Exercise for Engineering Secure Software Systems

November 19, 2020: Authentication Protocols

Henning Schnoor

Institut für Informatik, Christian-Albrechts-Universität zu Kiel

Crypto and (Auth) Key Exchange

Example Real-Life Protocols

let's model …

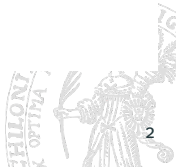
- online banking
- online shopping
- electronic elections

discussion

- goals of these protocols?
- tools to achieve them?
- common elements in these protocols?

consequence

we always need some setup/infrastructure



Class of Protocols: Key Exchange

recap

symm crypto

- every communicating pair of people: shared key
- used for encryption, decryption, signature, verification

asym crypto

- everybody: public, private key
- public key for encryption, verification
- private key for decryption, signature

adv asym crypto

- key exchange problem simplified
- fewer keys (in system)

adv symm crypto

fast

Best of Both Worlds

goal

- Alice and Bob want to exchange encrypted streaming data (video chat)
- encrypt stream with symmetric encryption
- need shared key k_{AB} known only to Alice and Bob
- also want authentication (be sure nobody else can decrypt video)

key exchange protocols

- goal: “exchange” shared symmetric key
- key should be randomly generated in protocol

required

- PKI: Alice and Bob need public keys (authentication)
- assume this is in place

Authenticated Key Exchange: Attempt

task

Alice and Bob want to exchange messages “securely.”

idea

1. Alice chooses long random string N_A, sends a message to Bob containing
   - 1.1 Alice’s name
   - 1.2 the encryption of N_A with Bob’s public key
2. Bob replies with
   - 2.1 Bob’s name
   - 2.2 the encryption of N_A with Alice’s public key
3. then use N_A as session key

notation

$$1 \quad A \to B \quad (A, enc^a_{k_B}(N_A))$$
$$2 \quad B \to A \quad (B, enc^a_{k_A}(N_A))$$

analysis

- what is the idea behind the protocol?
- does it work—is the protocol secure?

Another Attempt

new idea

1. Alice chooses long random string N_A, sends a message to Bob containing
   - 1.1 the string N_A,
   - 1.2 Alice's name,

   both encrypted with Bob's public key.
2. Bob decrypts message, chooses random string N_B, sends message containing
   - 2.1 pair consisting of N_A and N_B,
   - 2.2 Bob's name.

   both encrypted with Alice's public key.
3. both compute $k_{sess} = N_A \oplus N_B$ as session key (internal step, no message)

notation

1 $A \to B \quad (enc^a_{k_B}(N_A), enc^a_{k_B}(A))$
2 $B \to A \quad (enc^a_{k_A}(N_A, N_B), enc^a_{k_A}(B))$

analysis

did we fix it?