MSocks

Fig. 2. The MSOCKS architecture. Parts shown in gray are where MSOCKS alterations are made to the standard parts of proxy based client/server system.

- Idea: Isolate the mobile end of the connection using a mobility aware proxy
- Proxy maintains connections while a mobile moves
- Connection re-established to new location after move

Fig. 3. Packet exchange diagram for connection establishment between a MSOCKS client and a correspondent host.
Host Identity Protocol – Motivation

- End points (machines) have multiple interfaces
- Interfaces not tied to IP addresses
- Transport layer coupled to IP addresses
- Use other namespaces?
  - Domain Names: hierarchical with no anonymity
  - Email/SIP addresses: provide naming, but are extensions of domain names
  - Majority of systems don’t have an FQDN or email/SIP address
  - RFC points out 3 critical deficiencies

Deficiencies of Existing Namespaces

- Dynamic Readdressing cannot be directly managed
- Anonymity is not provided in a consistent trustable manner
- Authentication is not provided
More Problems Solved

- Name for transport layer binding
  - Clean multi-homing
  - Similar to Mobile IP (but arguably less complex)

- Name for security association binding
  - Independent of addressing
  - Mobile
  - Transparent to NAT

Using a Host Identity

- Each Host has at least one Identity
  - Assigned to the network stack
  - Cryptographic Identity for proofing—Identity is public key

- Host Identities can be well known or anonymous

- Higher layers only see identities, not addresses
  - Clean mobility and addressing realm spanning

- A payload and protocol for the secure exchange of identities
  - The Host Identity Payload or HIP

What Problems Does it Solve?

- Consistent name for a system regardless of how it connects to the Internet
  - Non-spoofable because its cryptographically based

- Separate routing and name spaces
  - No attempt at routability
  - Interface independent
I3 Approach

- Use a DHT/overlay network to do the mapping
- Apurva will talk to us about I3 next class
- Then summary/discussion paper and micro-mobility
- After that multi-hop network routing

Some more details

- HIP is not fixed size; complicates use in transport protocols
  - Use a hash of HIP (called HIT) as the identifier
  - 64 bits not enough for statistical uniqueness (1% hash collision with 640M population)
- HIT in DNS, unless anonymity is desired

Mobility Management Requirements

- Location independent identifier
  - Identifier should remain static across location changes
- Compatibility with IP routing
- Location Management
  - Must be able to locate a node as it moves (others—¿ mobile)
- Transparency— higher layers/applications should not be aware of mobility
- Security— additional vulnerabilities should not be introduced

Focus only on Mobility Aspect

- Transport layer uses HIT
- Translated to IP through DNS
- So, how does mobility get supported? DNS?
  - They use DNSSEC (secure DNS) to keep track of “rendevouz server” for the node
  - this server holds the current IP of the mobile host
- Responder vs. Initiator (if initiator moves, no mobility support needed)
  - May send a mobility packet to update HIT to IP mapping
Performance Issues

- MIP-HA
  - Suboptimal routing
  - Per packet encapsulation (tunneling)
  - Micro-mobility models being developed for fast handoff

- MIP-RO
  - Avoids suboptimal routing
  - Extra latency with each move

- MIP-LR: try to avoid home agent

Namespaces

- Mobile IP: IP address
- TCP-migrate: hostname
- HIP: New namespace, host identifier (public key)

Performance Issues

- Migrate
  - DNS records less cachable
  - What about non TCP applications? Loss of transparency or require their own development
  - Additional computation to generate secret upon SYN exchange

- HIP
  - Requires operation with and overhead of IPSEC's ESP
  - Computational overhead to generate keying material
  - Dynamic DNS or additional infrastructure for Rendevouz points

Alternative MM Solutions

- Transport Layer solutions:
  - Don't use IP in the addressing – IP now can change
  - MSocks

- Application Level Approaches (SIP): send a new SIP invite after moving

Session mobility: use a layer above TCP (at OSI session level) for mobility

Personal mobility/presence

Service mobility

Alternative architectures (e.g., I3 and IPNL)
Other Issues

• Mobile IP does not require changes at all hosts

• But does not work well with NAT

• Others face significant deployment challenges as well

• Security is a major concern
  – session hijacking vs. mobility
  – DoS attacks since cryptographic verification takes time
  – What is the security story for mobile IP?

• Scalability discussion

• Robustness discussion

Micro-mobility

- Environments where nodes change their attachment points quickly
  - Small cell/high mobility
    - Small cell
    - High mobility
  - High cell/low mobility
    - Large cell
    - Low mobility

- Would like seamless handover
  - Smooth handover = low loss
  - Fast handover = low delay (how low?)
  - Seamless handover = smooth + fast

- Micro-mobility solutions discussed in the context of Mobile IP next time