OMiN: An Opportunistic Microblogging Network

Providing Cryptographic Security in Opportunistic Networks

Neil Wells & Tristan Henderson

2014/15

University of St Andrews

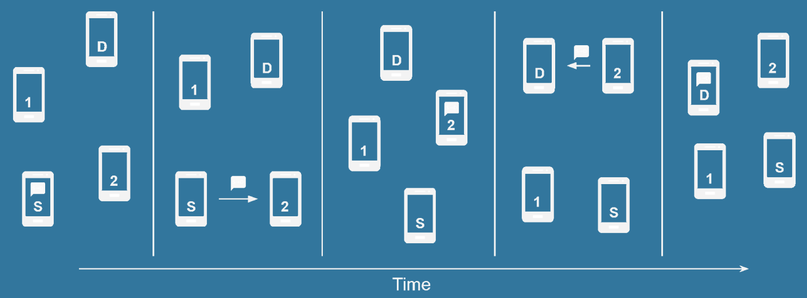
The Challenge: Security in Opportunistic Networks

Opportunistic Network

A form of computer network in which connections between nodes are rare and often random. Messages are stored by carrier nodes and can be forwarded opportunistically whenever the carrier node connects to another node.

Security

Messages may take a long time to reach a node, with the result that security mechanisms using central servers or handshakes are impractical.



The Software: OMiN

Use Cases

- Disaster areas
- Underground railways
- Developing countries
- Animal tracking
- Secure communication

Microblogging

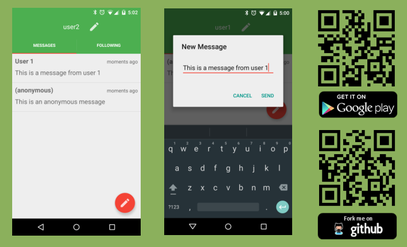
Microblogging services allow people to publish short public messages. The Facebook news feed and Twitter tweets are well-known microblogs.

Pocket Switched Network (PSN)

A form of opportunistic network where nodes are carried around by people - often using smartphones.

OMiN

OMiN is a microblogging service and PSN running on Android smartphones which connect using Bluetooth.



The Result: A New Security Mechanism

Secure

Cryptographically secure in almost all cases.

Available

One requirement: one node must have had Internet access at some point.

Quantifiable Risk

Nodes know how many other nodes must be trusted.

Minimising Risk

Nodes seek to minimise number of trusted parties. Nodes with an Internet connection are totally secure.

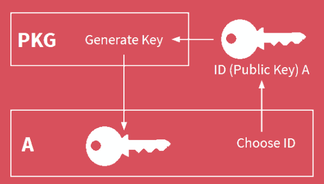
Minimal Side Effects

Minimal effect on routing .

The Solution: Cryptographic Key Delegation using HIBE

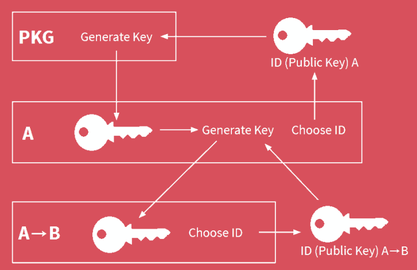
ID-Based Cryptography (IBC)

A form of asymmetric-key cryptography where a user's unique identifier (such as their email address) is their public key. A central Private Key Generator (PKG) must generate a private key and pass it securely to the user (known as delegation).



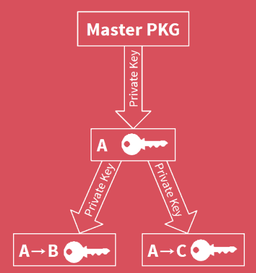
Hierarchical IBC (HIBC)

A form of IBC where any user can act as a PKG and delegate private keys to other users. A user's public key is the chain of IDs from a central master PKG to the user.



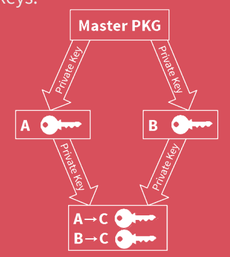
Securing Messages Using HIBC

Nodes with access to the Internet can use it to acquire a private key from the master PKG. Nodes without internet access can get a delegated private key from another node with a private key.



Minimising Trust

The ancestors of a node in a PKG chain are capable of deriving the node's private key - they must be trusted. In the proposed scheme, nodes can have multiple private keys and identities. Now the node has multiple sets of ancestors who must collaborate to discover the set of private keys.



Unsigned Messaging

If a node does not yet have a private key they can still send unsigned messages, but these could be modified en-route by malicious nodes. Nodes with a private key should sign the message on behalf of the sender as soon as possible to minimise the number of trusted nodes.