NSIS Threats
<draft-tschofenig-nsis-threats-01.txt>

Status of this Memo

Abstract

   As the work in the NSIS working has begun to describe requirements
   and the framework people started thinking about possible security
   implication. This document should provide a starting point for the
   discussion at the NSIS working group mailing list regarding the
   security issues that have to be addressed by a protocol or within
   the framework. This document does not describe vulnerabilities of a
   particular protocol or threats of published NSIS framework
   proposals. This memo is furthermore meant to create awareness for
   security issues within the NSIS group. Security requirements related
   to the threat scenarios are described in [1].

1 Introduction

   It is often argued that QoS signaling protocols are similar to other
   signaling protocols and one might re-use their security mechanisms
   for avoiding reengineering overhead. This is true up to some point:
   A QoS signaling protocol might borrow many security mechanisms from
   other protocols but different trust assumptions, and different
   protocol processing may demand different solutions or adaptations.
   This document tries to show threats that need to be addressed by the
   designers of a QoS signaling protocol. Although the base protocol
   might be sure, some extensions may cause problems when used in a
   particular environment. We think that it is necessary to investigate
   the context in which a QoS protocol is integrated and in which
   sequence protocols are executed (when combined together with other
   protocols). A particular focus of QoS signaling protocols should be
   given to the interaction with accounting and charging solutions:
   Without an appropriate integration of QoS and accounting protocols
   there is no good incentive for network operators to deploy them. The
   interaction between the protocols is subject of a framework. Some of
   these issues are therefore found in [5].

   Independent of the threat scenarios described in Section 3 we
   identify the following structural pieces, which require different
   security protection because of different trust relationships. The
   sub-parts are: access network part, intra and inter-domain part, and
   finally end-to-end communication between the two signaling end-
   points. These parts are briefly described. The threat scenarios in
   Section 3 can be assigned to the individual parts.

   a) Access Network

   This section addresses threats that arise when the QoS Initiator
   (QI) is attached to access network and transmits and receives QoS

signaling messages. In many mobility environments it is difficult to assume the existence of a pre-established trust relationship between a user and the access network.

Threat scenarios dealing with initial QoS security association setup, replay attacks, lack of confidentiality, denial of service, integrity violation, identity spoofing and fraud are applicable.

From a security point of view this part of the network causes the most problems.

b) Intra-Domain

After receiving a QoS signaling message and verifying the request somewhere in the access network the signaling messages traverse the network within the same administrative domain. Since the request has already been authenticated and authorized threats might likely be different compared to those described in the previous section. To differentiate the end-node-to-access network interface with the intra-domain communication (i.e. communication internally within one administrative domain) we assume that no user hosts are attached to the core-network. (That is: the interface between any host and the first router is part of the access network). We furthermore assume that nodes within one administrative domain have a stronger trust relationship between each other.

c) Inter-Domain

The security protection between the borders of different administrative domains largely depends on how accounting is done. If one domain transmits forged QoS reservations (for example stating a higher QoS reservation than a aggregated number of user did) to next domain then it is likely that the originating network domain has also has to pay for the reservation. Hence in this case, there is no real benefit for the first network domain to forge a QoS reservation. But if an end-node is directly charged by intermediate domains then this kind of attack may be reasonable. Security protection of messages transmitted between different administrative domains is still necessary to tackle attacks like spoofing, integrity violation, denial of service etc. The lower number of networks and higher trust relationship (compared in the access network case) usually causes fewer problems for the key management.

d) End-to-End

In our opinion end-to-end security for QoS signaling messages (in addition to hop-by-hop security) is rarely required if we assume that end-to-end issues like charging and the selection which user

has to pay for a reservation is already securely negotiated by
preceding upper layer protocols (for example SIP). Information
carried within a QoS signaling protocol for the purpose of charging
is therefore assumed opaque to the QoS protocol itself and
appropriately protected as part of the AAA interaction. For
accounting data, the QoS signaling protocol is therefore only used
as a transport mechanism. Note however that this assumption strongly
depends on the chosen solution of a protocol interaction with AAA,
QoS and application layer protocol. It is however possible to select
a charging solution that requires end-to-end protection of
information delivered within the QoS signaling protocol. The
following example requires some sort of end-to-end protection: Alice
wants Bob to pay for the QoS reservation (reverse charging). Bob
wants to be assured that the QoS signaling message he receives was

transmitted by Alice because he is only willing to pay for
particular users and not for everyone. Hence Bob requires Alice to
protect the reservation request.

Regarding end-to-end security one additional issue needs to be
clarified. Whenever a signaling protocol travels end-to-end and a
node along the path acts on behalf of the other endpoint then
further investigation is required how to solve this delegation
issue.

2 Terminology

Some threat scenarios in this document use the entity user instead
of the QoS Initiator (as introduced in [1]). This is mainly due to
the fact that security protocols allow a differentiation between
entities being hosts or users (based on the identities used). Since
the QoS Initiator as used in [1] also allows to act on behalf of
various entities including a network it is reasonable to distinguish
between these identities.

We use the term access network for a network to which a mobile node
is attached. Other terms often used in this context are foreign or
visited network. The missing direct trust relationship between the
mobile node and the access network is characteristic for such an
interface and complicates authentication and key agreement. Usually
AAA protocols (like Radius or Diameter) are used to provide the
initial authentication and key establishment. These protocols take
advantage of the infrastructure (AAAL, AAAH, Broker, etc.) and trust
relationships between the access network and the user's home
network. This trust relationship is usually based on some sort of
contract and hence it can be seen as symmetric whereas the
dynamically established trust relationship between the mobile node
and the access network is asymmetric. The mobile node has to trust

the access network in many regards. The access network usually does
not trust attached end-hosts.

The term security association is used to describe established
security-relevant data structure between two entities. This data
structure consists of keys, algorithms including their parameters,
values used for replay protection etc. Using this information two
(or more) nodes are able to protect QoS signaling messages.

3 Threat Scenarios

This section provides threat scenarios that are applicable to the
quality of service signaling protocols.

3.1 Man-in-the-Middle Attacks

This Section describes man-in-the-middle attacks of the following
type: During the process of establishing a security association an
adversary fools the QI with respect to the entity to which it has to
authenticate. The man-in-the-middle adversary is able to modify
signaling messages transmitted to the real network requesting

Tschofenig   Informational - Expires August 2002   4
                         NSIS Threats   July 2002

different QoS parameters. The QI wrongly believes that it talks to
the ôrealö network whereas it is actually attached to an adversary.
Note that a solution for protecting QoS signaling messages does not
necessarily need to establish a "long-lasting" security association.
Performance reasons may however require to create one.

For this attack to be successful, pre-conditions have to hold which
are described with the two scenarios below:

a) No authentication

The first case considers the case that no authentication between the
QI and other entity (access network, other networks, a single node)
takes places: Without authentication the QI is unable to detect an
adversary. It may seem to be strange why someone does not consider
to protect QoS signaling messages. However in some cases protection
available might be difficult to accomplish in a practical
environment either because the other end-point of the communication
is unknown, because of a failure in the network configuration or
because of misbelieved trust relationships in parts of the network.
If one of the communication endpoints is unknown then for some
security protocols it is not possible or difficult to select the
appropriate key. Regarding an assumed trust relationship, which is
not present in some environments, some network administrators refuse
to consider security protection of intra-domain signaling messages
because of various reasons. Such a configuration sometimes allows a
compromised node in the network to interfere the communication of

other nodes although it was never intended to actively participate
in the signaling.

b) Unilateral authentication

In case of only unilateral authentication (that is, a missing
authentication of the access network to the QI) the QI is not able
to discover the man-in-the-middle adversary. In the
telecommunication world this type of attack is known as the false
base-station attacks (if the unilateral authentication is executed
between a user and the access network).

The two threats described above are a general problem of network
access without appropriate authentication, not only for QoS
signaling protocol. Still these issues need to be correctly
addressed in a proposed protocol since the impacts may reach beyond
the local network. No authentication or unilateral authentication is
not only applicable for signaling messages transmitted between a QI
and the access network but also between all other nodes.

3.2 Missing real-time notifications of QoS reservation costs (cost control)

This type of threat is addresses a deployment problem when using QoS
signaling in a real-world environment. It is not a particular
attack. A large number of service providers with complex roaming
agreements create a non-transparent cost-structure. Using AAA

protocols in a subscription-based scenario (i.e. user is registered
with his home service provider) the user does not learn the identity
of the network using a regular message exchange. The user is only
authenticated to the home network (and possibly vice versa). The
identity of the access network is possibly not revealed. When
issuing a reservation request to the network the end-user does not
know the cost of such a reservation. Furthermore due to mobility and
route changes along the path the costs for a reservation and for
transmitted data packets might not be acceptable for the end-user.
However a missing protocol between the user and the network and
without the possibility for the user to interact with the network to
commit the credit withdrawal costs can reach unexpected amounts.

When selecting a new point of attachment in case of roaming the end-
host does not currently have an option to query the network for a
reservation cost. Some proposals which try to merge mobility
protocols with QoS signaling probe the access network up to the
cross-over router for the possibility making a QoS reservation
(without actually making the reservation itself). Without such a
mechanism to provide network providers a user cannot take reservation

costs into consideration when choosing between different networks.
Hence the user is unable to refuse the more expensive service
provider. The choice for selecting different providers might be
available not only because of overlapping frequency ranges but also
because of different access technologies (either using a WLAN card to
access the local network or to use UMTS/UTRAN based technology).

Although real-time notifications of quality of service reservation
costs (cost control) to the user are outside the scope of a quality
of service signaling protocol itself some interactions might be
required.

3.3 Eavesdropping and Traffic Analysis

This Section covers two threats: The first scenario is related to
privacy concerns whereas the second addresses problems caused by
weak authentication mechanisms and the increased risk of
eavesdropping on the wireless link in absence of appropriate
confidentiality protection.

The first threat case covers adversaries that are unable to actively
participate in the QoS signaling (passive adversary) but eavesdrop
messages. The collected signaling packets may serve for the purpose
of traffic analysis or to later mount replay attacks as described in
the next Section. By eavesdropping an adversary might violate a
userÆs privacy preference. Especially QoS signaling messages provide
information that may be interesting for an adversary since the
messages include user and/or application identities, policy
information, information about the desired QoS reservation, etc. The
information gathered by an adversary can be to learn usage patterns
of users requesting resources and track QoS reservations.

An adversary who is able to actively participate in the signaling
might be able to use the signaling protocol to discover the topology

of a network (e.g. using record route). Additionally it might be
possible to obtain diagnostic information usually used for network
monitoring and administration. Other options might allow an
adversary to route signaling messages specifically along a
particular route similar to source routing.

The second threat case addresses weak authentication mechanisms
whereby information transmitted within the QoS signaling protocol
may leak passwords and may allow offline dictionary attacks. This
threat is not specific to QoS signaling protocols by may also be
applicable and countermeasures must be taken.

3.4 Adversary being able to replay signaling messages

This threat scenario covers the case where an adversary eavesdrops
and collects signaling messages and replays them at a latter point
in time (or at a different place, or uses parts of them at a
different place or in a different way û e.g. cut and paste attacks).
The adversary may use this technique in absence of appropriately
protected messages to mount denial of service attacks. Furthermore
also theft of service is possible.

A more difficult attack that may cause problems even in case of
replay protection requires the adversary to crash a QoS aware node
(router, broker, etc.) to lose synchronization and to be able to
replay old QoS signaling messages.

Additionally it should be mentioned that the interaction between
different protocols based on authorization tokens requires some
care. Using such an authorization token it is possible to link state
information between different protocols. When returning an
authorization token to the end-host based for example on a SIP
message exchange eavesdropping an replay could allow an adversary to
steal resources without proper protection of the token delivery and
without verification of the hopefully protected content of the
token. The functionality and structure of such an authorization
token for RSVP is described in [3] and in [4].

3.5 Identity Spoofing

An adversary with the capability to spoof the identity may mount the
following attacks:

Eve, acting as an adversary, claims to be the registered user Alice
by spoofing the identity of Alice. Thereby Eve causes the network to
charge Alice for the consumed network resources. Using unprotected
signaling messages Eve may experience no particular problems in
succeeding. This attack can be classified as theft of service.

In case that the signaling request is properly protected the
adversary has to spent considerable more effort. This threat tries
to address possible problems with traffic classification based on
some identifiers (IP addresses, transport protocol id, ports, flow
label [6] and [7], etc.). Additionally concerns might occur if the

end-host performs the traffic marking for example by using a DSCP.
When the ingress router uses the DSCP of the incoming data traffic
then the situation might be worse since this field is not protected
by IPSec AH (and also by IPSec ESP). Issues of DiffServ and IPSec
protection are described in Section 6.2 of [RFC2745]. Other security
issues related to denial of service attacks are described in Section
6.1 of [RFC2745].

The following paragraph describes a possible threat caused by
identity spoofing of transmitted data traffic. After the network
receives a properly protected reservation request, transmitted by
the legitimate user Alice, traffic filters are installed at edge
devices. These traffic filters allow data traffic originated from a
given address to be assigned to a particular QoS class. The
adversary Eve now spoofs the IP address of the Alice (or whatever
identifier is used in the flow classification). Additionally AliceÆs
host may be crashed by the adversary as a result of a denial of
service attack or lost connectivity for a variety of other reasons.
If both nodes are located at the same link and use the same IP
address then obviously the usage of a duplicate IP address will be
detected. Assuming that only Eve is available at the link then she
is now able to receive and transmit data (for example RTP data
traffic), that receives preferential QoS treatment, using AliceÆs IP
address (or whatever identifier is used in the flow classification).
Assuming the soft state paradigm where periodical refresh messages
are required the absence of Alice will not be detected until the
next signaling message appears and forces Eve to respond with a
protected signaling message. Again this issue is not only applicable
to QoS traffic but the existence of QoS reservation causes more
difficulties since this type of traffic is more expensive.

3.6 Adversary being able to inject/modify messages

The next type of threat is caused by an integrity violation: An
adversary modifies signaling messages (e.g. by acting as a man-in-
the-middle) to achieve an unexpected network behavior with the bogus
request. Possible actions are reordering, delaying, dropping,
injecting and modifying.

Using a different identity the adversary may forward a modified a
QoS signaling message requesting a large amount of resources (using
a different identity). If granted it causes other user's resource-
request not to be successful and a different initiator (for example
a user) to pay for the QoS reservation. This attack is only
successful in absence of signaling message protection.

3.7 Missing Non-Repudiation Property

Repudiation in this context refers to a problem where one party
later denies to have made a reservation. This issue comes in two
flavors:

From a service provider point-of-view the following threat may be
worth an investigation because a user may deny to have issued

reservation requests for which it was charged. A service provider
may then like to prove that a particular user issued the reservation
request.

The same threat can be interpreted from the users point-of-view. A
service provider claims to have received a number of reservation
requests. The user in question thinks that he never issued those
requests and wants to have a proof for correct service usage for a
given set of QoS parameters.

In todayÆs telecommunication networks non-repudiation is not
provided. The user has to trust the network operator to correctly
meter the traffic, collect and merge accounting data and that no
unforeseen problems occur. If a signaling protocol is used to
establish QoS reservations with a higher volume (for example service
level agreements) then this issue might have a major impact on the
design of a protocol.

3.8 Malicious Edge-Router

Network elements within a domain (intra-domain) experience a
different trust relationship with regard to the security protection
of signaling messages compared to edge routers. We assume that edge
routers have the responsibility to perform cryptographic processing
(authentication, integrity and replay protection, authorization and
accounting). If however an adversary manages to take over an edge
router then the security of the entire network is affected. An
adversary is then able to launch a number of attacks including
denial of service, integrity violation, replay attacks etc. Note
that this problem is not only restricted to QoS signaling protocols.
The chain-of-trust principle applied in the hop-by-hop security
protection does not prevent the network from being vulnerable. An
adversary with full access to the edge router is then also able to
access the keys used to secure messages to other nodes.

Thus the edge router is a critical component that requires strong
security protection. This does not necessarily imply that all
routers within the core network do not need to cryptographically
verify signaling messages and that these routers cannot cause
security problems when acting maliciously. If the chain-of-trust
principle is deployed then the security protection of the path (in
this case within the network of a single administrative domain) is
as strong as the weakest link. In our case the edge router is the
most critical component of this network that may also act as a
security gateway/firewall for incoming/outgoing traffic. For
outgoing traffic this device has to act according to the security
policy of the local domain to apply the appropriate security
protection.

3.9 Denial of Service in a two phase reservation

This threat tries to address potential denial of service attacks
when the reservation setup is split into two phases i.e. path and
reservation (as for example used in receiver based reservation

setup). For this example we assume that the node transmitting the
path message is not charged for the path message itself (only for a
reservation) and is able to issue a high number of reservation
request (possibly in a distributed fashion). The reservations are
however never intended to be successful because of various reasons:
the destination node cannot be reached; it is not responding node or
simply rejects the reservation. An adversary can benefit from the
fact that resources are already consumed along the path for various
processing tasks including path pinning.

3.10   Denial of Service with a bogus signaling request

With a resource reservation request received at a network element
(for example by the first QoS aware router) processing is required
for authentication and authorization. Processing by other nodes
including policy servers, LDAP servers, etc. is also possible
depending on the network configuration. The verification of the
provided credentials requires computations and resources to be
allocated for state maintenance, setting timers, additional messages
transmitted to other nodes, cryptographic computations). If an
adversary is able to transmit a large number of reservation request
(flooding) with bogus credentials and assuming that the verification
is expensive in terms of resource consumption then the verifying
node may not be able to process further reservation messages by
legitimate user.

3.11   Disclosing the networking structure

In some architectural environments there is a desire by the network
provider not to reveal the internal network structure (or other
related information) to the outside world. An adversary might be
able to use NSIS messages for network mapping (e.g. discovering
which nodes exist, which use NSIS, what version, what resources are
allocated, capabilities of nodes along a paths etc.). This
requirement might conflict with a protocol solution that provides a
mean to automatically discover NSIS aware nodes and their identity.

3.12   Modification of subsequent reservation request

An adversary might be able to modify an existing reservation which
had already been established within the network as a result of a
previous QoS signaling message. This means that a QoS signaling
message that modifies established state must be subject to security
protection comparable to the original signaling message setting up

the reservation.

Furthermore it might be necessary to provide assurance for a correct
binding to a specific reservation state. Such a property can be
designated as reservation ownership. This threat addresses
operations for the reservation state established along the path. The
reservation state at routers which is created by signaling messages
is identified by a Reservation ID. The concept of the Reservation ID
is described in [5]. Whenever a signaling message has to refresh,
modify or delete a reservation it is necessary to process previously

created state. Therefore the newly transmitted signaling messages
have to be associated with an existing reservation. Hence there is a
requirement that it must not be possible for someone to use an
arbitrary Reservation ID to modify state where no ownership exits.
Especially in a roaming scenario where a mobile node retransmits
signaling messages from a different point of attachment it must be
assured that the routers along the path are able to verify whether
the entity transmitting the signaling messages is allowed to modify
the established state.

Potential problems caused by this threat are denial of service,
theft of service, service disruption, etc.

3.13   Faked Error/Response messages

An adversary may be able to use false error/response messages as part
of a denial of service attack. This could be either at the
reservation level or at the protocol level.

4 Security Considerations

This entire memo discusses security issues. Some additional threats
are applicable for a framework where a NSIS protocol is used. Some
of these threats are described in [2].

5 References

[1] Brunner, M., "Requirements for QoS Signaling Protocols", draft-
ietf-nsis-req-02.txt, Work In Progress, May 2002.

[2] Kempf, J., Nordmark, E.: ôThreat Analysis for IPv6 Public
Multi-Access Linksö, <draft-kempf-ipng-netaccess-threats-01.txt>,
(work in progress), December, 2002.

[3] Hamer, L-N., Gage, B., Broda, M., Kosinski, B., Shieh, H.:
ôSession Authorization for RSVPö, <draft-ietf-rap-rsvp-authsession-
02.txt>, (work in progress), February, 2002.

[4] Hamer, L-N., Gage, B., Shieh, H.: ôFramework for session set-up
with media authorizationö, <draft-ietf-rap-session-auth-03.txt>,
(work in progress), February, 2002.

[5] Freytsis, I., Hancock, R., Karagiannis, G., Loughney, J., Van
den Bosch, S.: ôNext Steps in Signaling: A Framework Proposalö,
<draft-hancock-nsis-fw-00.txt>, (work in progress), June, 2002.
[RFC2745]

[6]   Partridge, C.: "Using the Flow Label Field in IPv6", RFC
1809, June, 1995.

[7] Rajahalme, J., Conta, A., Carpenter, B., Deering, S.: "IPv6
Flow Label Specification", <draft-ietf-ipv6-flow-label-02.txt>, (work
in progress), June, 2002.

6 Acknowledgments

I would like to thank (in alphabetical order) Marcus Brunner, Jorge
Cuellar, Mehmet Ersue, Xiaoming Fu and Robert Hancock for their
comments to this draft. Jorge and Robert gave me an extensive list
of comments and provided information on additional threats.

7 Author's Addresses

Hannes Tschofenig
Siemens AG
Otto-Hahn-Ring 6
81739 Munich
Germany
Email: Hannes.Tschofenig@mchp.siemens.de