Entity Authentication and Key Exchange in Ad Hoc Networks

Katrin Höper, Guang Gong
University of Waterloo, Waterloo, Ontario

Introduction & Objectives

- Definition
  - Latin: “Ad hoc” = “formed for” or “concerned with one specific purpose”
  - Ad hoc networks are networks instantly formed to serve a specific purpose.
  - Ad hoc networks do not rely on fixed infrastructure and the network devices are usually always mobile.
  - Ad hoc networks + wireless mobile networks

- Objectives
  1. Device Authentication
  2. Secure Key Establishment
  3. Secure Routing
  4. Tamper Resistant Memory

Categorization

- Ad hoc networks
  - Mobile ad hoc networks (MANETs)
  - Smart sensor networks

Networks

- Network Phases
  1. Authentication Phases
    - All devices that want to securely communicate have to exchange key data a priori:
      - symmetric scheme: secret key
      - asymmetric scheme: authentic public key
    - The actual authentication by the use of challenge/response using the shared data

Solutions

- Symmetric Schemes
  - All devices share a secret a priori
  - Secret is used directly as symmetric key for encryption and authentication

- Asymmetric Schemes
  - All devices share public keys a priori

Authentication

- Incorrectly formed phrase: “notional” instead of “notational”

Security Model

- Symmetric solutions should be implemented where applicable
  - we focus on asymmetric and identity based solutions.

- Security Model for asymmetric solutions – 3Phases
  - exchange public keys
  - use the Internet Key Exchange Protocol (IKE) for authentication and key establishment

Identity-based Cryptography

- Idea: human readable identities are used as public key, e.g. names, email addresses, etc.
  - identities are self-certifying, e.g. P=Alice
- Gain: 1. no key exchange required!
  2. no need for certificates!
- Expose: TTP is a key escrow, if desirable its power could be limited by:
  - threshold scheme, requiring k TTPs to reconstitute a private key
  - expiration date of master secret
- Revocation: easy to implement, e.g. timestamp identities P=Alice/apr03

Identity-based Authenticated Key Exchange Protocol “IDAKE”

- Objective: mutual authentication and key establishment
- Features
  - combination of Identity-based Signature Scheme [Fiat/Shamir ’86] and IKE
  - cheap and few computation steps
- Set-up phase: TTP generates the secret keys for each device:
  - unique string Ii={name, address, userID, etc.}
  - computes hash values H(Ii), with p=1,...,k
  - computes x=H(Ii) and sends secret keys {s1, …, sk} to device i
- Public initial information: (each device holds)
  - Identity-based signature scheme: prime m, generator g
- Protocol messages
  - m, T, fg(x)

References: galloppe.uchicago.edu/~khoep

For more information, contact:
Katrin Höper,
Department of Electrical & Computer Engineering
University of Waterloo
Waterloo, Ontario, N2L 3G1, Canada
E-mail: khoeper@engmail.uwaterloo.ca