RSA AND DIGITAL CERTIFICATES CONT.

Lecture 7a

COMPSCI 726

Network Defence and Countermeasures

Muhammad **Rizwan** Asghar

August 2, 2021

THE UNIVERSITY OF AUCKLAND
NEW ZEALAND

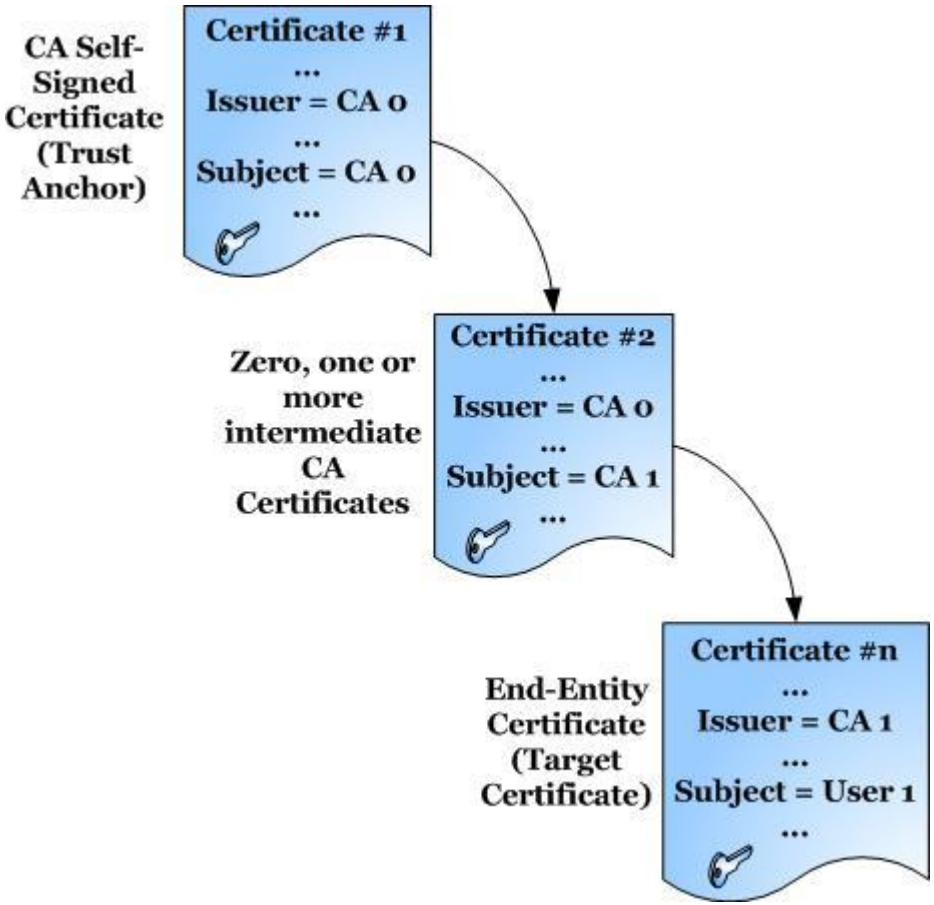
X.509 CERTIFICATES

- Use of digital certificates issued by a trusted Certificate Authority (CA)
  - E.g., VeriSign
- A digital certificate contains information to assert an identity claim
  - Version and serial number
  - Issuer and interval of validity
  - Subject's name and public key
  - Signature algorithm and signature
  - Some other fields
- Certificate Revocation List (CRL)

CERTIFICATE VALIDATION

- Obtain the subject's public key
- Decipher the signature
- Re-compute hash of the certificate and compare
- Check validity of the interval
- Also check if the certificate is not revoked

VERIFY CERTIFICATE PATH



Source: www.oracle.com

ROOT CERTIFICATE AUTHORITY

- Manages lifecycle of digital certificates
- A trusted third party
- A root CA issues a self-signed root certificate
- A verifier must know the root certificate
- A set of root certificates are pre-installed
- Check installed root certificates
  - E.g., Windows: Open run and type ‘certmgr.msc’

SUMMARY

- RSA is used for signing or encrypting
- PGP or X.509 certificates could be used for key binding
- In PKI, there is a chain of certificates ending with a root CA
- A root CA is a self-signed certificate

RESOURCES

- Read Chapters 3 and 4 of
  Network Security Essentials – Applications and Standards
  Fourth Edition
  William Stallings
  Prentice Hall
  ISBN 0-13-706792-5

Questions?

Thanks for your attention!