Security in the last mile
---DHCP is going to help

Extended DHCPv6 for Piggybacking
Security Association Configuration

Di MA
madi@cnnic.cn
China Internet Network Information Center
Background

• The importance of DHCP
  – DHCP is typically the first protocol executed by a mobile host when it enters a new network.
  – *DHCP service is typically provided by a centralized service composed of fewer managed components, so DHCP server misconfiguration is less likely than delivery of misconfigured Route Advertisements.* (As in draft-droms-dhc-dhcpsv6-default-router-00 by Ralph Droms)
  – The other IP address associated configuration could be accomplished via DHCP as well.
Background

• IPSec is pervasive in many scenarios to build the channel of security mechanism to protect the communication between the host and the local servers.
  – DNS recursive name server
  – SIP server

• Security Association (SA) Configuration is indispensable for IPSec.
  – Manually
  – IKE
Motivation

• DHCP is widely used in wireless access network
  – If DHCP is indispensable, why bother to employ another interaction to configure SA to invite delay in operation

• IPSec is IP address-oriented
  – IPSec connection cannot survive renumbering
  – SA configuration might go with IP address assignment as well
Intended Scenarios

- Public Wireless Access Network
- Access Network where IP addresses are assigned dynamically
Is DHCP ready for that?

- The desired preparation
  - Pre-shared secret configured on DHCP server and the other local server respectively
  - It is especially appropriate for those local servers that already interpret DHCPv6 messages.
New DHCPv6 Roles

• target server
  – A local server of the access network, who is to be configured with SA by DHCP. The target server works as a DHCP client listening for DHCP messages on UDP port 546

• requestor
  – A host that wants to establish SA with a target server. The requestor works as a DHCP client requesting configuration parameters for SA.
Extended DHCP Operation

Request or DHCP Server Target Server

- SOLICIT
- ADVERTISE
- REQUEST
- SCONFIGURATION
- SCONFIGURATION-REPLY
- REPLY
Message Exchange

• New defined DHCPv6 messages
  – SACONFIGURATION and SACONFIGURATION-REPLY

• Confidentiality of key
  – DHCP server uses requestor’s public key to encrypt the symmetric key of SA
  – DHCP server uses pre-shred key to encrypt the symmetric key of SA
New DHCPv6 Options

• Client Public Key Option
  – To specify the requestor’s public key

• Requestor's Parameters Option
  – To specify security parameters provided by the requestor

• SA Request Option
  – To encapsulate SA Requestor's Parameters Option(s) for different target server

• SA Option
  – To specify SA parameters shared between a requestor and a specific target server

• SA List Option
  – To contain one or more SA Options in response to the SA request
Other Considerations

- SA configuration after DHCP phase
  - DHCPv6 Information-Request message
- Rogue DHCP server
  - DHCP Authentication
  - In public wireless access network, secured link layer is going to help.
Thanks!

You will find more details in this document

http://tools.ietf.org/id/draft-madi-dhc-dhcpv6-psac-00.txt
Q&A