SECURITY ASPECTS OF NDN

Basic Overview of NDN

One of the advantages of NDN over HTTPS is that security in inbuilt in NDN. The key aspect of NDN is that HTTP’s request and response mechanism is replaced by Interest packet-Data packet mechanism.

NDN forwards each interest packet based on names and recording the interface from which it was received and once interest request gets the desired packet it will follow the reverse path to reach the consumer. Every other packet will have a different name even if producer wants to change data of a packet they have to use a new name for that packet. Every packet is signed with producer’s key so its producer’s name is bound with the message.

Basic security concepts

How Public Key Cryptography Actually Works

When A wants to send a message to B, A encrypts his message using B’s public key and also generates a digital signature using his own(A’s) private key. Now when B receives this message only he can decrypt it using his(B’s) private key. He also verifies the digital signature by using A’s public key.

No one who is able to intercept the message can decrypt it as this is how cryptographic functions work.

As mentioned earlier NDN encryption is automated. Because NDN secures data directly it can be received from anywhere and one need not worry about its authenticity or the possibility that the data has been tampered with.

NDN certificates(which contain info about everyone’s public keys) are present as a certificate chain available to anyone.

NDN security utilizes public-key cryptography and relies on the use of digital keys. In addition to keys, NDN also uses trust policies and NDN certificates.

All network communication participants are known as Entity and each entity possesses one or more names plus one or more cryptographic public-private key pairs. The NDN certificate bind the user name and its key together and it certifies the ownership of the name and each certified ownership is called identity.

Trust anchor: In NDN trust anchor is an authority which keeps the public key along with the names of all the producers.

Certificates: An NDN certificate is a Data packet that carries public key information and can be fetched using normal Interest packets. Data requested along with the producer’s name are cryptographically attached with the certificates.

These trust anchors are to be installed in a safe manner to ensure there is no tampering with it while installing. These trust anchor should provide certificates whenever asked for and as the certificates are authorized previously by trust anchor they can be cached and be used before expiry. Instead of relying on third party for certificates NDN gives capability configure own local trust anchor and then entities can rely on these anchors for certificates and trust policies.

Trust policies: these are the set rules or policies which an NDN data packet needs to follow to be considered as trustworthy valid packet.

SECURITY ASPECTS OF SETTING UP NDN

1)Obtaining Trust Anchors: An entity needs trust anchors to authenticate other entities and get the certificates. These are to be configured and installed in a secure manner.

2)Obtaining certificates: Trust anchors are asked to provide certificates for authenticating a received packet is from a trusted producer or not. In case of IoT devices Certificates can also be used to verify whether a particular interest is from authentic source or not.

3)Learn Trust policies: entities need to learn trust policies from trust anchor to determine a received packet is valid and trustworthy or not.

AUTHENTICITY AND INTEGRITY

NDN requires producers to sign every Data packet, enabling consumers to verify each incoming Data’s signature, hence ensuring data authenticity and integrity.

Validation by Trust Policies: Even before verifying for signatures it is checked whether a given named packet is structured according to the policies or not.

Signature verification: Consumer retrieve the certificate of the producer then checks whether producer’s name and signature are same in the certificate as provided in the packet.

How NDN Compares to HTTPS

The standout difference in security between NDN and HTTP is that HTTP secures the channel and NDN secures the data.

In HTTPS the public key of the server is shared with the client through the server’s SSL(Secure Sockets Layer) certificate. When a client wants to communicate with a server they first authenticate each other(using public / private keys) and then agree on new keys called session keys to encrypt further communication. These session keys basically ‘secure the channel’. However in NDN the data itself is encrypted by one party by using the other’s public key and thus ‘the data itself is secure’. This is an advantage as in HTTPS the data is secure only when it is in the channel. Also during multiparty communiation, every pair of endpoints have to be secured by a secure channel and this causes a lot of loss of efficiency. All these problems are avoided in NDN.

CONCLUSION

Since NDN secures every packet of data it requires computationally more work than the current architecture. However it is worth it. Today’s processors are capable of very high speeds of computation which is far more than that which NDN requires. All in all it is a good tradeoff.