including smartphones and PCs
- Extensible to about 90,000 employees and contractors
- Extensible to applications and systems beyond Microsoft Azure.
- An architecture extensible to expand use to 9 million Commonwealth citizens
- Supports 2-factor authentication (i.e. username and password PLUS “something you have”)
- Intelligent enough to determine the need to invoke MFA based on multiple configurable risk-based factors

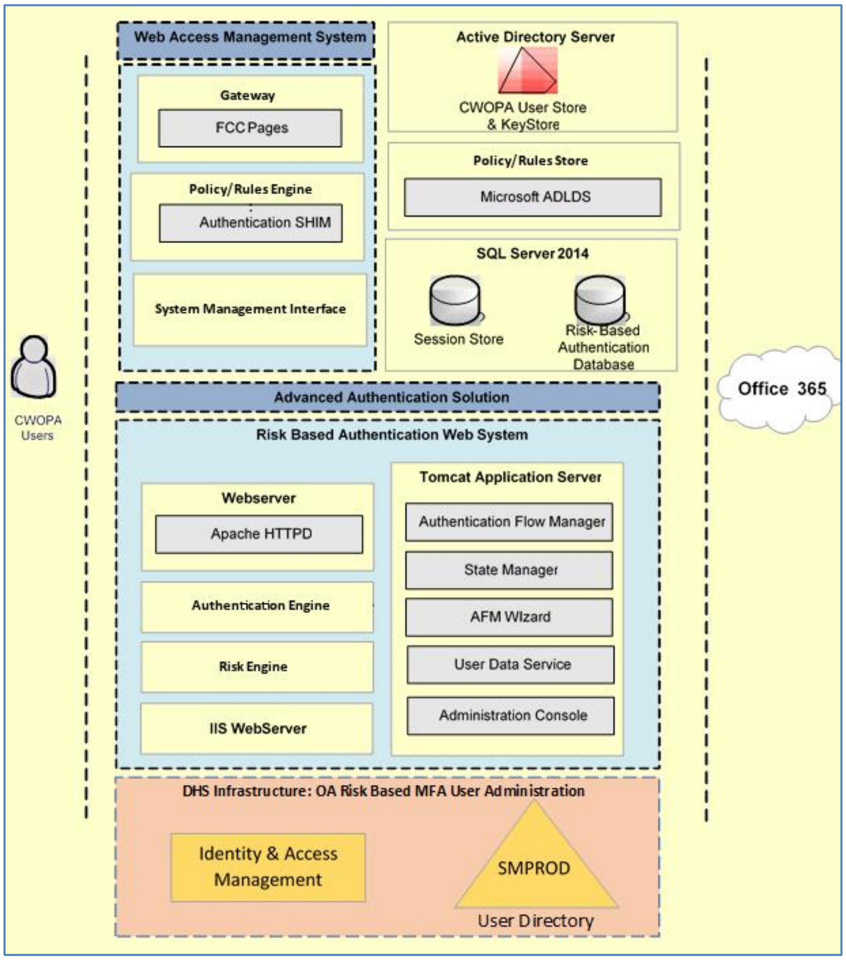
The Pennsylvania Department of Human Services (DHS) was in the process of instituting an MFA solution for their employees’ and business partners’ access to critical business applications. They shared their research data with the OA/OIT and it was determined that their chosen solution would also meet the requirements for an enterprise solution. Based on this, the OA/OIT developed and deployed an enterprise Risk-Based Multi-Factor Authentication (RBMFA) solution for use by all agencies. In doing so, it shared infrastructure and support functions with DHS to realize economies of scale. The RBMFA system went live in late June 2016 and is in use by all Commonwealth agencies residing on the state network.

Concept

In developing the Pennsylvania RBMFA system, OA/OIT chose to build upon foundational work done by DHS, including its selection of a software vendor’s product. It was decided to use a 2-factor form of MFA with the first factor being the worker’s username and password and the second being a software token placed on the worker’s device of choice – whether provided by the Commonwealth or a BYOD personal device. Once installed on a trusted device (e.g. a Commonwealth-issued or private PC), the software token was to be unlocked for each use by entering a preset PIN. In the case of an untrusted device (e.g. first time use or a public PC), the token would be unlocked by either correctly answering registered challenge/response questions or via providing a one-time code sent to an SMS text to a registered smart phone. In either case the preregistered PIN is also required. MFA was not to be evoked for access from Commonwealth devices connected to the Commonwealth’s network, but required for BYOD or access from any device located outside of the Commonwealth’s network.

The figure on the following page depicts a high-level overview of the architecture for the RBMFA system. The Risk Authentication system evaluates the user and his or her access attempt based on several criteria including what resource are they trying to access, where they are coming from, and what device is being used for the access. Based on such criteria, the system determines to invoke MFA or not.

A worker needing to access a resource protected by RBMFA is required to pre-register for the system in advance, from a Commonwealth device located on the Commonwealth's network. In this process, the worker is authenticated against the enterprise active directory and is prompted to set up their challenge/response questions and permanent PIN.


Web Access Management System
Gateway
FCC Pages
Policy/Rules Engine
Authentication SHIM
System Management Interface
Active Directory Server
CWOPA User Store & KeyStore
Policy/Rules Store
Microsoft ADLDS
SQL Server 2014
Session Store
Risk-Based Authentication Database
CWOPA Users
Office 365
Advanced Authentication Solution
Risk Based Authentication Web System
Webserver
Apache HTTPD
Authentication Engine
Risk Engine
IIS WebServer
Tomcat Application Server
Authentication Flow Manager
State Manager
AFM WIzard
User Data Service
Administration Console
DHS Infrastructure: OA Risk Based MFA User Administration
Identity & Access Management
SMPROD
User Directory

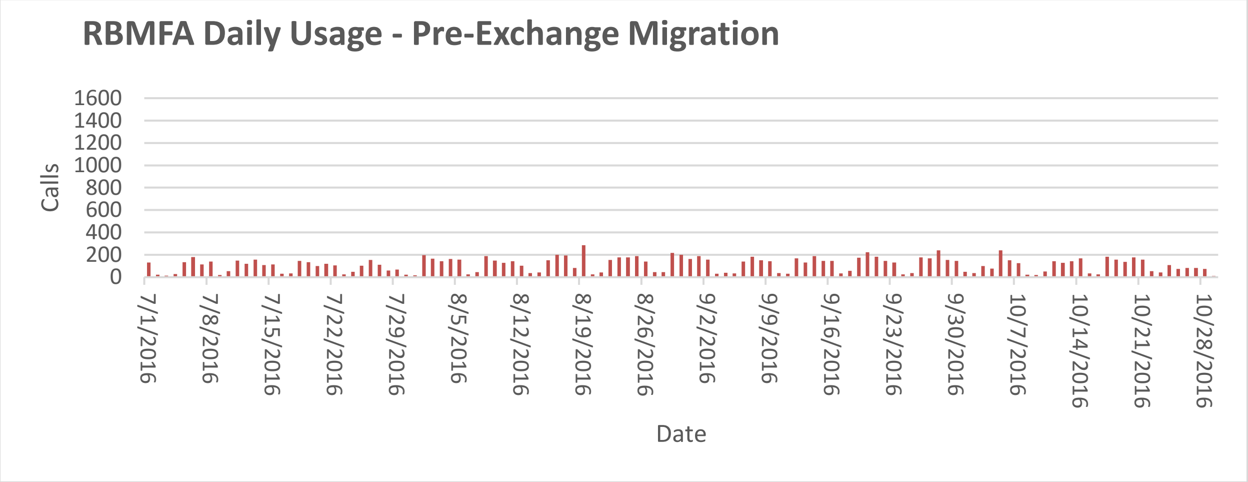
Once the user is registered, he is given the option of registering the current device as either trusted or not. If trusted, the software token is installed on the device and locked by the user's PIN and the device is registered with the system.

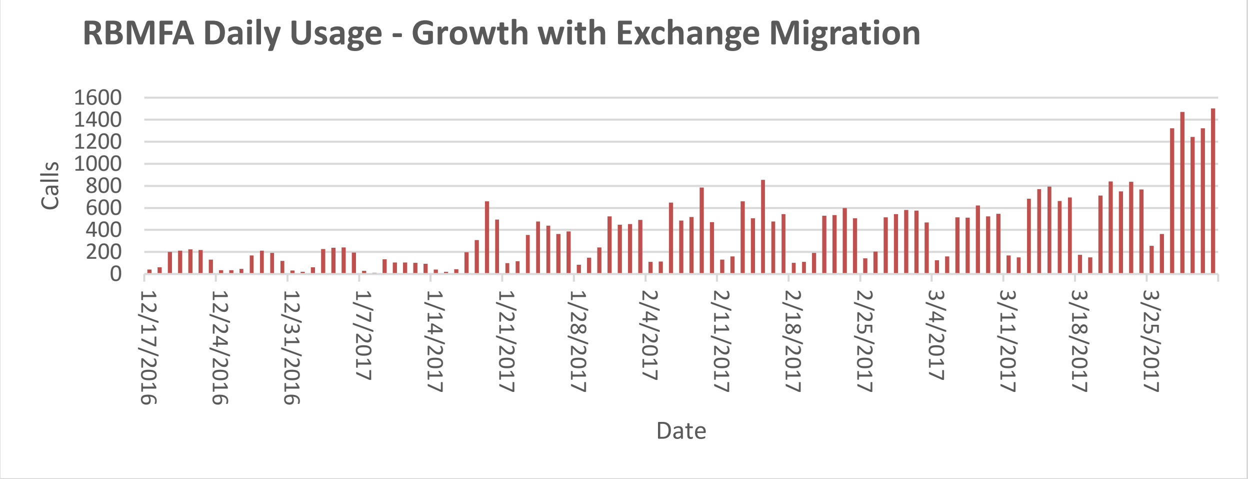
Subsequently, if the user attempts to access a protected resource from a new device or an untrusted one, the user is prompted to register it with either challenge/response or an SMS text to a registered phone. In addition, the user's PIN is required and the user is prompted to declare the device as trusted or not. Once registered as a trusted device, the user's PIN is sufficient to unlock the software token if MFA is required.

Significance

The RBMFA system was rolled out in production at the end of June 2016. The first application of the system was to protect the use of Microsoft Azure OneDrive. We saw fairy constant usage of the new system. In the latter part of 2016, the Commonwealth began testing a migration of its

Exchange email system to Microsoft's cloud offering in lieu of on premise Exchange servers. Since we officially began the staged migration of agencies mid-January 2017, we have seen a dramatic rise in the use of the solution. As of the end of March 2017, we have about 6900 registered users of the system. By the end of the Exchange migration, we expect to exceed 50,000 registered users. The following shows the growth in the usage of the MFA solution





By implementing the RBMFA solution, we have enabled the migration of our Exchange system to Microsoft Azure and raised the overall security posture of the Commonwealth. We are looking at further integrations as well, including our VPN system, privileged user access, as well as additional systems that are in the cloud or are planned to be migrated there. The cost of a single stolen credential, for example through a phishing attack, can cost the taxpayers a significant amount.

Impact

While we are still in the process expanding the use of the RBMFA system, we are already seeing benefits from it. Benefits include:

- Enhanced security
    - Protects constituents' data stored in the cloud from unauthorized or fraudulent

access

  - Enables the secure remote access to Commonwealth email from a variety of Commonwealth-issued or personal devices
  - Enables compliance with regulatory or legislative requirements
- Cost savings
  - Provides a reusable solution that can be applied to other systems and applications where an enhanced level of authentication is required
  - Faster development lifecycle with reusable components
  - Centralized service not needing to be duplicated across the agencies
  - Enablement of cloud services with resulting costs savings
  - Cost avoidance from enhanced security thereby lessening the chances of a potentially expensive breach
  - Reduction in need for help desk calls
- Improved user experience and acceptance
  - Utilization of a common security system across multiple systems and applications
  - No need for the user to carry a hardware token

By providing a single, enterprise-wide system, we have driven down the on-going per-user cost of our MFA solution from around $15/year to about $1/year. Our first-year costs, including the initial procurements and deployment costs ran about $1M to support 64,000 staff. Our ongoing annual costs for the solution are estimated to be about $300K. At this rate, we expect to break even in our ROI during our second year of operations.

MFA was a requirement for moving our email systems to the cloud. Deployment of MFA has supported the annual savings of over $1M which will be realized by our migration of Exchange to the Microsoft cloud. The further expansion to other endpoints such as VPN will enable us to eliminate the need of costly and difficult to manage digital certificates and other such “tokens” in favor of a system that is in place and reusable.

The RBMFA solution will be the foundation for secure citizen access to Commonwealth applications and resources. This will enable our efforts to allow citizens to enroll and use their social media accounts to access applications conveniently and securely, furthering Governor Tom Wolf’s three key priorities – Jobs that Pay, Schools that Teach, and Government that Works – by providing our citizenry with enhanced security and assurance their credentials are secured.

And from a pure risk mitigation perspective, RBMFA is an important control which lessens the risks associated with compromised user accounts through phishing attacks. Based on recent data breaches in the news, authenticated credentials have been used in some of the most successful and costly attacks on state governments. With the added controls the RBMFA service provides, the risk from these types of attacks are significantly reduced. As such RBMFA is an important tool to and protect the citizen data we steward. With further expansion of the use of RBMFA to additional systems and applications, we will see growing savings, cost avoidance, and increased security.