CGA Extension header for IPv6

Paddy Nallur

Introduction

- Source address validation
  - One of the charter of SAVI is “no changes to host”
  - Why not relax some of these charter points and come up with alternative approaches to sav

Overview

- The ‘CGA extension header’ proposal is to validate the source IPv6 address in a packet so that it cannot be forged by anyone else e.g., attacker;
- Basically proposal is to provide Anti-IP-spoofing

Description

- Applies only to IPv6
- IPv6 address selection gives an opportunity for end host/device to select the lower 16 bits of the address
- We can use this flexibility to associate a private key/public key pair with a specific IP address
  - CGA (Cryptographically Generated Address) is used already to perform this function
  - The chances of another person finding the key and address association is very low

Description

- The proposal is to add an extension to IPv6 header that includes the CGA address and CG parameters
- The originating host/device can optionally include the CGA header in the IPv6 packet.
- The header includes among other parameters:
  - Signature signed using private key associated with the IP address
  - Public key

Description

- Any receiver can compute the signature using the public key and compare with the signature in the CGA-header. If it does not match it means that the source address is forged
- The source address validation can be implemented anywhere in the network (from the first node all the way to the end-host).
- All nodes that don’t understand this new extension header simply pass this on with the packet. No change here.

Description

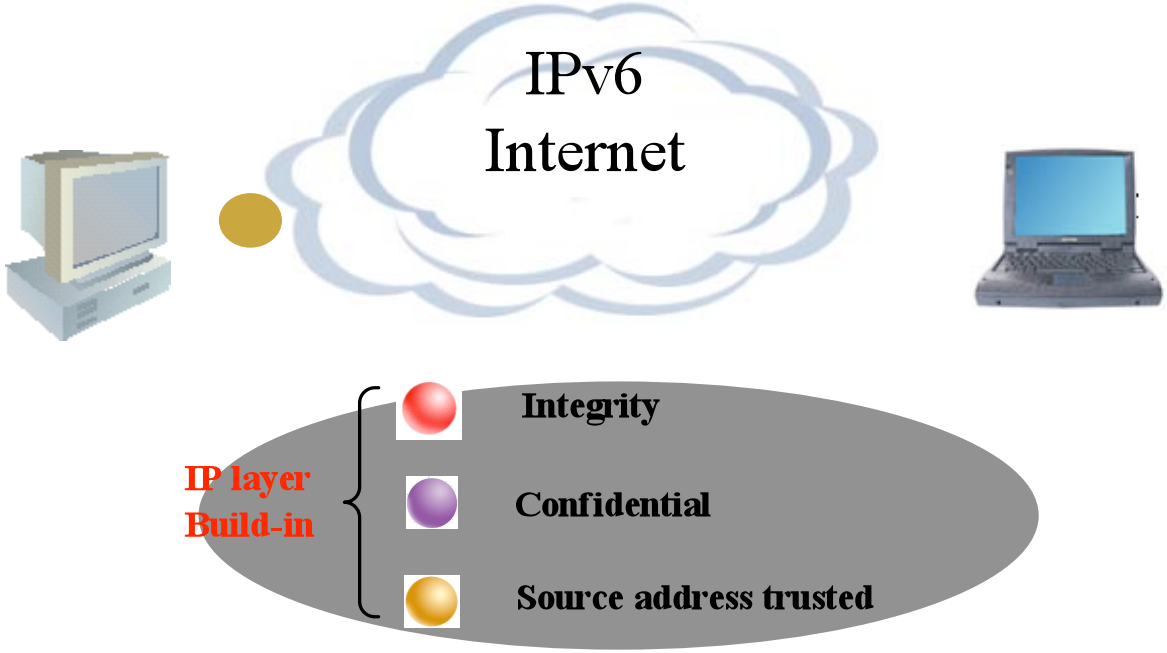
- From security perspective
  - Assumptions about security (see Evolution of the IP Model draft-iab-ip-model-evolution-01.txt)
    - Packets are unmodified in transit
    - Packets are private
    - Source address are not forged
  - Corresponding Approach
    - Unmodified: AH
    - Private: ESP
    - Not forged: ?? (Why not build-in this function for IPv6 ?)

Description

- For IPv6 we have extension headers for AH and ESP already.
- Addition of CGA header will give an anti-IP-spoofing built-in capability at the IP layer
- Other uses for CGA extension header
  - Security protocols (e.g., IPSEC) can also use the CGA header for deriving the public key

Benefits

- The users can be assured that someone else (attackers) cannot use their IP address to send packets
- For vendors: IP address based traffic analysis becomes more meaningful
- Applications that use IP address to identify device can be assured that the packet was originated by the specific address.
- IETF drafts
  - draft-dong-savi-cga-header-00.txt
  - draft-dong-esp-sa-cga-00.txt


IPv6
Internet
IP layer
Build-in
Integrity
Confidential
Source address trusted

- Questions?