Guard Me If You Can: A Novel Passwordless-to-Password Attack

Yuya Chudo

FUJITSU

uvance Wayfinders

Whoami

Yuya Chudo

- Principal Security Consultant @ Fujitsu
- Talked at Blackhat Asia & Europe, Troopers
- Author of several tools
  - BAADTokenBroker
  - Pytune
  - mprecon

Agenda

FUJITSU

- Background
- Windows Hello for Business Refresher
- Passwordless-to-Password Attack
- Limitations in Credential Guard
- Conclusion

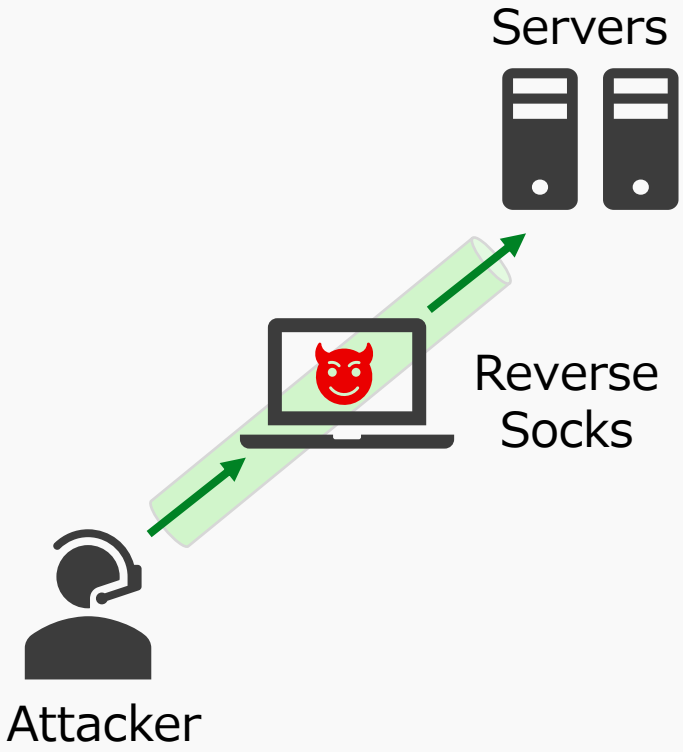
FUJITSU

Background

Stealth Operations in Red Teaming

FUJITSU

- Want to use a victim’s host as a network proxy for stealthy operation
  - Not want to load .NET tooling
  - BOFs are better than proxying in some cases :)
- For authenticated access, credentials must be obtained



Credential Theft

FUJITSU

- In Active Directory–based environments, obtaining plaintext passwords, NTLM hashes, or TGTs is ideal

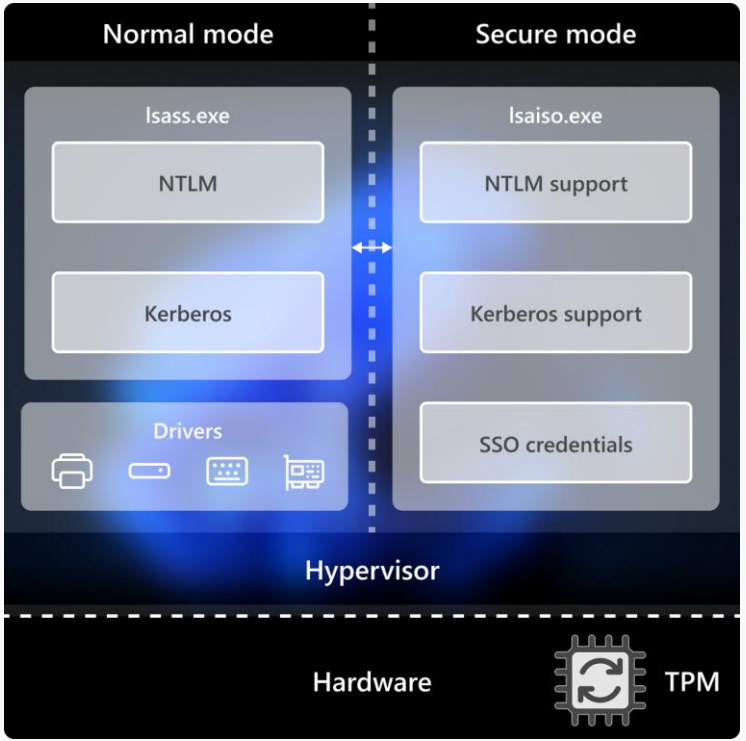
- However, acquiring these is becoming more difficult, particularly due to protections such as Credential Guard

```
[+] No domain specified! Using the USERDNSDOMAIN environmental variable...
[+] Found a DC for the domain
[+] No SPN specified! Using default SPN...
[+] Successfully obtained a handle to the current credentials set!
[+] Successfully initialized the Kerberos GSS-API!

Error! Client is not allowed to delegate to the target SPN.
Error! tgtdelegation failed!
```

Credential Guard

- Prevents credential theft by isolating NTLM hashes, TGTs and other secrets within a virtualized environment
- Devices running Windows 11, 22H2 or later have Credential Guard enabled by default if they meet requirements



https://learn.microsoft.com/en-us/windows/security/identity-protection/credential-guard/how-it-works

Research Goal

FUJITSU

- Even on endpoints with Credential Guard enabled, we need to find a way to obtain user credentials
- For this, we turned our attention to **Windows Hello for Business**

Windows Hello for Business Refresher

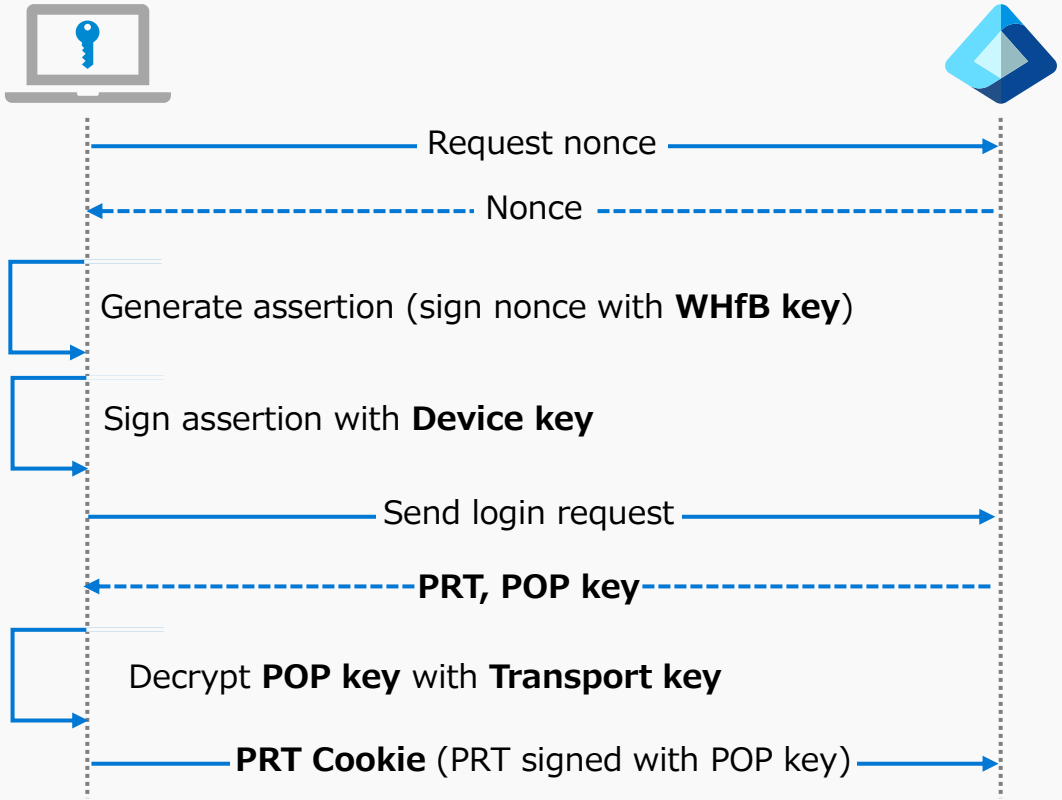
Windows Hello for Business (WHfB)

FUJITSU

- Passwordless authentication provided by Microsoft

- User ID keys are registered to IdPs (Identity Provider) such as Entra ID
  - The keys can be used for authentication when being unlocked with PIN or biometric gestures

Authentication to Entra ID



Hybrid Deployments

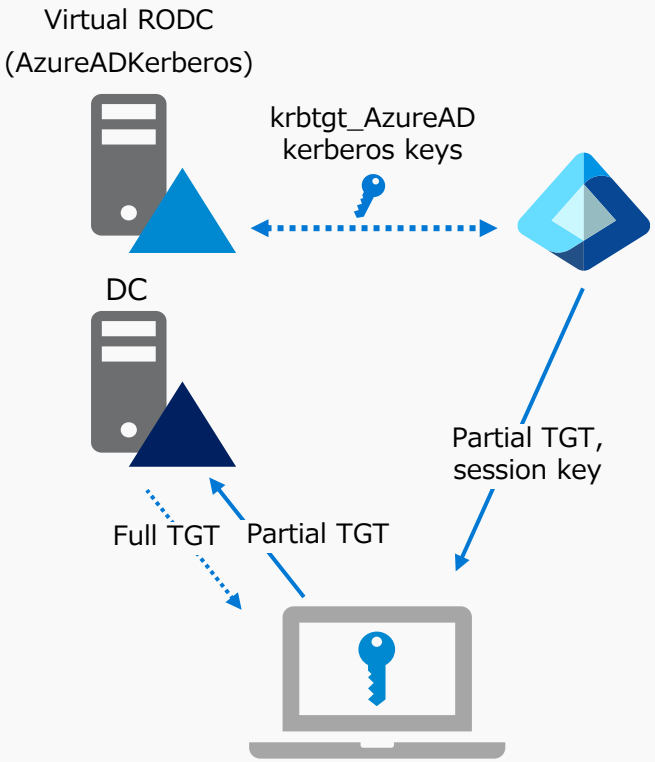
FUJITSU

- Active Directory also allows users to use WHfB keys for authentication

- Microsoft introduced three methods for hybrid deployment
  - Cloud Kerberos trust deployment
  - Key trust deployment
  - Certificate trust deployment

Cloud Kerberos Trust Deployment

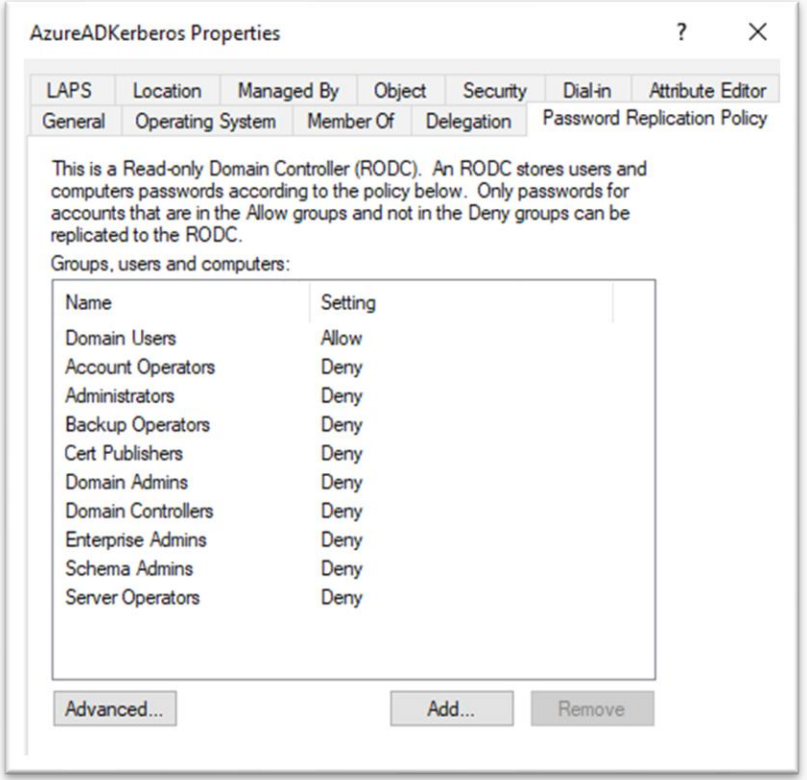
FUJITSU



- Microsoft Entra Kerbros server object (**AzureADKerberos**) is created as a virtual Read-Only Domain Controller (RODC) in Active Directory
- **krbtgt_AzureAD** account is also added and linked to the RODC
- Its Kerberos keys are synced to Entra ID for issuing **partial TGTs**
  - Partial TGT contains user's security identifier (SID) but no group claims
  - Needed to be Exchanged for **full TGT**

Password Replication Policy

- RODC has a password replication policy that defines which users' passwords can be replicated from DC
  - This is stored in *msDS-RevealOnDemandGroup* and *msDS-NeverRevealGroup* attribute of the RODC
- Partial TGT can be exchanged for full TGT if the user is allowed in the replication policy
  - In case of AzureADKerberos, Domain Users are allowed by default and privileged users are not



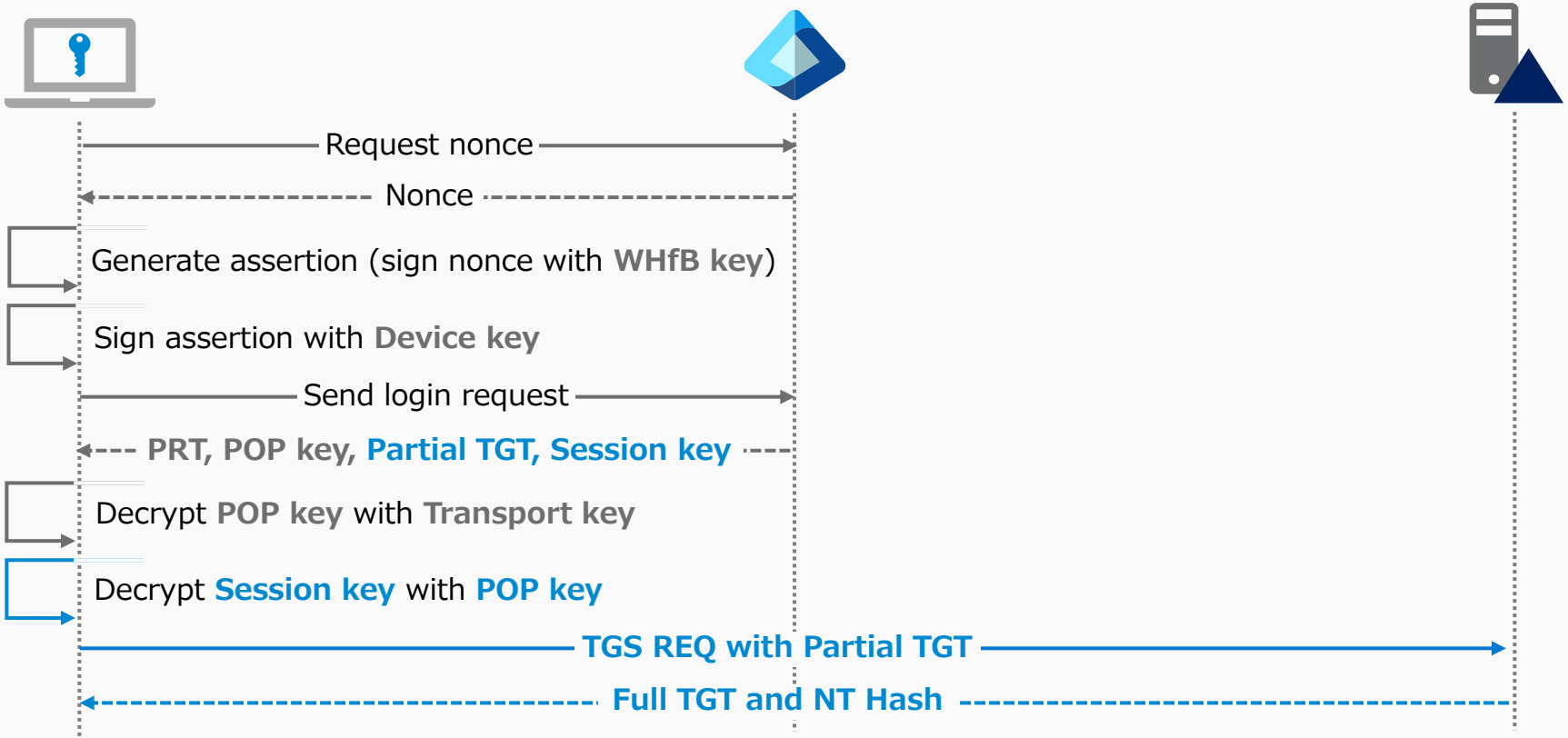
NTLM Support in Passwordless Environment

FUJITSU

- When exchanging partial TGT with full TGT, the on-premise Active Directory include a user’s NT hash in the TGS-REP
- With the password hash, users can authenticate to servers not supporting Kerberos
  - This was researched by Leandro Cuozzo and documented in hist blog
    The Kerberos Key List Attack: The return of the Read Only Domain Controllers

Authentication to Entra ID & Active Directory

FUJITSU



Login Request to Entra ID

FUJITSU

```
POST /common/oauth2/token HTTP/1.1
Host: login.microsoftonline.com
User-Agent: python-requests/2.32.3
Accept-Encoding: gzip, deflate, br
Accept: */*
Connection: keep-alive
Content-Length: 3985
Content-Type: application/x-www-form-urlencoded

windows_api_version=2.2&grant_type=urn%3Aietf%3Aparams%3Aoauth%3Agrant-type%3Ajwt-be
eyJhbGci0iJSUzI1NiIsICJ0eXAi0iJKV1QiLCAieDVjIjoiTUlJRDh6QONBdHVnQXdJQkFnSVFPZ2Q1ZDBN
tpRzl3MEJBUXNGQURCNElYWXdFUVlLQlpJbWlaUHlMRlFCRlJZRGJtVjBNQlVHQ2dtUUpvbVQ4aXhrQVJrV
TlV5MVBjbWRoYmlsNllYUnBiMjROUVd0alpYTnpNQ3NHQTFVRUN4TWtPREprWW1GallUUXRNMlUOTVMwME5
lUazNNQjRYRFRJMRlESXlNVEV5TXpReE9GblhEVEOyTURJeU1URXpNRFF4TOZvd0x6RXRNQ3NHQTFVRUF4
SmtMVOV4WVdZdFpHRTROR015WVRnMk9HWXhNSU1CSWpBTkJna3Foa21HOXcwQkFRUZBQU9DQVE4QU1JSU
NVeGdtdE9FbzZTMVwvcm13VWt2eDlVQkFDVlUybGcyWjdsUrJsQlhjMkN2dzhnakxjVndIZmc4VUpnTVlWW9N
L3ho0TFcLzgrQW1lNEZWbEZvZXIyK3RWeFpuNGpBMOJcL3AzR29PdWxTakIeEJCRlppanFPaWlkZkRSakwwRW
BKTnd0eGlCbVNKTU5IWmZ0RmFFSkNleFhjYOFRSFhQWVlbWVIZDI2VjklanRRdFwvRnBjRVZVQmdpR2VGSVhh
NDMOYU5mUVRFYlZ0NFNIWXpOK1EyZjZmd3RM0WRsUFJjazF0TUVHUFJMVVozdjR0N3FIdGJVaytIQ0RITElyYj
hCTUlHK01Bd0dBMVVkRXdFQlwvdlFDTUFBd0ZnWURWUjBsQVFIXC9CQXd3Q2dZSUt3WUJCUVVIQXdJd0lnWUxI
V3E0Vll5dHIxTW5hXC9h
FXQ0hBVUVFdlNCRUlybl
RUJJRUJNVEF0QmdrcWhr
hlYmlYMWpVemJhMXZWM2
VGU0ZGtNMmxZVzhyaXY2
NFclFJb2J4dlZKcURzSV
0UQzbVpuZCtuc3BLS2VP
wic2NvcGUiOiJvcGVuaW
aUlzSW5SNWNDSTZJa3BY
A5SWl3aWRYTmxJam9pYm
ZENJNrlDQXh0emN5TURj
5salIyeHRXVmRPTUd0Ml
WGJYSnlkMWhhUXp0RFlVaFJWbnBGTWlaVE9YWnpZVEJYVTBSRO5rdFhNRVF3WrUlbVQzYzRaMEZCSW13aVlYVmtJam9nSUNJMllUTmtaVC
lqWmhMVFExWWlNdFlqQXhNQzAzWWpaak5EZGlZbUtyTlRVaUxDSnBjMOlpT2lBZOluWnBZMlJwYlVCMFpYSnVjQzVqYjIwaWZRLmkiTkpi
WUNhTlgONnBRTHNoWlluT2FsQUOwckI4SOF4UTh6S3NJYjBxTOlYTk8zZOlHLXF5VHFnVTdwSUc3UW5QZHZi0DYzcVNHZmtiNVJKanJIQ
ktRGtNQ3ltbWl5eHZLTWdlSOFicWNSXOhSazhMamthSWMwSlRLXONKRldoY3JvVHB5UWZvLTllcmZ4VOxLbmRPUlVQTlR3Nzdsb1JtbGVx
cm9Ub2MyYktlOVAwQThzenIOS2tYT3JNVmxBMG0tROtiTTZnclVmNOJOcklhQ1dlTWNodnhoMV9fLWZlaE1XSENEMndrd2JLWr9FdG4teT
9wclhldDdYTjVIREZSNUhKaHFTUkFLOUZ0NGdFbjh00GxnZhsRGlM0ClWdERQV3VZTlNOb3BKROd4blElenN3WWdRb3lvRFFYQSIsInJ
bmSuY2Ui0iJBdOFCRWdFQUFBQURBT3pfQlFEMF8wVjJiMU4wYzBGeWRHbG1ZVO4wY3dVQUFBQUFBQ2NQTzVaZVNjUnJtcElwSEVxVjYlbj
9rYlN4TTRnUV9nMrVYZXl2VVdtcnJ3WFpDMONhSFFWekUyZlM5dnNhMFdTREY2S1cwRDBkTmZPdzhnQUEiLCJncmFudF90eXB1IjoidXJu
cGFyYWlz0m9hdXRo0mdyYW50LXR5cGU6and0LWJlYXJlciIsImNsaWVudF9pZCI6Ijl5ZDllZDk4LWE0NjktNDUzNilhZGUyLWY50DFiYz
J9.iJve4UHx9-sbCPvmorqRCqRHAyzXISPcmGwo53wD43UsEWuThWYc_VGHdybgrJF4zVBYItPHldh_RZxbLEvy-9cV-Hg6T5cRDgPqOb
TKEEmuS3CXYtPqJRy3zP9Khkw028Dwx7iquigeiWLZs1_2Q3oE0lOqOuoWzNlp0uBkOM_BNxUW4QPfLQoDipmECk6Hl7d6PXYIbo0ZgKd
ciFhT9h3ogZHZouB_iRBoJxQAfZzMMM_glRZteD6pZW8pl5g5_WEonhcvpBbuIILBbvjwfEFzqvI4LwIsVL5Tp5dN75sAlzlbXuUcEp7eA
OAA&tgt=True
```



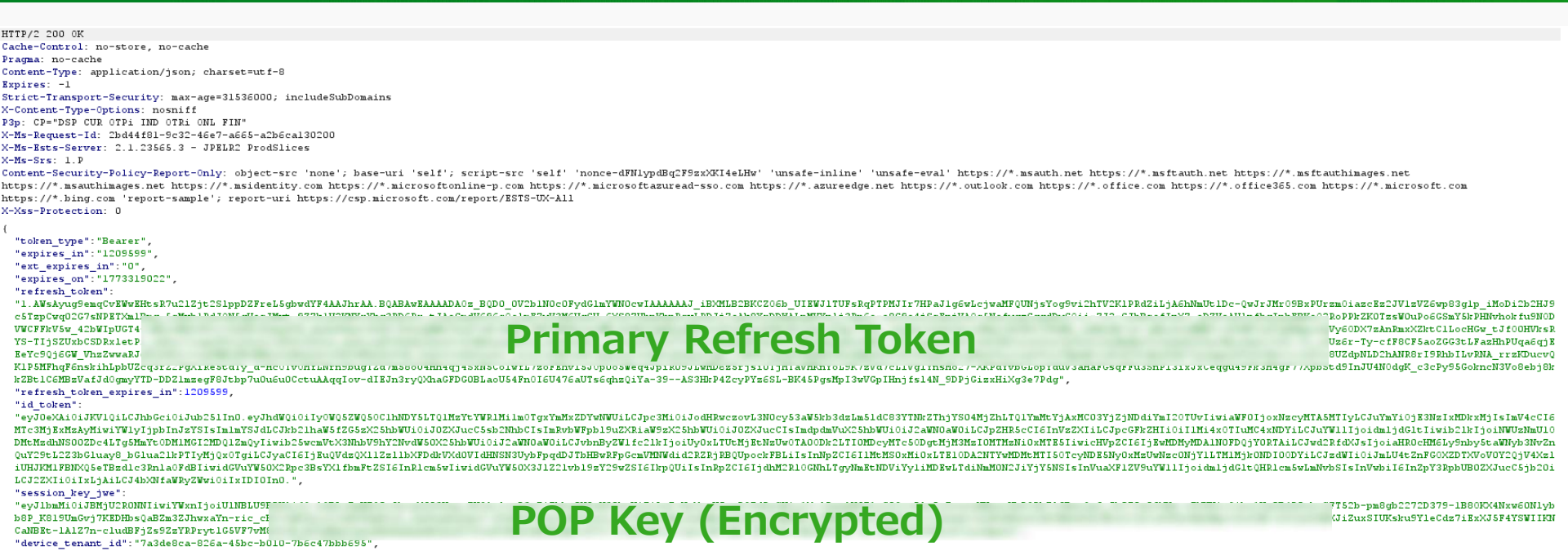
```
{
  "win_ver": "10.0.19041.3996",
  "scope": "openid aza ugs",
  "username": "victim@ternp.com",
  "assertion":
"eyJhbGci0iJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6InBHTE950GZlbWxwcVpyamh0RTBZcDg3d0FscXh
rczdIUlpVYnY1QVhLb009IiwidXN1Ijoibmdj In0.eyJzY29wZSI6Im9wZW5pZCBhemEgdWdzIiwiZXhwIjo
gIDE3NzIxMDk
6X0JRRDBfMFY
va2JTeE0OZ1F
iYXVkIjogICI
0ZXJucC5jb20
QnPdvb863qSG
rfxWLKnd0RUP
l__-fehMWHCD2wkwbKZ0Etn-y3d7tJz0psXut7XN5HDFR5HJhqSPAK9FN4gEn8N8lge81DiL8-VtDPWuY0St
opJGGxoQ5zswYgQoyoDQXA",
  "request_nonce":
"AwABEgEAAAADA0z
4gQ_g2EXeyvUWmrr
  "grant_type":
  "client_id":
```



```
{
  "scope": "openid aza ugs",
  "exp": 1772109396,
  "iat": 1772073396,
  "request_nonce":
"AwABEgEAAAADA0z_BQD0_0V2b1N0c0FydGlmYWN0cwUAAA
AACcP05ZeScRrmpMpHEqV65n5h0KMaokrbSxM4gQ_g2EXey
vUWmrrwXZC3CaHQVzE2fS9vsaOWSDF6KW0D0dNf0w8gAA",
  "aud":
"7a3de8ca-826a-45bc-b010-7b6c47bbb695",
  "iss": "victim@ternp.com"
}
```

Nonce

Response from Entra ID



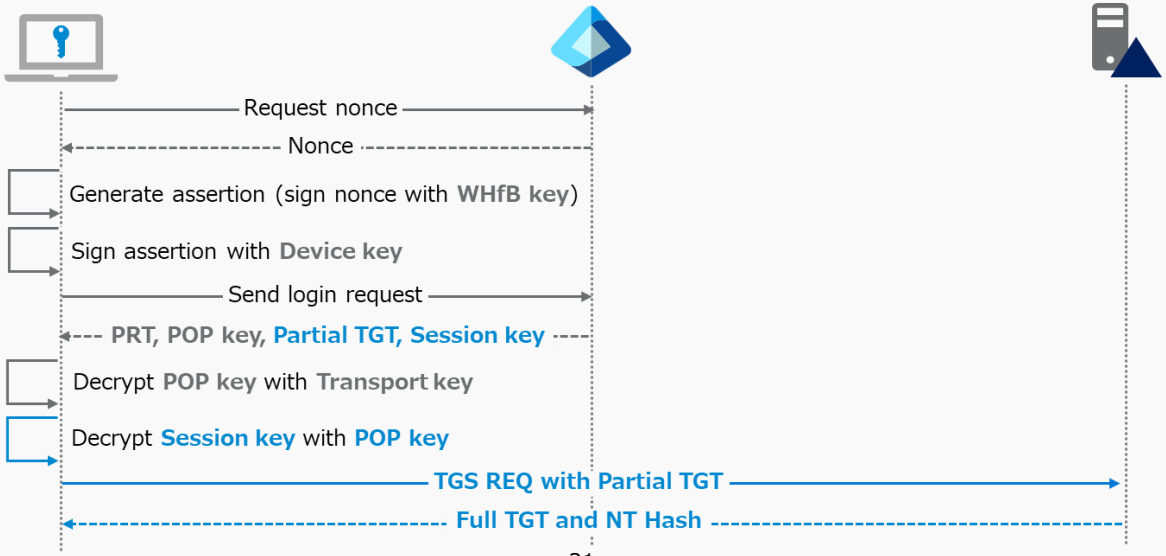
FUJITSU

Passwordless-to-Password Attack

Credential Theft against WHfB user

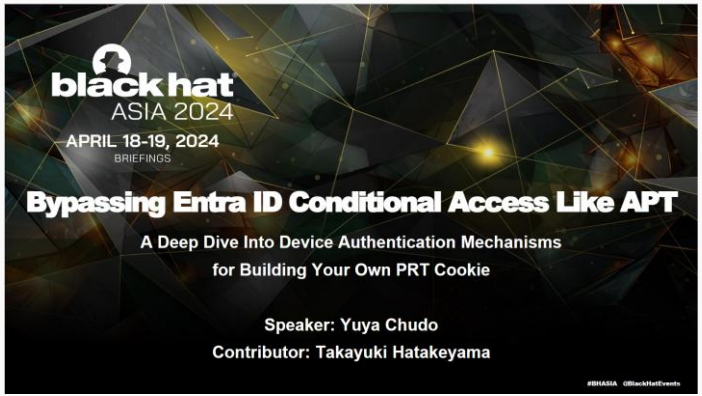
FUJITSU

- Is it possible to replicate the authentication flow from WHfB user context and steal credentials even in a Credential Guard-enabled endpoint?



Living-off-the-Land-Key

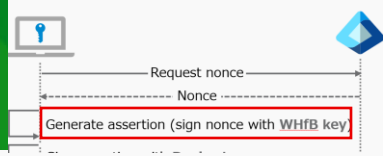
- All of the keys needed are securely protected in TPM (Trusted Platform Module)
  - However, they are accessible through various ways as previously presented at Black Hat Asia 2024



Bypassing Entra ID Conditional Access Like APT: A Deep Dive Into Device Authentication Mechanisms for Building Your Own PRT Cookie

https://blackhat.com/asia-24/briefings/schedule/index.html#bypassing-entra-id-conditional-access-like-apt-a-deep-dive-into-device-authentication-mechanisms-for-building-your-own-prt-cookie-37344

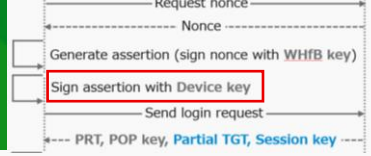
WHfB User ID Key



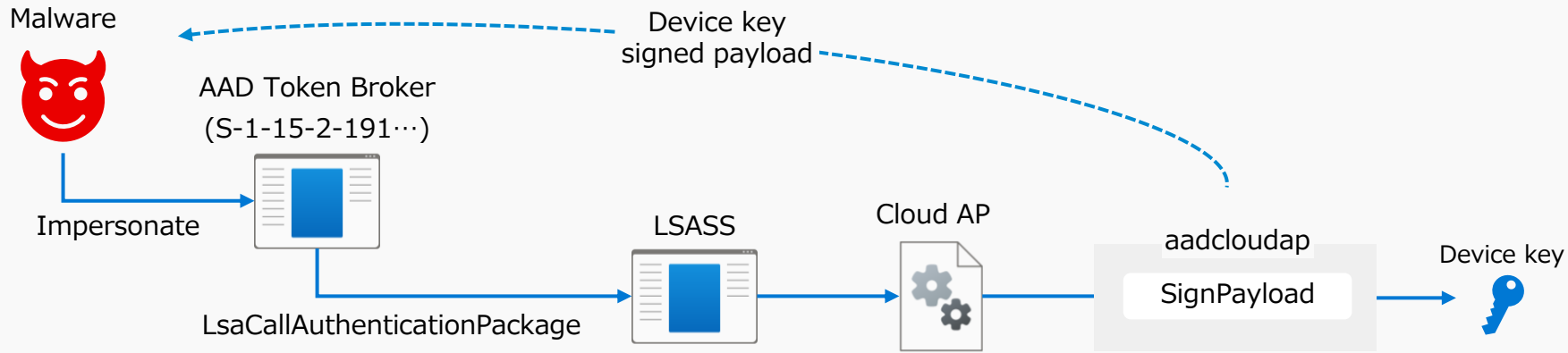
- WHfB user ID keys (ukpub/ukpriv) are accessible through several Windows APIs and used for generating WHfB assertion
  - Examples:

Function	Description
NgcGetUserIdKeyPublicKey	Export specified WHfB user ID public key (ukpub) blob data
NgcSignWithUserIdKey	Generate signature for the specified input with WHfB user ID private key (ukpriv)
NgcEnumUserIdKeys	Retrieve WHfB user ID key info matched with the specified user

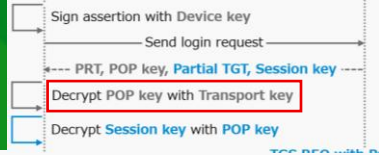
Device Key



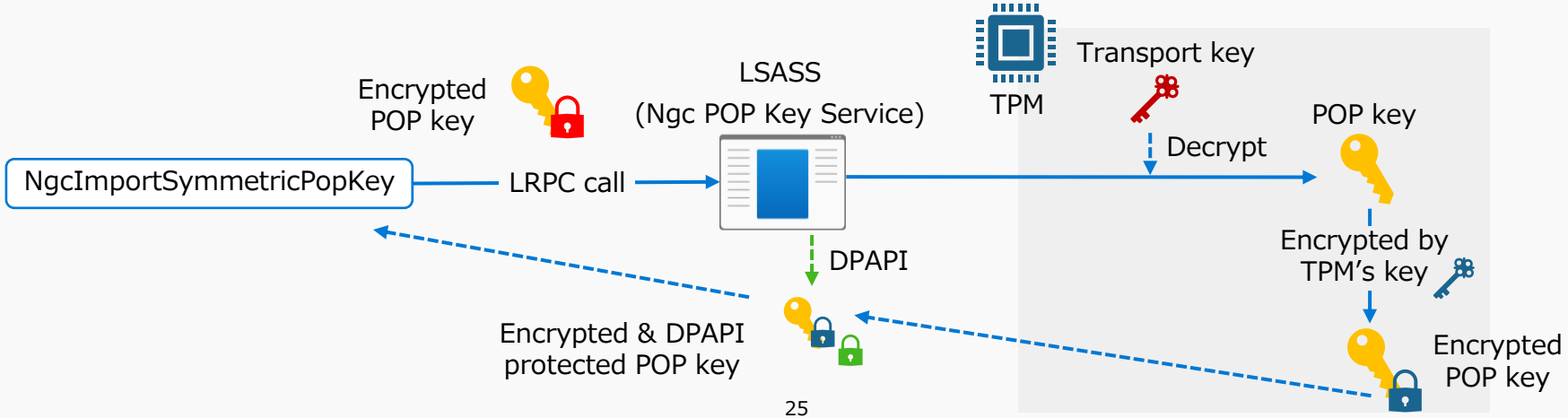
- Device keys are registered to Entra ID during Entra join/register and used for device authentication
  - Device keys are available through interacting with cloud authentication package and its plugin called aadcloudap



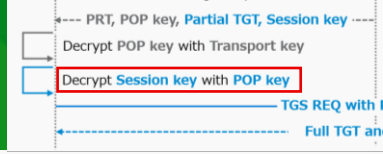
Transport Key



- Transport keys are also registered during Entra join/register and used to protect POP key
- Through RPC calls, POP key can be decrypted by Transport key
  - POP key is encrypted again by TPM and protected by DPAPI for later use



POP Key

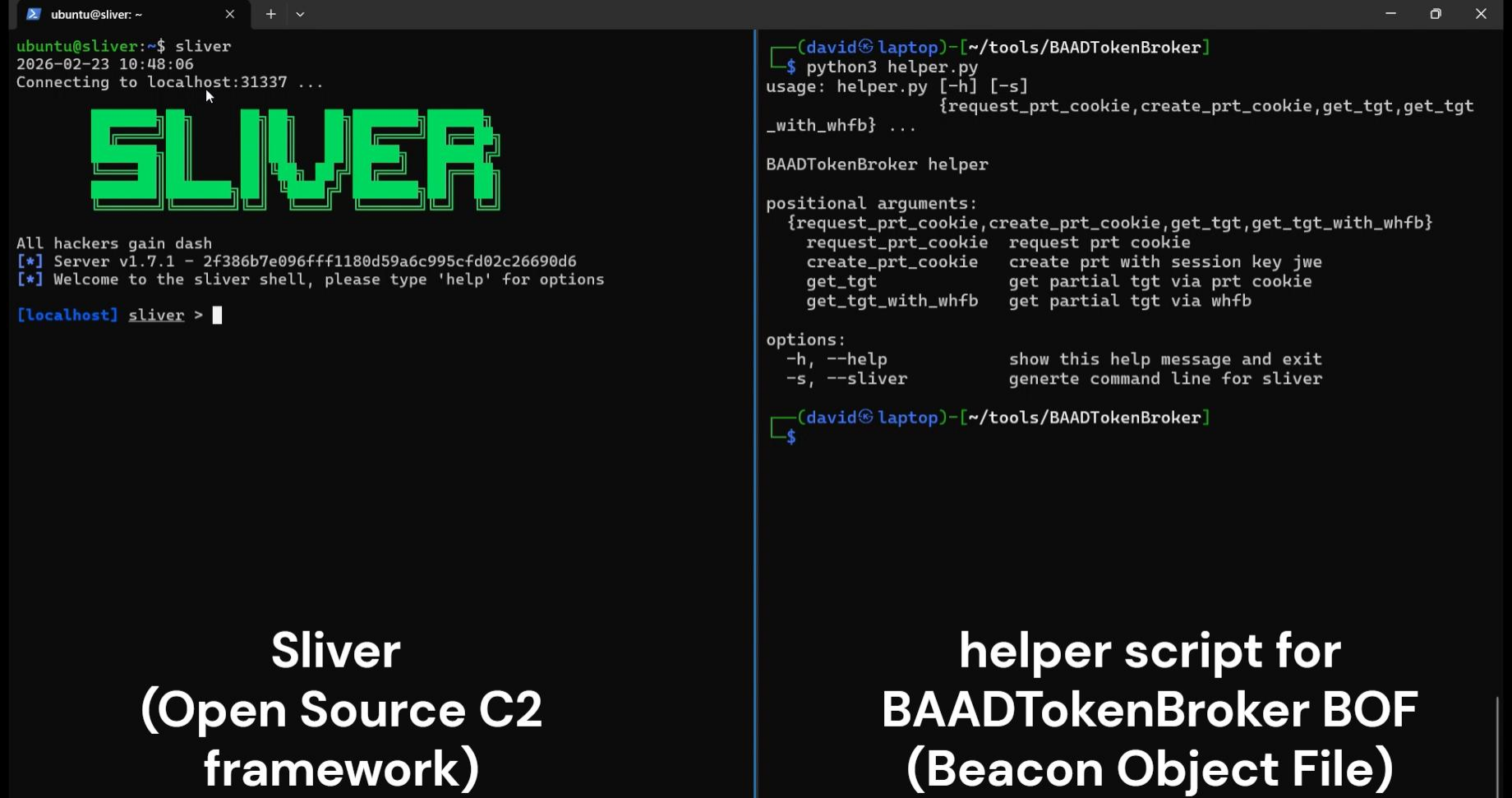


- Various cryptographic operations are possible using the encrypted POP key through the Windows APIs
  - Examples:

Function	Description
NgcSignWithSymmetricPopKey	Generate a signature of the provided input using POP key
NgcEncryptWithSymmetricPopKey	Encrypt the provided input using POP key
NgcDecryptWithSymmetricPopKey	Decrypt the provided input using POP key

Partial TGT to Full TGT

- By sending TGS REQ with the partial TGT and its session key, TGS REP can be received containing the full TGT and NT hash
  - This is already implemented in partialtofulltgt.py in roadtools_hybrid repository
    - https://github.com/dirkjanm/roadtools_hybrid/



Sliver
(Open Source C2
framework)

helper script for
BAADTokenBroker BOF
(Beacon Object File)

Credential Theft against Non-WHfB user

FUJITSU

- TGTs and NT hashes can be stolen from the context of a WHfB user

- But what if we have access to non-WHfB user instead?
  - Microsoft states that the TGT is issued when passwordless authentication

> If the user signs in by using a passwordless method (such as FIDO2 or Windows Hello for Business) on devices with Windows 10 (2004 or later) or Windows 11, Microsoft Entra ID issues an OnPremTgt for the user's on-premises Active Directory domain. This OnPremTgt contains the user's SID but no authorization data.

https://learn.microsoft.com/en-us/entra/identity/authentication/kerberos

Partial TGT issuance

FUJITSU

- As Dirk-jan described in his blog, Entra ID issues a partial TGT even when users authenticate with their passwords

`talkdevice.pem` and `talkdevice.key` respectively. Something interesting to note here is that while this mechanism is designed for passwordless authentication methods, Azure AD will also include the TGT if we authenticate with a password. With the password we could as well request a full TGT directly from Active Directory, but this will be relevant later in this blog.

https://dirkjanm.io/obtaining-domain-admin-from-azure-ad-via-cloud-kerberos-trust/

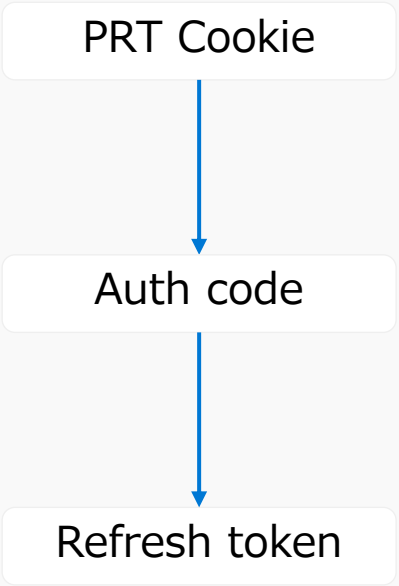
Partial TGT issuance

FUJITSU

- Partial TGT is issued whenever PRT is requested

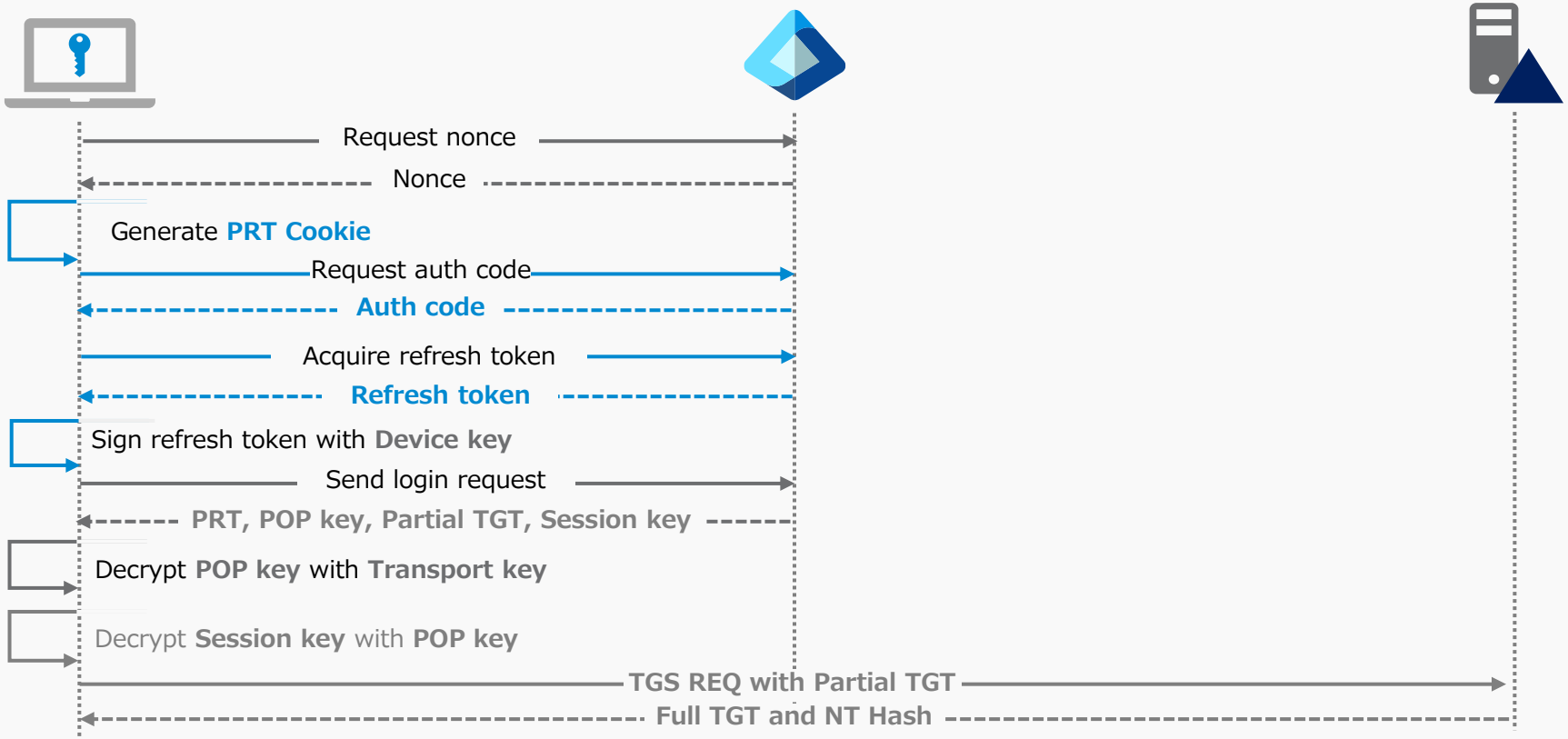
- Attackers can request a PRT and receive a partial TGT with;
  - Windows Hello for Business assertion
  - Passwords
  - Kerberos service ticket when Desktop SSO is enabled
    - This flow is recently added to ROADtools by Mauriceter
  - Refresh token with Microsoft Authentication Broker’s client id

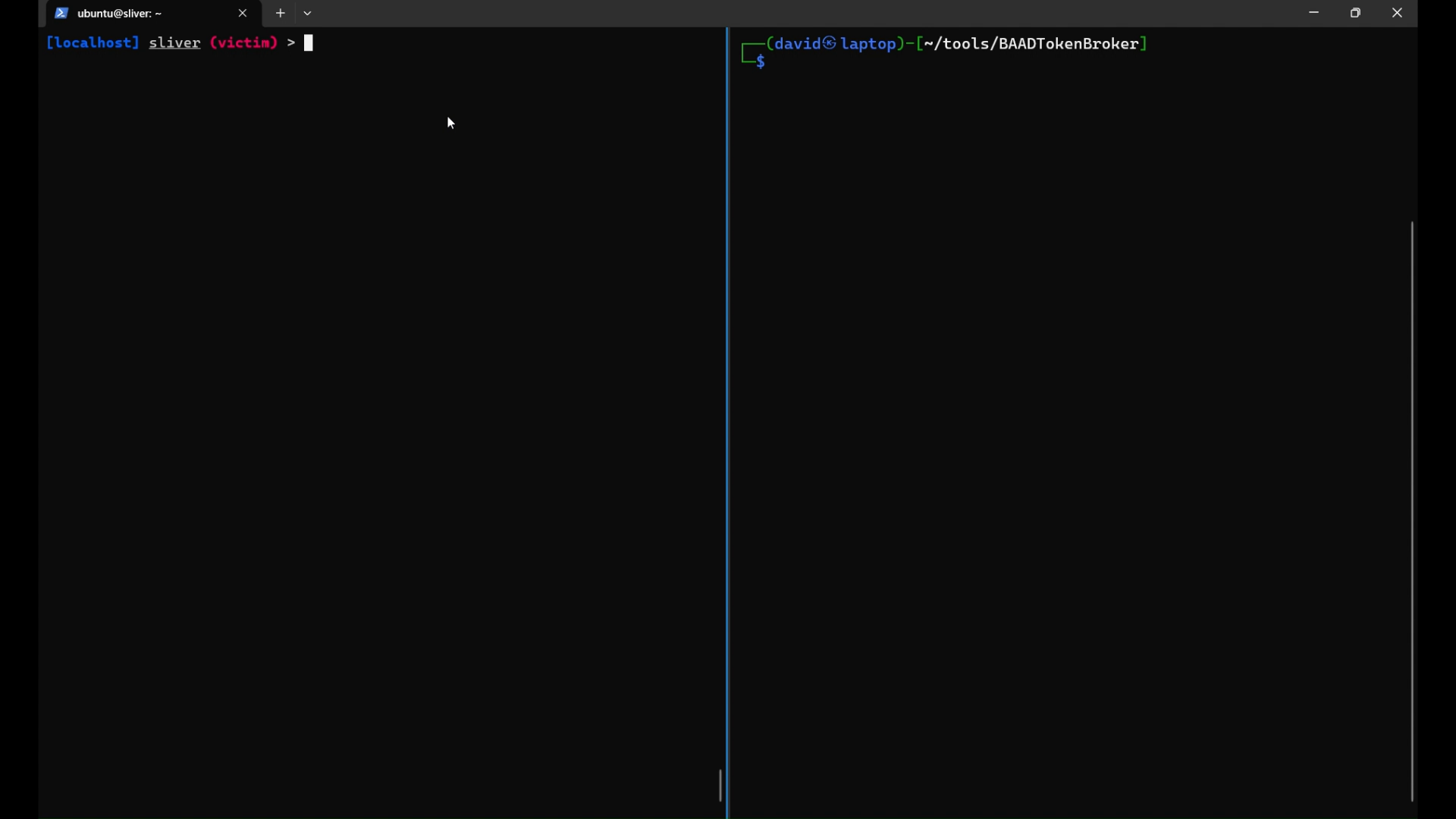
Journey to Refresh Token



- PRT Cookie can be stolen from a user’s context by abusing aadcloudap
- Authorization code can be requested with the PRT Cookie
- Refresh token with Microsoft Authentication Broker client id can be acquired with the auth code

Authentication Flow for Non WHfB User




ubuntu@sliver: ~
[localhost] sliver (victim) >
(david㉿laptop)-[~/tools/BAADTokenBroker]
$

Passwordless-to-Password Attack

FUJITSU

- Attackers can abuse the Microsoft Entra ID passwordless authentication to steal users' password hashes (NT hashes) and TGTs

- Prerequisites;
  - The target user exists in both Active Directory and Microsoft Entra ID
  - The attacker has code execution with the user's context
  - The environment is configured with the cloud Kerberos trust

FUJITSU

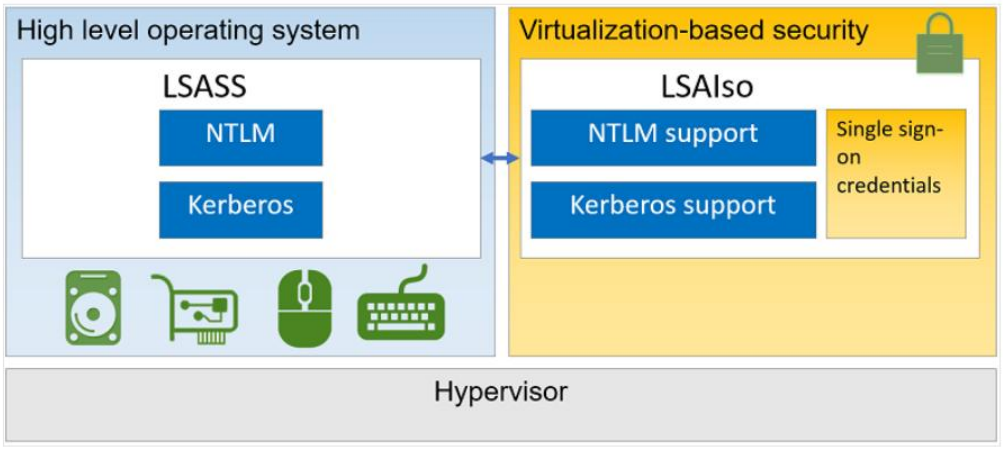
Limitations in Credential Guard

Protecting secrets in secure VM

FUJITSU

- LSAIso encrypts credentials and decrypts them when needed
  - LSASS only stores the encrypted blobs and can not access the decrypted credentials

- LSASS talks to LSAIso via its interface over ALPC/RPC
  - To interact with the interface, you need privileged access to LSASS as documented by Oliver Lyak
  - Or you can abuse Remote Credential Guard researched by Valdemar Carøe



Session key protection in Credential Guard

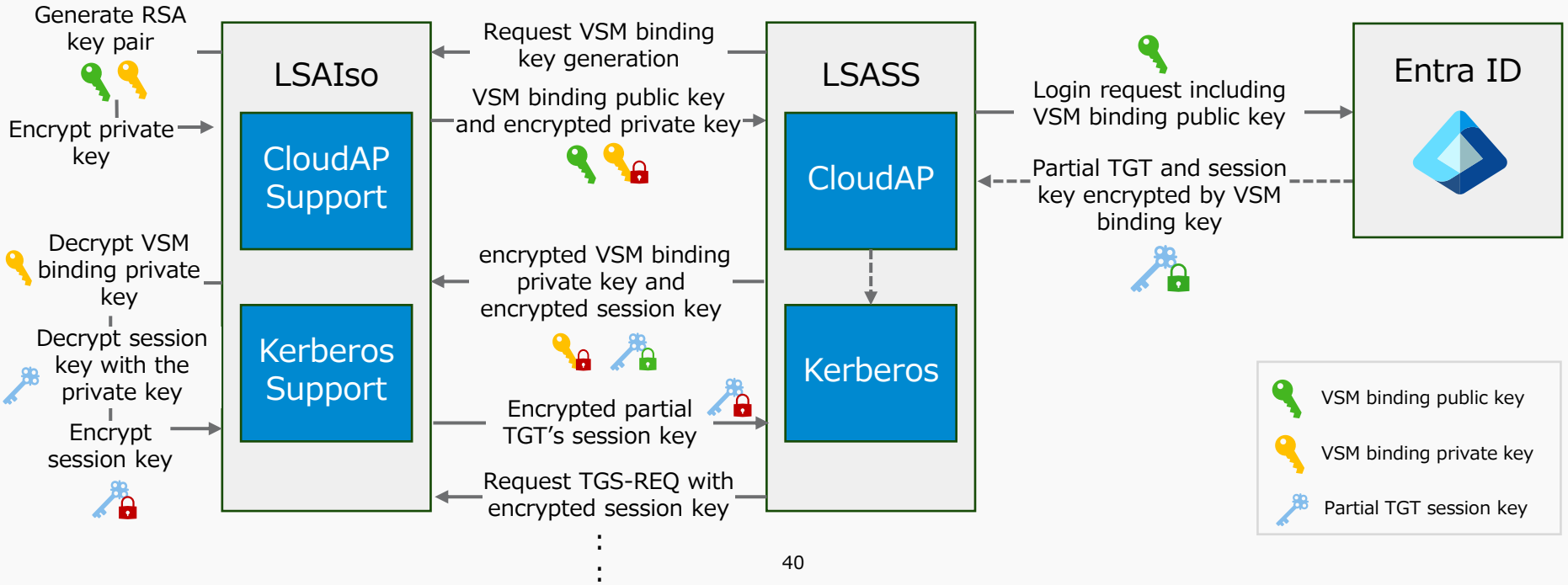
FUJITSU

- POP key can be used to decrypt the partial TGT session key that we directly received from Entra ID in a host with Credential Guard
- I initially thought the partial TGT session key cached in LSASS was protected by the **POP key on both systems with and without Credential Guard**
- Further analysis revealed that **LSAIso has a different interface for supporting Cloud Authentication package** and an RSA key pair called **VSM binding key** is used for protecting the session key

Session key protection in Credential Guard

FUJITSU

- On systems with Credential Guard, VSM binding key is used to decrypt partial TGT's session key but never leaves the secure VM



Session key protection in Credential Guard

FUJITSU

- Encrypted VSM binding private key and encrypted partial TGT session key is cached in LSASS
- They can be dumped through GetTokenBlob function in CloudAP without administrative privileges
  - lsa-whisperer by Evan McBroom was used as a reference for the implementation
- However, they cannot be used without code execution in LSASS and the session key cannot be exported in plaintext
  - Protected by Credential Guard


```
[+] get_token_blob success!
{
  "Version": 3,
  "UserInfo": {
    "Version": 2,
    "UniqueId": "5e36e583-37a5-4d78-892f-8350b6045fd2",
    "PrimarySid": "S-1-12-1-1580656003-1299724197-1350774665-3529442486",
    "DisplayName": "victim",
    "FirstName": "victim",
    "LastName": "",
    "Identity": "victim@ternp.com",
    "DownlevelName": "victim",
    "DomainDnsName": "ternp.local",
    "DomainNetbiosName": "ternp",
    "PasswordChangeUrl": "https://go.microsoft.com/fwlink/?linkid=2224198",
    "PasswordExpiryTimeLow": 3583418367,
    "PasswordExpiryTimeHigh": 2147483446,
    "PublicInfoPublicKeyType": 0,
    "Flags": 0
  },
  "Prt": "MS5BV3NBeXVnOWVtcUN2RVd3RUh0c1I3dTJsWWM3cWpodG9CZElzblY2TVdtSTJUc0FBSmhyQUEuQlFBQk...(omitted)...TWtiTG85dWZMejFpUQ",
  "PrtReceivedtime": 1772414983,
  "PrtExpirytime": 1773624582,
  "ProofOfPossesionKey": {
    "Version": 1,
    "KeyType": "ngc",
    "KeyValue": "AQAAAAIAAAABAAAA0Iyd3wEV0RGMegDAT8KX6wEAAACE...(omitted)...YKyC8SfJEpQlPKq8fpCByPA9A1XJnDsqJTqgC6xhw"
  },
  "SessionKeyImportTime": 1772414983,
  "VsmBindingPublicKey": "MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAoZgp6HncPG4BYaciqeN8lASERfmaONy-MzDXDEoDeFQJWOetzLGdEq473MMmJ11x2kTzsmZah...(omitted)...M8JJb7We7vYHYmtIFwh6BvgZvmcbrsoMeQIDAQAB",
  "VsmBindingPrivateKey": "EQUAAAAAAAASAAAAZAAAAAEAAAABAQAAAQAAAOfc_IgtilejTA6yeJ896yJaF4ZpV0jhHMiR-ts_drvdFCqFPu44VEP7rgCyY2IgUgEAAAAAAAAAAAAAAAAAAAAAAAAABAAAAm...(omitted)...SbqfOVrz37OqKVXwSLNddbDPDBQ_gk_lz0RH8cuwbRcByL4SnEck-0QTfnb5kseBgDb1kI2ThcGPg",
  "TgtMessage": "a4IF-DCCBfSgAwIBBaEDAgELow0bC1RFUk5QLkxPQ0FMpBMwEaADAgEBoQowCBsGdmljdGltpYIEnWGCBJkwggSVoAMCAQWhDRsLVEVSTlAuTE9DQUyiIDAeoAMCAQKhFzAVGwZrcmJ0Z3QbC1RFUk5QLkxPQ0FMo4IEWzCCBFegAwIBEqEGAgR7VQAAooIE...(omitted)...6-kH4kVeepH7h7rYqVZ7x4LK-tqSpeXkyWhqNFb2WpDlLjXm1F8GHIi37wmdmNWKFPKkz5KjbfBFCnj-E1bmrHg6pA8w9AYgYs_Uvkw2TSQ",
  "TgtClientKey": "Pr-5m8T9owNaLWRxrLarD3NHWEOQx58_5JXP99XdzI...(omitted)...9bjuwD2K1-8mVit
```

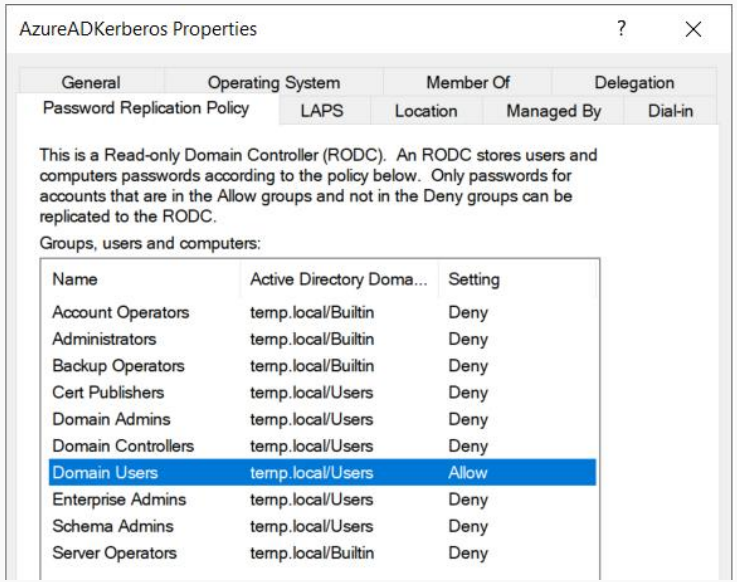
Limitations in Credential Guard

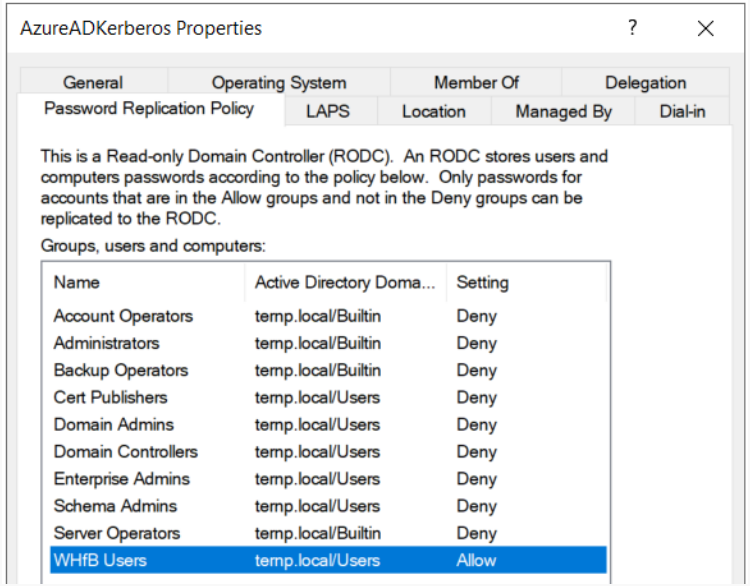
FUJITSU

- Credential Guard doesn’t protect the use of the POP key and the results of decryption using the key
  - Any type of blobs, including the partial TGT session key, can be decrypted by a POP key
  - POP key can be interacted without executing code inside LSASS nor administrator privileges
- This behavior appears to be part of the intended design but reported to Microsoft (2025/11/1)
  - I was told they are planning a fix for this case but it still has not been fixed after 139 days since the report

Mitigation

- Audit Kerberos Service Ticket request (Event 4769)
- Modify AzureADKerberos's msDS-RevealOnDemandGroup to only allow users using passwordless authentication
  - Examples: Remove "Domain Users" group from allowed groups and add another group





FUJITSU

Conclusion

Take Aways

FUJITSU

- By abusing the keys on the device, credentials can be easily extracted even from endpoints where Credential Guard is enabled
- Credential Guard does not protect all credential types, particularly those associated with Entra ID
- Limit the use of partial TGTs to only the users who require them

Tools Release

FUJITSU

- BAADTokenBroker
  - BOF version of the previous release ☺

https://github.com/temp43487580/BAADTokenBroker

Reference

FUJITSU

- The Kerberos Key List Attack: The return of the Read Only Domain Controllers by Leandro Cuozzo
- I Trusted You: A Demonstrated Abuse of Cloud Kerberos Trust by Daniel Heinsen and Elad Shamir
- Obtaining Domain Admin from Azure AD by abusing Cloud Kerberos Trust by Dirk-jan Mollema
- Pass-the-Challenge: Defeating Windows Defender Credential Guard by Oliver Lyak
- Unguarding Microsoft Credential Guard by Ceri Coburn
- Catching Credential Guard Off Guard by Valdemar Carøe
- lsa-whisperer by Evan McBroom

FUJITSU

Thank you