Windows Kerberos Custom Pre-authentication

Luke Howard, PADL Software, September 2021

Kerberos Pre-authentication

- Authenticates user (client) to KDC
- Typical mechanisms
  - Encrypted timestamp (RFC 4120)
  - Public key certs (RFC 4556)
- Client gets a ticket-granting ticket (TGT)
- KDC authenticates itself to client through proof of key possession or PKI
- TGT contains shared session key with KDC

GSS-API, SSPI

- Generalised framework for network authentication
- Exchange of an arbitrary number of opaque tokens, transport agnostic
- Upon completion: shared session key, authenticated client/server identities
- Typical mechanisms
  - Kerberos (RFC 4121)
  - NTLM
  - EAP (RFC 7055)

GSS Pre-authentication for Kerberos

- draft-perez-krb-wg-gss-preauth
- Uses GSS-API to authenticate client to KDC, KDC to client
- KDC maps GSS-API client to Kerberos principal name
- Client need not know Kerberos principal name
- KDC response encrypted in key derived from GSS-API session key
- Useful for federated authentication with EAP (RFC 7055)
- Open source implementation in Heimdal KDC

EAP SSP

- Implements EAP GSS-API mechanism (RFC 7055) as Windows SSP/AP
- Works with existing applications that support SSPI and Negotiate, such as SSH, LDAP, HTTP Negotiate, Exchange, etc.
- No source code changes required
- When used for interactive logon, user has no Kerberos credentials, thus:
- All services must also support EAP or have synchronised credentials
- This is a deployment barrier

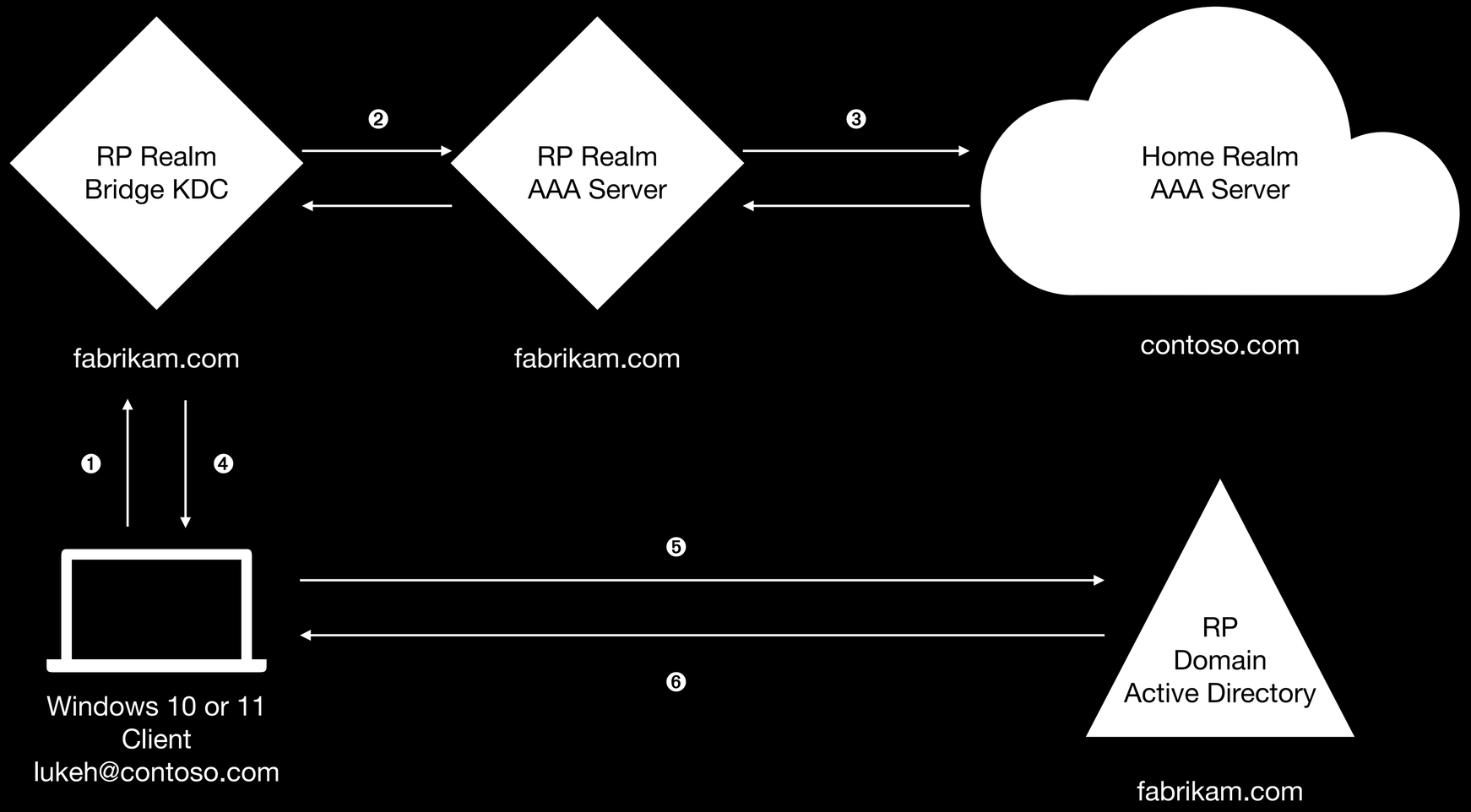
Surrogate Authentication Packages (AP)

- Undocumented API introduced by Microsoft to support FIDO
- Allows APs to supplement logon AP with additional data before authentication
- Compare with supplementary credentials which provide credentials to non-logon APs *after* authentication
- CloudAP authenticates user’s FIDO credentials in Azure AD
- Provides partial TGT (AS-REP) to Kerberos
- Kerberos package exchanges partial TGT for TGT containing authorisation data

TktBridgeAP

- New surrogate authentication package
- Implements GSS-API pre-authentication using SSPI
- Credential type agnostic, GSS/SSPI mechanism agnostic
- Bridge KDC shares restricted (RODC) krbtgt secret with Active Directory
- TktBridgeAP uses SSPI to pre-authenticate to KDC
- Passes partial TGT from KDC to Kerberos package
- Kerberos package exchanges partial TGT for full TGT, logs user on

TktBridgeAP with EAP SSP



1. User signs in using NAI; Workstation performs GSS EAP pre-authentication to bridge KDC in its realm (domain)
2. Bridge KDC forwards EAP messages to local AAA server
3. Local AAA server forwards EAP messages to user's home realm
4. Bridge KDC issues partial TGT for user lukeh@contoso.com in Kerberos realm FABRIKAM.COM, mapping user via UPN or altSecID attribute
5. Kerberos package on client workstation sends partial TGT to local AD KDC
6. AD exchanges partial TGT for full TGT containing user authorisation data, workstation logs user on

What’s the catch?

- Undocumented API, depends on internal data structures
- TktBridgeAP pretends to be CloudAP with FIDO credentials
  - Breaks distributing primary credentials to other SSPs
- Would prefer a stabler API
  - Change Kerberos AP to not require FIDO credentials before honouring AS-REP surrogate credentials
  - Change CloudAP to not release AS-REP surrogate credentials if it did not issue them (validate callback matches)

Further reading

- TktBridgeAP source code
  https://github.com/PADL/TktBridgeAP
- Heimdal GSS-API pre-authentication implementation
  https://github.com/heimdal/heimdal/tree/master/lib/gss_preauth
- Internet Draft (new update coming soon)
  https://datatracker.ietf.org/doc/html/draft-perez-krb-wg-gss-preauth
- SSO to Active Directory using FIDO2
  https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-authentication-passwordless-security-key-on-premises