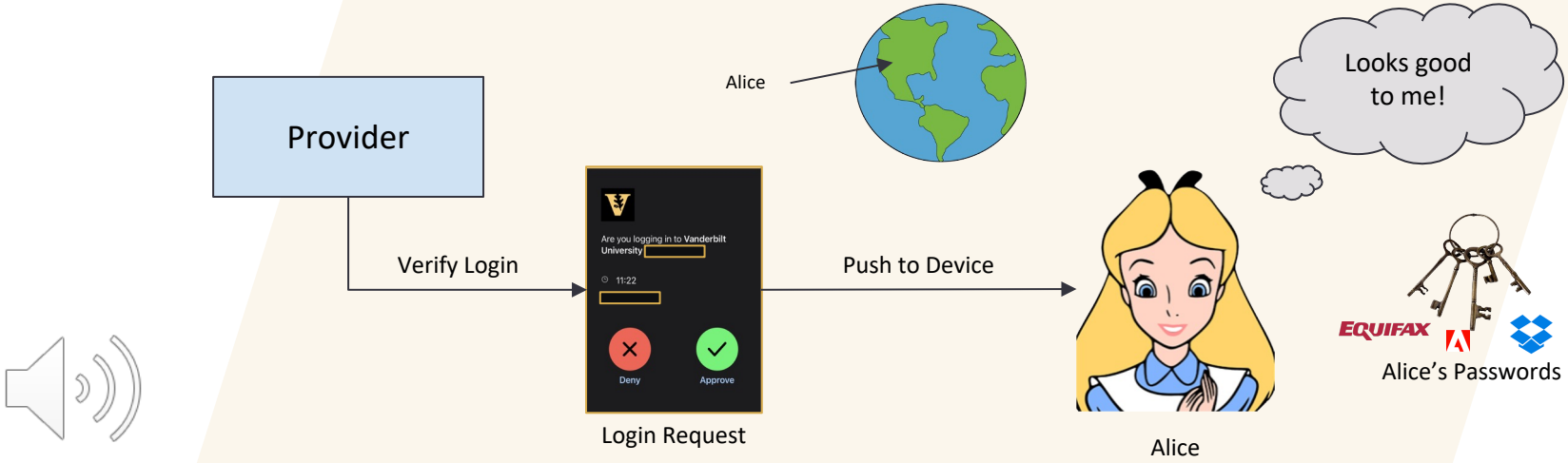
(WIP) Reducing the Efficacy of Phishing due to Poor User Behavior

Sam Hays, Michael Sandborn, Dr. Jules White
Dept. of Computer Science, Vanderbilt University, Nashville, TN, USA
Magnum Research Group

VANDERBILT
UNIVERSITY

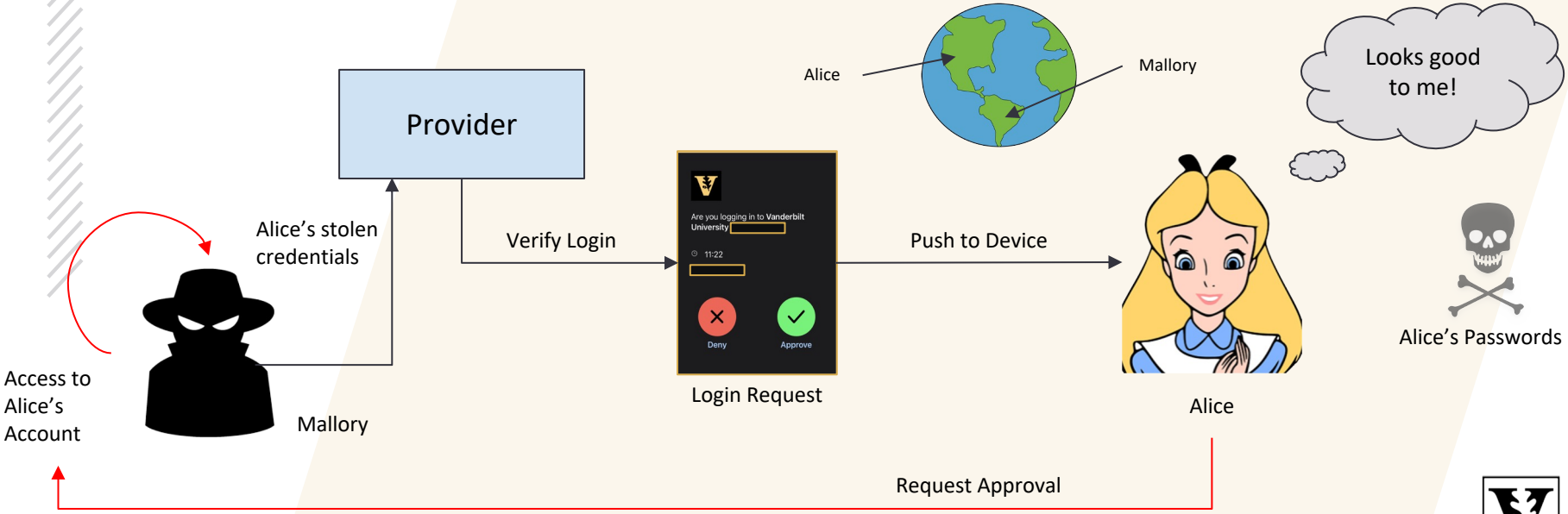
Introduction

What happens when a user approves a login request regardless of the timing or reality of whether the true user is logging in?



Introduction

What happens when a user approves a login request regardless of the timing or reality of whether the true user is logging in?



Problem

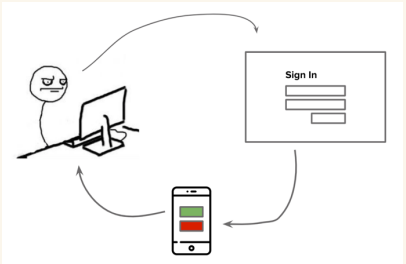
Phishing Alert Update: Do Not Approve Duo Push Alerts If You Did Not Initiate a Login [1]

Top 3 types of data compromised in phishing attacks: credentials, PII, Medical[2]

A Google study of **12.4M phishing victims** and **1.9B stolen credentials** from March 2016-2017 concludes "**7–25% of stolen passwords** in our dataset would enable an attacker to **log in to a victim's Google account** through password reuse"[3]

- MFA = security + risk of fatigue
- Fatigue + unsuspecting user = careless login request approval
- Careless approval + (phished/reused/stolen) credentials = **compromised user account(s)**

Key Question: How to prevent a successful breach assuming **adversary possesses phished or stolen credentials** and a **step-up fatigued end user**?

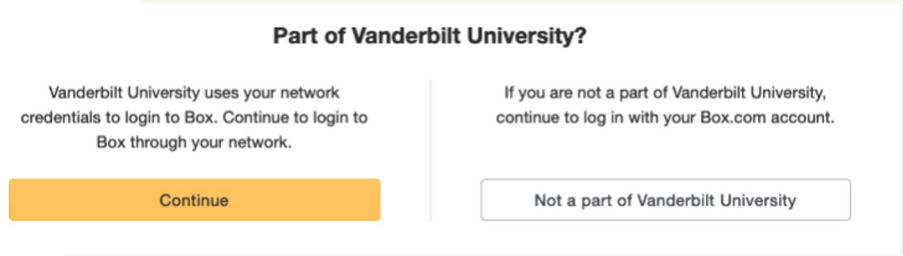


1 https://news.unchealthcare.org/2022/02/phishing-alert-update-do-not-approve-duo-push-alerts-if-you-did-not-initiate-a-login/
2 https://www.tessian.com/blog/phishing-statistics-2020/
3 https://research.google/pubs/pub46437/

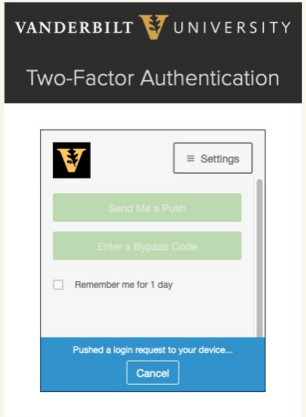
VANDERBILT UNIVERSITY

Background

- SAML 2.0 common in corporate environments (others e.g. Google OpenID Connect)
  - We focus on SAML but our solution is protocol-agnostic
- Single Sign-On (SSO) paradigm provides multi-service access using one set of credentials
- SAML 2.0 terms (analogs exist in other protocols)
  - Identity Provider (IdP): System that authenticates the user (e.g. Duo)
  - Service Provider (SP): Application of interest to user (e.g. Box)
  - Assertions: Indicate to the SP that the principal (user) is logged in
- Authentication (user **identity**) vs. Authorization (user **privilege**)



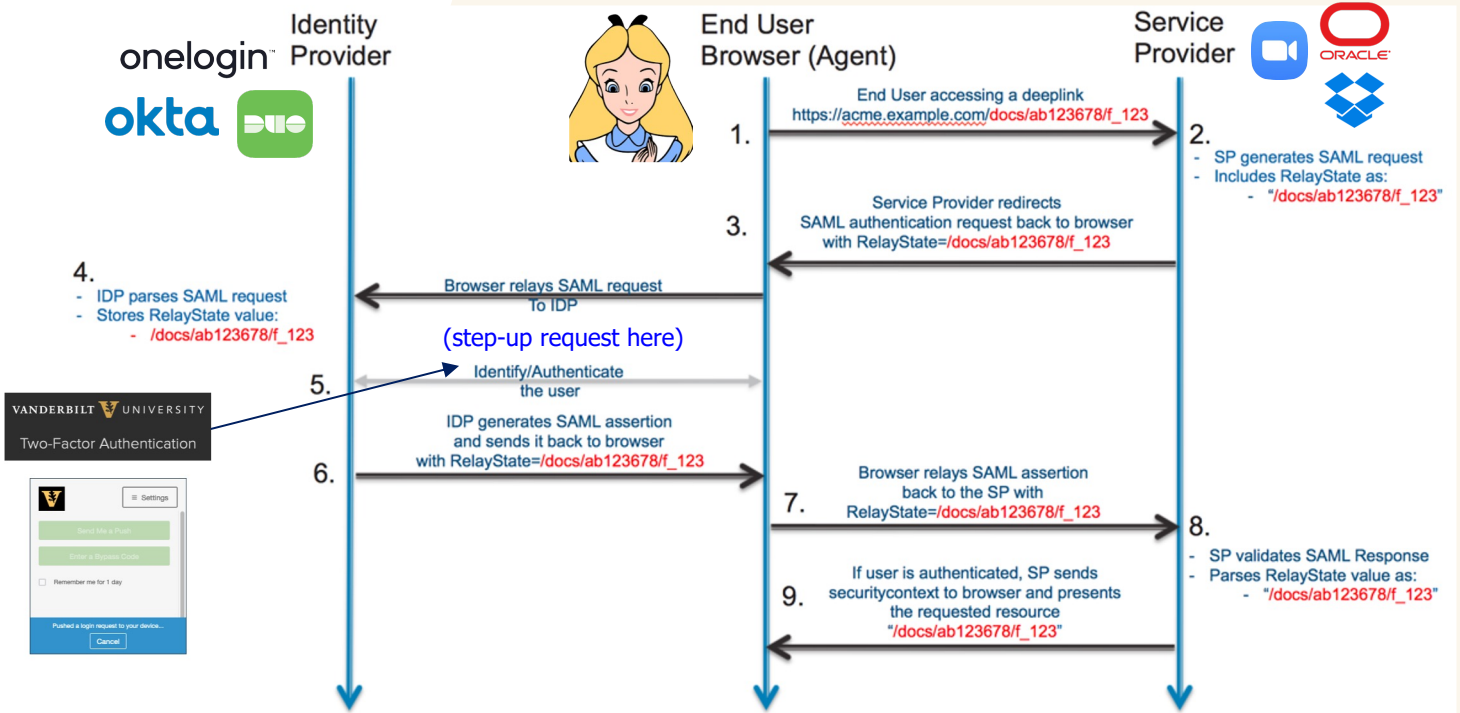
Service Provider



Identity Provider

VANDERBILT UNIVERSITY

Background



https://developer.okta.com/img/saml_guidance_deeplink.png

VANDERBILT UNIVERSITY

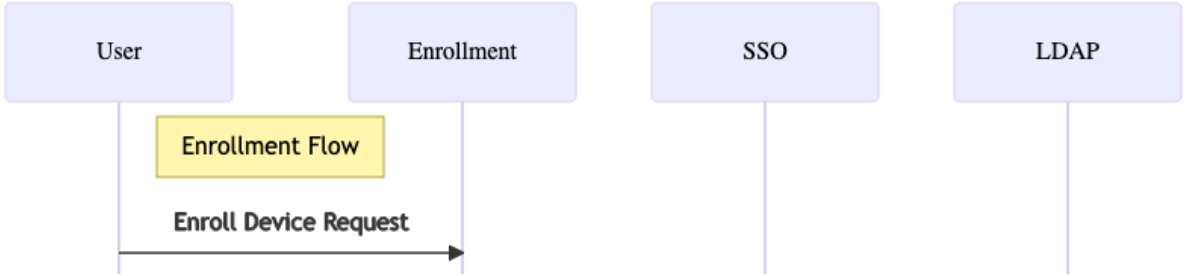
Proposed Approach

- **Goal:** Prevent successful phishing from mishandled login requests
- **Insight**: Keep signed JSON Web Tokens (JWTs, “jots”) in localStorage to manage enrolled devices and users requesting login
  - Problem: localStorage is NOT safe out of the box!
    - Solution: store jwt-count and jwt-version attributes to verify token integrity
- **Implementation**: Provide enrollment (uses jwt-count, prescribed to user) and login (uses jwt-version, opaque to user) endpoints managed by security policy
  - (WIP) require hashed nonce as additional layer

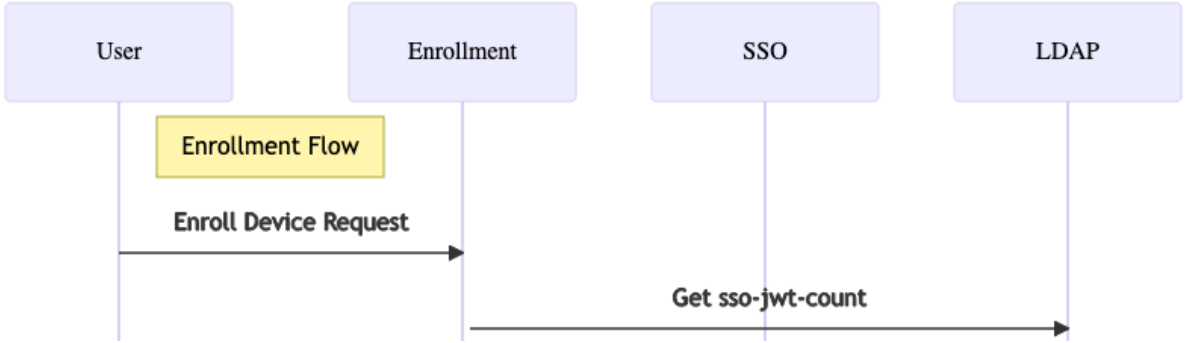
- aka The Unavailable LogIn Page

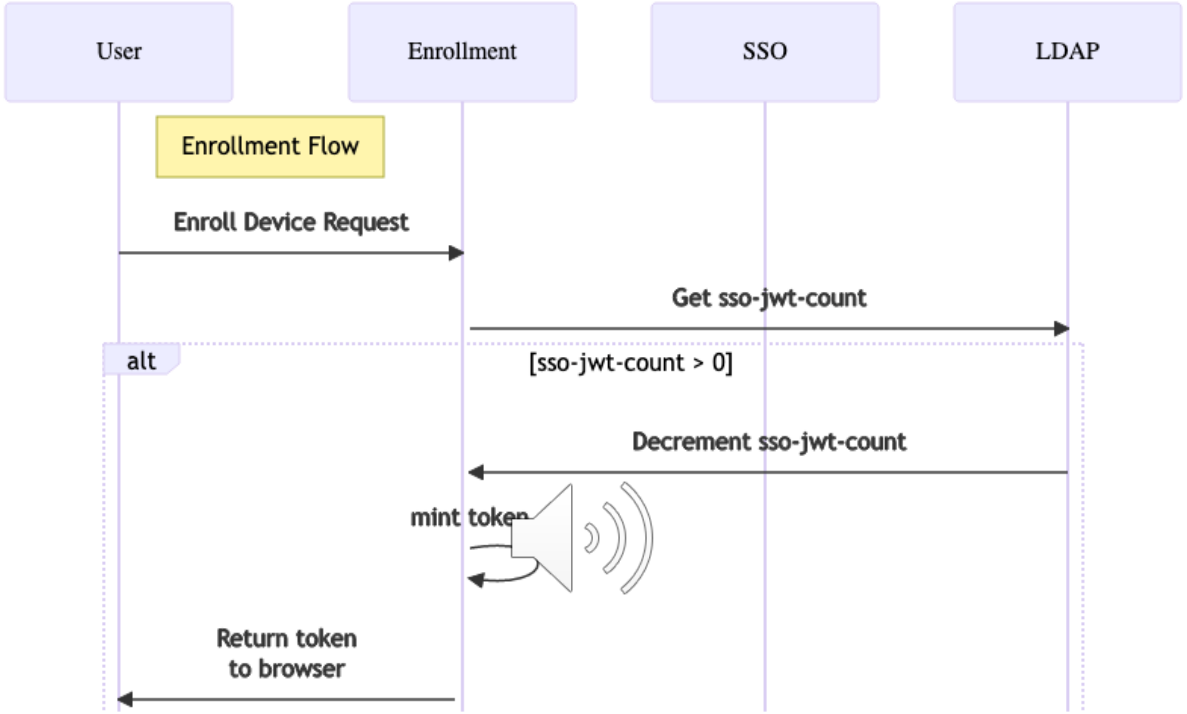
https://i.pinimg.com/originals/26/1c/68/261c68215446b6984a85d29b6482159c.png

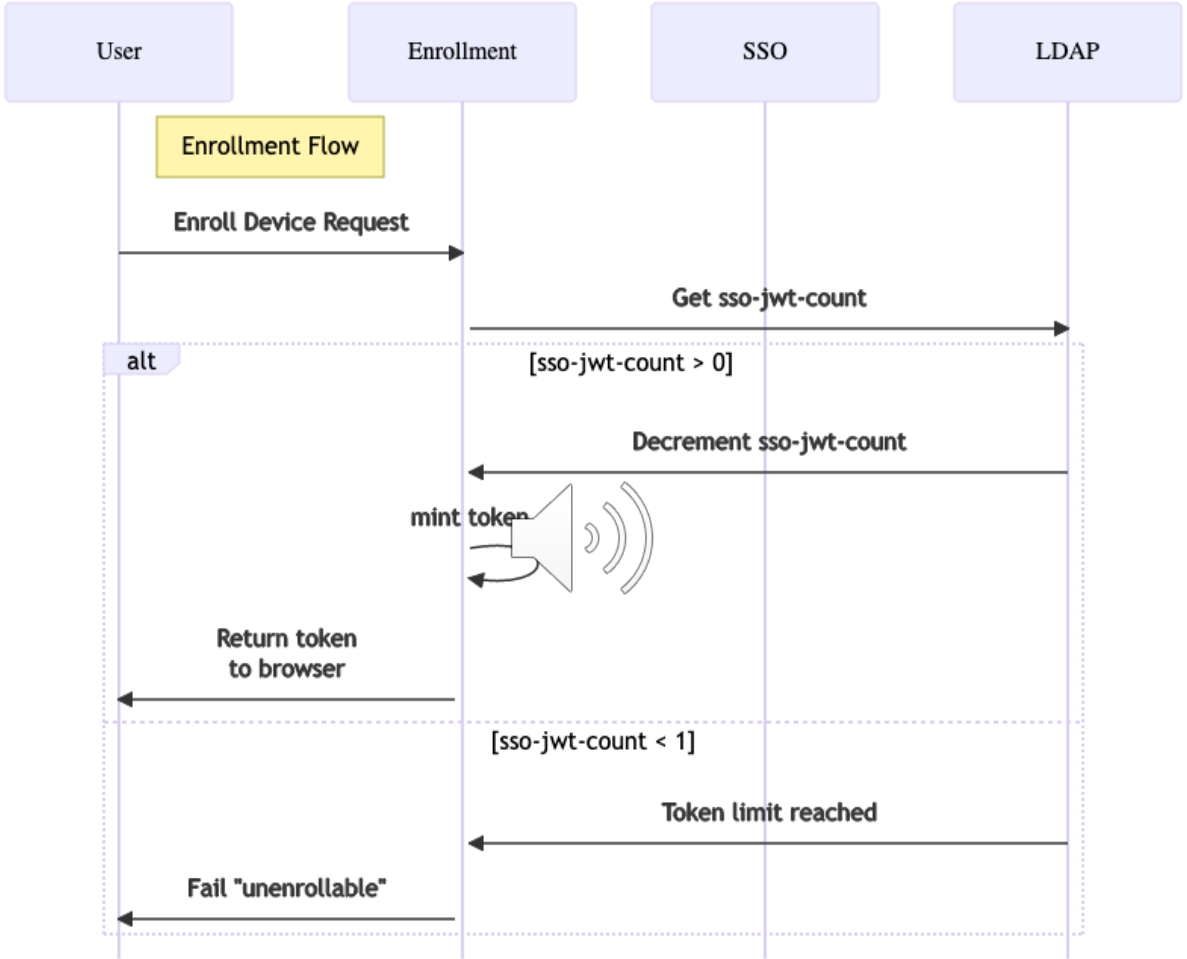
VANDERBILT UNIVERSITY

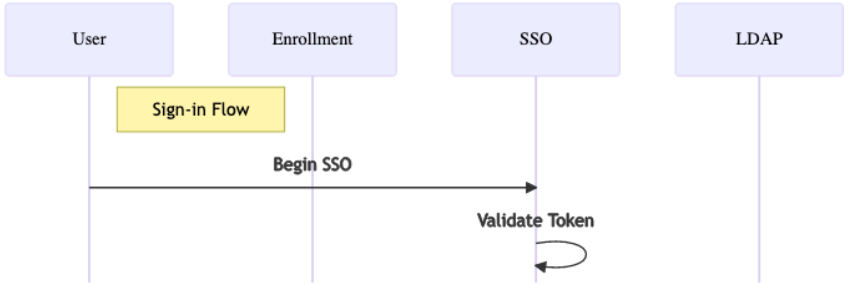


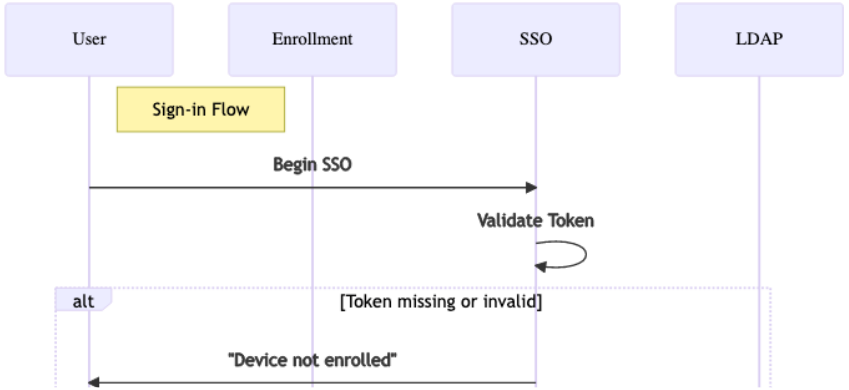
VANDERBILT UNIVERSITY


User
Enrollment
SSO
LDAP
Enrollment Flow
Enroll Device Request
Get sso-jwt-count

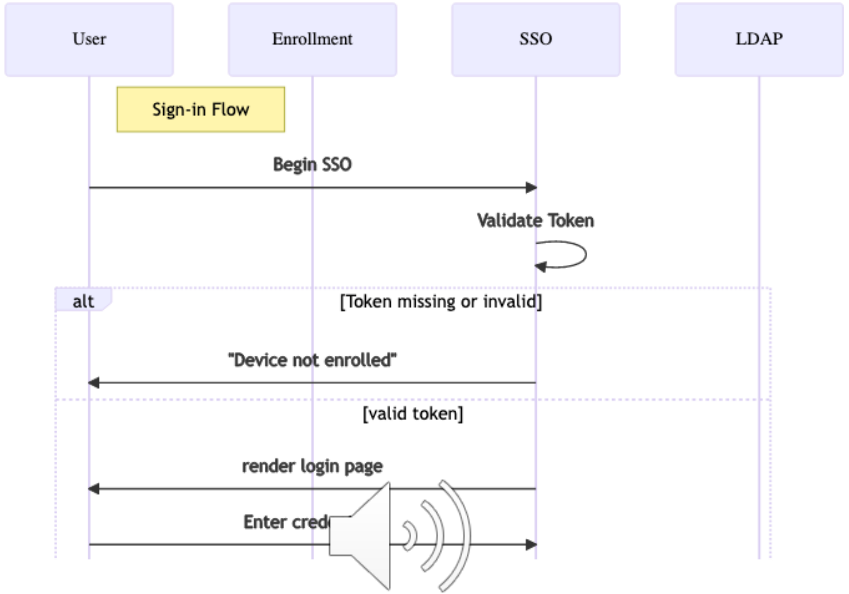

User
Enrollment
SSO
LDAP
Enrollment Flow
Enroll Device Request
Get sso-jwt-count
alt
[sso-jwt-count > 0]
Decrement sso-jwt-count
mint token
Return token
to browser

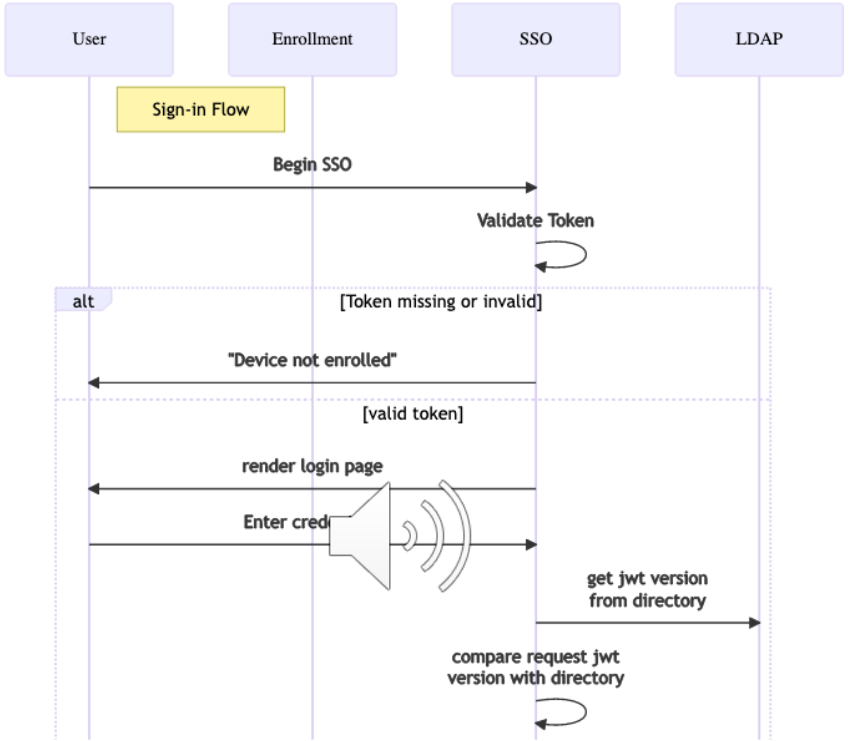

User
Enrollment
SSO
LDAP
Enrollment Flow
Enroll Device Request
Get sso-jwt-count
alt
[sso-jwt-count > 0]
Decrement sso-jwt-count
mint token
Return token
to browser
[sso-jwt-count < 1]
Token limit reached
Fail "unenrollable"

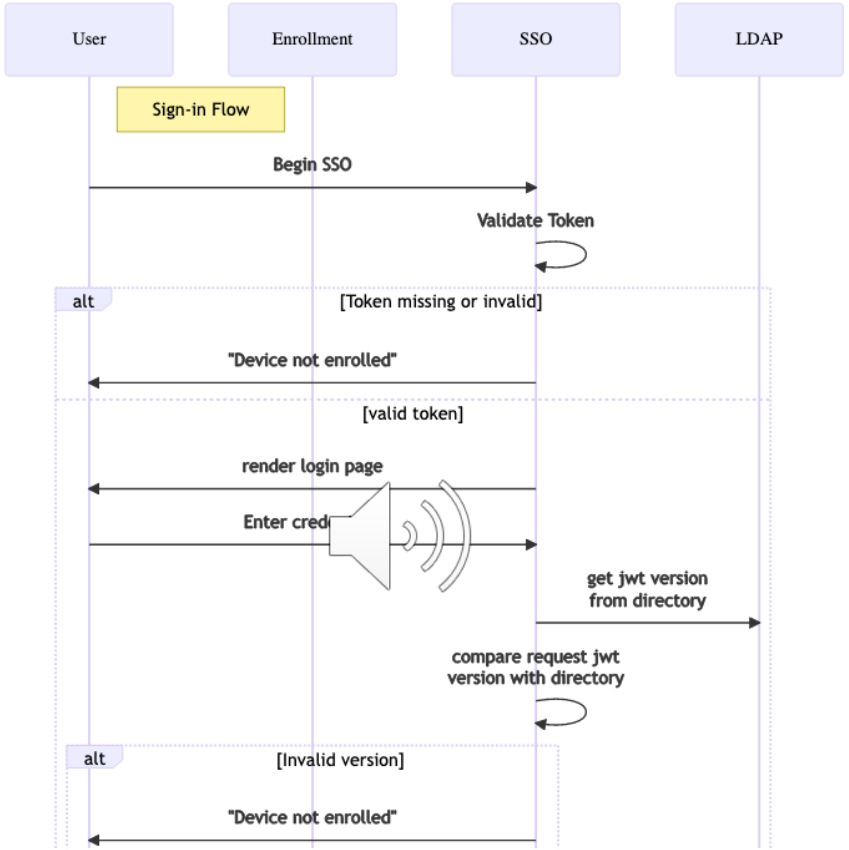

User
Enrollment
SSO
LDAP
Sign-in Flow
Begin SSO
Validate Token

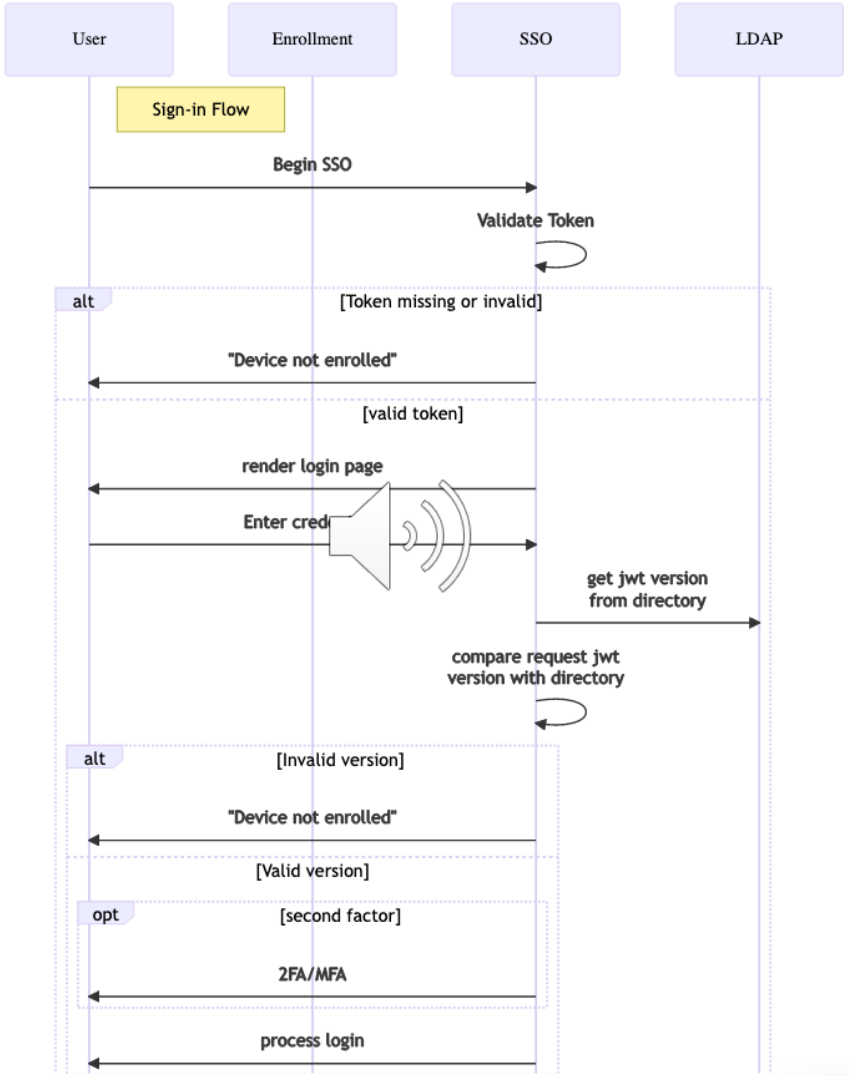


VANDERBILT UNIVERSITY

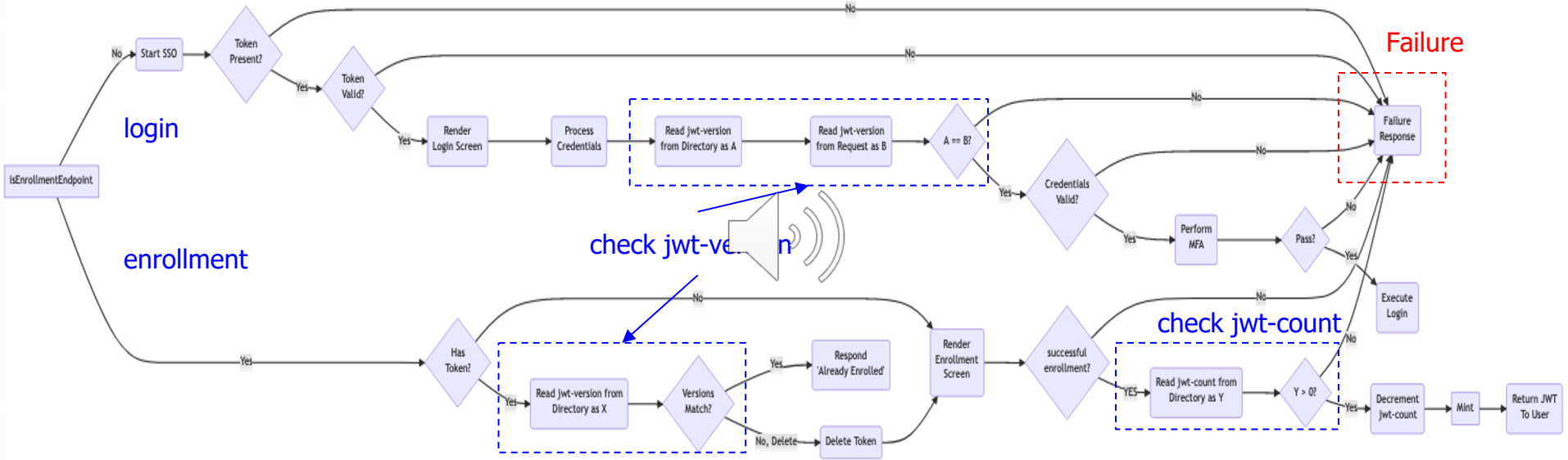

User
Enrollment
SSO
LDAP
Sign-in Flow
Begin SSO
Validate Token
alt
[Token missing or invalid]
"Device not enrolled"
[valid token]
render login page
Enter cred


User
Enrollment
SSO
LDAP
Sign-in Flow
Begin SSO
Validate Token
alt
[Token missing or invalid]
"Device not enrolled"
[valid token]
render login page
Enter cred
get jwt version
from directory
compare request jwt
version with directory


User
Enrollment
SSO
LDAP
Sign-in Flow
Begin SSO
Validate Token
alt
[Token missing or invalid]
"Device not enrolled"
[valid token]
render login page
Enter cred
get jwt version
from directory
compare request jwt
version with directory
alt
[Invalid version]
"Device not enrolled"


User
Enrollment
SSO
LDAP
Sign-in Flow
Begin SSO
Validate Token
alt
[Token missing or invalid]
"Device not enrolled"
[valid token]
render login page
Enter cred
get jwt version
from directory
compare request jwt
version with directory
alt
[Invalid version]
"Device not enrolled"
[Valid version]
opt
[second factor]
2FA/MFA
process login

Failure Paths



Thank You

Please contact michael . sandborn @ vanderbilt . edu with questions

VANDERBILT UNIVERSITY