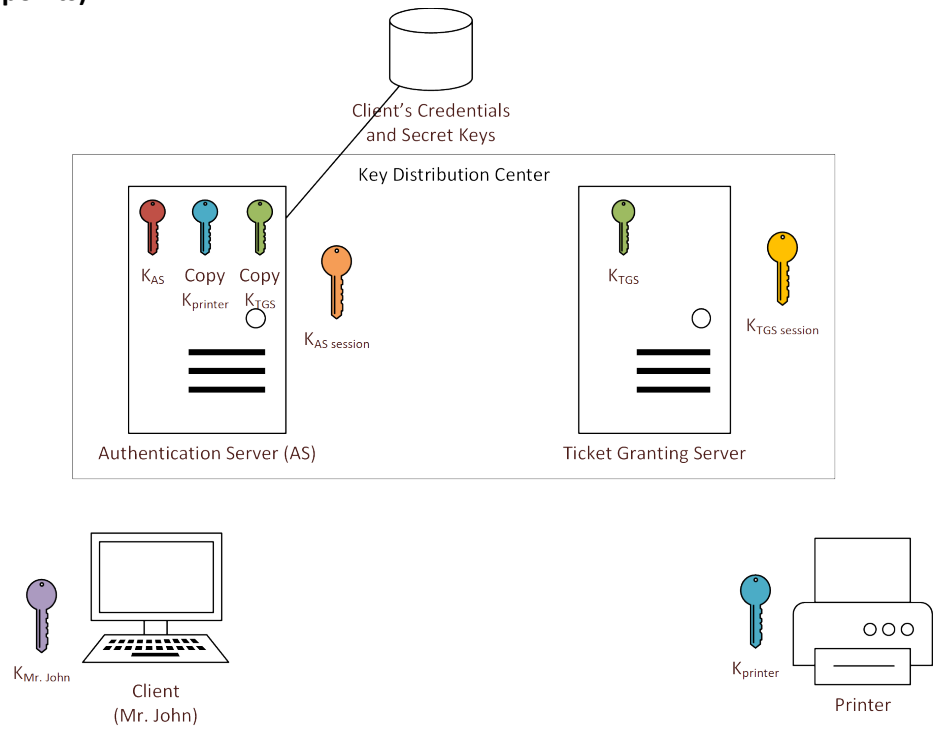
Sarah Tse

Assignment 2: Identity and Access Management

1) ABC Inc uses Kerberos authentication scheme in their organization to verify user credentials in their network infrastructure. Users can have access to various systems like unix servers, databases, printers, etc. If a user, say Mr. John for example, wants to connect to a network printer on Kerberos authentication scheme, describe in detail, the steps involved in authenticating John and letting him access the printer. (10 points)

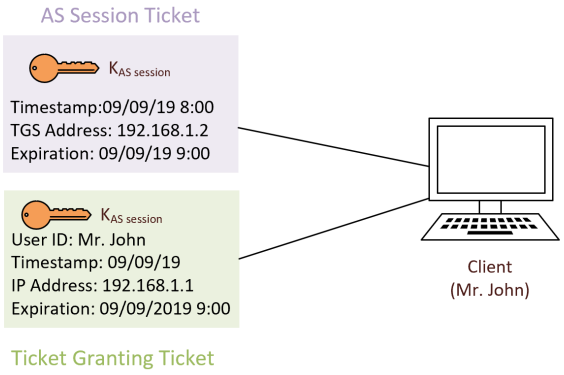


The Kerberos authentication scheme can be broken down into a few simple steps but behind the scenes, there is a lot more detail that happens in the background.
Before this process starts, the AS within the KDC maintains copies of the printer and TGS keys.

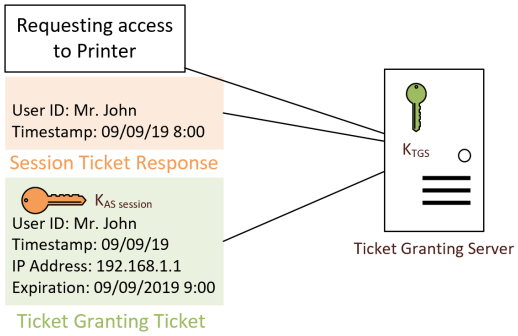
1. The KDC verifies the credentials and sends back an encrypted TGT
    - Mr. John first enters his password which is packaged with a timestamp, user ID, name of resource and his IP address. This package is encrypted with Mr. John's key (purple).

    - The package is sent to the AS which is then decrypted with a copy of Mr. John's key previously shared. This proves Mr. John's identity to the AS.

- The AS then sends two packages back:
    a. The first package is the session package that contains the AS generated short lived session key (orange), the timestamp, TGS IP address, and expiration time. The package is then encrypted with the copy of Mr. John's key stored in the AS. This package ensures that Mr. John is the only person who can receive the request.
    b. The second package is the Ticket Granting Ticket (TGT) and also contains a copy of the AS session key(orange), Mr. John's user ID, timestamp, Mr. John's IP address, and expiration time. The TGT is then encrypted with the Time Granting Server's Key (green)



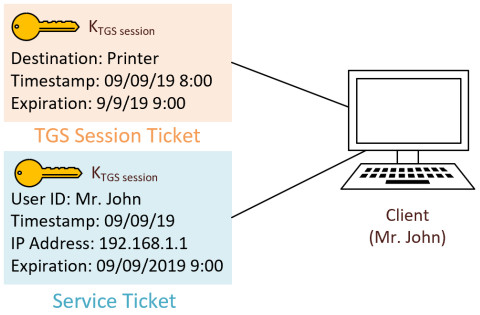
2. The client stores the TGT and when it expires the local session manager will request another TGT
    - Mr. John will receive both packages but can only decrypt the AS session package with his own key and get the TGS address and the AS session key.
    - The TGT cannot be decrypted but will be cached and used later.
3. The client sends the current TGT to the TGS with the service principle name (SPN) of the resource the client wants to access.
    - Mr. John will then construct two new packages. The first one is another session package that contains his user ID and timestamp and is then encrypted with the AS short session key. The second is just a plaintext request. Both packages are forwarded to the TGS address received from the step before.
    - Mr. John also forwards the TGT to the TGS.



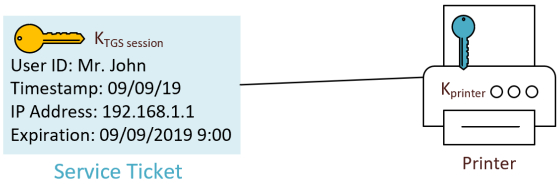
4. TGS sends a valid key session for the service to the client
    - The TGS will receive all three packages and will decrypt the TGT with it's own key to receive the AS session key which will decrypt the session package. If all the information matches, then this verifies that Mr. John is really the one who sent the request.

- The TGS will grab the printer's key (blue) from the AS and create a TGS session key.
- A service ticket package will be constructed which contains the TGS session key, user ID, Mr. John's IP address, timestamp and expiration time. This package is encrypted with the TGS key.

- A TGS session package will also contain the printer's key with the destination name (printer), timestamp and expiration date. This package is encrypted with the AS session key.
- Both the service ticket and TGS session package are sent to the client.



5. Client forwards the session key to the service for access
   - Mr. John can decrypt the TGS session package with the AS session key (received earlier) to get the TGS session key. The printer session package is then created with Mr. John's user ID, and timestamp and encrypted with the TGS session key.
   - Mr. John cannot decrypt the service ticket but will forward it and the printer session package to the printer.



6. Printer receives the service
   - The printer will decrypt the service ticket with its own key and receive the TGS session key to decrypt the printer session package.

Once all these steps are completed, the printer will fulfill its request. In the event that any of packages expire, the re-authentication process must be completed again. (Mangiacapre, 2018)

2) Describe the differences between the following protocols – Diameter, Radius, TACAS and TACAS+ (10 points)

Radius stands for Remote Authentication Dial-In User Service and is a protocol used to send authenticate and authorize between the authentication server and network authentication server(NAS), whether the person is using dial-up, wireless access, or VPN. The protocol mainly utilizes the User Datagram Protocol at the link-layer of the network stack, specifically port 1812 for authentication and 1813 for accounting. To transport the data, Radius uses 8 bit long attribute-value pairs (AVPs) which allow data points to

be sent together (Narasimhan, 2019). Lastly, not all packets are encrypted, only the ones that carry the passwords are.

Diameter is based off of Radius but has slight improvements such as:

- Peer to Peer architecture: Unlike Radius, Diameter introduces agents or intermediaries between the NAS and AS which helps with load balancing, scalability, and efficiency when processing requests (Ribbon Communications, n.d.).
- TCP and TLS: To deliver the packets, Diameter uses Transmission Control Protocol which is slower but more reliable and orderly than UDP (Diffen, n.d.). Additionally, Diameter includes Transport Layer Security(TLS) which secures the data from disclosure.
- Failover mechanisms: Since Diameter uses TCP, which is connection based, error packets can be sent back and forth allowing proper responses (Diameter Protocol Explained, n.d.). This is different than Radius because UDP is a connectionless protocol.
- Bigger AVPs: The AVPs are now 32 bits long which allows for more variety.

TACACS stands for Terminal access controller access control system and is also used for remote authentication but uses UDP through port 49, encrypts all packets and does not support the Kerberos authentication protocol (Difference Between, 2012).

TACACS+ is a derivative of TACACS and is different in that it separates authentication, authorization, and accounting and improved protection.

- Separation of AAA: This allows for granular control meaning that users can run commands on the different devices.
- Improved Protection: Among many of the changes is that TACACS+ uses TCP which is more secure and reliable than UDP. The protocol also supports two factor authentication and encrypts the entire packet. Additionally, the “accounting” part is different than TACACS because the protocol allows for command logging (IPWithEase, 2017).

Sarah Tse

References

Cyber Security Entertainment. (2019). TACACS, XTACACS, RADIUS, TACACS+, DIAMETER. Retrieved from https://www.youtube.com/watch?v=k_wu6sOawKg

Diameter Protocol Explained. (n.d.). Improvements of Diameter over RADIUS. Retrieved from https://ribboncommunications.com/company/get-help/glossary/diameter-protocol

Diffen. (n.d.) TCP vs. UDP. Retrieved from https://ribboncommunications.com/company/get-help/glossary/diameter-protocol

Difference Between. (2012). Difference Between Diameter and Radius. Retrieved from https://www.differencebetween.com/difference-between-diameter-and-vs-radius/

IPWithEase. (2017). TACACS Vs. TACACS+. Retrieved from https://ipwithease.com/tacacs-vs-tacacs/

Mangiacapre, Tom. (2018). Kerberos Explained. Retrieved from https://www.youtube.com/watch?v=2WqZSZ5t0qk

Narasimhan, Prithi. (2019). ITSS 4V95 IT Cybersecurity Identity and Access Management (Asset Security). 42-45. Retrieved from

Ribbon Communications. (n.d.). What is Diameter Protocol?. Retrieved from https://ribboncommunications.com/company/get-help/glossary/diameter-protocol

TACACS.net. (2011). The Advantage of TACACS+ for Administrator Authentication. Retrieved from https://tacacs.net/docs/TACACS_Advantages.pdf