Lecture 16: Transport layer mobility

Mythili Vutukuru

CS 653 Spring 2014

March 20, Thursday

Transport Layer Mobility

- Mobile IP – deals with network mobility, i.e., the support needed at the IP layer to enable mobility of end-hosts (change in IP address).
- This lecture – transport layer mobility. Instead of changing all the IP routers, can we just change the TCP end-points to cope with changing IP addresses of end hosts?
- We look at two proposals for transport layer mobility – Migrate and MSOCKS. Please see the references on the class website for complete details.
- Main challenge: TCP identifies connections by (src-addr, src-port, dst-addr, dst-port). Mobility changes this 4-tuple.

The key ideas in “Migrate”

- Changes to TCP to handle end point IP address change securely.
- Negotiate the migration support option during initial connection establishment.
- Obtain a “token” that is used to identify a connection even after changes in IP address change the TCP 4-tuple.
- Upon migration to a new address, send a new Migrate SYN with the earlier token, so that the old connection can be continued.
- When one end point does not hear from other, it waits in a MIGRATE_WAIT state for possible migrations before timing out and closing out the connection.
- Please refer to the paper for more details.

The key ideas in “Migrate” (2)

- End points share a secret key using a Diffie Helman style key exchange algorithm.
- The connection identifier (“token”) is a hash of the secret key and initial sequence numbers.
- However, other nodes also can learn of the token by eavesdropping. So what prevents them from hijacking the connection and issuing a new migrate SYN?
  - For every migration, the mobile client generates a request number, and creates a hash that includes this request number (among other things). It sends the req. no and hash with every migrate request.
  - The server that receives the migrate SYN regenerates the hash using the secret key and checks that it matches. This ensures “freshness” of migrate SYN requests, and prevents malicious nodes from replaying migrate SYN requests.

Key ideas in “MSOCKS”

- Use case: mobile hosts move within an organization
- Key idea: A TCP proxy at the edge of the organization handles the TCP connections on behalf of mobile clients, and hides mobility from the remote host.
- The idea of TCP splicing: use a proxy that acts as end point of connections from mobile host, and opens another TCP connection to server. These two connections are then joined to appear as one connection to the end hosts.
- The mobile hosts get a connection identifier which they can show the proxy when they move.
- Mobility is simply handled by opening a new connection on the mobile side, unsplicing connection to old IP, and re-splicing new connection to the connection to remote server.
- Socket system calls such as connect and accept are modified to implement splicing. Please refer to the paper for more details.