Network Working Group
Request for Comments: 3634
Category: Standards Track

K. Luehrs
CableLabs
R. Woundy
Comcast Cable
J. Bevilacqua
N. Davoust
YAS Corporation

December 2003

Key Distribution Center (KDC) Server Address Sub-option for the Dynamic Host Configuration Protocol (DHCP) CableLabs Client Configuration (CCC) Option

Status of this Memo

Copyright Notice

Abstract

This document defines a new sub-option for the CableLabs Client Configuration (CCC) Dynamic Host Configuration Protocol (DHCP) option code for conveying the network addresses of Key Distribution Center (KDC) servers.

1. Introduction

A CableLabs Client Configuration (CCC) Dynamic Host Configuration Protocol (DHCP) Option code providing the Key Distribution Center (KDC) server address will be needed for CableHome-compliant residential gateways configured to use Kerberos for authentication as the first step in establishing a secure SNMPv3 link between the Portal Service (PS) logical element [2,3] in residential gateways, and the SNMP entity in the cable operator’s data network.

The CCC DHCP option code will be used to address specific needs of CableLabs client devices during their configuration processes. This document proposes a sub-option for the CCC DHCP option.

Configuration of a class of CableLabs client devices described in [2] and [3] will require a DHCP sub-option to provide the client with the network address of a KDC server in the cable operator's data network.

The class of devices assumed in [2] and [3] is unlike the class of devices considered in [1], which perform a DNS lookup of the Kerberos Realm name to find the KDC server network address.

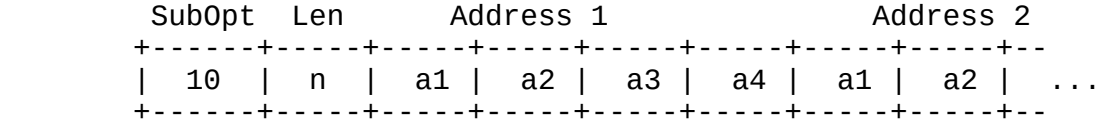
This document proposes a sub-option of the CCC DHCP option code for use with CableLabs client devices. The proposed sub-option encodes an identifier for the network address of each of one or more Key Distribution Center servers with which the CableLabs client device exchanges security information.

The key words "MUST", "MUST NOT", "SHOULD", "SHOULD NOT" and "MAY" in this document are to be interpreted as described in BCP 14, RFC 2119 [4].

2. Key Distribution Center IP Address Sub-option

CableHome specifications will specify the Key Distribution Center network address encoding as a sub-option of the CCC DHCP Option code. This field will be used to inform the client device of the network address of one or more Key Distribution Center servers.

The encoding of the KDC Server Address sub-option will adhere to the format of an IPv4 address. The minimum length for this option is 4 octets, and the length MUST always be a multiple of 4. If multiple KDC Servers are listed, they MUST be listed in decreasing order of priority. The format of the KDC Server Address sub-option of the CCC option code is as shown below:



3. Security Considerations

This document relies upon the DHCP protocol [5] for authentication and security, i.e., it does not provide security in excess of what DHCP is (or will be) providing. Potential exposures to attack in the DHCP protocol are discussed in section 7 of the DHCP protocol specification [5] and in Authentication for DHCP Messages [6].

The CCC option can be used to misdirect network traffic by providing incorrect DHCP server addresses, incorrect provisioning server addresses, and incorrect Kerberos realm names to a CableLabs client

device. This misdirection can lead to several threat scenarios. A Denial of Service (DoS) attack can result from address information being simply invalid. A man-in-the-middle attack can be mounted by providing addresses to a potential snooper. A malicious service provider can steal customers from the customer selected service provider, by altering the Kerberos realm designation.

These threats are mitigated by several factors.

Within the cable delivery architecture required by CableLabs' PacketCable, DOCSIS, and CableHome specifications, the DHCP client is connected to a network through a cable modem and the Cable Modem Termination System (CMTS). The CMTS is explicitly configured with a set of DHCP servers to which DHCP requests are forwarded. Further, a correctly configured CMTS will only allow downstream traffic from specific IP addresses/ ranges.

Assuming that server addresses were successfully spoofed to the point that a malicious client device was able to contact a KDC, the client device must still present valid certificates to the KDC before being service enabled. Given the computational overhead of the certificate validation process, this situation could present a DoS opportunity.

It is possible for a malicious (although certificate enabled) service provider to redirect a customer from the customer's selected service provider. It is assumed that all service providers permitted onto an access providers network are trusted entities that will cooperate to ensure peaceful coexistence. If a service provider is found to be redirecting customers, this should be handled as an administrative matter between the access provider and the service provider.

Another safeguard that can be taken by service providers to limit their exposure to their KDC server(s) is to configure their network so that the KDC(s) reside on a separate subnetwork.

Service providers can further protect their KDC server(s) by placing a firewall in front of the KDC(s) only allowing connections needed for its current provisioning processes. The IP temporary addresses given the client devices from the DHCP server could be sent directly to the firewall from the DHCP server to open a hole for Kerberos messages only for those particular IP addresses for a short period of time. If this was used it would be recommended that service providers authenticate their DHCP server to the KDC as well. This could be done via password authentication rather than digital certificate due to the co-location of the DHCP server to the KDC.

Finally, Kerberos requires mutual client-server authentication. Therefore, the client device must authenticate itself with its digital certificate and the KDC is required to authenticate it to the client device. If a hacker tries to redirect the client device by replacing the service provider-configured KDC Server Address sub-option with another IP address, it is not likely to be a valid service provider's KDC server and authentication will fail.

4. IANA Considerations

The KDC Server Address sub-option described in this document is intended to be a sub-option of the CableLabs Client Configuration (CCC) option described in [1]. IANA has assigned and registered sub-option code 10 of the CCC option to the KDC Server Address sub-option.

5. Intellectual Property Statement

6. Normative References

[1] Beser, B. and P. Duffy, "DHCP Option for CableLabs Client Configuration", RFC 3495, March 2003.

[2] "CableHome 1.1 Specification", CableLabs, http://www.cablelabs.com/projects/cablehome/specifications/.

[3] "CableHome 1.0 Specification", CableLabs, http://www.cablelabs.com/projects/cablehome/specifications/.

[4] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[5] Droms, R., "Dynamic Host Configuration Protocol", RFC 2131, March 1997.

[6] Droms, R. and W. Arbaugh, "Authentication for DHCP Messages", RFC 3118, June 2001

7. Authors' Addresses

Kevin Luehrs
CableLabs
858 Coal Creek Circle
Louisville, CO 80027

Phone: (303) 661-9100
EMail: k.luehrs@cablelabs.com

Richard Woundy
Comcast Cable
27 Industrial Drive
Chelmsford, MA 01824

Phone: (978) 244-4010
EMail: richard_woundy@cable.comcast.com

John Bevilacqua
YAS Corporation
300 Brickstone Square
Andover, MA 01810

Phone: (978) 749-9999
EMail: john@yas.com

Nancy Davoust
YAS Corporation
300 Brickstone Square
Andover, MA 01810

Phone: (978) 749-9999
EMail: nancy@yas.com

8. Full Copyright Statement

Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.