Anonymous DTN routing: Attack scenario

October 2, 2013

1 Attack scenario

In our attack scenario, an adversary tries to track a victim node or infer trusted nodes of a victim node by exploiting 1) ephemeral ID of victim node and 2) packets stored in victim node. Since ephemeral ID of victim node keeps changing at reasonably short interval, leakage of ephemeral ID is not an issue in our protocol. From packets stored in victim node, an adversary is able to track or infer trusted nodes of the victim node through 1) ephemeral ID of packet destination, 2) packet ID or 3) packet payload.

1.1 Tracking a victim node

An adversary may track a victim node by injecting a "marker packet" to the victim node. Marker packet can be identified by its destination ephemeral ID, packet ID or payload.

Upon encountering a victim node V, an adversary A sends a marker packet p with non-existing or inactive destination. If V only can relay packets pulled by other encountered nodes, the marker packet p would not be relayed to other nodes. Therefore, A can track the victim node V until V drops the marker packet p by testing if a node has p.

Remedy (Applied to simulation code) Our protocol allows V relays packets that are not pulled by the encountered node when V relays all the pulled packets. (Or V can relay unpulled packets even before all pulled packets are relayed.) Therefore, A may be able to track V in the short term but in the long term, A cannot assure that a node with p is actually V or not.

1.2 Inferring victim's trusted nodes

An adversary A may infer trusted nodes of a victim node V by knowing which packets are pulled by V.

1.2.1 Attack 1: Destination ephemeral ID

Let's say V's trusted node are $\{a, b, c, d\}$. V has packets destined for $\{b, c\}$ and A prepares marker packets destined for $\{d, e\}$. When V and A encounters, A receives the packet digest of V, $\{b, c\}$. By the protocol, V pulls packet destined for $\{c\}$ through secure method such as PIR. Now A changes its ephemeral ID to A' and gets the packet digest of V. Since the packet digest of V is now $\{b, c, d\}$, A can infer that d is trusted by V.

Remedy (Applied to simulation code) Since V is able to change ephemeral ID of packets destined for its trusted nodes at the end of the current epoch, this attack is feasible only during the current epoch. If V does not include the packets received from untrusted nodes during the current epoch in its packet digest, the attack is not possible any more.

1.2.2 Attack 2: Packet ID

The attack is performed as in attack 1. Since packet ID is not changed at the end of the current epoch, A can infer the trusted nodes of V by getting all packets from V and checking packet IDs. This attack is feasible even after the current epoch is ended.

Remedy (Applied to simulation code) V makes copy of packets received from untrusted nodes and assign new packet IDs. When V encounters a untrusted node, V use the copy of packets, instead of the original packets.

1.2.3 Attack 3: Packet payload

The attack is performed as in attack 2. A can infer the trusted nodes of V by getting all packets from V and checking the payload of the packets.

Remedy No clear solution yet.

In the previous meeting, Dave told me about encrypting payload using symmetric key shared among the trusted nodes. (It's possible that I'm misunderstanding what Dave said.) But the destination may not be one of the trusted node and it may not be able to decrypted the encrypted payload.