[Return to Advance CAMP wiki]

Advance CAMP Thurs, Oct. 19, 2017

10:20pm-11:10pm

Pacific C Room

Browserless MFA(Duo) for Shibboleth

CONVENER: John Pfeifer (University of Maryland)

MAIN SCRIBE: Tom Jordan

ADDITIONAL CONTRIBUTORS:

# of ATTENDEES: 20

DISCUSSION:

Use cases for non-browser MFA. Example - AWS command-line tokens. MS applications that don't do Modern Auth / ADAL. ECP is another potential use case.

Duo allows you to pick a WebSDK integration, but can't use that same credential to do AuthAPI, but AuthAPI can do WebSDK and self-service portal. Don't need to manage two different sets of keys. John has a backend component that talks to Duo. Trying to figure out the frontend - currently passing in basicauth credentials and useragent that triggers the Duo flow to use.

Scott - biggest complexity is to do normalization. Easy way is to look at using JAAS and chain authentications to do username/password first and then Duo. Need to normalize username first before sending to Duo. Scott also working with AWS command-line.

John - another option is to send http headers that define login flow, etc. Another option is to make them parameters. May not always be invoked in web context. Probably have to allow for both.

Allan - one way to get around name normalization is with username aliases. Duo allows up to 4 aliases per user.

Scott - OSU has 4 different types of usernames that a user could enter. Some aren't appropriate to add as Duo aliases. Need to normalize and canonicalize before sending to Duo. Duo said not to use the AuthAPI - don't want institutions to reproduce UI elements, but this is not a situation where we're replicating the Duo UI.

John - additional use cases for testing - how to script a shib authentication with MFA to let application developers automate testing. Another use case is around ECP for apps that can't do shib normally. Current development work on backend is in node.js. Not yet generally available but could potentially make available. Could potentially incorporate into Shib if licensing issues can be worked through.

One concern about ECP is that it makes brute force easier. One solution is to create an app password by giving app owners a public key to encrypt their credential matching an institutional private key that can decrypt based on relying party. Also can use a custom lockout filter.

Gabor - when OIDC arrives in Shib, will command-line authentication using MFA still be applicable to OIDC.

Scott - generally browser only. Something else should be built to handle non-browser case. All redirect-based, maybe something could be done with useragent switching to change profile and look for different credentials. Would probably do a different endpoint for it. IdP code doesn't really know anything about the protocol that's being used. OIDC will assume a browser in the same way that SAML assumes a browser.

O365 - older clients and non-MS clients can require an ECP endpoint (e.g. Apple Mail, legacy SMTP clients). Any chance to do MFA through an ECP endpoint? Need to train people to use auto (automatically pick the method that you want to use), or train them to append the token into the password field.

MFA with TN3270 on IBM z/OS? Use VPN with MFA, or web 3270 client behind MFA. Best to have the app do MFA, but some MFA is better than none.

Duo labs presentation on MFA with SSH proxy, injecting credentials.
https://www.youtube.com/watch?v=FSbOgwLERaA

Database MFA - most seem to use VPN. UWisc is pusing to use Oracle Advanced Security to externalize auth by using RADIUS. Florida pushing to use virtual desktop. UNC issues with using ubikey.

PAM integration - Scott trying to configure second factor as a sudo challenge. UWisc config for doing Duo with public key authentication so that 2nd factor is used as a sudo challenge.

Any use of Duo smartcard? Nothing production. Some experimentation. Tedious, not fun.

Sorting out service accounts vs people accounts? One solution -- based on LDAP attributes only allow certain populations to get to the registration screen.

Others using non-Duo - UWisc Symantec, migrating to Duo. Entrust - decommissioning in favor of Duo. Duo migrations aren't saving money, but are providing new functionality. Some use of ubikey. SMS integration expensive - now pushing towards using smartphone authenticator or issuing hard tokens where folks object.

Anyone looking at U2F? Conference may have sparked some interest. Possibly useful as a phishing preventor. Discussion around UWash key-based login presented last year. UWash supports U2F in Duo. Very small adoption rate: 51K total users, 0.1% use U2F (mostly sysadmins)

U2F is bound to requestor's domain so flow will fail if domain doesn't match.

UW: U2F of practical use for certain users with disabilities as involves just pushing a button. Now supported feature in the cheapest Duo plan

ACTIVITIES GOING FORWARD / NEXT STEPS:

Text here

=====

Note: please be sure to link to or attach any key resources from this breakout session