             PacketCable Security Ticket Control Sub-Option
         for the DHCP CableLabs Client Configuration (CCC) Option

Status of this Memo

   This document specifies an Internet standards track protocol for the
   Internet community, and requests discussion and suggestions for
   improvements. Please refer to the current edition of the "Internet
   Official Protocol Standards" (STD 1) for the standardization state
   and status of this protocol. Distribution of this memo is unlimited.

Abstract

   This document defines a new sub-option for the DHCP CableLabs Client
   Configuration (CCC) Option. This new sub-option will be used to
   direct CableLabs Client Devices (CCDs) to invalidate security tickets
   stored in CCD non volatile memory (i.e., locally persisted security
   tickets).

1.   Conventions used in this document

   The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT",
   "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this
   document are to be interpreted as described in BCP 14, 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.

   STC - Security 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
        [8] 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 implement the PacketCable
   Security Specification [4] (based on Kerberos V5 [5]), to support CCD
   authentication and establishment of security associations between
   CCDs and application servers.

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

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

   It should be noted that, although based on the Kerberos V5 RFC [5],
   the PacketCable Security Specification is not a strict implementation
   of this RFC. See [4] for details of the PacketCable Security
   Specification.

4.   Security 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
   +-----+-----+-----+-----+
   |  9  |  2  | m1  | m2  |
   +-----+-----+-----+-----+
```

   The length MUST be 2. The TCM field is encoded as an unsigned 16 bit
   quantity per network byte order. Each bit of the TCM is assigned to
   a specific server or server group. A bit value of 0 means the CCD
   MUST apply normal invalidation rules (defined in [4]) to the locally

persisted ticket for the server/server group. A bit value of 1 means the CCD MUST immediately 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 store tickets, it MUST ignore this sub-option. Bit values not known to the CCD MUST be ignored.

5.   IANA Considerations

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

   IANA has also set-up a new registry and will maintain a new number space of "CableLabs Client Configuration Option Ticket Control Mask Bit Definitions", located in the BOOTP-DHCP Parameters Registry. The initial bit definitions are described in section 4 of this document. IANA will register future bit mask definitions via an "IETF Consensus" approval policy as described in RFC 2434 [3].

6.   Security Considerations

   Potential DHCP protocol attack exposure is discussed in section 7 of the DHCP protocol specification [6] and in Authentication for DHCP Messages [7]. Additional CCC attack exposure is discussed in [1].

   The STC sub-option could be used to disrupt a CableLabs architecture deployment. In the specific case of PacketCable [8], a deployment could be disrupted if a large number of MTAs are reset/power cycled, initiate their provisioning flow [9], and are instructed by a malicious DHCP server to invalidate all security 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 security infrastructure.

   However, the scenario described above is unlikely to occur. Within the cable delivery architecture required by the various CableLabs projects, the DHCP client is connected to a network through a cable

modem and the CMTS (head-end router). The CMTS is explicitly
configured with a set of valid DHCP server addresses to which DHCP
requests are forwarded. Further, a correctly configured CMTS will
only allow DHCP downstream traffic from specific DHCP server
addresses.

It should be noted that the downstream filtering of DHCP packets will
not prevent spoofed DHCP servers behind the CMTS, but the network
infrastructure behind the CMTS is assumed to be closely controlled by
the service provider.

7.   Intellectual Property Statement

The IETF takes no position regarding the validity or scope of any
intellectual property or other rights that might be claimed to
pertain to the implementation or use of the technology described in
this document or the extent to which any license under such rights
might or might not be available; neither does it represent that it
has made any effort to identify any such rights. Information on the
IETF's procedures with respect to rights in standards-track and
standards-related documentation can be found in BCP-11. Copies of
claims of rights made available for publication and any assurances of
licenses to be made available, or the result of an attempt made to
obtain a general license or permission for the use of such
proprietary rights by implementors or users of this specification can
be obtained from the IETF Secretariat.

The IETF invites any interested party to bring to its attention any
copyrights, patents or patent applications, or other proprietary
rights which may cover technology that may be required to practice
this standard. Please address the information to the IETF Executive
Director.

8. References

8.1. Normative

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

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

   [3] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA
       Considerations Section in RFCs", RFC 2434, October 1998.

   [4] "PacketCable Security Specification", PKT-SP-SEC-I09-030728,
       http://www.packetcable.com/downloads/specs/
       PKT-SP-SEC-I09-030728.pdf

8.2. Informative

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

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

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

   [8] "PacketCable 1.0 Architecture Framework Technical Report",
       PKT-TR-ARCH-V01-991201,
       http://www.packetcable.com/downloads/specs/
       pkt-tr-arch-v01-991201.pdf

   [9] "PacketCable MTA Device Provisioning Specification",
       PKT-SP-PROV-I07-030728,
       http://www.packetcable.com/downloads/specs/
       PKT-SP-PROV-I07-030728.pdf

9. 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, Venkatesh Sunkad (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).

10. Author's Address

   Paul Duffy
   Cisco Systems
   1414 Massachusetts Avenue
   Boxborough, MA 01719

   EMail: paduffy@cisco.com

11. Full Copyright Statement

Acknowledgement