u20734621

Matthew Gotte

COS330 – Practical 2

Certificate-based authentication

What is used for identification?

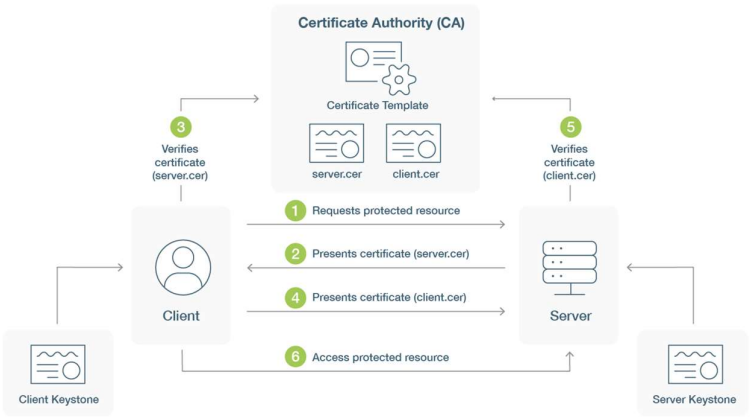
A digital certificate (an official document attesting a fact) is used to identify the user, machine, or device of sort before granting access to some resource. The certificate is granted by some entity known as a CA (Certificate Authority).

What is used for authentication?

Single sign on process and certificated are used to authenticate the sender by having the client digitally sign a piece of data using their private key, then send the signed data and the client certificate across the network. The receiver then compares the signed data with the public key stated within the certificate and if the results match authentication is complete. Thus, a matching signed piece of data and the public key is used for authentication.

How does it work?

A client will request a protected resource and then be presented with the server certificate. The client will then provide their certificate as well as a signed piece of data to the to the trusted third-party CA who will compare the signed data using the public in their certificate as well as to the server they are requesting. The server then independently verifies the received certificate with the third party to determine validity. The client is then granted access to the protected resource based on the outcome of the validation with the third party.



How can it be attacked?

Digital certificates are stored on a device meaning they can commonly be attacked through trying to steal them (certificate theft). Attackers then use the stolen certificate to spoof a trusted website and trick clients into sharing information with them as they appear to be authenticated.

Countermeasures?

Monitoring of digital certificated through IP-based monitoring by scanning the network and detecting if a certificate is out of the ordinary or near expiry.

References:

GMO. (2022). *What Is Certificate-Based Authentication and Why Should I Use It?* Retrieved from Global Sign: https://www.globalsign.com/en/blog/what-is-certificate-based-authentication#:~:text=Certificate%2Dbased%20authentication%20is%20the,such%20as%20username%20and%20password.

GMO. (2022). *What is Public-key Cryptography?* Retrieved from Global Sign: https://www.globalsign.com/en/ssl-information-center/what-is-public-key-cryptography

RAMAMOORTHY, N. (2021). *How to Prevent Digital Certificate Theft – A Lesson From a Recent Breach*. Retrieved from appviewx: https://www.appviewx.com/blogs/how-to-prevent-digital-certificate-theft-a-lesson-from-a-recent-breach/

yubico. (2022). *What is Certificate-Based Authentication?* Retrieved from yubico: https://www.yubico.com/resources/glossary/what-is-certificate-based-authentication/#:~:text=A%20certificate%2Dbased%20authentication%20server,both%20sent%20across%20the%20network