ECE 543 Quiz 4

Alan Palayil
A20447935
Due Date: 4/22/2023

1. Strong password protocols necessitate no user-specific information for authentication and should prevent impersonation or eavesdropping from yielding information useful for dictionary attacks. To enhance security, avoid using messages that are a function of the password and other known parameters, and integrate Diffie-Hellman key exchange with password-based authentication.

2. To protect against server reading attacks, augmented protocols such as Augmented PDM, RSA-Augmented EKE, and Secure Remote Password (SRP) can be implemented. These protocols enhance security by incorporating additional encryption or authentication mechanisms, minimizing the risk of sensitive data being compromised even if the server is breached.

3. To maintain privacy with remote distribution list exploders, Alice can establish a long-term key with the exploder. She then selects a random per-message key S and sends the message encrypted with S to the exploder. The exploder decrypts S and re-encrypts it using each recipient's public key before forwarding the message. This process does not require the exploder to decode the message and is more efficient compared to sending encrypted messages directly to the exploder. Authentication can be achieved using public key methods, while secret key methods may involve the exploder authenticating Alice and using its own authentication information with each recipient. However, this model is not as strong or safe as public key authentication methods.

4. In the context of Toy SSL, a truncation attack occurs when an attacker forges a TCP connection close segment, causing one or both sides to believe there is less data than actually present. The solution involves using record types, such as type 0 for data and type 1 for closure, and computing the MAC as MAC(Mx, sequence||type||data). Toy SSL is not complete, as it does not specify field lengths, encryption protocols, or negotiation processes to allow clients and servers to support different encryption algorithms and collaboratively choose a specific algorithm before data transfer.