WPA2 with Decentralized Authentication servers

(Term Project for CS6500 : Network Security)

Presented By:

Devashish Dewangan
CS21M017

Nagaraj Chandru
CS20M041

Problem Statement

- **Goal:**
  - Implement WPA2 using decentralized Authentication with using blockchain to store user credentials.
- **Objectives:**
  - to implement WPA2 with AS server to authenticate users and provides tokens with validity which are used between user and access point over the wireless network.
  - The tokens generated by AS can be used by client to connect any AP.
  - Blockchain technology will be used to maintain identical user credentials among servers to overcome single point of failure.

Network Protocols being considered

- **<u>Kerberos:</u>**
  - Client & AS will have secret key (password) shared between Client and AS, stored on blockchain.

    C –> AS: ID || E[PSK(C), ID]

  - User can be authenticated at AS by UserID & password (secret key), after which AS will generate token for client.

    AS –> C: E[PSK(C), (SK || ID || ExpiryTime)]

    Token : E[PSK(AP), (SK || ID || ExpiryTime)]

    SK(session key can used between AP & client to share data confidentially)

  - At AP user can be authenticated using token(certificate).

Network Protocols being considered contd...

- **BlockChain:**
  - To overcome single point of failure we are using blockchain technology to store user credentials. A block consist of “PrevBlockHash” + “userID” + Hashed[“password”] + “BlockHash”.

Security Aspects

- Authentication (at AS) : is achieved by userID & password at AS.
- Authentication (at AP) : is achieved by a token at AP.
- Confidentiality (b/w user & AP) : is achieved by secret key shared between the AP and client.
- Confidentiality (user credentials) : we are using blockchain technology to store user credentials. A block consist of “PrevBlockHash” + “userID” + Hashed[“password”] + “BlockHash”.

Development Environment

- Language : Python
- Major Components : Authentication Server & Blockchain Database.
- Packages : Cryptography.

Implementation status

- As of now we have implemented:
  1. Client
  2. AP
  3. AS (storing credentials is left)
- we are working on:
  - Blockchain part, synchronizing the store credentials among servers .
  - Message integrity.


Thank You