Leveraging Social Contacts for Message Confidentiality in Delay Tolerant Networks

Karim El Defrawy, John Solis and Gene Tsudik
{kedefra,jsolis,gts}@ics.uci.edu
University of California, Irvine

Summary

- This project focuses on the problem of initial secure context establishment in Delay Tolerant Networks (DTNs).
- We observe that users can take advantage of social information to send confidential messages.
- The source (SRC) and destination (DST) users can use common affiliations, that know the public key or have an established shared secret, as intermediaries to securely send messages.

Motivation

- DTNs have high node mobility and infrequent connectivity
  - No complete end-to-end path
  - Multi-round protocols break (e.g., SSL/TLS)
- No or limited infrastructure
- Can not assume that all nodes can query a PKI or receive a response in a timely manner

Problem Formulation

How can SRC send a confidential message to DST without any prior security context, i.e., SRC neither pre-shares a secret key with DST nor does it know DST's public key (if one exists)?

Intra/Inter Region Messaging:

- **Step 1:** SRC determines DST is affiliated with t > 1 common entities: AE1, AE2...
- **Step 2:** SRC has a shared secret key \( K_{i} \) and constructs the DTN message: \( M_{i} = [\text{HDR}_{i}, \text{BODY}_{i}] \) where:
  \[
  \text{HDR}_{i} = \langle 1, \{ AE_{i}, E_{HDR_{i}}^{AE_{i}}(K_{i}) \}, ..., \{ AE_{i}, E_{HDR_{i}}^{AE_{i}}(K_{i}) \} \rangle \\
  \text{BODY}_{i} = [m \oplus \text{PRF}(K_{i}) \oplus ... \oplus \text{PRF}(K_{i})]
  \]
  Note: \( \text{HDR}_{i} \) represents a loose source route
- **Step 3:** \( M_{i} \) reaches the first hop \( AE_{i} \), \( AE_{i} \) decrypts \( E_{HDR_{i}}^{AE_{i}}(K_{i}) \) found in \( \text{HDR}_{i} \), re-encrypts \( K_{i} \) as \( E_{AE_{i}}^{AE_{i}}(K_{i}) \), and constructs \( M_{2} = [\text{HDR}_{2}, \text{BODY}_{2}] \) where: \( \text{BODY}_{2} = \text{BODY}_{1} \) and
  \[
  \text{HDR}_{2} = \langle 2, \{ AE_{i}, E_{HDR_{2}}^{AE_{i}}(K_{i}) \}, \{ AE_{i}, E_{HDR_{2}}^{AE_{i}}(K_{i}) \}, ..., \{ AE_{i}, E_{HDR_{2}}^{AE_{i}}(K_{i}) \} \rangle \\
  \]
  The process repeats until message \( M_{i} \) reaches \( AE_{t} \)
  \[
  \text{HDR} = \langle t, \{ AE_{i}, E_{HDR_{i}}^{AE_{i}}(K_{i}) \}, ..., \{ AE_{i}, E_{HDR_{i}}^{AE_{i}}(K_{i}) \}, \{ AE_{i}, E_{HDR_{i}}^{AE_{i}}(K_{i}) \} \rangle \\
  \]
- **Step 4:** Upon receiving \( M_{i} \), for each \( AE_{i} \), DST can decrypt the corresponding \( E_{HDR_{i}}^{AE_{i}}(K_{i}) \) to obtain \( K_{i} \). Finally it computes:
  \[
  m \equiv \text{BODY}_{i} \oplus \text{PRF}(K_{i})
  \]
  Note: Stream ciphers do not require a fixed order for decryption. The above process holds regardless of specific route traversal.

Security Analysis

- **Security Model:** Honest-but-curious
  - No active attacks
  - Messages stored beyond TTL
- **Collusion:**
  - Secure if \( n < t \) nodes collude
  - Pick associations unlikely to collude (e.g. University, Corporations, Common Friends)

Sample DTN Scenario

Network Coverage

- Affiliated entities know/can easily obtain DST’s public key
- All T nodes must be active/available
- Low robustness

Simulation Results

Network Coverage

ICNP 2008 – Orlando, FL