NSIS Working Group
Internet Draft
Document: draft-ietf-nsis-threats-00.txt
Expires: April 2003

Hannes Tschofenig
Siemens AG

October 2002

NSIS Threats
<draft-ietf-nsis-threats-00.txt>

Status of this Memo

This document is an Internet-Draft and is in full conformance with all provisions of Section 10 of RFC2026.

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/1id-abstracts.txt
The list of Internet-Draft Shadow Directories can be accessed at
http://www.ietf.org/shadow.html.

Abstract

This threats document provides a starting point to security discussions at the NSIS working group. It therefore tries to help the NSIS interested reader to understand various security considerations in the NSIS Requirements, Framework and Protocol proposals. This document does not describe vulnerabilities of specific NSIS related protocols.

1 Introduction

Section 1.1 tries to introduce the reader into the overall process of addressing the security of work done in the NSIS working group. Section 1.2 gives a big picture about the different network parts which are traversed by a signaling protocol. Each part is characterized by a different set of requirements and different trust relationships. The threats described in Section 2 can be assigned to the individual parts.

Note that this document tries to use the terminology introduced and used in the NSIS Framework document [5]. Some of the terms which demand additional clarifications are briefly explained introduced in Section 1.3

1.1 NSIS Security Process

Whenever a new protocol has to be developed or existing protocols have to be modified potential security threats should be evaluated. The process of securing protocols in separated into individual steps. To address security in the NSIS working group a number of documents have been produced:

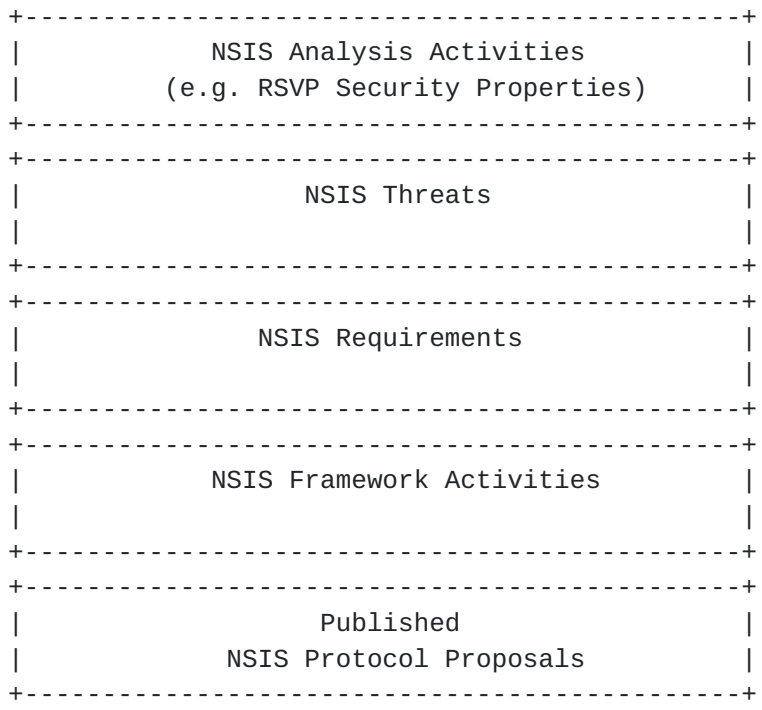

Figure 1: NSIS Security related Documents

In order to reach a satisfactory security protection for a NSIS protocol a number of steps are necessary. The relevant information is

distributed over a number of documents as depicted in Figure 1. The purpose of each of these documents is briefly described below to give the reader a more insights into the development process.

The primary goal of the NSIS analysis activity is the investigation of existing approaches in the area of quality of service signaling protocols. Several of the published approaches contain directly security relevant descriptions whereas other requirements can be derived from different protocol behavior or different scenarios in which such a protocol is used. Document [8] points to the reduced complexity if RSVP is used without multicast support. This modification also comes with some simplifications for security handling. In [10] security issues raised by some example configurations are given. In [9] the security properties of RSVP are described. There are, however, a number of other analysis documents available but they do not directly address security issues.

Threats relevant for NSIS are discussed in this document.

To address threats described in this document requirements were specified in the NSIS Requirements document [1]. In addition to the requirements the document describes some basic scenarios where a QoS signaling protocol might be deployed.

Signaling information to a number of devices located in different parts in the network with different trust assumptions and possible interactions with a large number of other protocols require some framework thoughts. A few proposals were submitted and a few authors cooperatively produced a NSIS framework document [5], which also address security issues.

Finally there are documents describing concrete protocol proposals. These proposals either rely on existing security mechanisms or develop their own if the existing mechanisms cannot be solve all security threats or if they are inappropriate for other reasons. In practice a protocol proposal might use existing security mechanisms but is likely to require some additional protection mechanisms or to combine them in a specific manner.

Note that the process of developing the above-mentioned documents is not linear. Instead various iterations are required to reach a satisfactory final status.

This document tries to identify the basic threats that need to be addressed by the NSIS signaling protocol design. Although the base protocol might be secure, some extensions may cause problems when used in a particular environment. Furthermore it is necessary to investigate the context in which a signaling protocol is used and the architecture where it is integrated. As an example of such an interaction accounting and charging is often mentioned in relationship with QoS signaling protocols. Without an appropriate

integration of the two there is no good incentive for network

operators to deploy QoS signaling protocols. This interaction is subject of a framework and some aspects are discussed in [5].

1.2 Involved Network Parts

Independent of the threat scenarios described in Section 2 end-to-end signaling messages traverse different network parts, which demand different security mechanisms caused by the difference in trust relationships. The sub-parts are: access network part, intra and inter-domain part, and finally end-to-end communication. These parts are briefly described in this section and the threat scenarios of Section 2 can be assigned to the individual parts.

a) Access Network (or First-Peer) Communication

The term access network is fuzzy but in this context we refer to the communication between an end host and the first NSIS aware entity in the network to which this host is attached. Therefore threats are addressed where an NSIS Initiator (NI) transmits and receives signaling messages to some entity in the access network. 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 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 largest number of problems.

b) Intra-Domain Communication

After receiving a NSIS signaling message and verifying the request somewhere in the access network the signaling message traverses the network within the same administrative domain. Since the request has already been authenticated and authorized threats are different compared to those described in the previous section. To differentiate the end-node-to-access network interface with the intra-domain communication we assume that no user hosts are logically 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 Communication

The threat assumptions between the borders of different

administrative domains largely depends on how accounting is done. If one domain transmits forged QoS reservations 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), the fewer problems for key management arise.

d) End-to-End Communication

In our opinion end-to-end security for NSIS 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 NSIS signaling protocol for the purpose of charging is therefore assumed opaque to the NSIS protocol itself and appropriately protected as part of the AAA interaction. 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 issues.

1.3 Clarification

Some threat scenarios in this document use the term user instead of NSIS Initiator. This is mainly due to the fact that security protocols allow a differentiation between entities being hosts and users (based on the identities used). Since the NSIS Initiator as

used in [5] also allows to act on behalf of various entities including a network it is reasonable to distinguish between these identities.

The term access network is used for networks 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 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 AAA infrastructure (AAAL, AAAH, Broker, etc.) and trust relationships between the access network and the users home network. This trust relationship is usually based on some sort of business contract. The trust relationship between the

two networks is considered to be symmetric (network A trusts network B and vice versa) whereas the dynamically established trust relationship between the mobile node and the access network is often asymmetric. In today's network a mobile node has to trust the access network with regard to collection and processing of accounting data. 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 signaling messages.

2 Threat Scenarios

This section provides threat scenarios that are applicable to signaling protocols.

2.1 Lack of Authentication and 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 signaling message initiator with respect to the entity to which it has to authenticate. The man-in-the-middle adversary is able to modify signaling messages to mount DoS attacks. The signaling message initiator wrongly believes that it talks to the ôrealö network whereas it is actually attached to an adversary.
For this attack to be successful, pre-conditions have to hold which are described with the following two cases:
a) Missing Authentication

The first case addresses missing authentication between the neighboring peers: Without authentication a NI, NR or NF is unable to

detect an adversary. However in some cases protection available might be difficult to accomplish in a practical environment either because the other peer of the communication is unknown 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 security association. Sometimes network administrators refuse to consider security protection of intra-domain signaling messages. Such a configuration would then allow an adversary at a compromised node to cause security problems. Even if there was no intention that this compromised node actively participates in the signaling message exchange its interference cannot be prevented.

b) Unilateral Authentication

In case of only unilateral authentication the NI is not able to discover the man-in-the-middle adversary. Although authentication of signaling message should take place between each peer participating in the protocol operation special focus is given to the communication in the end host and the access network.

The two threats described above are a general problem of network access without appropriate authentication, not only for an NSIS signaling protocol. Obviously there is a strong need to correctly address them in a future NSIS protocol. The signaling protocols addressed by NSIS are different to other protocols where only two entities are involved. The impacts of a security breach likely reach beyond the directly involved entities (or even beyond a local network).

Finally it should be noted that the signaling protocol should be considered as a peer-to-peer protocol where the roles of initiator and responder can be reversed at any time. This leads to the conclusion that unilateral authentication is not very useful for such a protocol. However there might be a need to have some form of asymmetry in the authentication process whereby one entity uses a different authentication mechanism than the other one. As an example the combination of symmetric and asymmetric cryptography should be mentioned.

2.2 Missing Authorization

Authentication as described in Section 2.1 is a very important step for providing the foundation for authorization and accounting. Unlike some other protocols where authorization can be verified without huge difficulties NSIS protocols might experience some difficulties. First

there is the question what authorization means in the context of NSIS signaling and particularly for quality of service and middlebox communication. The possible range is broad and could range from pure monetary policies to traditional role-based access control policies. Second there is a question where this authorization data can be retrieved. Especially in a mobile environment this might be more complicated to securely exchange this information between different network domains. Finally there is an issue of representing authorization information if it has to be shared between a number of network domains.

Currently the above-mentioned issues have not been appropriately addressed and might cause obstacles for deployment.
In a discovery phase an additional issue of authorization was raised. Whenever a node wants to discover the next NSIS aware node then authentication might not be sufficient. In many cases the IP address or FQDN of a particular router in an unknown network does not add too much trust. An end host for example might want some assurance that this node belongs to a network with which some sort of business relationship (directly or indirectly) is available.

2.3 Missing Cost Control

This type of threat addresses a deployment problem of 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. In a traditional subscription-based

scenario users are registered with their home networks and use this trust relationship to dynamically establish other security associations. In these scenarios users do not learn the identity of the access network as part of a regular message exchange. The user is therefore only authenticated to the home network (and hopefully vice versa). The identity of the access network is possibly not revealed. When issuing a reservation request to an entity in the access 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 an end-to-end QoS reservation might not be transparent or unacceptable.

Today there is no protocol available which allows users to communicate cost limits, to request costs for network resources or to learn the currently accumulated costs for a particular reservation.

Especially in mobility environments where many networks might be contacted in a short period of time cost control is even more complicated.

Some proposals which try to merge mobility protocols with QoS signaling probe the access network (towards the cross-over router or the MAP) for the possibility making a QoS reservation (without actually making the reservation itself). Without a query mechanism a user cannot take reservation costs into account when choosing between different access networks. Hence the user might not be unable to refuse the more expensive service provider. To allow a user to choose different providers might be required not only because of the availability of different access technologies (either using a WLAN card to access the local network or to use UMTS/UTRAN based technology) and the different service quality offered but also for cost reasons.

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. Note that payment issues should be discussed independently of cost-control since other mechanisms are required to negotiate which involved party actually has to pay the costs (and how).

2.4 Eavesdropping and Traffic Analysis

This section covers two threats: The first 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 which are able to eavesdrop signaling messages but are unable to actively participate in the QoS signaling (i.e. passive adversary). 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 user's privacy preference. Especially QoS

signaling messages provide information that may be interesting for an adversary since the messages reveal user and/or application identities, policy information, information about the desired QoS reservation, etc. The information gathered by an adversary can be used to learn communication patterns of users requesting resources (QoS, firewall, NAT, etc.).

An adversary 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 but may also be applicable and countermeasures must be taken.

2.5 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). Without proper replay protection an adversary might be able to mount denial and/or theft of service attacks.

A more difficult attack that may cause problems even in case of replay protection requires the adversary to crash a NSIS aware node to loose state information (sequence numbers, security associations, etc.) and to be able to replay old 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. Returning an authorization token to the end host might allow an adversary to steal resources without proper protection of the token delivery or without proper 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].

2.6 Identity Spoofing

The following paragraph gives an example of an adversary using identity spoofing:

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.

If a signaling message is properly protected the adversary is unlike to succeed.

A non-traditional identity spoofing attack exploits flow classification (required for QoS and Midcom specific signaling

protocols). Some identifiers such as IP addresses, transport protocol identifiers, port numbers, flow labels [6, 7] and others are communicated in these protocols and represent an attractive target for an adversary. Modification of these flow identifiers cause quality of service reservations or policy rules at middleboxes to be either ineffective or beneficial for adversaries.

Additional concerns might occur if end hosts perform traffic marking (for example by using a DSCP). Whenever an ingress router uses only marked incoming data traffic for admission control procedures then various attacks are possible. These problems are known in the DiffServ community for a long time and documented in various DiffServ related documents. The IPSec protection of DiffServ Code Points is described in Section 6.2 of [11]. Related security issues (for example denial of service attacks) are described in Section 6.1 of the same document.

The following paragraph describes a possible threat caused by identity spoofing of transmitted data traffic. The spoofed identity is thereby the source IP addresses. Assume that accounting records are collected based on the source IP address and not on a SPI due to IPSec protection. After the network receives a properly protected reservation request, transmitted by the legitimate user Alice, Traffic Selectors are installed at the corresponding devices (for example edge router). These Traffic Selectors are used for flow identification and allow to match data traffic originated from a given source address to be assigned to a particular QoS reservation. The adversary Eve now spoofs the IP address of the Alice. Additionally AliceÆs host may be subject of a DoS attack by and by the adversary. If both nodes are located at the same link and use the same IP address then obviously a duplicate IP address will be detected. Assuming that only Eve is present at the link then she is able to receive and transmit data (for example RTP data traffic), which receives preferential QoS treatment based on the previous reservation. Depending on the installed Traffic Selector granularity Eve might have more possibilities to exploit the QoS reservation or a pin-holed firewall. 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. The same procedure is also applicable to a Middlebox communication protocol.

2.7 Adversary being able to inject/modify messages

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

An adversary may inject a signaling message requesting a large amount of resources (using a different user 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.

2.8 Missing Non-Repudiation

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

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 today's 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 it might impact protocol design.

2.9 Malicious NSIS Entity

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 verification, replay protection, authorization, etc.). Depending on the protocol functionality every NSIS aware router should be able to issue signaling messages. 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. In case of policy rule installation a rogue firewall can cause harm to other firewalls by

modifying the policy rules accordingly.

The chain-of-trust principle applied in the peer-to-peer security protection cannot provide proper protection. An adversary with full

access to the edge router is then also able to retrieve security associations to secure signaling messages. Note that even non-peer-to-peer security protection might not be able to fully prevent this problem.

Thus the edge router is a critical component that requires strong security protection. Strong security policy applied at edge routers does not imply that intra-domain routers do not need to cryptographically verify signaling messages. 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.

2.10 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 path discovery/path pinning and reservation (as for example used in a receiver-initiated reservation). For this example we assume that the node transmitting the path message is not charged for the path message itself and is able to issue a high number of reservation request (possibly in a distributed fashion). Charging is activated only after successful verification of the reservation request. The reservations are however never intended to be successful because of various reasons: the destination node cannot be reached; it is not responding 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.

2.11 Denial of Service with a bogus signaling request

With a resource reservation request received at a network element (for example by the first NSIS 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 infrastructure. Verification requires cryptographic computations, state maintenance, setting timers, transmitting messages and other processing actions. If an adversary is able to transmit a large number of reservation request 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 users. This assumes that verification is expensive (especially cryptographic computations).

2.12 DoS Attack at the Discovery Phase

Signaling information to a large number of entities along a data path requires some sort of discovery. This discovery process is vulnerable to a number of attacks since it is difficult to secure. An adversary

can use the discovery mechanisms to convince an entity to signal information to another entity which is not along the data path or to cause the discovery process to fail. In the first case the signaling protocol could be correctly continued with the problem that policy rules are installed at incorrect firewalls or QoS resource reservations take place at the wrong entities. For an end host this means that the protocol failed for unknown reasons.

2.13 Disclosing the networking structure

In some architectures there is a desire 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.). A requirement of not disclosing a network structure might conflict with another requirement to provide means for automatically discovering NSIS aware nodes and to provide diagnostic facilities.

2.14 Modification of Session State Information

An adversary might be able to modify an existing reservation which has already been established within the network as a result of a previous signaling message exchange.
Hence it might be necessary to provide assurance for a secure binding between an owner of the established session state and the session state information distributed at various entities along the data path. The state information created at nodes along the path created by signaling messages is the uniquely identified Session ID as described in [5]. Whenever a signaling message has to refer to existing state information (for a refresh, modify or delete operation) then the existing session identifier is used. Hence there is a requirement that it must not be possible for someone to use an existing session identifier to modify state information of someone else. An adversary might have learned a session identifier by

eavesdropping the signaling messages. 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.

To make processing even more difficult it must be mentioned that not only the initial signaling message originator is allowed to signal information during the lifetime of an established session. As part of the protocol any node along the path (and the path might change over time) could be involved in the signaling message exchange and it might be necessary to provide mobility support or to trigger a local repair procedure. Hence if only the initial signaling message originator is allowed to trigger signaling message exchange some protocol behavior will not be possible.

In case that this threat is not addressed an adversary can launch denial of service, theft of service, and various other attacks.

2.15 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 message signaling protocol level, at the level of each client layer protocol (QoS, Midcom, etc.) or at the transport level protocol. An adversary might cause unexpected protocol behavior or produce denial of service attacks. Especially the discovery protocol shows vulnerabilities with regard to this threat. In case that no separate discovery protocol is used by addressing signaling messages to end hosts only (with a Router Alert Option to intercept message as NSIS aware nodes) then an error message might be used to indicate a path change. Such a design is a combination of a discovery protocol together with a signaling message exchange protocol.

3 Security Considerations

This entire memo discusses security issues in the context of NSIS. Some additional threats are applicable for a framework where an NSIS protocol is used. Some other relevant threats especially for end hosts to access network communication described in [2].

4 Open Issues

A future version of this draft will experience a minor restructuring to add deployment threats, to separation between attacks during security association setup and attacks which aim to attack the signaling messages itself, middlebox communication specific threats and a discussion of threats applicable to the transport level vs. the

application level (according to a 2-level-architecture).

5 References

[1] Brunner, M., "Requirements for QoS Signaling Protocols", <draft-ietf-nsis-req-04.txt>, (work in progress), August, 2002.

[2] Kempf, J., Nordmark, E.: ôThreat Analysis for IPv6 Public Multi-Access Linksö, <draft-kempf-ipng-netaccess-threats-02.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-04.txt>, (work in progress), October, 2002.

[4] Hamer, L-N., Gage, B., Shieh, H.: ôFramework for session set-up with media authorizationö, <draft-ietf-rap-session-auth-04.txt>, (work in progress), June, 2002.

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

[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), September, 2002.

[8] Fu, S., Kappler, C., Tschofenig, H.: "Analysis on RSVP Regarding Multicast", <draft-fu-rsvp-multicast-analysis-01.txt>, (work in progress), October, 2002.

[9] Tschofenig, H.: "RSVP Security Properties", <draft-tschofenig-rsvp-sec-properties-01.txt>, (work in progress), October, 2002.

[10] de Meer, H., Feher, G., Blefari-Melazzi, N., Tschofenig, H., Karagiannis, G., Partain, D., Rexhepi, V., Westberg, L.: "Analysis of Existing QoS Solutions", <draft-demeer-nsis-analysis-03.txt>, (work in progress), October, 2002.

[11] Terzis, A., Braden, B., Vincent, S., Zhang, L.: "RSVP Diagnostic Messages", RFC 2745, January, 2000.

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@siemens.com