CSCI968 Advance Network Security: Assignment #1

Mei Wangzhihui 2019124044

Problem 1

One-time password SecureID system
Google Authenticator. User enter a initializing code to generator a one-time password changing each period. It use the AES-128 algorithm.
S/Key System The authentication to Unix-like operating system replacing long-term password. A user's real password is combined in an offline device with a short set of characters and a decrementing counter to form a single-use password. Because each password is only used once, they are useless to password sniffers. After password generation, the user has a sheet of paper with n passwords on it. It use the Random Oracle.
Challenge response protocol Challenge–response authentication can help solve the problem of exchanging session keys for encryption. Using a key derivation function, the challenge value and the secret may be combined to generate an unpredictable encryption key for the session. This is particularly effective against a man-in-the-middle attack, because the attacker will not be able to derive the session key from the challenge without knowing the secret, and therefore will not be able to decrypt the data stream.

Problem 2

Problem 3

Problem 4

‘’