Banana: An Anonymous/Pseudonymous Encrypted Low Latency Overlay Network

Background
Cryptography allows us to hide the content of our messages from an eavesdropper.
Anonymous networking seeks to prevent an eavesdropper from knowing who sent or received specific communications.
Banana is an improvement on previous designs, with the intention of having anonymous internet use approach the efficiency and thus ease of use of typical activity, while enhancing security.

Security or Usability?
Mix networks rely on the presence of large quantities of messages to be batched before forwarding, so that it is hard to discern who most recently forwarded a message.
In order to achieve a sufficient amount of traffic to hide a message in, the mix must wait longer. Here we find a tradeoff between having low latency communications and having anonymity.

Banana's Approach
Banana uses a combination of existing techniques such as onion routing, but includes new techniques to provide a stronger argument towards the system's anonymity.
Each member of the network, or node, connects to others it trusts. These friends exchange constant cover traffic; regardless of the quantity of legitimate data to be passed between them, an eavesdropper will notice no change in the connection's behavior.
Communication is performed through tunnels constructed over the existing network of friends. Because of the cover traffic, relaying may occur immediately without loss of security.

Conclusion
Through the use of friends and cover traffic, individuals are capable of hiding their activities on the network from a global observer without greatly increasing latency and still maintaining a high level of anonymity.
Because we connect directly only to trusted friends, we experience some restrictions but gain many benefits.

Carl Mackey
Faculty Advisor: Jonathan Smith

Senior Project Poster Day 2008, CIS Dept. University of Pennsylvania