Internet Draft
Expires: January 2007

Hormuzd Khosravi, Intel
Paul Sangster, Symantec

Working Group: NEA

July 2006

# Requirements for Network Endpoint Assessment (NEA)
# draft-khosravi-nea-requirements-01.txt

## Status of this Memo



## Copyright Notice



## Conventions used in this document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC-2119].

## Abstract

This document defines the interface (protocol) requirements between the components of the NEA (Network Endpoint Assessment) conceptual architecture. NEA provides owners of networks (e.g. an enterprise

offering remote access) a mechanism to learn the operational state or posture of a system requesting network access and then apply this knowledge to the network admission decision. In this case, operational posture refers to information about the configuration and use of hardware and software capabilities available or running on the system. This information is frequently useful for detecting systems that are lacking (or have out of date) security protective mechanisms (e.g. anti-virus, firewall.)

In order to provide context for the requirements, a conceptual architecture and terminology is introduced. This architecture is provided for informational purposes but is based on the models used by NAC[9], NAP[10] and TNC[8].

## Authors

The participants in the NEA Requirements Team who were instrumental in the creation of this requirements draft are:

Kevin_Amorin, Diana Arroyo, Uri Blumenthal, Steve Hanna, Thomas Hardjono, Hormuzd Khosravi, Ravi Sahita, Mauricio Sanchez, Paul Sangster, Jeff Six, Joseph Tardo, Susan Thompson, John Vollbrecht, Hao Zhou

1. Introduction.....2
2. Definitions.....3
3. Architecture and Components.....4
4. Common Requirements Across Architecture.....5
5. Protocol Requirements.....6
5.1 .Posture Attribute (PA) Protocol Requirements.....6
5.2 .Posture Broker (PB) Protocol Requirements.....7
5.3 .Posture Transport (PT) Protocol

Requirements.....8
5.3
.1
.EAP Usage Within
PT.....9
6. Security Analysis/Requirements.....10
7. Operational Considerations.....12
8. Security Considerations.....13
8.1
.Scope
and Over
lap.....13
8.2.Relevant
Classes
of
At
tack.....14
8.2
.1
.Man-
in-the-Middle
(MITM).....14
8.2
.2
.Message Modification.....14
8.2.3
.Message Replay or
Theft.....15
9. References.....15
9.1
. Normat
ive
References.....15
9.2. Informat
ive
References.....16
Authors' Addresses & Acknowledgments.....16

## 1. Introduction

Today, most network providers can leverage existing standards-based technologies to restrict access to the network based upon the requesting system's user or host-based identity, source IP address or physical access point. However these approaches still leave the network prone to malware-based attack, when an authorized but infected system is admitted and the malware is able to spread throughout the internal network.

As a result, network operators need the ability to preemptively detect systems that are prone or already contain malware potentially dangerous to the network. If a system is determined to be prone to attack by lacking proper defensive mechanisms such as the absence of up to date firewall and anti-virus software, there should be a way to safely repair (remediate) the system so that it can be subsequently trusted to join and operate on the network.

The Network Endpoint Assessment (NEA) system is a complementary technology to existing authentication and authorization approaches allowing the network to have visibility into the contents of the system (security posture) requesting access so that its risk profile can be factored into the admission decision. NEA typically involves the use of trusted agents running on the requesting machine which observe and report on the posture of the system to network infrastructure. The infrastructure has equivalent components which are capable of evaluating the posture information and feeding the result to an appropriate network admission decision maker. Finally the admission decision is provisioned to the enforcement mechanisms on the network and/or system requesting access. The decision might allow for no access, limited access (possibly to allow for remediation), or full access to the network.

Architectures, similar to NEA, have been defined in the industry (e.g. TNC, NAP, NAC) to assess the software or hardware configuration of endpoint devices for the purposes of monitoring or enforcing compliance of endpoints to an organization's policy on access to the network. These architectures are not interoperable since most of the technologies used to implement the architecture are not standards.

The NEA working group is working on defining standard protocols so as to enable interoperability between devices from different vendors allowing network owners to deploy truly heterogeneous solutions. This document describes the requirements for NEA candidate technologies and protocols.

## 2. Definitions

Component Software, hardware or firmware entity performing a particular logical function within the NEA conceptual architecture.

For the purposes of assessment, a component may be a particular vendor product (e.g. Symantec Anti-Virus), class of application (e.g. Firewall), or be more general to represent groupings of software services (e.g. Operating System kernel.)

Dialog Sequence of request/response messages exchanged over one or more sessions.

Message Self contained unit of communication between components. For example, a PA message might carry a set of attributes from a Posture Collector to a Validator.

Session Common PB transport connection capable of carrying one or more messages from multiple subscribed Posture Collectors and Validators.

Please refer to [3] for the NEA terminology.

## 3. Architecture and Components

The major components of NEA architecture are shown in Figure 1. The PV and NAE protocols are identified for completeness but are not the focus of the initial phase of NEA work items.

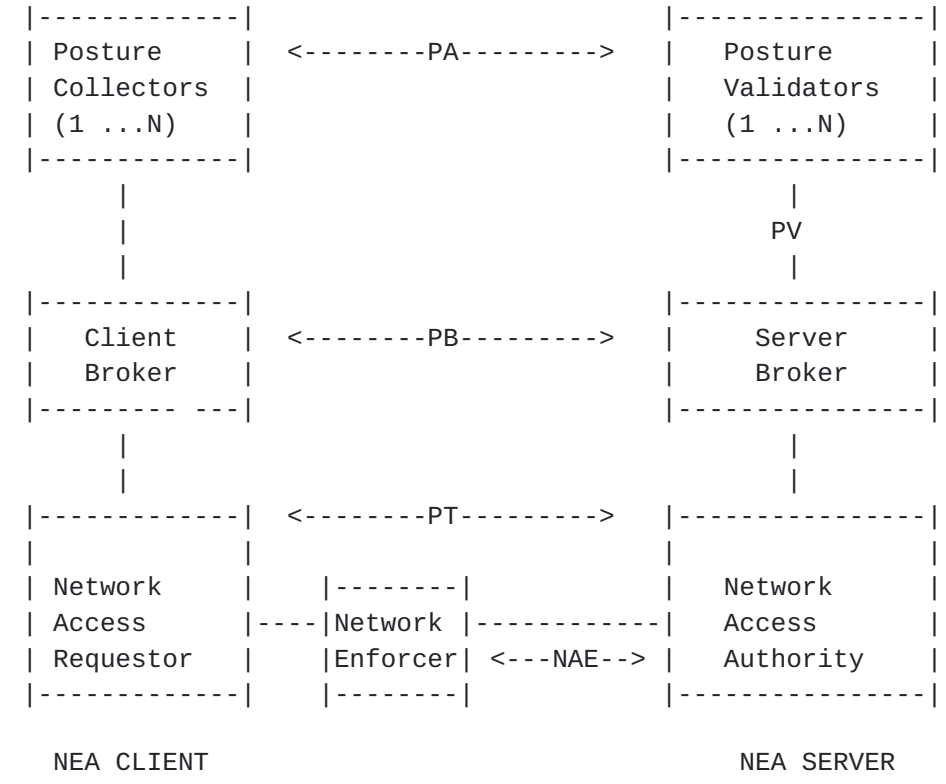


Figure 1: NEA Components and Protocols

## 4. Common Requirements Across Architecture

The following are the common requirements that apply to the PA, PB and PT protocols in NEA conceptual architecture:

1. NEA protocols MUST be capable of performing a multiple message dialog between the client (agent) and server. This enables the server to request additional information or updates to the posture data already reported. The updates allow for detection of recent changes in the client state (e.g. possibly due to a remediation.)

2. NEA protocols MUST allow the NEA server to initiate requests for posture information prior to network access and at any time after the client has established an identity on the network (e.g. IP address.) This enables the NEA server to evaluate posture prior to allowing access and to periodically re-validate systems already admitted to the network to assure they are still in compliance with the current policies.

3. NEA protocols MUST provide a way for the NEA client to initiate a posture re-evaluation request as needed. This allows the client to proactively request a posture re-evaluation by the NEA Server after detection of a potentially suspicious event.

4. NEA protocols MUST provide protection against active and passive attacks by intermediaries (e.g. man-in-the-middle.) Such protection might come from a strong (e.g. cryptographic) binding between the authenticated identity of the requesting system and the reported posture information. This protection MUST prevent replay based attacks (preventing a malicious machine from later replaying a healthy posture report.)

5. The PA and PB protocols defined by NEA MUST be agnostic of the transport i.e. PT protocol. For example, the PB protocol must provide a transport independent interface allowing the PA protocol to operate without change across a variety of network protocol environments (e.g. EAP/802.1X, PANA, and IKE/IPsec.)

6. The selection process for NEA protocols MUST evaluate and prefer the reuse of existing open standards that meet the requirements before defining new ones. The goal of NEA is not to create additional alternative protocols where acceptable solutions already exist.

7. NEA protocols MUST be highly scalable allowing for many Posture Collectors on large deployments of NEA Clients to be assessed by numerous Posture Validators residing on multiple NEA Servers. For example, the protocols need to be capable of naming large numbers of types of collectors, validators, and components.

# 5. Protocol Requirements

## 5.1. Posture Attribute (PA) Protocol Requirements

The PA protocol defines the transport and data model to carry posture and validation information between a particular Posture Collector associated with a NEA client and a Posture Validator associated with a NEA Server. The Posture Attribute protocol carries collections of core attributes and vendor defined attributes. The PA protocol will be carried inside the Posture Broker (PB) protocol. The following requirements define the desired properties that form the basis for the working group s comparison and evaluation of candidate PA protocols. The requirements do not require that deployers use these properties merely that the candidate protocol be capable of offering the property should it be needed.

1. The PA protocol MUST support transport of the required (core) attributes defined in the data model to report information determined by a Posture Collector. Examples of core attributes include Vendor id, Application version, and Operational status.

2. The PA protocol MUST support the transport of vendor defined attributes enabling communication of a richer, potentially vendor specific set of attributes describing the requested component.

3. The PA protocol MUST enable the Posture Validator to request posture information about particular components on the NEA Client system. The posture information may be represented as one or more attributes (core and/or vendor specific) that describe the operational properties of the component.

4. The PA protocol MUST allow for the Posture Validator to request posture information on more then one occasion using an existing or if unavailable on a new session. This enables the Posture Validator to re-assess the posture of a particular component (in case it has changed) or to request information about additional components (possibly due to something learned from an earlier request.)

5. The PA protocol MUST be capable of returning the Posture Validator s results and any necessary remediation instructions. This allows the Posture Collector to learn the specific reason for a failed assessment to aid in remediation and notification of the system owner.

6. The selection process for the PA protocol MUST evaluate and prefer the reuse of existing open standards that are applicable to the transport and representation of an extensible set of attributes.

In particular, extensible structured data formats such as XML should be considered.

7. The PA protocol SHOULD support expression of core attributes to describe remediation state of components for example, last update time, remediation server used. These attributes are used after remediation so that a Posture Validator can synchronize with a Posture Collector and continue remediation.

8. The PA protocol MUST support authentication, integrity and confidentiality of attributes, results and remediation instructions sent between a Posture Collector and Validator. This enables end to end security across an NEA deployment that might involve the traversal of several systems. Deployers of Posture Collectors and Posture Validators should use at least authentication and integrity protection for their messages, and may also employ confidentiality protection if necessary for their environment.

9. The PA protocol SHOULD optimize transport of messages and minimize Posture Broker protocol round trips. To achieve this, the PA protocol should support configuration/negotiation of the maximum size and timeout period for interaction of a Posture Collector with a Posture Validator.

## 5.2.Posture Broker (PB) Protocol Requirements

The PB protocol supports multiplexing of Posture Attribute messages (based on PA protocol) from multiple Posture Collectors associated with a NEA Client and de-multiplexing these messages to multiple Posture Validators associated with a NEA Server. The PB protocol transports the global decision made by the Server Broker, taking into account the results of the Posture Validators involved in the assessment, to the Client Broker.
The PB protocol also transports the aggregated remediation instructions from one or more Posture Validators.

1. The PB protocol MUST be capable of carrying the global decision and, if appropriate, the global remediation instructions from the Server Broker to the Client Broker.

2. The PB protocol MUST contain information used by the Brokers to route (deliver) messages between particular types of Posture Collectors and Posture Validators. Such message routing information should enable dynamically (de)registered Posture Collectors and Validators to receive appropriate messages. For example, a dynamically registered Anti-Virus Posture Validator should be able to subscribe to receive messages from its respective Anti-Virus Posture Collector on NEA Clients.

3. The PB protocol MUST support a message dialog to occur between one or more Posture Collectors and Posture Validators. This allows each party to send multiple messages before the dialog is complete.

4. The PB protocol MUST support authentication, integrity and confidentiality of the PA messages, broker global decision and remediation instructions sent between an NEA Client and Server. This provides security protection for the aggregated set of PA messages exchanged and the result between the NEA Client and Server. Such protection is orthogonal to PA protections (which are end to end) and allow for simpler Posture Collector and Validators to be implemented and consolidation of cryptographic operations possibly improving scalability and manageability.

5. The PB protocol SHOULD support grouping of attributes to optimize transport of messages and minimize round trips.

### 5.3.Posture Transport (PT) Protocol Requirements

The PT is the transport protocol between the Network Access Requestor (NAR) in the NEA Client and the Network Access Authority (NAA) within the NEA Server present on the network owner s infrastructure. PT is responsible for providing a protected transport (frequently using a tunnel) for the PB protocol. The PT protocol may in turn be transported by a lower layer protocol such as: 802.1x, RADIUS, TLS, IKE/IPsec or TCP,UDP/IP. This section defines the requirements which candidate PT protocols must be capable of supporting. The deployer s policy will dictate how these apply to a particular environment.

1. The PT protocol SHOULD incur low overhead to accommodate for use on low bandwidth links.

2. The PT protocol SHOULD be capable of supporting a half duplex communication environment.

3. The PT protocol MUST NOT attempt to interpret the contents of the PB messages being transported, i.e. the data it is carrying must be opaque to it.

4. The PT protocol MUST be capable of protecting the integrity and confidentiality of the PB messages being transported between the NAR and NAA.

5. The PT protocol MUST provide reliable delivery of PB messages. This includes the ability to perform fragmentation, detect duplicates, and reorder data, if necessary.

6. The PT protocol MUST be capable of supporting mutual authentication of the communicating parties. This MAY occur by initially authenticating the NEA Server and leveraging byproducts (e.g. keys) associated with this authentication to construct a confidential channel where the NEA Client can authenticate.

7. The PT protocol MUST be able to establish a restricted session between the NAR and the NAA prior to the NAR granting general network access.

8. The PT protocol MUST allow the NAR or NAA to initiate the establishment of a restricted session for use by NEA when both parties have necessary network addresses established.

### 5.3.1. EAP Usage Within PT

When EAP is being used within PT, the PT protocol can be split into two groups: Posture Transport Tunnel (PTT) and Posture Transport Carrier (PTC). PTT is the EAP method used between the NAR and NAA (e.g. EAP-FAST, PEAP, EAP-TTLS), and PTC is the transport protocol carrying EAP. When Network Enforcer (NE) is a separate entity from Network Access Authority, PTC is further broken into two protocols, one between NAR and NE (named NRE) and one between NE and NAA (named NAE). Examples of NRE are EAPOL, PPP, IPSec etc. Examples of NAE are RADIUS, Diameter, etc. This section defines the requirements which candidate PTT and PTC protocols must be capable of supporting, in addition to those outlined in Section 4 Common Requirements Across Architecture. The deployer's policy will dictate how these apply to a particular environment.

PTT EAP Method Requirements:

1. The PTT EAP Method SHOULD be standardized from one or more existing methods if possible or modifying existing methods if where necessary to make them appropriate to be standardized. The use of existing standard EAP method for PTT SHOULD be giving preference over creating a new EAP method.

2. The PTT EAP Method MUST NOT attempt to interpret the contents of the PB messages being transported, i.e. the data it is carrying must be opaque to it. This is mapped to PT Requirement 3.

3. The PTT EAP Method MUST support integrity and confidentiality to protect key material and data. This is mapped to PT Requirement 4.

4. The PTT EAP Method MUST support fragmentation of payloads larger then the minimum EAP MTU, and reassembly. This is mapped to PT Requirement 5.

5. The PTT EAP Method MUST have support for mutual authentication. This is mapped to PT Requirement 6.

6. The PTT EAP Method MUST have support and have protection for PB protocol in the form of "inner EAP methods" or TLV/AVP. It SHOULD support transporting of arbitrarily large posture data or fragmentation of the data.

7. The PTT EAP Method MUST be lower layer agnostic and have support for multiple carrier protocols (RADIUS, Diameter, EAPOL, etc.).

8. The PTT EAP Method MUST be able to dynamically generate key material.

9. The PTT EAP Method MUST support transport PB with or without identity authentication, before or after identity authentication.

10. The PTT EAP Method MUST support multiple message dialogs of PB protocol.

11. The PTT EAP Method SHOULD use open (publicly available and proven) algorithms in its encryption and key creation.

12. The PTT EAP Method SHOULD be able to perform key negotiation, and cipher suite negotiation.

PTC Requirements

PTC MUST meet the following requirements, in addition to the requirements described in RFC 3748 Section 3 Lower Layer Behavior.

1. The PTC protocol MUST be able to establish an assessment session between the NAR and the NAA prior to the NAR being granted general network access. This is mapped to PT Requirement 7.

2. The PTC protocol MUST allow the NAR or NAA to trigger reassessment when there are changes in client posture and/or server policy after network access is granted. This is mapped to PT Requirement 8.

## 6. Security Analysis/Requirements

There are several entities that comprise the described NEA conceptual architecture. From security viewpoint, their relations and communications should adhere to the following requirements.

End-points must be able to authenticate their peers (i.e. Posture Collector and Posture Validator), for without that no meaningful posture information exchange is possible.

1. PA Protocol

- Posture Validator MUST be able to ascertain that the traffic (posture) it received is "fresh". This freshness prevents a third party from replaying the posture information produced by an earlier Posture Collector use without detection.

- It may be necessary (especially in case of multiple exchanges between Posture Collector and Posture Validator) that Posture Collector "recognizes" and trusts the given Posture Validator. This ensures that Posture Collector is doing work on behalf of authentic Posture Validator.

2. PB Protocol

- Communications between Client Broker and Server Broker MAY need to be protected at least from active attacker (integrity, confidentiality, timeliness). Integrity and timeliness are of the utmost importance, to prevent third parties (any parties - including Network Enforcer) from interfering with posture validation and affecting PDP decisions. Confidentiality may be useful here, for example to prevent attackers from determining which host would be the most vulnerable target based on its posture information. However there is privacy concern that the host should be able to "see" what potentially privacy sensitive information about it is being sent out. This concern may prevent encryption from being used or force a pre-screening of the posture information against a privacy policy before allowing it to be sent over the network.

3. PT Protocol

- This communication channel MUST be protected: endpoint mutual authentication with subsequent secure pipe establishment. Otherwise third parties could launch a variety of attacks.

4. Communications between Posture Collector(s) and Client Broker MAY need protection, especially if those are different software entities. It is important that a Client Broker be allowed to communicate with only the authorized Posture Collectors because of the trust issue. Denial of Service is the most obvious threat here. Forging a posture should not be feasible because of PA protocol.

5. Communication between Client Broker and Network Access Requestor MAY need protection.

6. Communication between Server Broker and Network Access Authority MAY be protected.

## 7. Operational Considerations

The NEA technology intends to address a major issue for owners of networks by extending their existing ability to limit admission to the network by inspection of the security posture of the system. In order to offer a solution to this issue, NEA needs to provide a scalable solution addressing a vast majority of the systems deployed while remaining manageable. This introduces several issues which should be considered during the definition of the protocols, interfaces, architecture and their policies.

1. Some network devices (e.g. printers, legacy systems) will not have support for NEA agents present. In this situation, the NEA server must be able to detect that the system requesting access is incapable of responding to NEA protocols and thus will not be able to report its security posture. The NEA architecture should allow for this event to be detected and reported to other components which might be able to evaluate risk via other mechanisms (e.g. using scanning techniques) and report back a suggested action.

2. Admission policy should be capable of being combined with authentication policy so differentiated posture evaluation is possible based on the identity and other factors about the requesting system. For example, in many cases customers may wish to allow certain individuals (e.g. executives) to always be allowed access to the network even if NEA detects a problem. Similarly, different posture checking profiles might be applied depending on the requesting system or user s identity.

3. Due to the potentially large number of systems offering and/or evaluating posture information and the quantity of enforcement devices, this presents a distributed policy issue for NEA deployers. The NEA components should be manageable using data model definitions associated within existing management protocol environments (e.g. SNMP, CIM.)

4. Because the NEA infrastructure is involved in making decisions about every system s request to join and remain on the network, NEA deployments should have mechanisms that protect it from direct attack or operational situations where it might be unavailable. Highly available, distributed deployment architectures should help minimize downtown and avoid single point of failure scenarios. However NEA solutions may need to offer deployers some policy-driven flexibility in how the NEA components respond when faced with an unavailable NEA Server component.

# 8. Security Considerations

This document defines the requirements for the interfaces (protocols) for a security mechanism assessment and enforcement scheme. As such, it does not define a specific solution or set of technologies, so this section will highlight security issues that may apply to NEA in general or to particular aspects of the eventual technical architecture.

## 8.1. Scope and Overlap

Inherent in the requirements is a desire for NEA candidate protocols throughout the architecture to accommodate the use of strong security mechanisms as dictated by the deployer. In some cases, these mechanisms may appear to provide overlapping protections. The overlaps may be desired by deployer to offer a defense in depth approach; however because of the layering of the protocols each mechanism offers slightly different protection benefits and levels of granularity.

For example, a deployer may wish to encrypt traffic at the PT layer to protect against some forms of traffic analysis or interception by an eavesdropper. Additionally, the deployer may also selectively encrypt a Posture Collector's set of reported attributes at the PA layer to allow the peer Posture Verifier to achieve end to end confidentiality. In particular, this might be desired when the NEA Server side decision point spans several systems so the NAA is on a different system from the Verifier.

In general, the NEA architecture's protocols are intending to provide to the Posture Collector the ability to safely send its measurement attributes across an untrustworthy network to a peer Posture Validator and receive protected requests/responses. The architecture is not intending to provide local integrity protection for the proper operation of the Posture Collector itself. For example, NEA technologies do not claim to prevent a carefully crafted piece of malware (e.g. rootkit) from tricking the Posture Collector into inaccurately reporting the state of the system so it can remain undetected. Such integrity protection of the Collector and other aspects of the system might be offered by orthogonal security mechanisms leveraging security hardware and/or protected trusted software.

Different use cases and environments for the NEA technologies will likely influence the selection of the strength and security mechanisms employed during an assessment. The goal of the NEA

requirements is to encourage the selection of technologies and protocols that are capable of enforcing the necessary protections for a wide variety of assessment use cases.

### 8.2. Relevant Classes of Attack

A variety of attacks are possible against current assessment technologies. This section does not include a full threat analysis, but wishes to highlight a few attacks which influenced the requirement definition and should be considered by deployers selecting use of protective mechanisms within the conceptual architecture.

The following types of attacks are possible against each of the network protocols defined in the conceptual architecture and thus should be considered by deployers.

#### 8.2.1. Man-in-the-Middle (MITM)

MITM attacks against a network protocol exist when a 3rd party can sit between two legitimate communicating parties without detection. For example, a malware infested machine might wish to join the network using measurements collected by a clean system by inserting itself into and proxying an assessment message exchange. The impact of the damage caused by the MITM can be limited or prevented by selection of appropriate protective mechanisms.

The requirement for PT to be capable of supporting bi-directional authentication prevents the attacker from inserting themselves as an active participant (proxy) within the communications without detection (assuming attacker lacks credentials convincing either party it is legitimate.) Re-usable credentials should not be exposed on the network to assure the MITM doesn't have a way to impersonate either party.

However the MITM might still act as a message relay between the parties and change, eavesdrop, or steal and replay the communications. These forms of attack require additional protections discussed below.

#### 8.2.2. Message Modification

Without message protection, an attacker capable of interception of an assessment message would be capable of modifying the contents and causing an incorrect action to occur. For example, the attacker might change the measurement attributes to always reflect incorrect values and thus prevent a system from joining the network. Unless the NEA Server could detect this change, the attacker could prevent network admission to large numbers of clean systems. Conversely, the

attacker could allow malware infested machine to be admitted by changing the attributes.

In order to protect against such attacks, the PT includes a requirement for strong integrity protection (e.g. including a protected hash of the message) so this change will be detected. PA includes a similar requirement to enable end to end integrity protection of the message.

It is important that integrity protection schemes leverage secret information (not known by the attacker) that are bound to the transaction such as an encrypted message hash or HMAC [REF] linked to the authentication. Message hash keys from prior transactions possibly involving other systems must not be re-usable without detection.

### 8.2.3. Message Replay or Theft

A passive attacker might listen to the network recording messages from a healthy client for later re-use to the same NEA Server or just to build an inventory of software running on other systems. The NEA Server needs to be capable of detecting the replay or the architecture must assure that the eavesdropper can not obtain the attribute values in the first place.

The protection of the PT, PB or PA messages using encryption prevents the passive listener from learning the exchanged attribute values for theft or replay. By linking the encrypted transaction to the authentication event and leveraging a per-transaction freshness exchange, this prevents a replay of the encrypted transaction.

As discussed, there are a variety of protective mechanisms included in the requirements for candidate NEA protocols. Different use cases and environments may cause deployers to decide not to use some of these mechanisms; however this should be done with an understanding that the architecture may become vulnerable to some classes of attack. As always a balance of risk vs. performance, usability, manageability and other factors should be taken into account.

## 9. References

### 9.1. Normative References

1. S. Bradner, "The Internet Standards Process -Revision 3", RFC 2026, October 1996.

2. S. Bradner, "Keywords for use in RFCs to Indicate Requirement Levels", RFC2119 (BCP), IETF, March 1997.

3. S. Hanna, et. al., "Network Endpoint Assessment (NEA) Problem Statement", draft-thomson-nea-problem-statement-01.txt, March 2006.

4. Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J., and H. Levkowetz, "Extensible Authentication Protocol (EAP)", RFC 3748, June 2004.

5. Rigney, C., Willens, S., Rubens, A., and W. Simpson, "Remote Authentication Dial In User Service (RADIUS)", RFC 2865, June 2000.

6. T. Dierks, E. Rescorla, The Transport Layer Security (TLS) Protocol Version 1.1 , RFC 4346, April 2006.

7. S. Kent, R. Atkinson, Security Architecture for the Internet Protocol , RFC 2401, November 1998. (IPSec)

## 9.2.Informative References

8. TCG Trusted Network Connect (TNC) Architecture for Interoperability , https://www.trustedcomputinggroup.org/specs/TNC/TNC_Architecture_v1_1_r2.pdf, May 2006.

9. Cisco Network Admission Control (NAC), http://www.cisco.com/go/nac

10. Microsoft Network Access Protection (NAP), http://www.microsoft.com/technet/itsolutions/network/nap/default.mspx

11. IEEE, "Local and Metropolitan Area Networks: Port-based Network Access Control", 2004. (802.1x)

12. Forsberg, D., "Protocol for Carrying Authentication for Network Access (PANA)", draft-ietf-pana-pana-11 (work in progress), March 2006.

## Authors' Addresses & Acknowledgments

Hormuzd Khosravi (co-editor)
Intel
2111 NE 25th Avenue
Hillsboro, OR 97124 USA
Phone: +1 503 264 0334

Email: hormuzd.m.khosravi@intel.com

Paul Sangster (co-editor)
Symantec Corporation
6825 Citrine Dr
Carlsbad, CA 92009 USA
Email: paul_sangster@symantec.com

Kevin Amorin
Harvard University
79 JFK St.
Cambridge, MA 02138
Phone: +1 617-384-6699
Email: Kevin_Amorin@Harvard.edu

Diana Arroyo
IBM
11501 Burnet Road
Austin, Tx 78758
Phone: +1 512-838-0088
Email: darroyo@us.ibm.com

Uri Blumenthal
Intel Corporation
1515 Route 10,
Parsippany, NJ 07054
Phone: +1 973-967-6446
Email: uri.blumenthal@intel.com

Steve Hanna
Juniper Networks, Inc.
35 Forest Ridge Road
Concord, MA 01742
Phone: +1 978-371-3980
Email: shanna@juniper.net

Thomas Hardjono
SignaCert, Inc.
707 SW Washington St./Suite 700,
Portland, OR 97205
Phone: +1 503-227-2207
Email: thardjono@signacert.com

Ravi Sahita
Intel Corporation
2111 NE 25th Ave
Hillsboro OR 97124
Email: Ravi.sahita@intel.com

Mauricio Sanchez
Email: mauricio.sanchez@hp.com

Jeff Six
Email: jeffsix@thematrix.ncsc.mil

Joseph Tardo
Nevis Networks
500 N. Bernardo Ave.
Mountain View, CA 94043
Email: joseph.tardo@nevisnetworks.com

Susan Thomson
Cisco Systems
499 Thornall Street, 8th floor
Edison, NJ 08837
U.S.A
Email: sethomso@cisco.com

John Vollbrecht
9682 Alice Hill Drive
Dexter, Mi. 48130
Email: jrv@merit.edu

Hao Zhou
Cisco Systems
4125 Highlander Parkway
Richfield, OH 44286
U.S.A.
Email: hzhou@cisco.com