                  Security Threats and Security Requirements for the
                         Access Node Control Protocol (ANCP)

Abstract

   The Access Node Control Protocol (ANCP) aims to communicate Quality
   of Service (QoS)-related, service-related, and subscriber-related
   configurations and operations between a Network Access Server (NAS)
   and an Access Node (e.g., a Digital Subscriber Line Access
   Multiplexer (DSLAM)). The main goal of this protocol is to allow the
   NAS to configure, manage, and control access equipment, including the
   ability for the Access Nodes to report information to the NAS.

   This present document investigates security threats that all ANCP
   nodes could encounter. This document develops a threat model for
   ANCP security, with the aim of deciding which security functions are
   required. Based on this, security requirements regarding the Access
   Node Control Protocol are defined.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

   The Access Node Control Protocol (ANCP) aims to communicate QoS-
   related, service-related, and subscriber-related configurations and
   operations between a Network Access Server (NAS) and an Access Node
   (e.g., a Digital Subscriber Line Access Multiplexer (DSLAM)).

   [ANCP-FRAME] illustrates the framework, usage scenarios, and general
   requirements for ANCP. This document focuses on describing security
   threats and deriving security requirements for the Access Node
   Control Protocol, considering the ANCP use cases defined in
   [ANCP-FRAME] as well as the guidelines for IETF protocols' security
   requirements given in [RFC3365]. Section 5 and Section 6,
   respectively, describe the potential attacks and the different attack
   forms that are liable to take place within ANCP, while Section 7
   applies the described potential attacks to ANCP and its different use
   cases. Security policy negotiation, including authentication and
   authorization to define the per-subscriber policy at the policy/AAA
   (Authentication, Authorization, and Accounting) server, is out of the
   scope of this work. As a high-level summary, the following aspects
   need to be considered:

   Message Protection:

      Signaling message content can be protected against eavesdropping,
      modification, injection, and replay while in transit. This
      applies to both ANCP headers and payloads.

   Prevention against Impersonation:

      It is important that protection be available against a device
      impersonating an ANCP node (i.e., an unauthorized device
      generating an ANCP message and pretending it was generated by a
      valid ANCP node).

   Prevention of Denial-of-Service Attacks:

      ANCP nodes and the network have finite resources (state storage,
      processing power, bandwidth). It is important to protect against
      exhaustion attacks on these resources and to prevent ANCP nodes
      from being used to launch attacks on other network elements.

2. Specification Requirements

   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 [RFC2119], with the

qualification that, unless otherwise stated, they apply to the design
of the Access Node Control Protocol (ANCP), not its implementation or
application.

The relevant components are described in Section 3.

3. System Overview and Threat Model

As described in [ANCP-FRAME] and schematically shown in Figure 1, the
Access Node Control system consists of the following components:

Network Access Server (NAS):

   A NAS provides access to a service (e.g., network access) and
   operates as a client of the AAA protocol. The AAA client is
   responsible for passing authentication information to designated
   AAA servers and then acting on the response that is returned.

Authentication, Authorization, and Accounting (AAA) server:

   A AAA server is responsible for authenticating users, authorizing
   access to services, and returning authorization information
   (including configuration parameters) back to the AAA client to
   deliver service to the user. As a consequence, service usage
   accounting might be enabled and information about the user's
   resource usage will be sent to the AAA server.

Access Node (AN):

   The AN is a network device, usually located at a service provider
   central office or street cabinet, that terminates access-loop
   connections from subscribers. In case the access loop is a
   Digital Subscriber Line (DSL), this is often referred to as a DSL
   Access Multiplexer (DSLAM).

Customer Premises Equipment (CPE):

   A CPE is a device located inside a subscriber's premise that is
   connected at the LAN side of the Home Gateway (HGW).

Home Gateway (HGW):

   The HGW connects the different Customer Premises Equipments (CPEs)
   to the Access Node and the access network. In case of DSL, the
   HGW is a DSL Network Termination (NT) that could either operate as
   a layer 2 bridge or as a layer 3 router. In the latter case, such
   a device is also referred to as a Routing Gateway (RG).

Aggregation Network:

    The aggregation network provides traffic aggregation from multiple
    ANs towards the NAS. ATM or Ethernet transport technologies can
    be used.

For the threat analysis, this document focuses on the ANCP
communication between the Access Node and the NAS. However,
communications with the other components (such as HGW, CPE, and the
AAA server) play a role in the understanding of the system
architecture and of what triggers ANCP communications. Note that the
NAS and the AN might belong to two different administrative realms.
The threat model and the security requirements in this document
consider this latter case.

```
                                              +--------+
                                              |  AAA   |
                                              | Server |
                                              +--------+
                                                  |
                                                  |
    +---+   +---+   +------+   +-----------+   +-----+   +--------+
    |CPE|---|HGW|---|      |   |Aggregation|   |     |   |        |
    +---+   +---+   |Access|   | Network   |   |     |   |Internet|
                    | Node |----|           |----| NAS |---|   /    |
    +---+   +---+   | (AN) |   |           |   |     |   |Regional|
    |CPE|---|HGW|---|      |   |           |   |     |   |Network |
    +---+   +---+   +------+   +-----------+   +-----+   +--------+
```
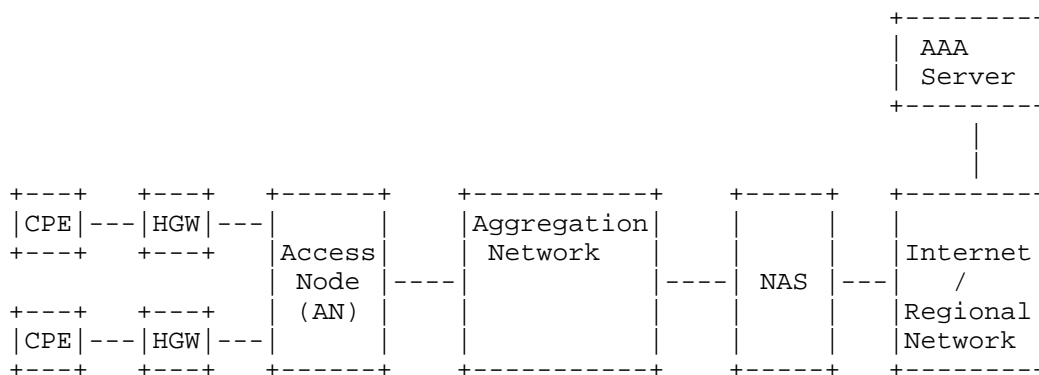
                     Figure 1: System Overview

In the absence of an attack, the NAS receives configuration
information from the AAA server related to a CPE attempting to access
the network. A number of parameters, including Quality of Service
information, need to be conveyed to the Access Node in order to
become effective. The Access Node Control Protocol is executed
between the NAS and the AN to initiate control requests. The AN
returns responses to these control requests and provides information
reports.

For this to happen, the following individual steps must occur:

o The AN discovers the NAS.

o The AN needs to start the protocol communication with the NAS to
   announce its presence.

o The AN and the NAS perform a capability exchange.

o The NAS sends requests to the AN.

o The AN processes these requests, authorizes the actions, and
   responds with the appropriate answer. In order to fulfill the
   commands, it might be necessary for the AN to communicate with the
   HGW or other nodes, for example, as part of a keep-alive
   mechanism.

o The AN provides status reports to the NAS.

Attackers can be:

o off-path, i.e., they cannot see the messages exchanged between the
   AN and the NAS;

o on-path, i.e., they can see the messages exchanged between the AN
   and the NAS.

Both off-path and on-path attackers can be:

o passive, i.e., they do not participate in the network operation
   but rather listen to all transfers to obtain the maximum possible
   information;

o active, i.e., they participate in the network operation and can
   inject falsified packets.

We assume the following threat model:

o An off-path adversary located at the CPE or the HGW.

o An off-path adversary located on the Internet or a regional
   network that connects one or more NASes and associated access
   networks to Network Service Providers (NSPs) and Application
   Service Providers (ASPs).

o An on-path adversary located at network elements between the AN
   and the NAS.

o An on-path adversary taking control over the NAS.

o An on-path adversary taking control over the AN.

4. Objectives of Attackers

   Attackers may direct their efforts either against an individual
   entity or against a large portion of the access network. Attacks
   fall into three classes:

   o Attacks to disrupt the communication for individual customers.

   o Attacks to disrupt the communication of a large fraction of
      customers in an access network. These also include attacks to the
      network itself or a portion of it, such as attacks to disrupt the
      network services or attacks to destruct the network functioning.

   o Attacks to gain profit for the attacker through modifying the QoS
      settings. Also, through replaying old packets (of another
      privileged client, for instance), an attacker can attempt to
      configure a better QoS profile on its own DSL line, increasing its
      own benefit.

5. Potential Attacks

   This section discusses the different types of attacks against ANCP,
   while Section 6 describes the possible means of their occurrence.

   ANCP is mainly susceptible to the following types of attacks:

5.1. Denial of Service (DoS)

   A number of denial-of-service (DoS) attacks can cause ANCP nodes to
   malfunction. When state is established or certain functions are
   performed without requiring prior authorization, there is a chance to
   mount denial-of-service attacks. An adversary can utilize this fact
   to transmit a large number of signaling messages to allocate state at
   nodes and to cause consumption of resources. Also, an adversary,
   through DoS, can prevent certain subscribers from accessing certain
   services. Moreover, DoS can take place at the AN or the NAS
   themselves, where it is possible for the NAS (or the AN) to
   intentionally ignore the requests received from the AN (or the NAS)
   through not replying to them. This causes the sender of the request
   to retransmit the request, which might allocate additional state at
   the sender side to process the reply. Allocating more state may
   result in memory depletion.

5.2. Integrity Violation

   Adversaries gaining illegitimate access on the transferred messages
   can act on these messages, causing integrity violation. Integrity
   violation can cause unexpected network behavior, leading to a
   disturbance in the network services as well as in the network
   functioning.

5.3. Downgrading

   Protocols may be useful in a variety of scenarios with different
   security and functional requirements. Different parts of a network
   (e.g., within a building, across a public carrier's network, or over
   a private microwave link) may need different levels of protection.
   It is often difficult to meet these (sometimes conflicting)
   requirements with a single mechanism or fixed set of parameters;
   thus, often a selection of mechanisms and parameters is offered. A
   protocol is required to agree on certain (security) mechanisms and
   parameters. An insecure parameter exchange or security negotiation
   protocol can give an adversary the opportunity to mount a downgrading
   attack to force selection of mechanisms weaker than those mutually
   desired. Thus, without binding the negotiation process to the
   legitimate parties and protecting it, ANCP might only be as secure as
   the weakest mechanism provided (e.g., weak authentication) and the
   benefits of defining configuration parameters and a negotiation
   protocol are lost.

5.4. Traffic Analysis

   An adversary can be placed at the NAS, the AN, or any other network
   element capturing all traversing packets. Adversaries can thus have
   unauthorized information access. As well, they can gather
   information relevant to the network and then use this information in
   gaining later unauthorized access. This attack can also help
   adversaries in other malicious purposes -- for example, capturing
   messages sent from the AN to the NAS announcing that a DSL line is up
   and containing some information related to the connected client.
   This could be any form of information about the client and could also
   be an indicator of whether or not the DSL subscriber is at home at a
   particular moment.

5.5. Management Attacks

   Since the ANCP sessions are configured in the AN and not in the NAS
   [ANCP-FRAME], most configurations of ANCP are done in the AN.
   Consequently, the management attacks to ANCP mainly concern the AN
   configuration phase. In this context, the AN MIB module could create
   disclosure- and misconfiguration-related attacks. [ANCP-MIB] defines

the vulnerabilities on the management objects within the AN MIB
module. These attacks mainly concern the unauthorized changes of the
management objects, leading to a number of attacks such as session
deletion, a session using an undesired/unsupported protocol,
disabling certain ANCP capabilities or enabling undesired
capabilities, ANCP packets being sent out to the wrong interface (and
thus being received by an unintended receiver), harming the
synchronization between the AN and the NAS, and impacting traffic in
the network other than ANCP.

6. Attack Forms

   The attacks mentioned above in Section 5 can be carried out through
   the following means:

   Message Replay:

      This threat scenario covers the case in which an adversary
      eavesdrops, collects signaling messages, and replays them at a
      later time (or at a different place or in a different way; e.g.,
      cut-and-paste attacks). Through replaying signaling messages, an
      adversary might mount denial-of-service and theft-of-service
      attacks.

   Faked Message Injection:

      An adversary may be able to inject false error or response
      messages, causing unexpected protocol behavior and succeeding with
      a DoS attack. This could be achieved at the signaling-protocol
      level, at the level of specific signaling parameters (e.g., QoS
      information), or at the transport layer. An adversary might, for
      example, inject a signaling message to request allocation of QoS
      resources. As a consequence, other users' traffic might be
      impacted. The discovery protocol, especially, exhibits
      vulnerabilities with regard to this threat scenario.

   Messages Modification:

      This involves integrity violation, where an adversary can modify
      signaling messages in order to cause unexpected network behavior.
      Possible related actions an adversary might consider for its
      attack are the reordering and delaying of messages, causing a
      protocol's process failure.

Man-in-the-Middle:

An adversary might claim to be a NAS or an AN, acting as a man-in-
the-middle to later cause communication and services disruption.
The consequence can range from DoS to fraud. An adversary acting
as a man-in-the-middle could modify the intercepted messages,
causing integrity violation, or could drop or truncate the
intercepted messages, causing DoS and a protocol's process
failure. In addition, a man-in-the-middle adversary can signal
information to an illegitimate entity in place of the right
destination. In this case, the protocol could appear to continue
working correctly. This may result in an AN contacting a wrong
NAS. For the AN, this could mean that the protocol failed for
unknown reasons. A man-in-the-middle adversary can also cause
downgrading attacks through initiating faked configuration
parameters and through forcing selection of weak security
parameters or mechanisms.

Eavesdropping:

This is related to adversaries that are able to eavesdrop on
transferred messages. The collection of the transferred packets
by an adversary may allow traffic analysis or be used later to
mount replay attacks. The eavesdropper might learn QoS
parameters, communication patterns, policy rules for firewall
traversal, policy information, application identifiers, user
identities, NAT bindings, authorization objects, network
configuration, performance information, and more.

7. Attacks against ANCP

ANCP is susceptible to security threats, causing disruption/
unauthorized access to network services, manipulation of the
transferred data, and interference with network functions. Based on
the threat model given in Section 3 and the potential attacks
presented in Section 5, this section describes the possible attacks
against ANCP, considering the four use cases defined in [ANCP-FRAME].

Although ANCP is not involved in the communication between the NAS
and the AAA/policy server, the secure communication between the NAS
and the AAA/policy server is important for ANCP security.
Consequently, this document considers the attacks that are related to
the ANCP operation associated with the communication between the NAS
and the AAA/Policy server. In other words, the threat model and
security requirements in this document take into consideration the
data transfer between the NAS and the AAA server, when this data is
used within the ANCP operation.

Besides the attacks against the four ANCP use cases described in the
following subsections, ANCP is susceptible to a number of attacks
that can take place during the protocol-establishment phase. These
attacks are mainly on-path attacks, taking the form of DoS or man-in-
the-middle attacks, which could be as follows:

o Attacks during the session initiation from the AN to the NAS:
   DoS attacks could take place affecting the session-establishment
   process. Also, man-in-the-middle attacks could take place,
   causing message truncation or message modification and leading to
   session-establishment failure.

o Attacks during the peering establishment:
   DoS attacks could take place during state synchronization between
   the AN and the NAS. Also, man-in-the-middle attacks could take
   place through message modification during identity discovery,
   which may lead to loss of contact between the AN and the NAS.

o Attacks during capabilities negotiation:
   Message replay could take place, leading to DoS. Also, man-in-
   the-middle attacks could take place, leading to message
   modification, message truncation, or downgrading through
   advertising lesser capabilities.

7.1. Dynamic Access-Loop Attributes

This use case concerns the communication of access-loop attributes
for dynamic, access-line topology discovery. Since the access-loop
rate may change over time, advertisement is beneficial to the NAS to
gain knowledge about the topology of the access network for QoS
scheduling. Besides data rates and access-loop links identification,
other information may also be transferred from the AN to the NAS
(examples in case of a DSL access loop are DSL type, maximum
achievable data rate, and maximum data rate configured for the access
loop). This use case is thus vulnerable to a number of on-path and
off-path attacks that can be either active or passive.

On-path attacks can take place between the AN and the NAS, on the AN
or on the NAS, during the access-loop attributes transfer. These
attacks may be:

o Active, acting on the transferred attributes and injecting
   falsified packets. The main attacks here are:

   * Man-in-the-middle attacks can cause access-loop attributes
      transfer between the AN and a forged NAS or a forged AN and the
      NAS, which can directly cause faked attributes and message
      modification or truncation.

* Signaling replay, by an attacker between the AN and the NAS, on
  the AN or on the NAS itself, causing DoS.

* An adversary acting as man-in-the-middle can cause downgrading
  through changing the actual data rate of the access loop, which
  impacts the downstream shaping from the NAS.

o Passive, only learning these attributes. The main attacks here
  are caused by:

* Eavesdropping through learning access-loop attributes and
  information about the clients' connection state, and thus
  impacting their privacy protection.

* Traffic analysis allowing unauthorized information access,
  which could allow later unauthorized access to the NAS.

Off-path attacks can take place on the Internet, affecting the
access-loop attribute sharing between the NAS and the AAA/policy
server. These attacks may be:

o Active attacks, which are mainly concerning:

* DoS through flooding the communication links to the AAA/policy
  server, causing service disruption.

* Man-in-the-middle, causing access-loop configuration retrieval
  by an illegitimate NAS.

o Passive attacks, gaining information on the access-loop
  attributes. The main attacks in this case are:

* Eavesdropping through learning access-loop attributes and
  learning information about the clients' connection states, and
  thus impacting their privacy protection.

* Traffic analysis allowing unauthorized information access,
  which could allow later unauthorized access to the NAS.

7.2. Access-Loop Configuration

   This use case concerns the dynamic, local-loop line configuration
   through allowing the NAS to change the access-loop parameters (e.g.,
   rate) in a dynamic fashion. This allows for centralized, subscriber-
   related service data. This dynamic configuration can be achieved,
   for instance, through profiles that are pre-configured on ANs. This
   use case is vulnerable to a number of on-path and off-path attacks.

On-path attacks can take place where the attacker is between the AN
and the NAS, is on the AN, or is on the NAS. These can be as
follows:

o Active attacks, taking the following forms:

   * DoS attacks of the AN can take place by an attacker, through
      replaying the Configure Request messages.

   * An attacker on the AN can prevent the AN from reacting on the
      NAS request for the access-loop configuration, leading to the
      NAS continually sending the Configure Request message and,
      hence, allocating additional states.

   * Damaging clients' profiles at ANs can take place by adversaries
      that gained control on the network through discovery of users'
      information from a previous traffic analysis.

   * An adversary can replay old packets, modify messages, or inject
      faked messages. Such adversary can also be a man-in-the-
      middle. These attack forms can be related to a privileged
      client profile (having more services) in order to configure
      this profile on the adversary's own DSL line, which is less
      privileged. In order that the attacker does not expose its
      identity, he may also use these attack forms related to the
      privileged client profile to configure a number of illegitimate
      DSL lines. The adversary can also force configuration
      parameters other than the selected ones, leading to, for
      instance, downgrading the service for a privileged client.

o Passive attacks, where the attacker listens to the ANCP messages.
   This can take place as follows:

   * Learning configuration attributes is possible during the update
      of the access-loop configuration. An adversary might profit to
      see the configuration that someone else gets (e.g., one ISP
      might be interested to know what the customers of another ISP
      get and therefore might break into the AN to see this).

Off-path attacks can take place as follows:

o An off-path passive adversary on the Internet can exert
   eavesdropping during the access-loop configuration retrieval by
   the NAS from the AAA/policy server.

   o An off-path active adversary on the Internet can threaten the
      centralized subscribers-related service data in the AAA/policy
      server through, for instance, making subscribers' records
      inaccessible.

7.3. Remote Connectivity Test

   In this use case, the NAS can carry out a Remote Connectivity Test
   using ANCP to initiate an access-loop test between the AN and the
   HGW. Thus, multiple access-loop technologies can be supported. This
   use case is vulnerable to a number of active attacks. Most of the
   attacks in this use case concern the network operation.

   On-path active attacks can take place in the following forms:

   o Man-in-the-middle attack during the NAS's triggering to the AN to
      carry out the test, where an adversary can inject falsified
      signals or can truncate the triggering.

   o Message modification can take place during the Subscriber Response
      message transfer from the AN to the NAS announcing the test
      results, causing failure of the test operation.

   o An adversary on the AN can prevent the AN from sending the
      Subscriber Response message to the NAS announcing the test
      results, and hence the NAS will continue triggering the AN to
      carry out the test, which results in more state being allocated at
      the NAS. This may result in unavailability of the NAS to the ANs.

   Off-path active attacks can take place as follows:

   o An adversary can cause DoS during the access-loop test, in case of
      an ATM-based access loop, when the AN generates loopback cells.
      This can take place through signal replaying.

   o Message truncating can take place by an adversary during the
      access-loop test, which can lead to service disruption due to
      assumption of test failures.

7.4. Multicast

   In this use case, ANCP could be used in exchanging information
   between the AN and the NAS, allowing the AN to perform replication
   inline with the policy and configuration of the subscriber. Also,
   this allows the NAS to follow subscribers' multicast (source, group)
   membership and control replication performed by the AN. Four
   multicast use cases are expected to take place, making use of ANCP;
   these are typically multicast conditional access, multicast admission

control, multicast accounting, and spontaneous admission response.
This section gives a high-level description of the possible attacks
that can take place in these cases. Attacks that can occur are
mostly active attacks.

On-path active attacks can be as follows:

o DoS attacks, causing inability for certain subscribers to access
   particular multicast streams or only access the multicast stream
   at a reduced bandwidth, impacting the quality of the possible
   video stream. This can take place through message replay by an
   attacker between the AN and the NAS, on the AN or on the NAS.
   Such DoS attacks can also be done by tempering, for instance, with
   white/black list configuration or by placing attacks to the
   bandwidth-admission-control mechanism.

o An adversary on the NAS can prevent the NAS from reacting on the
   AN requests for white/black/grey lists or for admission control
   for the access line. The AN in this case would not receive a
   reply and would continue sending its requests, resulting in more
   states being allocated at the AN. A similar case happens for
   admission control when the NAS can also send requests to the AN.
   When the NAS does not receive a response, it could also retransmit
   requests, resulting in more state being allocated at the NAS side
   to process responses. This may result in the unavailability of
   the NAS to the ANs.

o Man-in-the-middle, causing the exchange of messages between the AN
   and a forged NAS or a forged AN and the NAS. This can lead to the
   following:

   * Message modification, which can cause service downgrading for
      legitimate subscribers -- for instance, an illegitimate change
      of a subscriber's policy.

   * Message truncation between the AN and the NAS, which can result
      in the non-continuity of services.

   * Message replay between the AN and the NAS, on the AN or on the
      NAS, leading to a DoS or services fraud.

   * Message modification to temper with accounting information, for
      example, in order to avoid service charges or, conversely, in
      order to artificially increase service charges on other users.

An off-path active attack is as follows:

o DoS could take place through message replay of join/leave requests
   by the HGW or CPE, frequently triggering the ANCP activity between
   the AN and the NAS. DoS could also result from generating heaps
   of IGMP join/leaves by the HGW or CPE, leading to very high rate
   of ANCP query/response.

8. Security Requirements

   This section presents a number of requirements motivated by the
   different types of attacks defined in the previous section. These
   requirements are as follows:

   o The protocol solution MUST offer authentication of the AN to the
      NAS.

   o The protocol solution MUST offer authentication of the NAS to the
      AN.

   o The protocol solution MUST allow authorization to take place at
      the NAS and the AN.

   o The protocol solution MUST offer replay protection.

   o The protocol solution MUST provide data-origin authentication.

   o The protocol solution MUST be robust against denial-of-service
      (DoS) attacks. In this context, the protocol solution MUST
      consider a specific mechanism for the DoS that the user might
      create by sending many IGMP messages.

   o The protocol solution SHOULD offer confidentiality protection.

   o The protocol solution SHOULD ensure that operations in default
      configuration guarantees a low number of AN/NAS protocol
      interactions.

   o The protocol solution SHOULD ensure the access control of the
      management objects and possibly encrypt the values of these
      objects when sending them over the networks.

9. Security Considerations

   This document focuses on security threats, deriving a threat model
   for ANCP and presenting the security requirements to be considered
   for the design of ANCP.

10. Acknowledgments

   Many thanks go to Francois Le Faucher for reviewing this document and
   for all his useful comments. The authors would also like to thank
   Philippe Niger, Curtis Sherbo, and Michael Busser for reviewing this
   document. Other thanks go to Bharat Joshi, Mark Townsley, Wojciech
   Dec, and Kim Hylgaard who have had valuable comments during the
   development of this work.

11. References

11.1. Normative References

   [RFC2119]   Bradner, S., "Key words for use in RFCs to Indicate
                  Requirement Levels", BCP 14, RFC 2119, March 1997.

   [RFC3365]   Schiller, J., "Strong Security Requirements for
                  Internet Engineering Task Force Standard Protocols",
                  BCP 61, RFC 3365, August 2002.

11.2. Informative References

   [ANCP-FRAME]   Ooghe, S., Voigt, N., Platnic, M., Haag, T., and S.
                  Wadhwa, "Framework and Requirements for an Access Node
                  Control Mechanism in Broadband Multi-Service
                  Networks", Work in Progress, October 2009.

   [ANCP-MIB]   De Cnodder, S. and M. Morgenstern, "Access Node Control
                  Protocol (ANCP) MIB module for Access Nodes", Work
                  in Progress, July 2009.

Authors' Addresses

   Hassnaa Moustafa
   France Telecom
   38-40 rue du General Leclerc
   Issy Les Moulineaux,   92794 Cedex 9
   France

   EMail: hassnaa.moustafa@orange-ftgroup.com

   Hannes Tschofenig
   Nokia Siemens Networks
   Linnoitustie 6
   Espoo 02600
   Finland

   Phone: +358 (50) 4871445
   EMail: Hannes.Tschofenig@gmx.net
   URI: http://www.tschofenig.priv.at

   Stefaan De Cnodder
   Alcatel-Lucent
   Copernicuslaan 50
   B-2018 Antwerp,
   Belgium

   Phone: +32 3 240 85 15
   EMail: stefaan.de_cnodder@alcatel-lucent.com