Use-case for CGA Proposal

draft-dong-savi-cga-header-02.txt

Dong Zhang
Padmanabha Nallur

Guiding principle

- There are all kinds of attacks initiated by hackers
- We have many solutions to mitigate or reduce the effect of these attacks.
- The desired solution to solve these attacks is by having the basic ability to identify the source of the entity with non-repudiation.
  - ➔ “EVERY PACKET MUST HAVE AN OWNER”
- Ultimate solution:
  - Every packet is signed by the sender of the packet
  - Every packet contains all information to validate the sender
  - Every packet can be validated by any node in the network all the way to the destination
  - There should be no need to communicate with the sender in order to verify the signature in a received packet

Use case 1: Mobile Network

- The nodes in the mobile network before delivering the packet to the radio access network can check that every packet is not forged.
- This will help protect the precious ‘radio resources’ in the network from being attacked
- The advantage of using CGA proposal will be that this capability is provided at the IP layer and is independent of the upper layers or types of mobile network (GSM, CDMA etc.,).

Use case 2: Network operator servers/clients

- The network operation resources like RADIUS server/clients, audit server/clients in the network can benefit form the check on every packet.
- The upper layer protocols like RADIUS etc., do not have to be modified to provide this capability.
- Today most of these employ password based security which is not desirable. Password management is complicated. Most operators end up using a single password for many servers. The CGA proposal does not involve any key management or key distribution.

Use case 3: Hosts (end users)

- Today, end users have no way of knowing whether a packet is forged unless they are using end-to-end security protocols.
- The CGA proposal does not involve the complex key management and key distribution protocols that these end-to-end security protocols use.

Use case 4: Non-repudiation service

- A website can advertise non-repudiation capability by including CGA information with each packet that it sends.
- The users are more likely to go to such websites as opposed to the ones that do not provide CGA information. This can become a selling point for such servers.

Use case 5: SAVI switch checks

- SAVI switches can perform an additional check for forging before installing the bindings for the specific IP addresses.
- The SAVI switches can also optionally authenticate each and every packet before it is injected into the rest of the network.

Use case 6: Per-packet billing

- Per-packet billing can be limited to certain applications or services (e.g., streaming video).
- Per-packet billing without sender non-repudiation would be difficult. The CGA proposal provides a method for sender non-repudiation.

Use case 7: Discovery protocols

- The discovery protocols like SEND etc., implement CGA at the application layer.
- If this capability is implemented at IP layer, then it can be applied to many other discovery protocols (e.g., in the wireless domain) with minimal changes in the application layer (e.g., configure the source IP addresses that should be authenticated).

Use case 8: Multicast packets

- Mutlicast is used in video streaming, IPTV etc.,
- The CGA parameters can provide stream authentication for every packet. Every recipient of multicast packet can verify the source of every packet
- Intermediate nodes can verify the source before multicasting the packet to other nodes. If it fails, the packet can be dropped immediately avoiding a multicast flooding.

Questions?

zhangdong_rh@huaweisymantec.com
pnallur@huawei.com