

Kerberos Ticket Control Sub-option
for the CableLabs Client Configuration Option.

Status of this Memo

This document is an Internet-Draft and is in full conformance with all provisions of [Section 10 of RFC 2026](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at <http://www.ietf.org/ietf/lid-abstracts.txt>

The list of Internet-Draft Shadow Directories can be accessed at <http://www.ietf.org/shadow.html>.

Copyright Notice

Copyright (C) The Internet Society (2003). All Rights Reserved.

Abstract

This document defines a new sub-option for the CableLabs Client Configuration (CCC) Option. This new sub-option will be used to direct CableLabs Client Devices (CCDs) to invalidate locally persisted Kerberos tickets.

1. Conventions used in this document

NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC 2119](#) [2].

2. Terminology

Definitions of terms/acronyms used throughout this document:

CCC - CableLabs Client Configuration option, described in [1].

CCD - CableLabs Client Device. A PacketCable MTA is an example of a CCD.

KTC - Kerberos Ticket Control. The CCC sub-option described in this document.

MTA - Media Terminal Adapter. The CCD specific to the PacketCable architecture.

PacketCable - multimedia architecture developed by CableLabs. See [6] for full details.

3. Introduction

The CableLabs Client Configuration Option [1] defines several sub-options used to configure devices deployed into CableLabs architectures. These architectures employ the Kerberos protocol [3] to support CCD authentication and establishment of security associations between CCDs and application servers.

CCDs are permitted to locally persist Kerberos tickets. Thus a power-cycled CCD is enabled to avoid expensive ticket acquisition for locally persisted, non-expired tickets. This feature greatly reduces the Kerberos overhead of a deployment.

This sub-option allows the service provider to control the lifetime of Kerberos tickets persisted locally on a CCD. The service provider requires this capability to support operational functions such as disabling a subscriber's service, forcing re-establishment of security associations, or for testing and remote diagnostic of CCDs.

Duffy

Expires July 2003

2

Internet Draft

Kerberos Ticket Control

January 2003

4. Kerberos Ticket Control Sub-option

This sub-option defines a Ticket Control Mask (TCM) that instructs the CCD to validate/invalidate specific application

server tickets. The sub-option is encoded as follows:

Code	Len	TCM	
TBD	2	m1	m2

The length MUST be 2. The TCM field is encoded as an unsigned 16 bit quantity per network byte-ordering rules. Each bit of the TCM is assigned to a specific server or server group. A bit value of 0 means the CCD MUST NOT invalidate the locally persisted ticket for the server/server group. A bit value of 1 means the CCD MUST invalidate the locally persisted ticket for the server/server group.

Bit #0 is the least significant bit of the field. The bit positions are assigned as follows.

Bit #0 - the PacketCable Provisioning Server used by the CCD.

Bit #1 - the group of all PacketCable Call Management Servers used by the CCD.

Bit #2 - #15. Reserved and MUST be set to 0.

If a CCD does not locally persist Kerberos tickets, it MUST ignore this sub-option.

5. IANA Considerations

IANA is requested to assign a sub-option code to this sub-option from the "CableLabs Client Configuration" sub-option number space (maintained within the BOOTP-DHCP Parameters Registry).

6. Security Considerations

Potential DHCP protocol attack exposure is discussed in [section 7](#) of the DHCP protocol specification [\[4\]](#) and in Authentication for DHCP Messages [\[5\]](#). Additional CCC attack exposure is discussed in [\[1\]](#).

Duffy
Internet Draft

Expires July 2003
Kerberos Ticket Control

3
January 2003

The KTC sub-option could be used to disrupt a CableLabs architecture deployment. In the specific case of PacketCable [\[6\]](#), a deployment could be disrupted if a large number of MTAs are reset/power cycled, initiate their provisioning flow [\[7\]](#), and are instructed by a malicious DHCP server to invalidate all

Kerberos tickets. This could lead to a Denial of Service (DoS) condition as this large set of MTAs simultaneously attempt to authenticate and obtain tickets from the Kerberos infrastructure.

However, the scenario described above is unlikely to occur. Within the cable delivery architecture required by PacketCable (and other CableLabs architectures), the DHCP client is connected to a network through a cable modem and the CMTS (head-end). 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.

7. References

7.1. Normative

[1] B. Beser and P. Duffy, "DHCP Option for CableLabs Client Configuration", <http://www.ietf.org/internet-drafts/draft-ietf-dhc-packetcable-06.txt>, January 2003.

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

7.2. Informational

[3] J. Kohl and C. Neuman, "The Kerberos Network Authentication Service (V5)", [RFC 1510](#), September 1993.

[4] R. Droms, "Dynamic Host Configuration Protocol", [RFC 2131](#), March 1997.

[5] R. Droms and W. Arbaugh, "Authentication for DHCP Messages", [RFC 3118](#), June 2001

Duffy	Expires July 2003	4
Internet Draft	Kerberos Ticket Control	January 2003

[6] "PacketCable Architecture Framework Technical Report", PKT-TR-ARCH-V01-991201, <http://www.packetcable.com/specifications.html>

[7] "PacketCable MTA Device Provisioning Specification", PKT-SP-PROV-I05-021127. <http://www.packetcable.com/specifications.html>

8. Acknowledgments

The author would like to acknowledge the effort of all those who contributed to the development of the PacketCable Provisioning

specifications:

Sumanth Channabasappa (Alopa Networks); Angela Lyda, Rick Morris, Rodney Osborne (Arris Interactive); Steven Bellovin and Chris Melle (AT&T); Eugene Nechamkin (Broadcom); John Berg, Maria Stachelek, Matt Osman (CableLabs); Klaus Hermanns, Azita Kia, Michael Thomas, Paul Duffy (Cisco); Deepak Patil (Com21); Jeff Ollis, Rick Vetter (General Instrument/Motorola); Roger Loots, David Walters (Lucent); Peter Bates (Telcordia); Patrick Meehan (Tellabs); Satish Kumar, Itay Sherman, Roy Spitzer (Telogy/TI), Aviv Goren (Terayon); Prithivraj Narayanan (Wipro), and Burcak Beser (Juniper Networks).

9. Author's Addresses

Paul Duffy
Cisco Systems
300 Apollo Drive
Chelmsford, MA, 01824
Email: paduffy@cisco.com

10. Full Copyright Statement

Copyright (C) The Internet Society (2003). All Rights Reserved.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to

Duffy	Expires July 2003	5
Internet Draft	Kerberos Ticket Control	January 2003

the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY

IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Acknowledgement

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

Duffy

Expires July 2003

6