

# Research Statement

Chin-Tser Huang

My dissertation work is aimed at solving security problems at the network layer of the Internet. There has been a standard network-layer security protocol suite called IPsec. However, after studying the protocols of IPsec, I found that there are several problems with IPsec, especially in its handling of resets and in the effectiveness of its anti-replay window protocol. Therefore, I proposed some revisions to IPsec to fix these two problems. In my papers [1] and [4] listed in my curriculum vitae, I proposed two operations, called SAVE and FETCH, which can be used to avoid the impact of resets. In papers [7] and [11], I proposed two variations of the anti-replay window protocol that largely enhance the protocol's performance against message reorders.

Moreover, IPsec by itself cannot solve the denial-of-service attacks. With IPsec installed, packets from a denial-of-service attack can still go undetected until they reach their destination, thereby cause the waste of network resources and computing resources. In papers [3] and [10], I proposed hop integrity protocol suite that can be implemented side-by-side with IPsec and can detect and discard most denial-of-service attack packets in their first hop. Besides, I showed that hop integrity protocol suite can also achieve the security of routing protocols, as reported in my paper [6].

For the next five years, I will focus my research on security issues at the higher layers of the protocol stack in the Internet: the transport layer and the application layer. To deal with the security problems at these two layers, I will work on certificates, authentication protocols, password protocols, and authorization protocols. In the long run, I will shift my focus to achieving security in network infrastructures other than the Internet, for example wireless networks, ad hoc networks, and sensor networks. Although these networks are still in their early development stages, security problems can emerge soon after they are fully developed, and I believe my research can fulfill some of the needs for security in these networks.