SALT generator

Both Seed With Initializer Value

Things It Knows
- Initializer value
- password

Things It Knows
- Initializer value
- Password
- Times used random

Client

Server

CONNECT Request

Number Of Times Used Random Response

Client Runs Random as much times as server did

SALT is following output of random for every command approved (or recent += 1 or something)

Hash(password + SALT + command)

Attack Vectors

- Resetting server so that random ouput will repeat itself
- DOS- modify server reponse so client will use incorrect SALT
- Modify server response to very large number so client will repeat random forever

Security mechanisems 1 עמוד