Encryption for Network Authentication
Research Paper by R. Needham and M. Schroeder

Methodology, Results and Take Away
Presented by:
Kanishk Jain
The focus is on **design concerns** of the protocols and the role of the **components**.

The presentation does not provide a step by step walk-through of the protocols.

Open for discussion.
Assumptions

- Decentralized environment
- Minimal Network Wide Services
  - Ex: single network clock not assumed
- Physically vulnerable network
Requirements

- Three main scenarios:
  - Secure Interactive communication
  - One way communication
    - A mailing system with two way authentication
  - Digital Signatures
Methodology

- **Message Based** Protocols which use encryption at their core
- Encryption is done using either **conventional** or **public key** methods
  - Minor changes in protocols depending on encryption method
  - Basic steps remain the same
Methodology

- The other player (s):
  - Authentication Server (s)
    - Lookup authority
    - Has knowledge of certain keys
      - Private keys in conventional method
      - Public keys in public-key method
  - Helps to establish identity
  - Role increases in absence of local caching
Methodology

Messages:

- Handshaking messages
  - To establish **identity** or **time integrity**
  - Knowledge of secret keys, or *valid* messages encrypted using secret keys, establishes identity
  - A nonce identifier helps verify time-integrity

- Text messages
  - Encrypted using an agreed-upon key
Purposes of Encryption:

- Privacy
  - Sending text messages only intended for a particular recipient
  - Comprehensible to only recipient

- Integrity
  - Messages which only a particular sender could have sent
  - Verify accuracy of the information in the message
    \[ AS \rightarrow A: \{PK_B, B\}^{SK_A} \]
  - Also applied in digital signatures
  - Time integrity is another concern
Methodology

- Some properties:
  - The following message is a self-authenticating message:
    \[ A \rightarrow B: \ (CK, A)^{KB} \]
  - The following message form makes signatures with public-key encryption "elegant":
    \[ A \rightarrow B: \ {(text-block)^{SKA}}^{PKB} \]
  - The inner encryption with the secret key prevents an adversary (with the knowledge of the public key) from changing the contents of the message
The protocols based on encryption can be applied to a variety of problem domains:

- Establishment of authenticated interactive communication
  - Interactive communication: messages in either direction
- One way communication
  - Still, must be Authenticated
- Signed communication
  - Third party authentication
The protocols provide a framework
- Provide basic concepts which can be extended

The aim is not for the solutions to be complete and readymade
- Ex: stopping adversary from matching cleartext-ciphertext pairs
The techniques assume the adversary has extreme powers:
- Can change or copy parts of messages
- Record and replay messages
- Cause transmission of false messages

Hence they are rigorous in their basic design
The protocols steps are outlined for two different encryption techniques, the conventional and public key methods.

- Often a **comparison** is in the offing
- Shows that the basic steps are “strikingly similar”

**Efficiency** tradeoff mechanisms such as caching are mentioned too.

- Other considerations such as a stateless authentication server are kept in mind
Take Away

- Gives an integrated view of how encryption can be applied to a variety of scenarios in network authentication.
- Shows how the protocols change if the encryption technique changes.
  - Newer encryption techniques could be discovered later.
  - Shows functional equivalence with two techniques.
The authors’ claim: the work provides an integrated approach to techniques which have been separately analyzed by others such as Diffie and Hellman (originators of the concept of public key algorithms).

- It furthers the work to a decentralized environment.
The work appeared in 1978 in an “Operating Systems” section
- Possibly ground breaking
- “Computer security” was not a specialized field of study