Cryptographic threat model for Hocnet

2017-01-07

1 Goal

This paper is designed to provide a concise summary of the security requirements and goals of the Hocnet protocol.

2 Application

A public mesh network where each node is paid for the bandwidth they forward. Participants can be anyone with a WiFi device. Some nodes may employ dedicated hardware like directional antennas, IR bridges, or self run wires in an attempt to provide the fastest lowest cost route to a gateway (a node selling access into the internet).

From the perspective of users and applications the mesh will act like layer 2 switch, software running in user land will not be able to distinguish the connection from some more mundane form of networking.

Hardware ranges from consumer grade hardware all the way up to corporate grade hardware depending on the user and how much traffic they which to route.

3 Threat model

An attacker will be able to modify packets, advertise false routes, man in the middle a connection, flood the network with fake nodes, or control some fraction of the network. Lets assume less than 50% for an organized attack.

Of course multiple attackers performing some combination of these is possible.

4 Security Properties

Hocnet must ensure that communication with any given node is valid, that communication itself does not open the system up to infection or compromise, and finally that routes are within some reasonable tolerance of the correct route despite possible attackers.

Exceptions include nodes with only a single connection into the wider mesh, where it is impossible to prevent a MITM and other situations where a single bad actor controls very high value routes. In a well connected network all attacks should be solvable.

5 Performance Constraints

Since the actual mesh is pretty light on CPU resources we can dedicate most of our processing to encryption, think 60% of a fast cell phone processor, memory is a bit tighter since we have to maintain a routing table of every node, so small keys are important think no more than 1GB ram for the routing table which minus crypto is a MAC address, transmission quality value (single precision FP), and gateway info. So 16 bytes per node without crypto, we need the routing table to be big enough for "the last mile", hard to define goal there without more research.

On the network traffic side overhead needs to be as low as is feasible, even at the cost of upgraded processor, ram, or dedicated hardware.