Chapter-4
Authentication Protocol and Key Establishment

4.1 – Nadir Mahmud (18701023)

4.1 – Ruhul Amin (18701063)
4.2 – Saifuddin Ahmed (18701048)
4.2 – Shakawat Hossain Hridoy (18701056)
4.3 – Abdul Kayum (18701033)
4.3 – Misbah Uddin (18701020)
4.4 – MD Habibul Basar Faruq (18701006)
4.5 – Arup Dutta Bappy (18701010)

4.1 Entity Authentication and Key Establishment

- Discusses authentication protocols involving cryptographic algorithm.
- Definitions
  - Entity Authentication
  - Cryptographic protocol
  - Authentication protocol
- Types of authentication
  - Unilateral authentication
  - Mutual authentication
- Key establishment
  - Key transport
  - Key agreement

Continue

- Authentication only, Unauthenticated key establishment.
- Integrating authentication with session key establishment.
- Key management.
- Reusing data or session keys.
- Initial keying material.
- Crypto strength keys, weak secrets
- How do we protect long-term secrets stored in software?
  - Point to point model with n^2 key pairs
  - Centralized symmetric-key servers – KDC and KTC

4.2 Authentication protocols: concepts and mistakes

Here we consider basic concepts about authentication protocols

Demonstrating knowledge of secret as proxy for identity:

- **Basic idea: (for two remote party A & B)**
  - Associate a secret with **B**
  - Carry a communication believed to be with **B**
  - If this approach involves full secret itself, then a reliable channel is required .
  - Hence its preferred to send convincing evidence of knowledge known as **"proof of knowledge"**
  - Yet there are some flaws in this method. For example:
  - **Simple Replay Attack**
  - **Dictionary Attack on Weak Secret**
  - **Reflection Attack**

Continue

- Some common attacks:

Attack	Short description
replay	reusing a previously captured message in a later protocol run
reflection	replaying a captured message to the originating party
relay	forwarding a message in real time from a distinct protocol run
interleaving	weaving together messages from distinct concurrent protocols
middle-person	exploiting use of a proxy between two end-parties
dictionary	using a heuristically prioritized list in a guessing attack
forward search	feeding guesses into a one-way function, seeking output matches
pre-capture	extracting client OTPs by social engineering, for later use

- Even some attackers use mixed method to get their work done.
- In defense **TVP (time variant parameters)** has been introduced.

Time Variant Parameters (TVP)

- There are three basic types of TVP
  - **Random numbers** (Guarantees freshness and convincing evidence of correct communication)
    - ✓ long length which is hard to reuse & fresh random number assures current protocol, not old.
  - **Sequence number** (Provides message uniqueness, not unpredictability. Exp: cheque number)
  - **Timestamp** (Certain time boundary, requires synchronized clock between both)

- RSA encryption used for key transport

  (RSA decryption used for entity authentication of B). Consider:

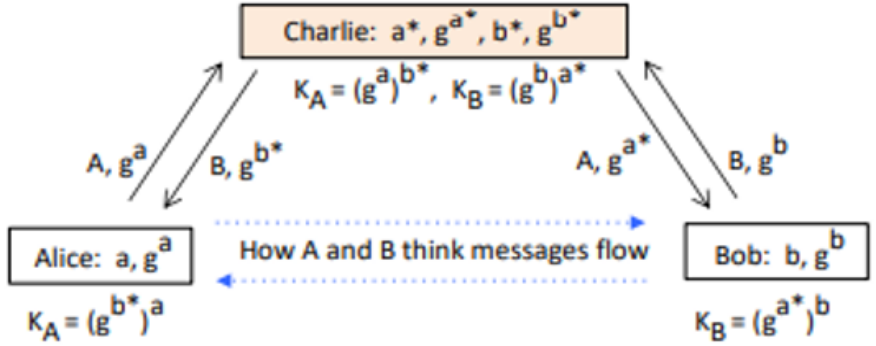
  (1) $A \rightarrow B : H(rA), A, EB(rA,A)$ ... EB(rA,A) is a public-key encrypted challenge

  (2) $A \leftarrow B : rA$ ... H(rA) showed knowledge of rA, not rA itself

4.3 Establishing shared keys by public agreement

- Diffie-Hellman key agreement (DH) - 1976
  - Two parties with no prior contact/any pre-shared keying material
  - Establish a shared secret by exchanging numbers over a channel readable by everyone else.
  - Params: prime p, generator g, two private values a, b
  - ElGamal encryption - used for key transport
- Passive Attack and MIDDLE-PERSON ATTACK (MITM)

A -> B	B -> A
a, g^a	b, g^b
A sends g^a B computes: $K_B = K = (g^a)^b$	B sends g^b A computes: $K_A = K = (g^b)^a$



STS PROTOCOL

- Station-to-Station protocol
- Turns unauthenticated DH into authenticated DH
- Uses digital signatures.
- The basic form of the protocol is three steps:
  1) $\text{Alice} \rightarrow \text{Bob} : g^x$
  2) $\text{Alice} \leftarrow \text{Bob} : g^y, \text{E}_K(\text{S}_B(g^y, g^x))$
  3) $\text{Alice} \rightarrow \text{Bob} : \text{E}_K(\text{S}_A(g^x, g^y))$
- Securities Properties of STS:
  - cryptographic key agreement scheme
  - provides mutual key and
  - entity authentication

Key authentication properties and goals

Protocol Goals and Properties:

- FORWARD SECRECY
  1. secrets (a, b) are fresh
  2. after the session, these secrets are securely deleted.
- KNOWN-KEY SECURITY
- ENTITY AUTHENTICATION, LIVENESS, KEY-USE CONFIRMATION.
- IMPLICIT AUTHENTICATION, EXPLICIT AUTHENTICATION.

Password Authenticated Key Exchange: EKE and SPEKE

- PAKE
  - Cryptographic key exchange protocol.
  - Symmetric key generation.
  - User-chosen passwords are converted.
  - Shared key – public key cryptography.
- DH-EKE
  - Unauthenticated.
  - Vulnerable to man-in-the-middle attacks.
  - Individual password guess is possible.

Password Authenticated Key Exchange: EKE and SPEKE (continue)

- EKE-Encrypted Key Exchange
  - Authenticate using a password.
  - Mutual authentication.
  - Effectively amplify a shared password into a shared key.

- SPEKE-Simple Password EKE
  - An elegant alternative to EKE.
  - Secure session key generation.
  - Communication over unreliable channel.
  - Shared secret key or password.

Thank You