**Certificate-Based authentication and asymmetric cryptography**

Passwords are the most commonly used form of authentication and this is one of the weakest. This type of authentication commonly uses a username and a password. There is a wide range of attacks that can be used to acquire a user's password and take over their identity such as phishing, brute force attacks, man-in-the-middle attack, keyloggers, etc. Despite that, most organizations continue to use password-based authentication. Password selection is a daunting task. A password must be complex enough that it can't be guessed right away and simple enough that it can be remembered. So, people tend to reuse passwords and write them down somewhere. In addition to authenticating users, machines that can access your network also need to be controlled. So, there is a need for stronger authentication. Certificate-based authentication is the solution.

**Certificate-based authentication:**

Security researchers Ron Rivest, Adi Shamir, and Leonard Adelman came up with the RSA cryptosystem in 1977. RSA is an asymmetric cryptography algorithm in which we calculate a key-pair using some mathematical computation and split it into two pieces: the private key and the public key. After generating a key pair, the private key holder shares its public key; the public key can then be used to encode secret messages that only the private key holder can decrypt. The reverse is also true, i.e., you can encrypt a message with your private key that only can be decrypted by the corresponding public key. Both keys encrypt to different hashes but one key can decrypt the other's encryption.

At first, it seems irrelevant to encrypt a message with your private key that can be decrypted by anyone having your public key. Let's say someone decrypted the message using your public key; however, he cannot change the content of that message because he doesn't have your private key to encrypt it back. This way, one can confirm if a message was really from you. In other words, you have digitally signed the message as we sign a message in the real world.

In Certificate-based authentication, Digital certificates (an electronic document which is used to prove ownership of a public key in cryptography) and signatures are used to confirm the identity of a user, machine, or device before giving access to the resource, network, application, etc. After a public key has been successfully associated with a particular user, the system requests a signed averment of identity rather than a password to establish credentials. Once credentials are established you are granted access to the requested resources. This is the basis of Public Key Infrastructure (PKI) and this form of authentication is called certificate-based authentication. This is a password-less authentication method.

Passwords are vulnerable to phishing attacks and are easy to crack, whereas user certificates are not. A major flaw in credential-based networks can be linked to human behaviour. People tend to reuse passwords or use weak passwords that they can remember easily. A man-in-the-middle (MITM) attack could very easily break into a credential-based network and steal the password (A man-in-the-middle attack sets up a rogue access point that can farm credentials from users). MITM attacks are scary and potentially lead to the loss of valuable data; certificates get rid of that risk. Password credentials are based on phrases or keywords made by the user, but certificates utilize public-private key encryption to encrypt the information sent by the network and are authenticated by EAP-TLS, the most secure authentication protocol. Certificates are themselves encrypted and can only be decrypted if you have the private key pair (which is never shared), so even if the user accidentally authenticates a rogue network, the data that is sent is worthless to the attacker.

**How is data transferred in certificate-based authentication?**

The sending and receiving machines exchange their public keys via a reliable channel like TCP/IP. The private keys are never shared.

The sending machine first signs the data using its private key so that receiver can confirm if the message was really from you and then encrypts the data using the receiving machine’s public key and some mathematical operation. The power of public-key encryption lies here, even with the public key it’s not possible to decrypt the data, it is a one-way function only its private key pair can be used to decrypt the data.

The sender can now safely send the data without worrying about any eavesdropper as the data would not mean anything without the private key.

Now the receiver receives the data and decrypts the message using its private key.

It may sound unrealistic that it is possible to encrypt some message with one key that can only be decrypted by a different key. For a long time, mathematicians were not sure if it was possible, but they found a way in the 1970s.

RSA algorithm is based on the fact that it is very difficult to factorize a large integer. The public key is divided into two parts; the first part contains the multiplication of two very large prime numbers chosen at random and the second part contains an exponent. The private key is also made using the same prime numbers. The safety of the algorithm lies in the key size as it will be more difficult to factorize a large number. So when we increase the size of the algorithm, the strength of encryption increases exponentially. Let’s understand RSA better with a bit of maths.

Encrypted data: me mod n = c

Decrypted data: cd mod n = m

Here,

m: message to be encrypted; c: ciphered message

n = P\*Q, P and Q are two random large prime numbers

e: 1 < e < ϕ (n), e must be an integer and not a factor of n

d = (1 mod ϕ(n))/e

No human could be expected to remember a secure public-private key since it is a very long string and not having any meaning that can be remembered, much less one for each system which he might be expected to authenticate. As a result, the key-pair needs to be stored by the end-user. The current recommended key length is 2048 or 3072 bits. If an RSA key is said to have the length of 2048, it means that the modulus(n) value lies between 22047 and 22048.

User certificates allow for the separation of roles which passwords can't do. However, they are still not very famous because of the lack of convenience. As client certificates are stored on a browser, we can't use it with some other device and this becomes inconvenient. It is not simple to use certificate-based authentication since it requires the technical capability to configure and manage it. So, it is too much to ask from users. To overcome the pitfall of passwords, we have come up with multi-factor authentication which is pretty easy to use. *Multi-factor Authentication* (MFA) requires two or more verification factor to gain access to a resource rather than just asking for a username and password, which decreases the probability of a successful cyberattack. As MFA does the job, companies don't feel the need to get certificate-based authentication involved.

Ankit

MCA 1st Year