DHCP Privacy Updates

draft-krishnan-dhc-dhcpv6-privacy-00
draft-jiang-dhc-dhcpv4-privacy-00

Suresh Krishnan, Sheng Jiang, Tomek Mrugalski

Goals

- Evaluate and document the potential privacy issues in the current DHCP protocol (both DHCPv6 and DHCPv4)
  - Enumerate the identifiers used in the protocol
  - Describe mechanisms that currently exist in DHCP that affect privacy
  - Describe potential attacks
    - Mitigation strategies and solutions to come later

Overview

- Identifiers
- Current Mechanisms
- Attacks
- Differences between DHCPv4 and DHCPv6
- Work Plan

Identifiers

DUID Client ID Server ID	IA_NA, IA Address IA_TA IA_PD, IA Prefix	Interface ID Subscriber ID Remote ID
Civic Location Geographic Location	ORO Vendor Class Client HW Address Client System Arch	Client FQDN

Overview

- Identifiers
- Current Mechanisms
- Attacks
- Differences between DHCPv4 and DHCPv6
- Work Plan

Attacks

- Device type and OS discovery (fingerprinting)
  - The type of device the client uses as well as the Operating system running on the device can be guessed using information in DHCP messages
- Finding location information of client
  - From DHCP options designed to provide such information to clients
- Finding previously visited networks
  - By looking at information that leaks from the DHCP messages on the *new* network

Attacks (2)

- Finding a stable identity & correlation of activities over time
  - Using stable DHCP identifiers that persist across networks and time
  - Possibility of location tracking
- Bulk information collection
  - Pervasive monitoring
    - Using one or more of the passive attacks described earlier
  - Leasequery & bulk leasequery

Overview

- Identifiers
- Current Mechanisms
- Attacks
- Differences between DHCPv4 and DHCPv6
- Work Plan

DHCPv6 and DHCPv4

- They have very similar behaviors
  - Consequently, existing mechanisms that affect privacy and potential attacks are similar
- The Options are a bit different

DHCPv6	DHCPv4
DUID	Client ID
IA_NA, IA_TA, IA_PD, IA Address and IA Prefix Options	'yiaddr' field and 'requested IP address' option
Client Link-layer Address Option	'htype' and 'chaddr' fields
ORO	Parameter Request List
Remote ID, Interface ID	Relay agent information option

Overview

- Identifiers
- Current Mechanisms
- Attacks
- Differences between DHCPv4 and DHCPv6
- **Work Plan**

Use cases

1. The obvious one: client discloses identifiers that can be used for tracking/identification
   - Identifiers: MAC, client-id, remote-id
   - Location: addresses in confirm
   - Identifying information: tomeks-laptop.isc.org
2. Tethering
   - A phone enables tethering, starts announcing its server-id
   - We need to also address server anonymity
3. Forget me!
   - Servers tend to assign the same address/prefix to returning clients
   - Some clients want to explicitly have their addresses/prefixes changing over time
   - Solution to #1 won’t work when client has to be identifiable by the operator, e.g. cable modem clients

Proposed schedule

Milestone	Planned date	Comments
Initial submission of problem analysis draft-jiang-dhc-dhcp-privacy-00 draft-krishnan-dhc-dhcpv6-privacy	Oct/Nov 2014	-00 submitted
Problem analysis adoption	Nov 2014	
Initial submission of mitigation drafts	End of 2014?	1 volunteer, looking for more
Mitigation drafts adoption	Feb 2015?	
WGLC on problem analysis	?	
WGLC on mitigation	?	
Problem analysis: submit to IESG	?	
Mitigation: submit to IESG	?	

Next Steps

- Adopt these drafts as WG items?