3.8

Monday, September 25, 2023 11:26 AM

TPM = store keys for hard drive/SSD

HSM = PKI

password key - USB token for connecting to PCs and smartphones

NFC / bluetooth

attr based AC = group + roles + loc + ...

fine tuning AC

OpenID

- trusted id provider IdP providers "Sign on w/"
- make account w/ relying party RP or the site itself

user-centric-controlled federated id manage

enterprised-controlled federated id manage

solution

ex: SAML

Sandbox mode

role-based AC

protect pc/net systems using DAC

misconfigs in DAC

prevents mal script from running

w/ privileges of logged in user

restrict access based on roles instead

of based on user

OpenID = JSON/JWT

SAML = XML sigs

≠ PKI

Terminal access controller access-control System + TACACS+

network admin of routers

encryption + working w/ mult routers at once

NT LAN Manager NTLM - not strong auth

challenge/response which requires pword to be encrypted

CHAP - auth remotely linked users

challenge, response, verify

Kerberos on-path

provides mutual auth

Credential dumping

more susceptible to pass-the-hash

"golden ticket"

Service request - first part of auth process

timestamping for replay