Position Paper: Exploring Deeper Issues of Separating Identity and Location for Mobile Hosts

James Kempf
Guangrui Fu
Jon Wood
Toshiro Kawahara
DoCoMo Labs USA, 181 Metro Drive, Suite 300, San Jose, CA, 95110, USA
Contact: kempf@docomolabs-usa.com, 408-451-4711

Our work on HIP has explored a couple of deeper issues involved in using HIP in large scale mobile networks. In particular, we are interested in extending HIP to expand the scalability and scope of trust establishment, and to address mobility and location management issues involved in networks where the primary communication pattern is mobile to mobile rather than mobile to fixed node. The following sections provide a preliminary report on our work.

Trust Establishment

Today's Internet has many problems with trust establishment. Identity theft, "phishing", and other such scams pervade the Internet. Although some people see it as a benefit that "on the Internet, nobody can tell if you are a dog" as the saying goes, for ordinary people who just want to be able to trust the other end of a connection when performing financial transactions and other operations that are sensitive, without being required to understand how certificates work, the lack of any basic ability to verify who you are talking to is a real detriment. While many of these problems might be viewed as a result of the lack of deployment of existing security mechanisms at the application level, we believe an interesting question from a research standpoint is what kind of Internet would result if basic identity establishment were built in at a lower level of the stack.

HIP relies on public keys of end hosts to identify each other. The base HIP protocol does not require that the public key be certified ("leap of faith"), although it is also possible to use certified keys. In that sense, the identifiers used in HIP can be viewed at a fairly fundamental level as transient computational objects, kind of like session identifiers, rather than being tied to any off-line identity of the parties involved.

If certified keys are required, certificate verification and PKI deployment are necessary to support the verification. However, there may be scalability problems with PKI which, while not a problem at the application level, may be a problem if PKI use is pushed further down the stack. Certificate exchange requires a large amount of bandwidth; online certificate verification has long delays; and offline certificate verification leaves windows open for attacks using revoked public keys. The scalability problem may become worse when PKI is pushed deeper into the stack, because the frequency of utilization for such mechanisms as on-line certificate revocation checks may increase, reducing the number of nodes that can be efficiently supported. Even though IPsec and IKE do have provisions for PKI use and they are at a deep layer in the stack, the lack of widespread deployment of IPsec and IKE for uses other than VPNs, where preconfigured keys can be used, suggests that these issues may be a problem in an Internet where one's cyber-identity is strongly tied somehow to one's off-line identity, and a requirement for establishing that identity is pushed deeply into the stack.

One potential approach to solving this problem is to use identity-based cryptography in HIP. Identity-based cryptography allows any type of identifier to serve as a host's public key, and therefore as a host identifier in HIP, rather than a generated public key. For example, the user's network access identifier (NAI) could be used, thereby tying the HIP identity to the off-line identity of user established with their ISP. An initial prototype using the Boneh-Franklin identity-based cryptosuite shows that HIP using identity-based cryptography uses less bandwidth in the HIP handshake message exchange compared to RSA/DSA based HIP with certificate exchange. On the other hand, setting up the HIP session takes longer than for RSA/DSA based HIP (excluding certificate revocation checking delay), because the Boneh-Franklin identity-based cryptosuite depends on computationally expensive Tate pairings. While theoretical progress is being made in reducing the burden of parings computation, there are other, simpler identity-based cryptographic algorithms that could reduce the computation cost significantly, and implementation optimization could further shorter the session setup delay. HIP based on identity-based cryptography might potentially be useful in an Internet where DNS was replaced by a next generation name resolution system based on distributed hash tables, and the primary mechanism for looking up addresses was, itself, identity-based (e.g. reverse HIT translation), to complement HIP.

Mobility and Location Management

In an Internet where the basic communication pattern is between mobile hosts, simultaneous movement of both hosts may become common. For the basic HIP protocol, after a secure channel is established, one host uses the ReAddr message to notify its correspondent about its movement. If the two hosts move at about the same time, however, the ReAddr message may get lost and the two hosts must initiate a new round of HIP handshake exchanges. The end hosts may even have to wait for a DNS update to get the new location information of their peers, delaying resolution of the handover even longer. Such long handover delays are unacceptable for voice communications and real time applications.

One solution to solving the double-movement problem is to use a rendezvous server as the anchor point for the moving host. Using a rendezvous server can also enable end hosts to hide their current location from their peers, which provides location privacy to end hosts. In our initial prototype, we use router advertisements to broadcast the information of nearby rendezvous servers, and the HIP end host chooses one rendezvous server. The host uses an address assigned by the rendezvous server to set up HIP sessions with its correspondent hosts. During movement, the end host only needs to notify the rendezvous server about its location changes, and such changes are transparent to the correspondent. An open research problem is rendezvous server placement. The rendezvous server should be placed to achieve a good balance between routing delay, handover frequency, and location privacy. Additionally, there is still an issue when a HIP host hands over from one rendezvous server to another. Temporary forwarding mechanisms are a possible solution to this problem.