SESSION 1 — INFOSEC @ OXFORD, M. JUNG

SECURITY IS CHESS + POKER.

4 CORE INFOSEC QS:

OXFORD NETWORK:

NO TRUSTED NETWORKS.

SERVICES BLOCKED TO INTERNET.

CONTROL AT = ISP.

STANFORD PASSWORD POL.

https://uit.stanford.edu/service/accounts/passwords/quickguide

ANTI PHISHING STRATEGIES

SESSION 2 – SPAM VECTOR / ATTACKS
SECURING THE SYSADMIN

WHAT ACCESS DO YOU HAVE AS A SYSADMIN?
IT MAKES YOU A TARGET.
NEED TO DEFEND YOURSELF + THE ORG.

2 TYPES OF ATTACKERS:

1) DOESN'T CARE WHAT ORG THEY ATTACK, JUST WANT SOME RESULTS. (EG CRYPTOLOCK SPREADS)
2) SPECIFICALLY TARGETING THE ORG; MORE DEDICATED, MORE RESOURCES. (OR A PERSON IN THE ORGANISATION)

IF YOU AS A SYSADMIN ARE COMPROMISED, HACKER CAN EASILY SPREAD MALICE / GET TO THINGS/RELEASE THEY WANT.

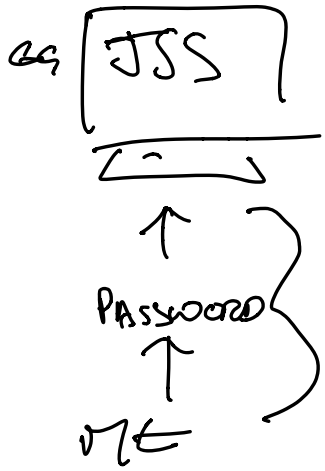
∴ YOU HAVE PRIVILEGED ACCESS TO MANY SYSTEMS +

SERVICES.

INTERNALIZE SECURITY; THINK ABOUT ATTACKS.

HACKERS HAVE LIMITED TIME; MAKE IT SO TIME CONSUMING THEY GIVE UP. (IF REALLY WANT, WILL FIND ANOTHER WAY; SPYING ETC)

THINK ABOUT WHEN YOU ENTER YOUR AD PASSWORD.



TLS, SO TRANSMISSION SECURE.

BUT IS JSS SERVER SECURE?

SHOULD I BE USING SERVICE A/Cs WITH LIMITED PERMISSIONS?

USE MORE KEYS?

PASSWORDS

MEMORABLE

SHORT

PWD IS THE SECRET.

✓ EASY TO USE

✗ EASY TO PHISH

✗ CRACKABLE.

✗ NO ABILITY TO VERIFY SINGLE POSSESSION

(IMPOSSIBLE TO KNOW HOW MANY DEVICES KNOW YR PWD)

KEYS

NOT MEMORABLE

LONG

PRIVATE KEY IS THE SECRET

✓ YOU CAN PROVE YOU HAVE CONTROL.

✓ HARD TO PHISH.

✓ EASY TO SECURE

✓ HARD TO INTERCEPT.

✗ DON'T USE SSH AGENT FORWARDING.

(DO WE?)

AI: MAKE IPASSWORD DEFAULT LONGER

AI: STOP USING GITHUB PWD; USE PUB KEY.

AI: DID I FORGET PASSPHRASE ON MY PUB KEY?

SCENARIO: HACKER CLONES MY ENCRYPTED H/D.
PHISHES MY PASSWORD.
GETS MY PRIVATE KEY.
I DON'T KNOW HE HAS MY P/KEY.

A1: STORE MY ~~[illegible]~~ PRIVATE KEYS ON A YUBIKEY? (GET 2, 1 FOR BACKUP). (+ USE U2F.) OR ACADEMIC VERSION

HOW MANY ACTIONS CAN U TAKE W/O REVIEW?
EG. SENDING MALICIOUS POLICY TO ALL JSS MACS.

BASIC JSS SECURITY:

YOUR JSS IS OPEN TO LOGIN FROM WORLD. HACKER USES LINKEDIN TO PHISH A LOGIN.

DO WE HAVE INTERNAL + EXTERNAL JSS?

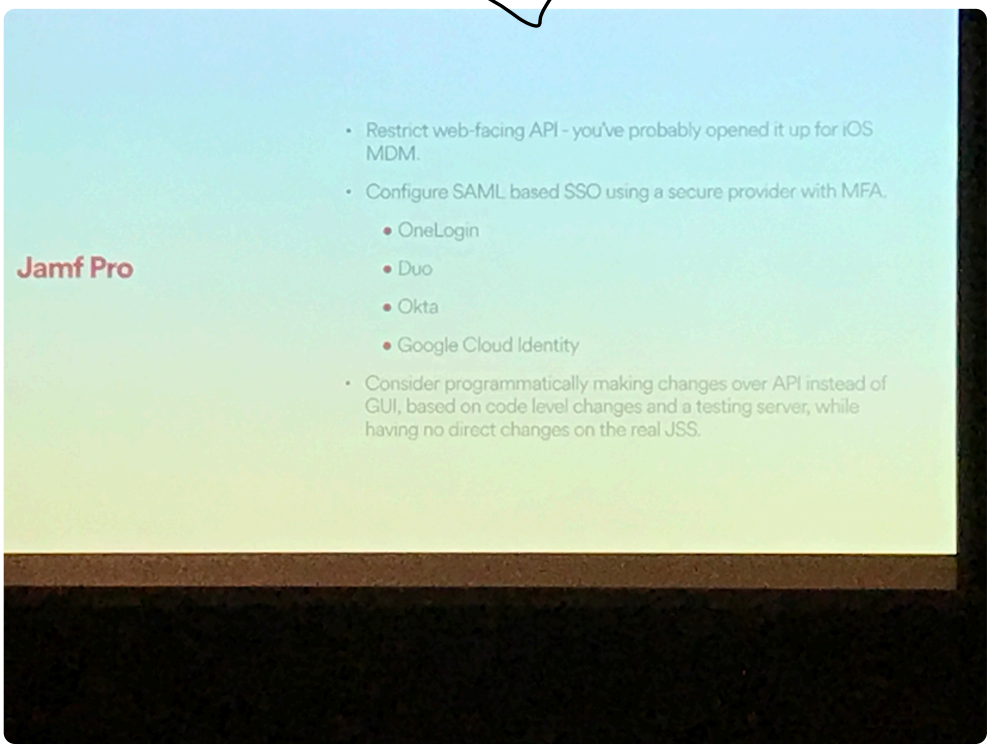
FOR

FOR ENROLLMENT, CHECK-INS ETC.

CAN'T DISABLE API, WHICH USES SAME CREDENTIALS.

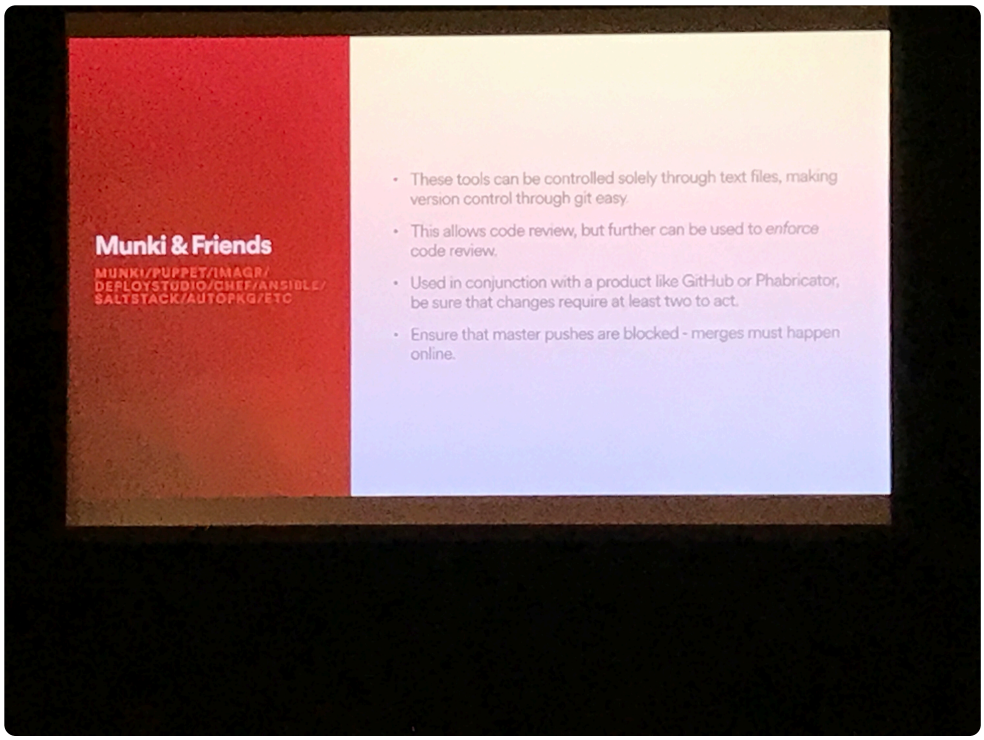
TL;DR how to turn off the jamf API when publicly-facing: delete the dir
http://sadtrombone.com (the actual code r)

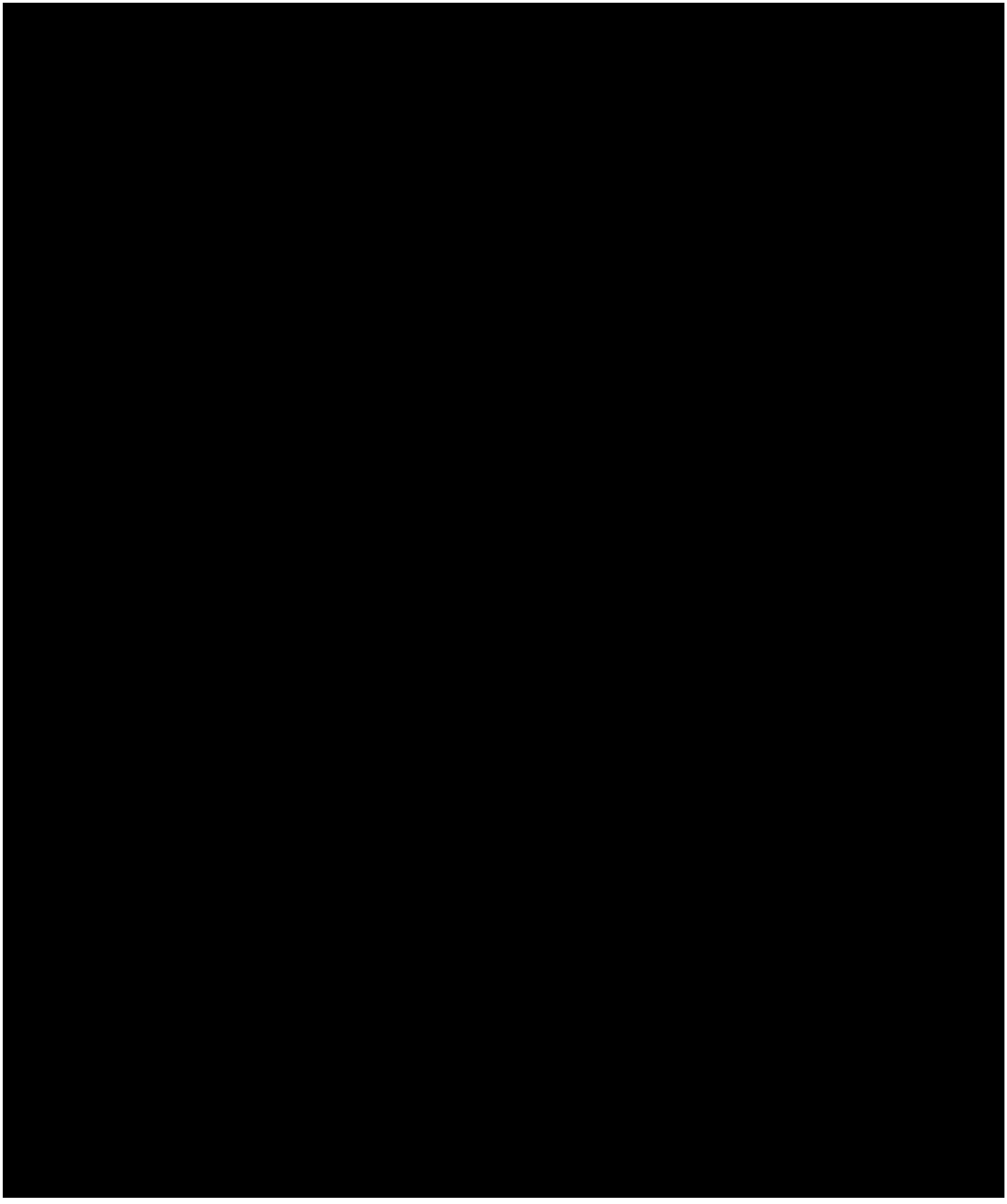
A1: ~~RANDOM~~ METHOD (→ LASPGA REMOTE (GO ADD).



MUNKI / AUTOPKG ETC

- FILE BASED APPLICATION (NO DB BASED)





[redacted]

SESSION 4 — APFS (DIVE INTO), TIM STRONDING (CORE OS)

HOW IS APFS DIFF TO HFS?
HOW WILL IT AFFECT ME + OTHERS?

https://www.smartalec.biz/ — DISK MONITORING; CAN USE OSS?

2014: CORE STORAGE INTRODUCED TO BE A LAYER UNDER HFS+ TO GET NEW FEATURES W/O TOUCHING HFS CODE.

WHY APPLE CREATED APFS:

APFS BASICS:

1 CONTAINER ≡ 1 PARTITION

↙ ↓ ↘

MANY VOLUMES

diskutil apfs list <disknumber>

'COPY ON WRITE'

VS HFS [DEBUG ON WHAT'S HAPPENING]

APFS ~ SLOW ON HDDS.

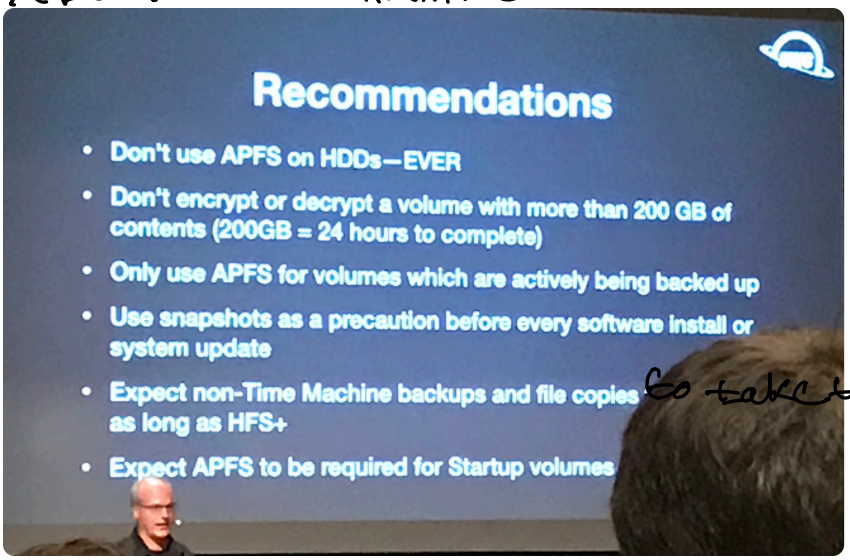
√ CREATING SNAPSHOTS ; GREAT FOR BACKUP & QUICK ROLLBACK.
(1) CREATE USING fmcbil
2) RESTORE USING RECOVERY/ROOT. ↖ √CMDS

√ ENCRYPT VOLUME ←

SUPPORTING APFS VOLUMES:
- DO OUR BACKUP TOOLS WORK?
- CAN WE RECOVER?
- (CAN DISK RECOVER COS RECOVER?)

FAKDRIVE 10.5 (WINDOWS APP) WILL READ APFS VOLUME.

X DOCUMENTATION MINIMAL.



Go take twice

SESSION 5 : AUTOMATION IN MACOS, IOS

SAL. OMNI-AUTOMATION.COM.

OMNIGROUP

AIM: SCRIPTING ARCHITECTURE FOR BOTH MAC + IOS.

WHAT IS OMNIAUTOMATION?

1) ~ JAVASCRIPT API FOR OMNI'S IOS APPLICATIONS. + MAC
↑
AVAILABLE ON IOS/MACOS AS PART OF WEBKIT.

'WORKFLOW APP. ← CAN INGEST URLS

TAKEAWAY: SAME ARCHITECTURE FOR GLUING MACOS + IOS APPS TO COMMUNICATE.

SESSION 6 - JOEL BENNICH, NOMAD 2.0

FUTURE NOMAD WALKTHRU

NOMAD = AD FUNCTIONALITY w/o BINDING.
= SSO &c
CONTROLLABLE VIA GP/MDM.

NOMAD 1.1

+ SHARE MOUNTING.
+ KEYCHAIN ITG

NOMAD 2

+SUPPORT FOR MULTIPLE USERS + DOMAINS.
|
(E MULTIPLEXING.

JOEL BUILT A SWIFT APP USING NOMAD FRAMEWORK.

POSSIBLE APPLICATIONS: DEP PROGRESS NOTIFIER
WHERE NEED TO CHECK
LDAP A/C AT SOME POINT.

SESSION 6 - ZACH HALMSTEAD, JAMF.

(A1:) WATCH GREG'S SCRIPTING VID FROM 2016.

SESSION 7 - JOEL RENNICH, "NO LO" NOMAD LOGIN

LOGIN WINDOW: "WORKS UNCANNY" (?)
CAN RUN AS 'SECURITY AGENT' OR ROOT.
USE ⟶ FOR UI.

IF ALL MECHANISMS AGREE: LOGIN → FINDER.

"MACKROLL"

CAN LIST ~~ALL~~ MECHS ~~BE~~ INVOKED USING 'security' CMD.

CAN REPLACE STD LOGIN WINDOW (OWN, BRANDED UI. + ~~SPECIFIC~~ LIST OF CUSTOM MECHANISMS)

USE TO IMPROVE DEP PROCESS "just in time account prov."; EXTEND AUTH OPTIONS + MAKE MORE ROBUST. (EG 2 FACTOR)

CAN CREATE A LOCAL USER. (MOBILE USER?)

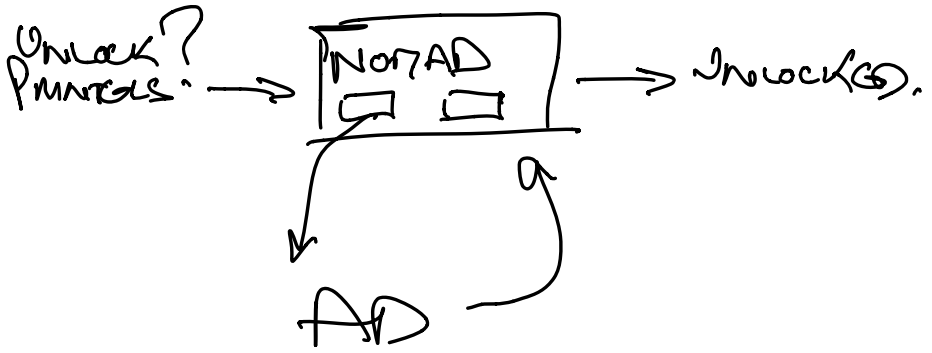
MAY BE ABLE TO DEAL W/ DEP TIMEOUT.

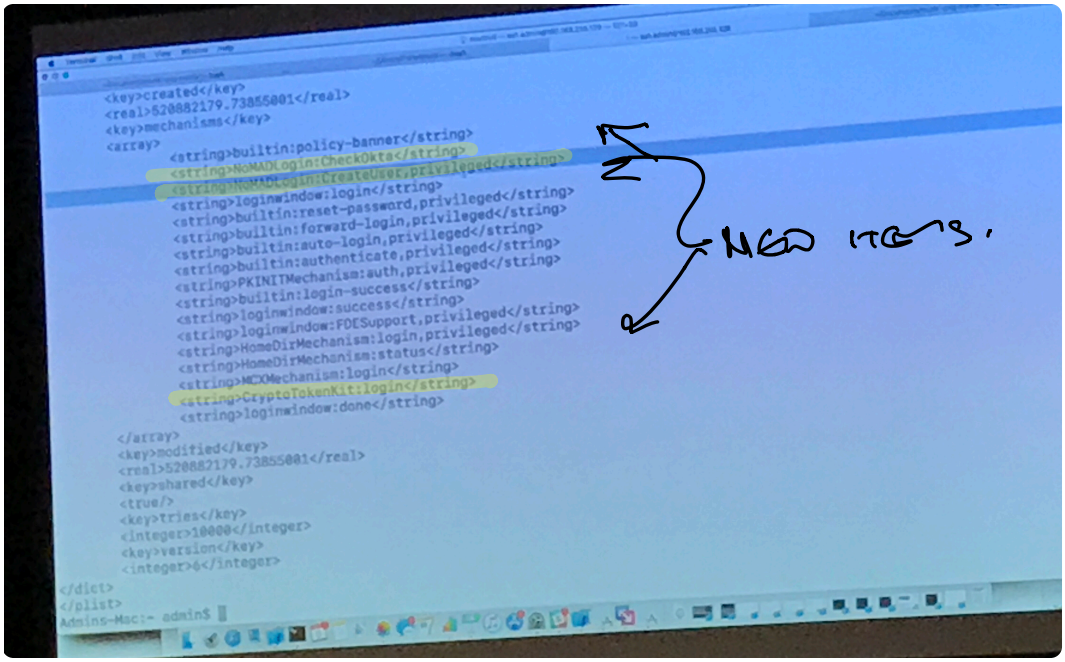
CAN REMOVE CUSTOM LOGIN WINDOW LATER.

AD AUTH
USER CREATE
SYSTEM UI
" AUTH

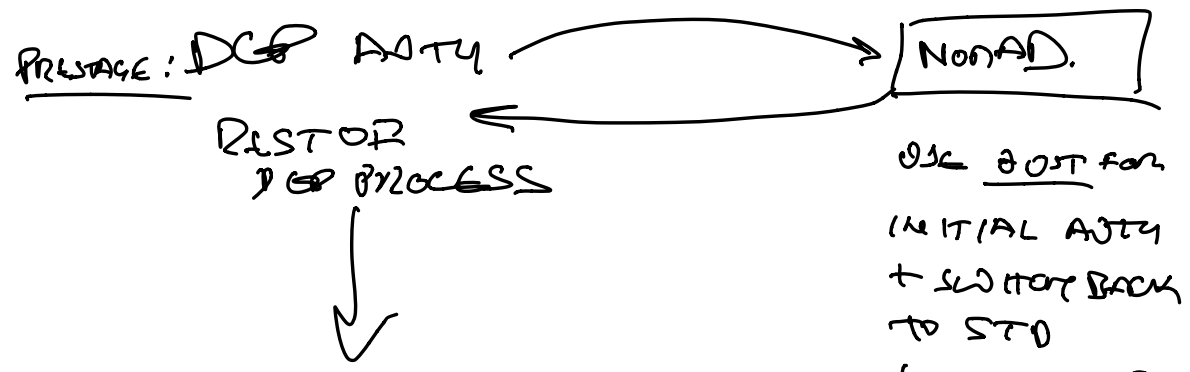
security authdb -- ds write com. .

CAN ADMIN NOMAD FOR LOCAL ADMIN BY EDITING AUTHDB SO TRYING TO ACCESS ADMIN ONLY FEATURES CALLS OUT TO NOMAD LOGIN.





DCP Process



✓ CAN PROTECT AD BEHIND AZURE SO NOT PUBLIC TO WORLD.