ECSE 414 Project Video Script
Problem Statement

Harley Wiltzer (260690006)

November 24, 2017

Suppose you wish to communicate very sensitive information to your friend over the Internet. Due to the confidentiality of the message, it is necessary that it should be extremely difficult for anyone observing the network to be able to read your message, and moreover, it should be extremely difficult for anyone observing the network to determine who your message is destined for. Of course, sending plaintext via HTTP and TCP/IP is not enough, as observers can read your message. Furthermore, using some sort of encrypted communication like HTTPS does not suffice, as your message can still be traced to its destination. One may consider using a VPN, which would hide your message and its destination from observers, however using a VPN requires one to trust that the VPN isn't keeping any logs when it's routing. A malicious VPN server can theoretically unveil where you're sending your messages.

A very interesting solution to this problem is *onion routing* - a technique compromising an array of intermediate routers that obfuscate your message's path from eavesdroppers. In an onion routing network, a user's messages are passed through a random selection of a fraction of thousands of *onion routers* before the final exit node sends your message to the destination. The message is first encrypted with layers of encryption, akin to the layers of an onion, in such a way that each intermediate node must peel off a layer of encryption to determine where to send the message next. This guarantees, first of all, that no one can read your message, as it is always encrypted across the onion network. Furthermore, due to the layered encryption, all onion nodes know only the location of the node before it in the random path and the location of the node after it, so as long as at least three nodes are in the path, *no one may know the location of both the sender and the destination*. So, when there is lots of traffic within the onion network, it is virtually impossible to trace a message across the path to its recipients. Since onion routing hides the contents of messages from eavesdroppers and further hides the endpoints of a message's path, it is a promising technique for communicating anonymously over the Internet.