Applied!

Data & Network Security

Behnam Amiri

ans.dailysec.ir

aNetSec.github.io

Spring 2025

User Authentication

Authentication

- User authentication is the process of determining whether some user or some application or process acting on behalf of a user is, in fact, who or what it declares itself to be.
- Authentication enables organizations to keep their networks secure by permitting only authenticated users (or processes) to access its protected resources.

Authentication Factors

Table 16.1 Authentication Factors

Factor	Examples	Properties
Knowledge	User ID Password PIN	Can be shared Many passwords easy to guess Can be forgotten
Possession	Smart Card Electronic Badge Electronic Key	Can be shared Can be duplicated (cloned) Can be lost or stolen
Inherence	Fingerprint Face Iris Voice print	Not possible to share False positives and false negatives possible Forging difficult

Multifactor Authentication (MFA)

- Multifactor authentication refers to the use of more than one of the authentication means in the preceding list.
- 2FA is common.

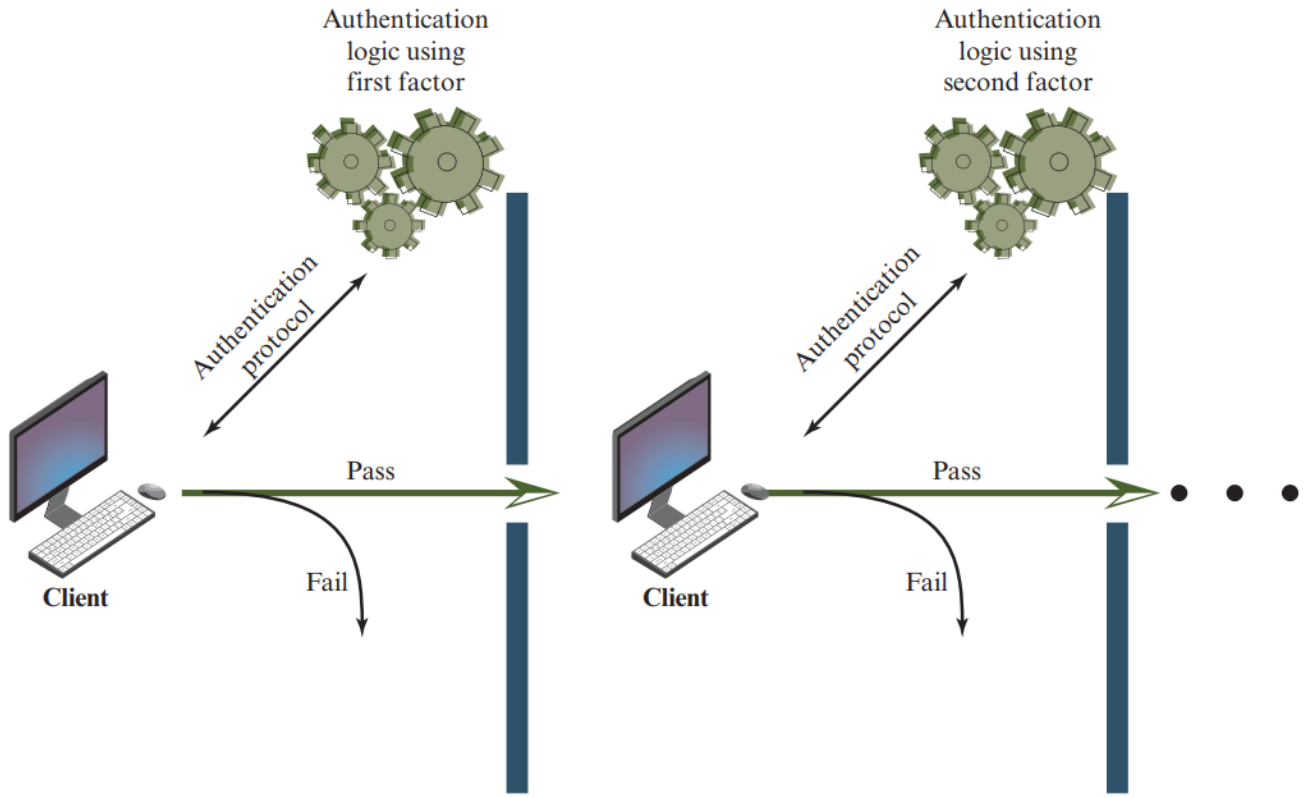
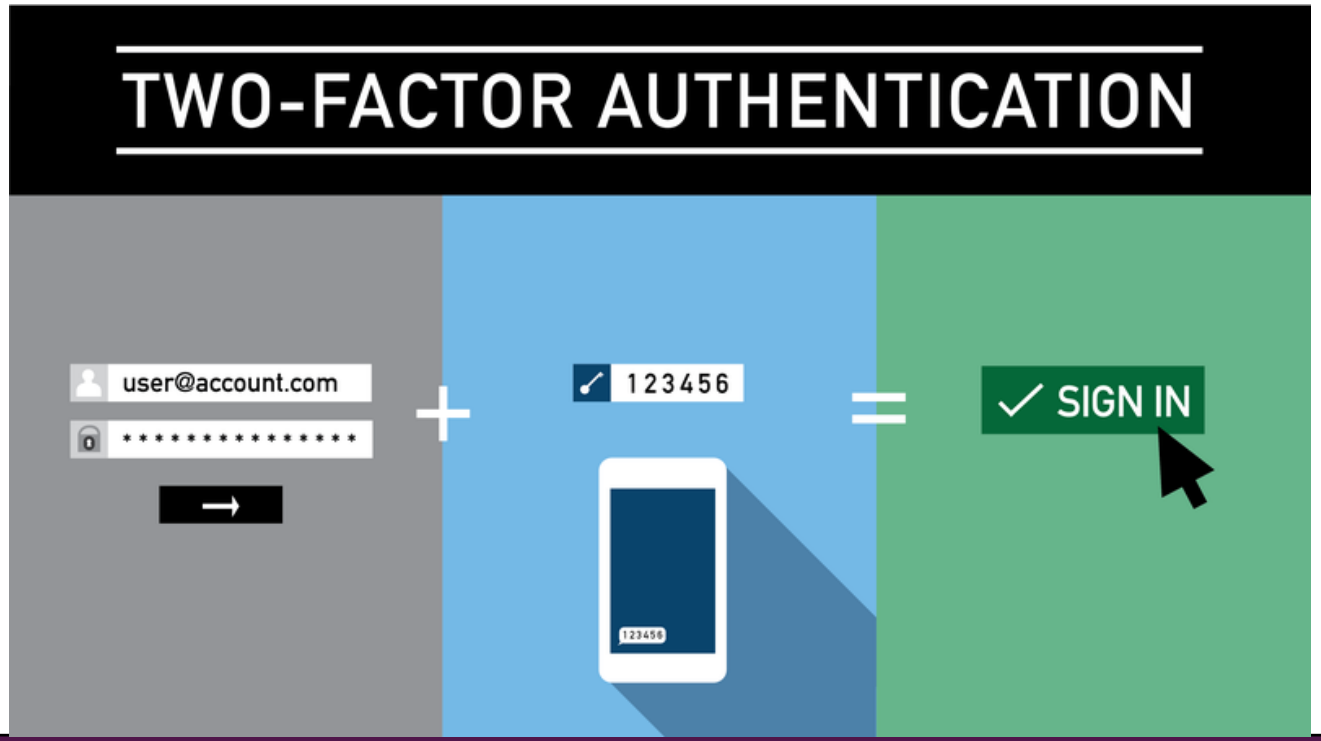


Figure 16.2 Multifactor Authentication

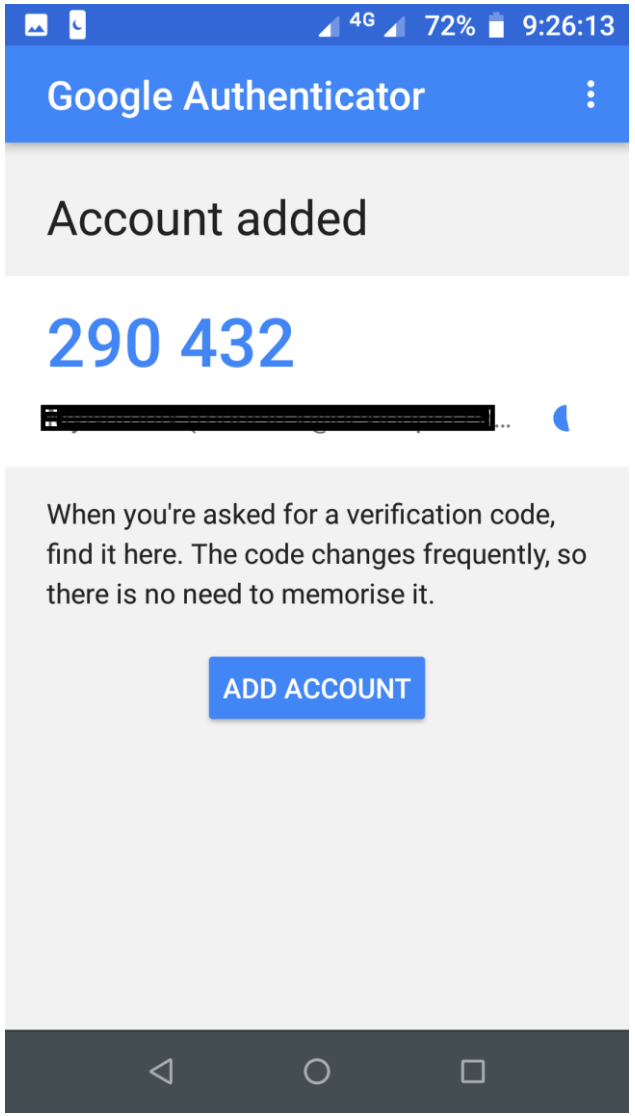
2FA

- SMS: Usage in Gmail, Banking, …
- Email: Usage in GitHub, Banking, …



2FA with App

- Authenticator Apps
- using the time-based one-time password
- TOTP; specified in RFC 6238
- using the HMAC-based one-time password
- HOTP; specified in RFC 4226



Replay attacks

1. The simplest replay attack is one in which the opponent simply copies a message and replays it later.
2. An opponent can replay a timestamped message within the valid time window. If both the original and the replay arrive within then time window, this incident can be logged.
3. As with example (2), an opponent can replay a timestamped message within the valid time window, but in addition, the opponent suppresses the original message. Thus, the repetition cannot be detected.
4. Replay back to the message sender. This attack is possible if symmetric encryption is used and the sender cannot easily recognize the difference between messages sent and messages received on the basis of content.

Remote User-authentication Using Symmetric Encryption

Mutual Authentication

- KDC -> trusted key distribution center.
- Each party in the network shares a secret key, known as a master key, with the KDC .
- The KDC is responsible for generating keys to be used for a short time over a connection between two parties.

Needham and Schroeder

- Secret keys Ka and Kb are shared between A and the KDC and B and the KDC, respectively.
- The purpose of the protocol is to distribute securely a session key *Ks* to A and B.

1. $A \rightarrow KDC: \quad ID_A \| ID_B \| N_1$
2. $KDC \rightarrow A: \quad E(K_a, [K_s \| ID_B \| N_1 \| E(K_b, [K_s \| ID_A])])$
3. $A \rightarrow B: \quad E(K_b, [K_s \| ID_A])$
4. $B \rightarrow A: \quad E(K_s, N_2)$
5. $A \rightarrow B: \quad E(K_s, f(N_2))$ where f() is a generic function that modifies the value of the nonce.

Denning

1. A → KDC: $ID_A \| ID_B$
2. KDC → A: $E(K_a, [K_s \| ID_B \| T \| E(K_b, [K_s \| ID_A \| T])])$
3. A → B: $E(K_b, [K_s \| ID_A \| T])$
4. B → A: $E(K_s, N_1)$
5. A → B: $E(K_s, f(N_1))$

T is a timestamp that assures A and B that the session key has only just been generated. Thus, both A and B know that the key distribution is a fresh exchange. A and B can verify timeliness by checking that

$$|\text{Clock} - T| < \Delta t_1 + \Delta t_2$$

Denning

- The Denning protocol seems to provide an increased degree of security compared to the Needham/Schroeder protocol.
- A new concern is raised:
- namely, that this new scheme requires reliance on clocks that are synchronized throughout the network.
- an opponent can intercept a message from the sender and replay it later when the timestamp in the message becomes current at the recipient’s site.

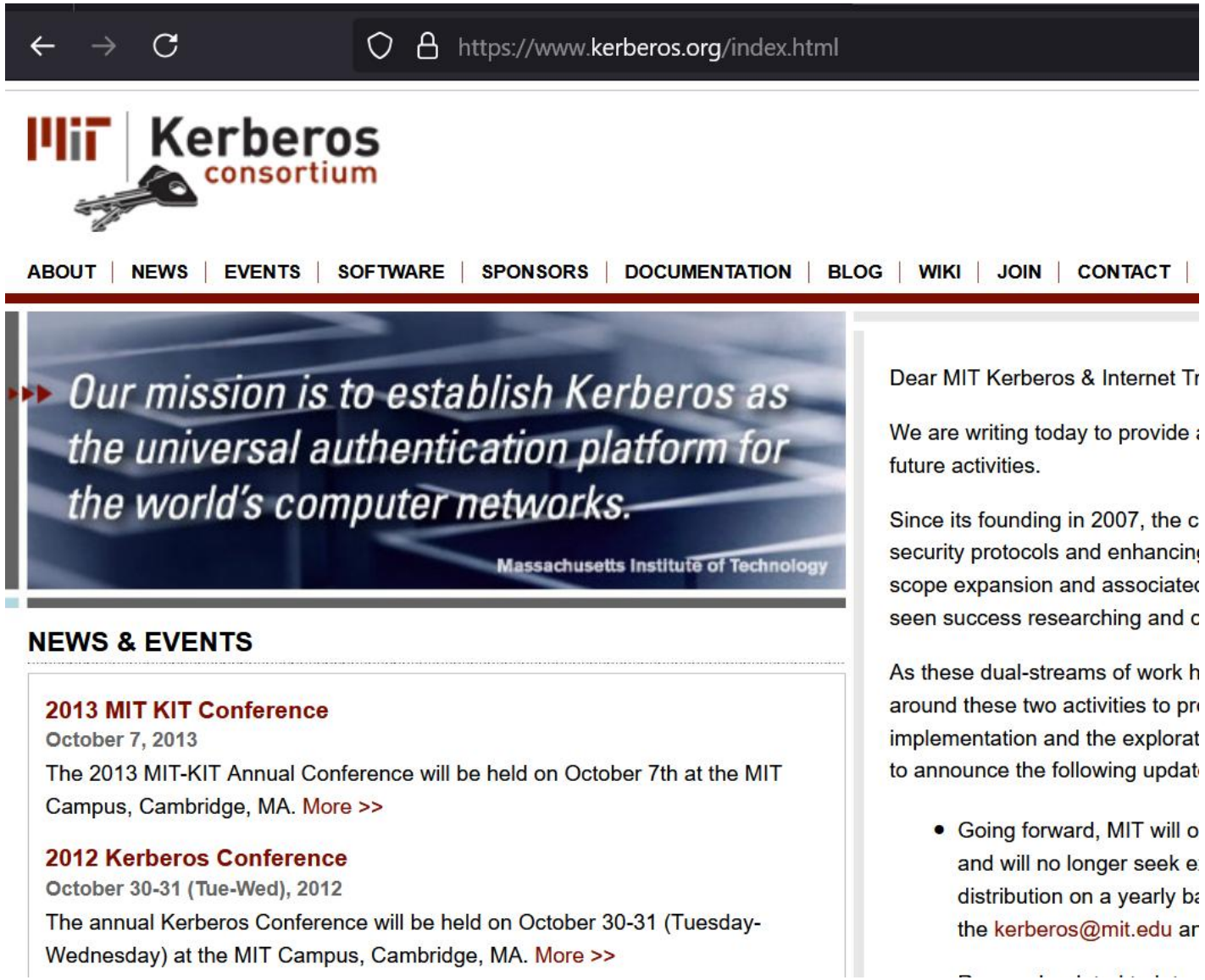
Kerberos

- Kerberos is the name of the three-headed dog from ancient Greek mythology that guarded the gates of Hades.
- Kerberos is a network authentication protocol invented at MIT in 1980.
- MIT released its Kerberos software as Open Source in 1987
- It became an IETF Standard in 1993.

Kerberos

- Kerberos has strong mutual authentication between client and server.
- Which makes it a very robust defense against phishing and so called, “man in the middle” attacks.
- Kerberos is built in to all major operating systems, from companies like Microsoft, Apple, Red Hat and Sun as well as others.
- Kerberos is the authentication mechanism for Microsoft’s Active Directory and even for some devices like the X-Box.
- The cable TV industry even uses Kerberos to authenticate set-top boxes and modems to their networks.

Kerberos


https://www.kerberos.org/index.html
Kerberos
consortium
ABOUT | NEWS | EVENTS | SOFTWARE | SPONSORS | DOCUMENTATION | BLOG | WIKI | JOIN | CONTACT
Our mission is to establish Kerberos as the universal authentication platform for the world's computer networks.
Massachusetts Institute of Technology
NEWS & EVENTS
2013 MIT KIT Conference
October 7, 2013
The 2013 MIT-KIT Annual Conference will be held on October 7th at the MIT Campus, Cambridge, MA. More >>
2012 Kerberos Conference
October 30-31 (Tue-Wed), 2012
The annual Kerberos Conference will be held on October 30-31 (Tuesday-Wednesday) at the MIT Campus, Cambridge, MA. More >>
Dear MIT Kerberos & Internet Tr
We are writing today to provide
future activities.
Since its founding in 2007, the c
security protocols and enhancin
scope expansion and associate
seen success researching and c
As these dual-streams of work h
around these two activities to pr
implementation and the explorat
to announce the following updat
Going forward, MIT will o
and will no longer seek e
distribution on a yearly ba
the kerberos@mit.edu ar

Kerberos

Table 16.2 Summary of Kerberos Version 4 Message Exchanges

(1)	**C → AS**	$ID_c \| ID_{tgs} \| TS_1$
(2)	**AS → C**	$E(K_c, [K_{c,tgs} \| ID_{tgs} \| TS_2 \| Lifetime_2 \| Ticket_{tgs}])$
		$Ticket_{tgs} = E(K_{tgs}, [K_{c,tgs} \| ID_C \| AD_C \| ID_{tgs} \| TS_2 \| Lifetime_2])$

(a) Authentication Service Exchange to obtain ticket-granting ticket

(3)	**C → TGS**	$ID_v \| Ticket_{tgs} \| Authenticator_c$
(4)	**TGS → C**	$E(K_{c,tgs}, [K_{c,v} \| ID_v \| TS_4 \| Ticket_v])$
		$Ticket_{tgs} = E(K_{tgs}, [K_{c,tgs} \| ID_C \| AD_C \| ID_{tgs} \| TS_2 \| Lifetime_2])$
		$Ticket_v = E(K_v, [K_{c,v} \| ID_C \| AD_C \| ID_v \| TS_4 \| Lifetime_4])$
		$Authenticator_c = E(K_{c,tgs}, [ID_C \| AD_C \| TS_3])$

(b) Ticket-Granting Service Exchange to obtain service-granting ticket

(5)	**C → V**	$Ticket_v \| Authenticator_c$
(6)	**V → C**	$E(K_{c,v}, [TS_5 + 1])$ (for mutual authentication)
		$Ticket_v = E(K_v, [K_{c,v} \| ID_C \| AD_C \| ID_v \| TS_4 \| Lifetime_4])$
		$Authenticator_c = E(K_{c,v}, [ID_C \| AD_C \| TS_5])$

(c) Client/Server Authentication Exchange to obtain service

Kerberos

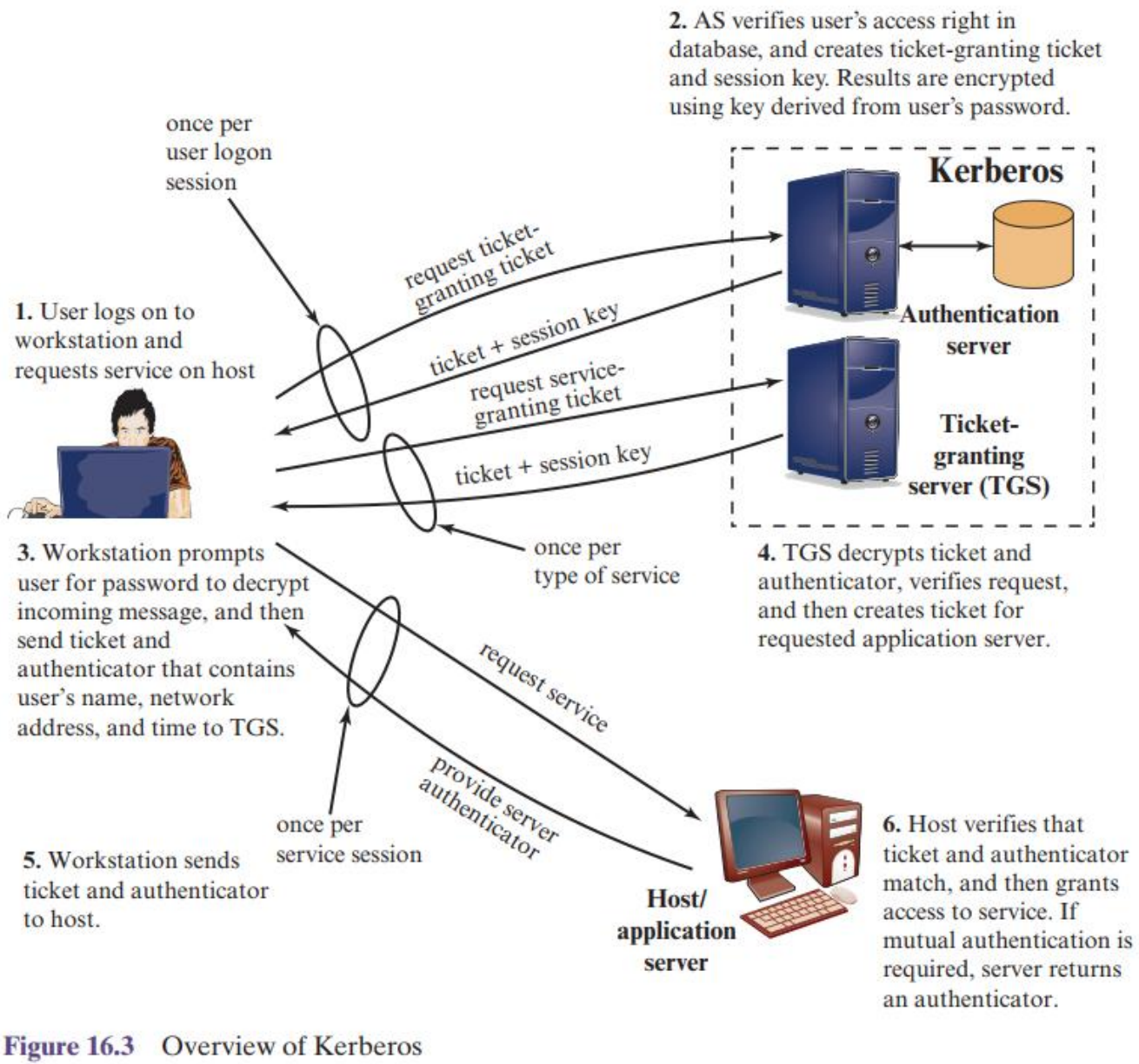


Figure 16.3 Overview of Kerberos

Kerberos

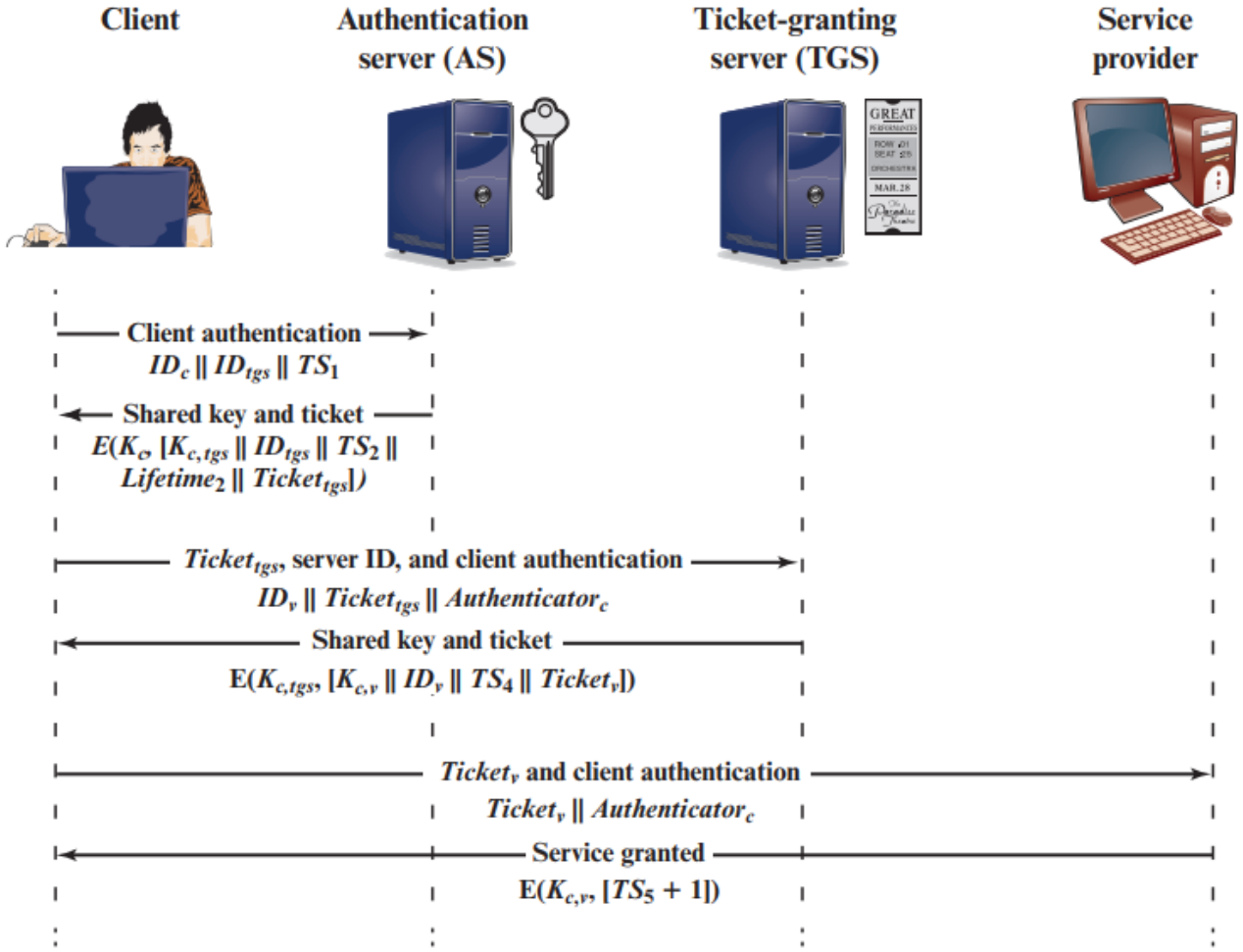
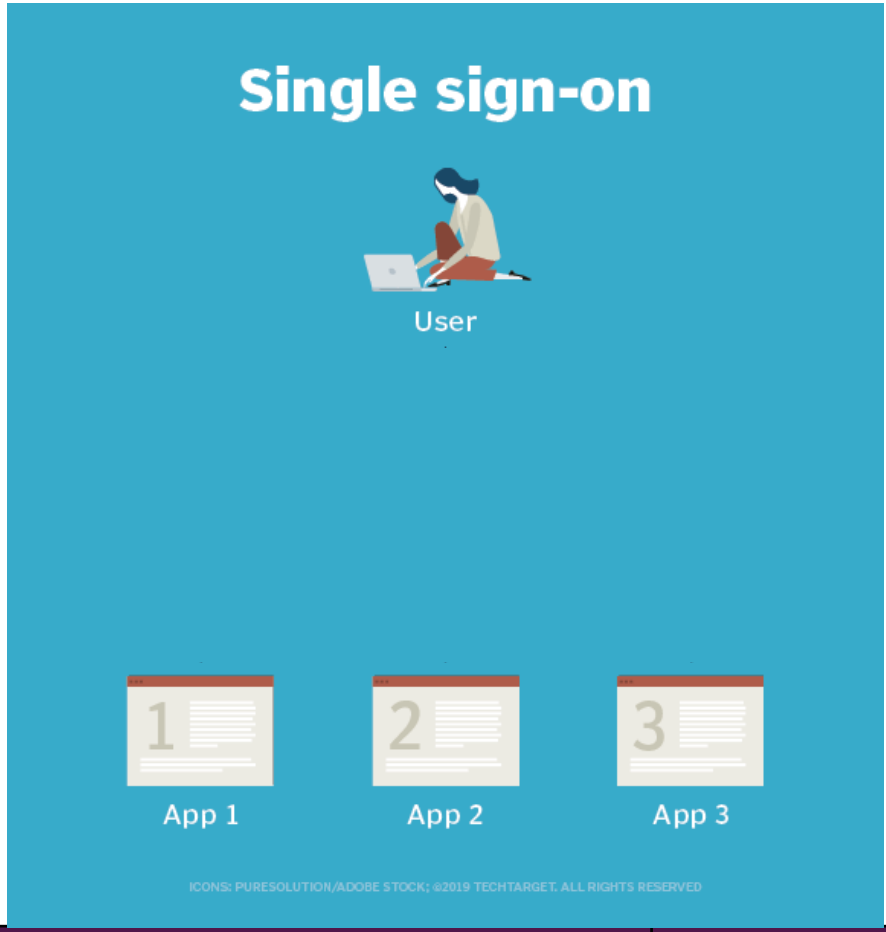


Figure 16.4 Kerberos Exchanges

Single sign-on (SSO)

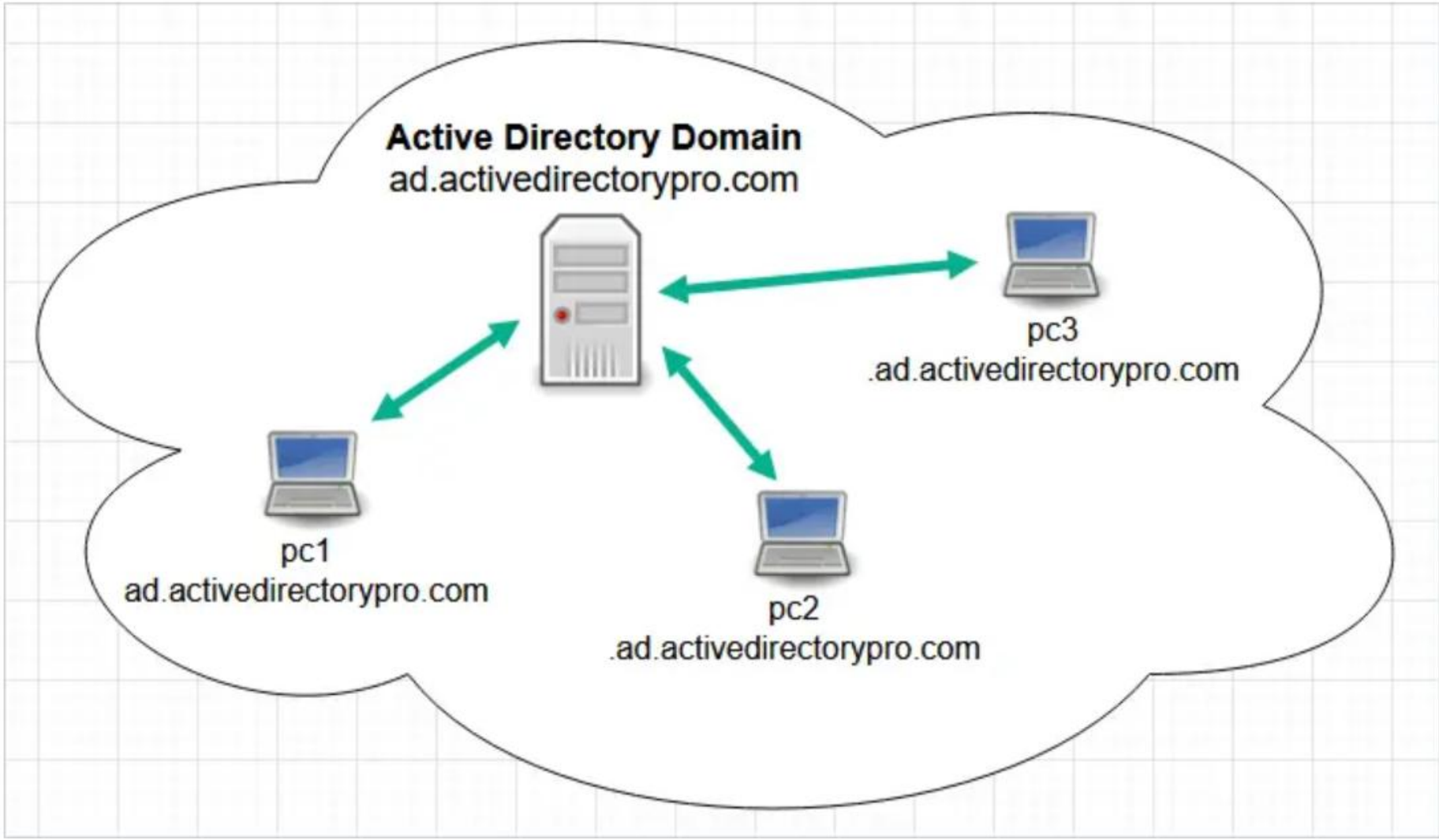
- One account for access to all app and resources.
- Easy management.
- Change one password!
- Disable/Enable one account.
- Active Directory give SSO to us.



Active Directory

- Active Directory (AD) is a Microsoft service that provides centralized authentication and authorization to network resources.
- Active Directory was first released with Windows Server 2000.
- **Authentication** is the process where Active Directory verifies a user's credentials (username and password).
- **Authorization** is the process that grants or denies a user to do something such as edit a file or access an application.

Active Directory

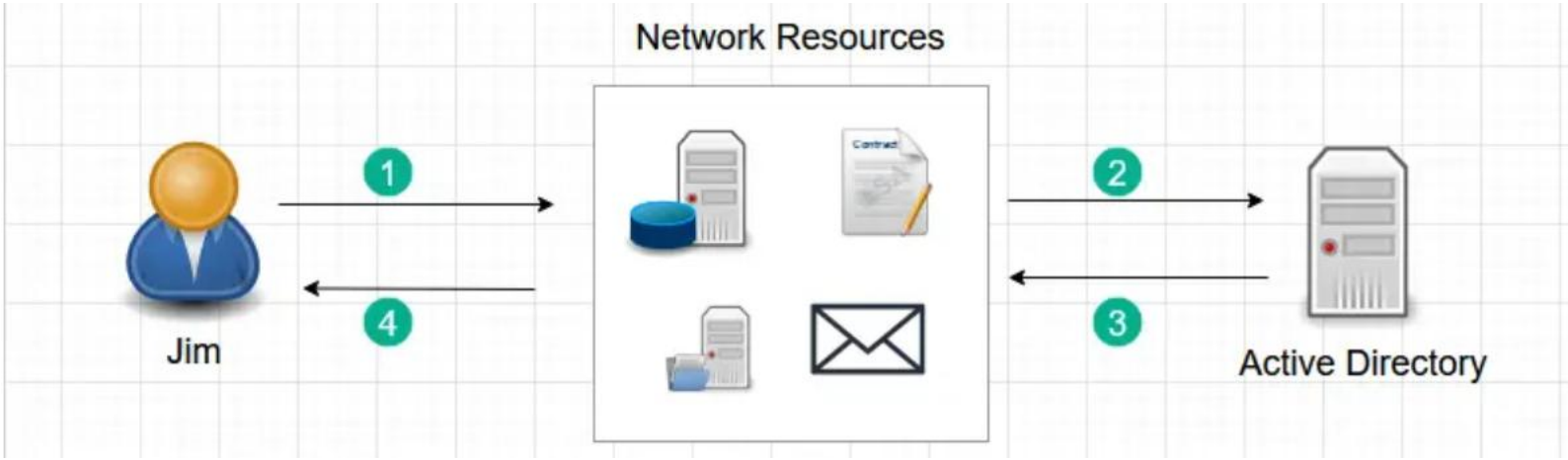


Example 1 – Authenticate Users

1. Jim logs into company PC with the provided username and password.
2. The logon request goes to the AD server to verify Jim's username and password.
3. Active Directory looks up Jim's account and verifies the username and password. The account has been verified.
4. Jim is now logged into to PC.

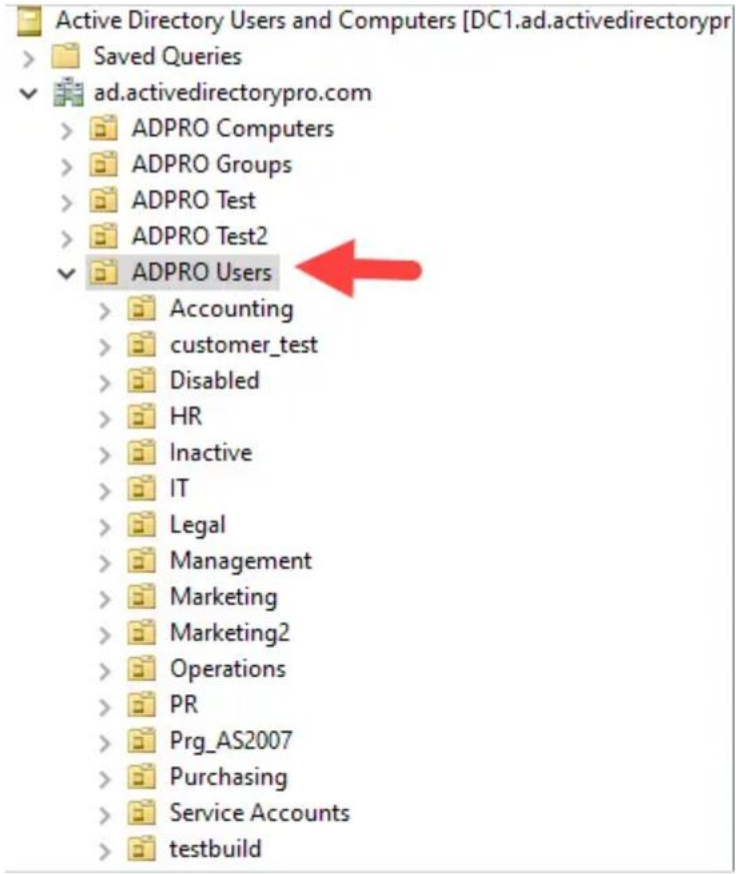
Example 2 – Authorize User

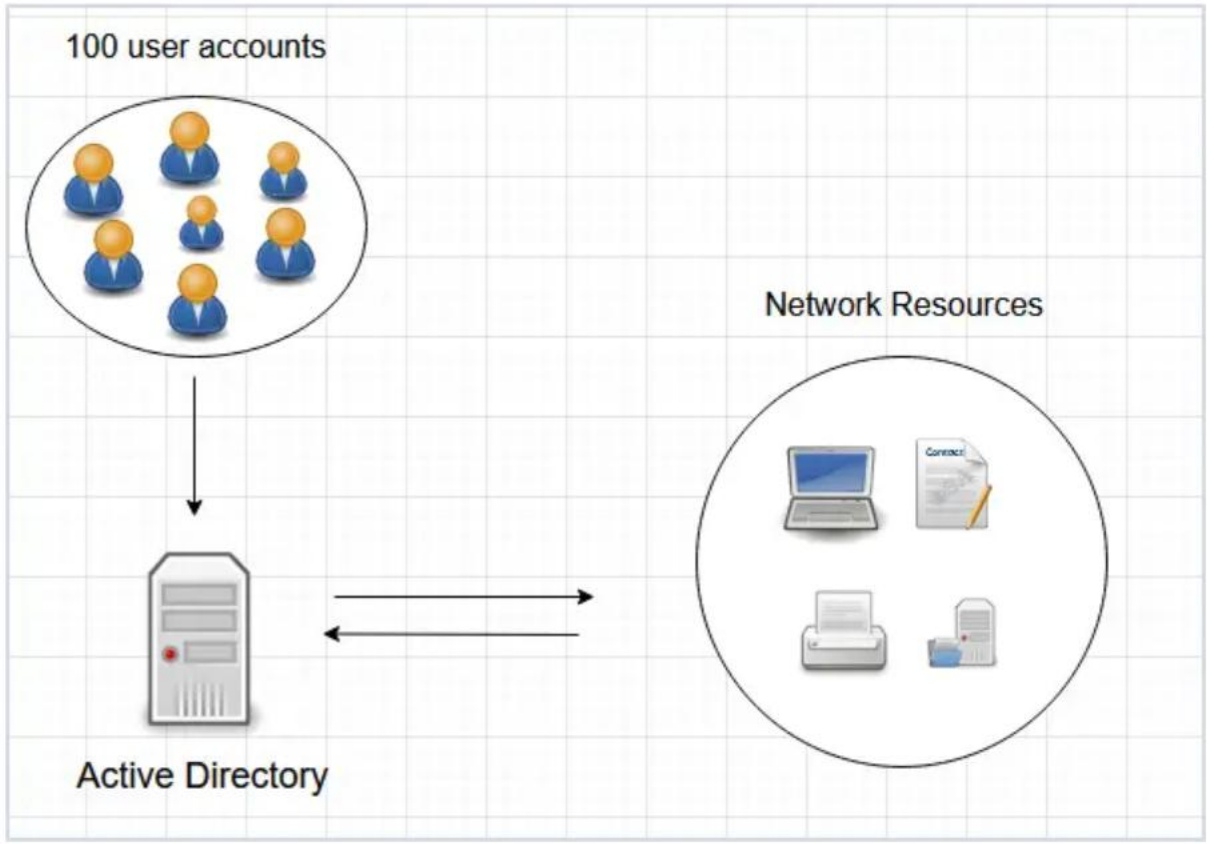
1. Jim logs into his computer using his username and password and wants to access his email, a contract file, and the accounting database server.
2. These network resources check with AD to see if Jim's account is authorized for access.
3. Active Directory verifies Jim's account is authorized for access.
4. Jim's account is granted access. Jim can now check email, modify the contract file and work on the database server.



Centralized Management of User Accounts

- you could organize all users into their own department folders.





Active Directory

- More at:
- https://activedirectorypro.com/what-is-active-directory/

Kerberos Attacks

- Kerberoasting
- Golden ticket
- Silver ticket