Network Security - C2 Assignment 2
Date: 18-10-20

Question:When do we use the hierarchical architecture in the trust model and when do we use the mesh architecture. Explain how a user under one CA can obtain the certificate of a user under another CA in both the architectures using examples

Solution: Hierarchical architecture in the trust model is implemented as an inverted tree structure, where the tree is the starting point of trust. For better visualization, we can see it like this:

- Root is the starting point of the trust.
- The top-down parts of the branches have a CA.
- The leaf node is the user.

All nodes of the model have to trust the root CA and communication between any two users for validating each other's public key must be achieved through the root CA. As it can be seen, the root CA is the trust center of all it's users and in case of any crisis in root CA's trust occurs, then a trust crisis occurs throughout the PKI system. Hierarchical PKIs are scalable; certification paths are easy to develop because they are unidirectional and certification paths are relatively short This particular property makes it extremely useful in the chaotic Internet environment. It's use is done in the military, government or within the industry so that the upper and lower hierarchical department can be segregated making it easier to find the breach of security in the system.

Mesh architecture is a decentralized security model in which participants authenticate the identities of other users. The mesh architecture bears a great deal of resemblance to how people trust each other in day-to-day life. This model finds use in small groups who have pre-existing relationships but since the certification paths might get quite long, it doesn't fare well in large groups or where consistency of assurance is important. If a single CA in this

model were to be compromised, the system would still be able to function quite well since there is no central authority.

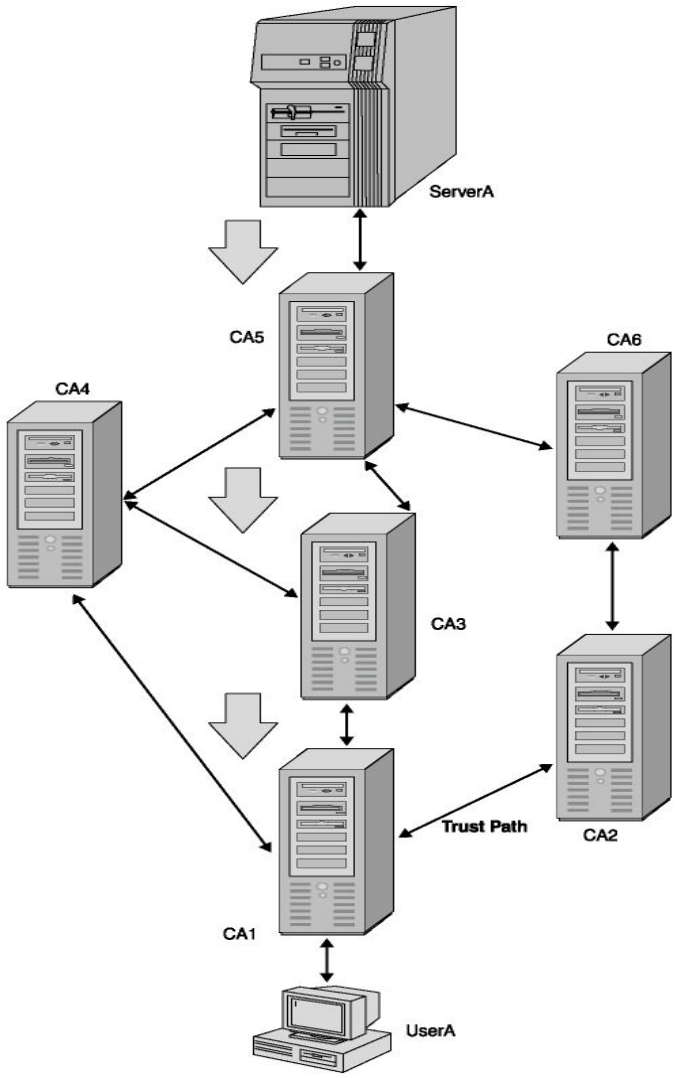
Example of the working of Mesh Architecture-

UserA has a certificate issued by CA1 and needs access to data on ServerA. ServerA has a certificate issued by CA5.

The process follows like this:

1. UserA presents its certificate to ServerA.
2. ServerA verifies UserA certificate with CA1.
3. ServerA verifies CA1 certificate with CA3.
4. ServerA verifies CA3 certificate with CA5.

Because ServerA relies on CA5 and CA5 trusts CA3, CA3 trusts CA1, and CA1 issued the certificate for UserA, the certificate is valid with ServerA.



Example of the working of Hierarchical architecture-

UserA has a certificate issued by CA1 and needs access to data on ServerA. ServerA has a certificate issued by CA5.

The process follows like this:

1. UserA presents its certificate to ServerA.
2. ServerA verifies UserA certificate with CA1.
3. ServerA verifies CA1 certificate with CA3.
4. ServerA verifies CA3 certificate with RootCA.

Because all certificate holders know the root CA, ServerA relies on RootCA, RootCA trusts CA3, CA3 trusts CA1, and CA1 issued the certificate for UserA, the certificate is valid with ServerA.