Network Endpoint Assessment (NEA) Problem Statement

draft-thomson-nea-problem-statement-01.txt

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with Section 6 of BCP 79.

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.

This Internet-Draft will expire on September 5, 2006.

Copyright Notice

Copyright (C) The Internet Society (2006).

Abstract

Architectures have been implemented in the industry 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 fully interoperable since some of the protocols used to
implement the architecture are not standards.

This document describes the problem these architectures are intending to address, defines common terminology and concepts, and identifies interfaces that are candidates for standardization.

Requirements Language

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 [RFC2119].
Table of Contents

1. Introduction ......................................................... 4
2. Terminology ......................................................... 4
3. Problem Statement .................................................... 5
4. Goals ............................................................... 6
5. Deployment Scenarios .................................................. 7
   5.1. Wired LAN access .................................................. 7
   5.2. Wireless LAN Access ............................................... 7
   5.3. Remote access VPN ............................................... 8
   5.4. Gateway Access .................................................. 8
6. Components and Interfaces ............................................. 8
   6.1. Mapping to existing architectures .................................. 9
   6.2. Components .................................................... 10
       6.2.1. NEA Client .................................................. 10
       6.2.2. Network enforcer ............................................ 11
       6.2.3. NEA server .................................................. 12
   6.3. Interfaces ..................................................... 13
       6.3.1. Posture Attribute interface (IF-PA) ...................... 13
       6.3.2. Posture Broker Interface (IF-PB) ...................... 13
       6.3.3. Posture Transport Interface (IF-PT) .................... 13
       6.3.4. Network Access Enforcement Interface (IF-NAE) ........ 13
       6.3.5. Posture Validation Interface (IF-PV) ................. 14
7. Scope of Standardization .............................................. 14
8. IANA Considerations .................................................. 15
9. Security Considerations .............................................. 15
   9.1. Secure channel between the Client Broker and Server Broker .......... 16
   9.2. Authorization for Plug-in/Broker interaction ...................... 16
   9.3. Self-Integrity of the NEA Client and NEA Server .................. 16
   9.4. Protection of parameters exchanged across Interfaces ............. 16
   9.5. Identity authentication of communicating end-points .............. 17
10. Acknowledgements .................................................. 17
11. References ....................................................... 17
   11.1. Normative References .......................................... 17
   11.2. Informative References ........................................ 18
Authors’ Addresses .................................................... 19
Intellectual Property and Copyright Statements ......................... 20
1. Introduction

Architectures have been implemented 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 fully interoperable since some of the protocols used to implement the architecture are not standards.

This document describes the problem these architectures are intending to address, defines common terminology and concepts, and identifies interfaces that are candidates for standardization.

Note that this document is not intended to define a new architecture or framework for network endpoint assessment. There are already several existing architectures for this purpose. The network endpoint assessment effort aims only to identify common interfaces that are used in these architectures, and define standard protocols that can be used by the existing architectures to reduce duplication and achieve interoperability.

2. Terminology

Endpoint: An endpoint is a host connected to the network. This broad definition includes (but is not limited to) desktop or laptop computers, servers, phones, printers.

Posture: Posture refers to the hardware or software configuration of an endpoint as it pertains to an organization’s security policy. Posture may include knowledge about the types of hardware and software installed and their configurations, e.g. OS name and version, application patch levels, and anti-virus signature file version.

NEA client: The NEA client is a set of software components on the endpoint that request access to the network. The NEA client comprises three logical components: Posture collector, Client broker and Network access requestor.

Posture collector: A Posture collector is the component of the NEA client that is responsible for collecting and maintaining posture information about the endpoint device. There may be multiple NEA Posture collectors on an endpoint device each targeted at a particular security application from a particular vendor.

Client broker: A Client broker is the component of the NEA client that aggregates posture information from multiple Posture collectors.
Network access requestor: The Network access requestor is the component of the NEA client responsible for requesting access to the network.

Network enforcer: The Network enforcer is a network component that controls endpoint access to the upstream network. It enforces network authorization decisions from the network access authority.

NEA server: The NEA server is a server that evaluates the posture of an endpoint device and provides network authorization decisions. The NEA server comprises three logical components: Posture validator, Server broker and Network access authority.

Posture validator: A Posture validator is the logical component of the NEA server that assesses posture information from a Posture collector and determines the result of the assessment. There may be multiple Posture validators each targeted at a particular security application from a particular vendor.

Server broker: A Server broker is the component of the NEA server that aggregates posture information from multiple posture servers.

Network access authority: The Network access authority is the component of the NEA server that authorizes endpoints based on a number of criteria including the identity of an endpoint machine and/or user as well as the results of posture assessment.

3. Problem Statement

Network endpoint assessment (NEA) architectures are systems that enable the network to learn the posture of an endpoint device, and optionally use that information in addition to machine or user authentication to influence a network admission decision. Endpoint posture may include information about the operating system as well as information about security applications running on the endpoint such as anti-virus software, personal firewalls and host intrusion protection systems.

NEA technology may be used for several purposes. One purpose is to monitor or enforce compliance of endpoints to the organization’s security policy. Organizations often require endpoints that are vulnerable to attack through viruses, worms and other exploits to run an IT-specified OS configuration and have certain security applications enabled, e.g. anti-virus software, host intrusion protection systems, personal firewalls, and patch management software. Without NEA technology, ensuring compliance of endpoints to corporate policy is a time-consuming and difficult task. Not all
endpoints are managed by a corporation’s IT organization, e.g. lab assets, guest machines. Even for assets that are managed, they may not receive updates in a timely fashion because they are not permanently attached to the corporate network, e.g. laptops. With NEA technology, the network is able to assess an endpoint when it accesses the network and while connected, providing an opportunity to monitor compliance of all endpoints using the network as well as providing the opportunity to improve endpoint compliance. The decision for how to handle non-compliant endpoints is up to the network administrator. Remediation instructions or warnings may be sent to the endpoint. Also, network access may be restricted to protect the endpoint from infection and to protect the network in case the endpoint is already infected.

Another use of NEA technology may be to supplement information in inventory databases. In organizations that attempt to keep track of their assets, inventory databases tend to be incomplete and out-of-date. NEA technology may be used to verify or supplement information stored about an organization’s assets.

As has been mentioned, many NEA architectures have been developed in the industry to address the above purposes. Certain instantiations of these architectures leverage the EAP framework to enable network admission decisions to be based on both authentication and posture assessment. However, while these instantiations leverage standard protocols to the extent possible, e.g. 802.1X[802.1X], EAP[EAP] and RADIUS[RADIUS], these architectures are still not fully interoperable because other needed protocols have not been standardized. The intent of the proposed NEA effort is to identify those interfaces where standardization is needed in the IETF, define requirements for these interfaces, and work within the IETF to define standards to meet these requirements.

4. Goals

The goals of architectures that support network assessment technology include some or all of the following:

- Support assessment of endpoints across a range of network access technologies, leveraging existing technology to the extent possible

- Support authorization decisions based on authentication of user or endpoint device, assessment of the state of the endpoint device, or both
- Support endpoint assessment at various locations in the network i.e. at a L2 hop or a L3 hop, both of which may be a single hop or multiple hops away from the endpoint.

- Support endpoint assessment at possibly multiple hops on a path e.g. at both a L2 and a L3 hop.

- Support network isolation of non-compliant endpoints from compliant endpoints for remediation or other purposes.

- Support endpoint re-assessment when state of endpoints change, or rules in the NEA server change.

- Enable integration of 3rd-party security applications so that one or more applications can assess the posture of an endpoint and the aggregate of all results can be used in network admission decisions.

- Support endpoints with a NEA client and without a client.

5. Deployment Scenarios

Network assessment architectures have been targeted primarily at enterprise deployment scenarios to date. The deployment scenarios include:

5.1. Wired LAN access

In this deployment scenario, network admission control would typically take place at the first L2 hop from the endpoint i.e. a switch port. However, there are cases where the first L2 device may not support network endpoint assessment for some reason, and network endpoint assessment may happen behind the first hop, e.g. a switch behind a wireless access point.

Wired LAN access deployment scenarios may need to support single or multiple hosts per switch port. Deployment scenarios with multiple hosts per port include IP phones + PC, or multiple PCs connected behind a hub.

802.1X is an example of a standards-based network access technology that supports access control based on authentication for a single host per port in first L2 hop deployment scenarios.

5.2. Wireless LAN Access

In this deployment scenario, network admission control would
typically take place at the first L2 hop from the endpoint i.e. a wireless access point. Wireless LAN access supports multiple hosts per wireless access point.

802.11 is a standards-based network access technology that supports wireless access control based on authenticating the endpoint.

5.3. Remote access VPN

In this deployment scenario, network admission control is done at the VPN concentrator that acts as the gateway between remote users and access to the enterprise network.

IPSEC VPN and SSL VPN are example of network access technologies that support remote access VPN deployment scenarios.

5.4. Gateway Access

In this deployment scenario, network admission control is enforced at a L3 boundary in a distributed campus network. The L3 boundary may be one or more L3 hops away from the endpoint.

This deployment scenario may be used during the transition period while an organization gradually upgrades network equipment to support network endpoint assessment. In some cases, the technology may not be available immediately for first-hop L2 or L3 deployments and a general-purpose gateway deployment e.g. at a router behind a VPN concentrator, may be a reasonable first step.

This deployment scenario may also be used between network security domains e.g. at the border between a less trusted/managed branch office and main campus, at the border between main campus or a visitor site and access to the Internet, at the border between extranet and intranet, and on access to protected servers in a data center.

It follows from this deployment scenario that there may be multiple Network enforcers on any path that an endpoint may use in a network, thus resulting in it being authorized more than once. It is also possible that different posture rules may be assessed at different network locations and a different authorization decision made.

6. Components and Interfaces

This section provides a general overview of NEA architectures, with a particular emphasis on the EAP/RADIUS instantiation of these architectures, since this is the focus of the initial standards
effort. (Other instantiations of the high-level architecture may be standardized in future.)

Figure 1 shows the components of an NEA system and identifies specific interfaces.

---
| Posture Collectors (1 ...N) | Posture Validators (1 ...N) |
---|---|---|
| | | |
| Client Broker | Server Broker |
| | | |
| Network Access Requestor | Network Enforcer Access Authority |
| | | |

NEA CLIENT                                   NEA SERVER
Figure 1: NEA Components and Interfaces

6.1. Mapping to existing architectures

For convenience, we map the terms used in this document with that of three architectures developed in the industry: Trusted Network Connect (TNC) architecture [TNC], Microsoft’s Network Access Protection (NAP) architecture [NAP], and Cisco’s Network Admission Control (NAC) architecture [NAC].
6.2. Components

6.2.1. NEA Client

The NEA client resides on an endpoint device and comprises the following components:

- Posture collector
- Client broker
- Network access requestor

6.2.1.1. Posture Collector

The Posture collector is software that provides posture information about the endpoint device to the Client broker. There may be many
Posture collectors on an endpoint, one per vendor and application type. Examples of Posture collectors include a host Posture collector that provides information about the OS and patch levels, anti-virus Posture collector that provides information about the anti-virus application, firewall Posture collector that provides information about the configuration of the personal firewall.

A Posture collector is responsible for:

- Receiving and responding to requests for posture information on a per vendor and application type basis
- Receiving a notification of the result of the posture assessment and information about any actions to perform, e.g. URL of a remediation server
- Indicating when the posture of the host has changed

6.2.1.2. Client Broker

The Client broker aggregates posture information from multiple Posture collectors. The Client broker is responsible for:

- Maintaining a record of Posture collectors
- Multiplexing and demultiplexing posture messages between the NEA server and the relevant Posture collectors
- Determining from Posture collectors when posture has changed and triggering re-assessment where supported by the underlying transport
- Providing user notifications

6.2.1.3. Network access requestor

The Network access requestor is responsible for communicating with the NEA server to transport the necessary information to gain access to the network and for subsequent re-assessment. There may be multiple Network access requestors on an endpoint representing different technologies for accessing the network.

6.2.2. Network enforcer

The Network enforcer is a network component that controls access of endpoints to the upstream network. The Network enforcer may be a network device or a logical component on an endpoint. The NEA enforcer enforces network authorization decisions from the Network

access authority. There are different types of Network enforcers supporting different technologies for accessing the network.

6.2.3. NEA server

The NEA server comprises the following logical components:

- Network access authority
- Server broker
- Posture validator

6.2.3.1. Network access authority

The Network access authority is responsible for authorizing endpoints based on a number of criteria including the identity of an endpoint and/or user as well as the results of posture assessment from the Server broker.

6.2.3.2. Server broker

The Server broker aggregates posture information from potentially multiple Posture validators into an overall system result, and provides this information to the Network access authority. Responsibilities of the Server broker include:

- Maintaining a record of Posture validators
- Multiplexing and demultiplexing posture messages between the NEA client and the relevant Posture validators
- Aggregating posture assessment results from all Posture validators into an overall system result
- Triggering posture reassessment where supported

6.2.3.3. Posture validator

A Posture validator is a server that is responsible for assessing information from the corresponding Posture collector and determining the result of the assessment. There may be multiple Posture validators each targeted at a particular security application from a particular vendor. In some architectures, the Posture validators are not co-located with the NEA server.

A Posture validator is responsible for the following:
Requesting and receiving posture information from a particular Posture collector
Assessing the endpoint posture and providing a result to the Server broker
Sending to the Posture collector information on remediation actions to be taken
Indicating to the Server broker when posture reassessment may be needed

6.3. Interfaces

6.3.1. Posture Attribute interface (IF-PA)

The IF-PA is a protocol between a Posture collector and the associated Posture validator for the particular vendor and application. The interface is used to pass information gathered by a Posture collector to the Posture validator, and to pass the results of the assessment and information needed for remediation from the Posture validator to the Posture collector.

6.3.2. Posture Broker Interface (IF-PB)

The IF-PB is a protocol that carries aggregated posture information between all requested Posture collectors on an endpoint and the corresponding Posture validators. This protocol also carries the overall system posture result from the Server broker to the Client broker.

6.3.3. Posture Transport Interface (IF-PT)

The IF-PT is the transport protocol between the Network access requestor and the Network access authority that carries the IF-PB protocol.

In EAP instantiations of this architecture, the IF-PT interfaces consists of two protocols: 1) Posture Transport Tunnel (IF-PTT), which is an EAP tunneling method between the Network access requestor in the NEA client and the Network access authority in the NEA server that can carry posture information in addition to authentication information, and 2) Posture Transport Carrier (IF-PTC), a protocol that carries EAP, e.g. EAP over 802.1X, EAP over RADIUS.

6.3.4. Network Access Enforcement Interface (IF-NAE)

The IF-NAE is the protocol between the Network enforcer and Network
access authority used to carry network authorization decisions between the Network enforcer and the Network access authority.

In EAP Instantiations of this architecture, the IF-NAE interface is RADIUS.

6.3.5. Posture Validation Interface (IF-PV)

In some instantiations of the architecture, the Server broker and the Posture validators are not co-located. The IF-PV protocol between the Server broker and Posture validator forwards posture information and returns posture validation results.

7. Scope of Standardization

Protocols that are candidates for standardization in the IETF include the following:

- Posture attributes interface (IF-PA): This interface can be defined independently of the underlying transport interfaces, while keeping in mind performance and other constraints imposed by the underlying protocols. Many of the posture attributes will be vendor-specific and need only be understood by the corresponding Posture collector and its associated Posture validator. However, there may be common attributes that would benefit from standardization, e.g. an attribute representing the result of evaluating posture information from a Posture collector.

- Posture broker interface (IF-PB): This interface is also largely independent of the underlying transport, although it should be defined in such a way that it can be used in posture transport protocols that are likely to be used, such as EAP tunneling methods based on TLS.

- Posture transport tunnel interface (IF-PTT): As described in the section above, in an EAP instantiation of an NEA architecture, an EAP tunneling method is needed to carry posture information in addition to authentication credentials. Standardization of certain EAP methods for authentication is the proposed charter of the EMU WG. The need to support posture assessment in addition to authentication may place additional requirements on the EAP methods that need to be standardized. In particular, standardization of EAP tunneling methods is a high priority.

- Posture transport carrier interface (IF-PTC): Some EAP carrier methods are standards today e.g. 802.1X. However, there is no standard EAP transport to support gateway and other "multi-hop"
deployment scenarios as defined in this document. The PANA WG [PANA] has proposed a specification of EAP over a UDP transport, although not explicitly for this use case. Other protocols have been designed and used for this purpose e.g. Network Access control Protocol [NACP].

- Network access enforcement interface (IF-NAE): Existing standards exist including RADIUS and Diameter. The initial focus of the proposed NEA standardization effort is on RADIUS. The Radext WG has the charter to standardize RADIUS extensions. It’s not clear that NEA would require any extensions that fall outside of the scope of the existing charter of that WG.

- Posture validator interface (IF-PV): This protocol acts as a carrier for posture attributes between a Server broker and a Posture validator that is not co-located in the NEA server. Depending on the choice of protocol for this purpose, this may or may not fall within the scope of the IETF.

The proposed initial scope of the NEA effort is the following:

- IF-PTT
- IF-NAE
- IF-PB
- IF-PTC

The remaining interfaces, IF-PA and IF-PV, may be addressed at a later date.

8. IANA Considerations

This document makes no request of IANA.

Note to RFC Editor: this section may be removed on publication as an RFC.

9. Security Considerations

NEA systems include a number of functional components and interfaces, and thus there are a number of security aspects pertaining to the system as a whole which need to be highlighted. Some of these are discussed in the following sections.
9.1. Secure channel between the Client Broker and Server Broker

The Client broker needs to be able to communicate the posture information regarding the endpoint to the Server broker with communications integrity and confidentiality. One possible avenue towards establishing this secure channel (at the peer layer of the Client broker and Server broker) is to establish it end-to-end between Network access requestor (NAR) and the Network access authority (NAA). This end-to-end secure channel would prevent any intermediate entity, including the Network enforcer from gaining access to the posture information. The exact implementation of this secure channel is dependent on the domain of application and network configuration.

9.2. Authorization for Plug-in/Broker interaction

There is a functional separation between the Posture collector and the Client broker (at the NEA client side) and also between Posture validator and the Server broker (at the NEA Server side). It is important that a Client broker be allowed to communicate with only the authorized Posture collectors. Similarly, the Server broker should only communicate with authorized Posture validators. Recall that the Posture collector is software that provides posture information about the endpoint device to the Client broker. Note that there may be many Posture collectors in a NEA client, one per vendor and application type. Without protection, a bogus Posture collector (Posture validator) can open communications with the Client broker (Server broker), thereby opening the possibility of a Denial-of-Service attack (at the very least) against the Client broker and Server broker respectively.

9.3. Self-Integrity of the NEA Client and NEA Server

The trustworthiness of the posture information being reported by the NEA client to the NEA Server is dependent on and is only as good as the self-integrity of the NEA client and NEA Server respectively. If malicious code or other malware are present in the NEA client actively modifying posture information being communicated by the NEA client, the NEA Server may be basing its decision-making on inaccurate or bogus posture information. Thus, it is important that both the NEA client and the NEA Server are protected against attacks that illegally modify the system configurations and system components of these entities.

9.4. Protection of parameters exchanged across Interfaces

An important aspect of an NEA system is the protection of parameters being communicated between the various interfaces defined in the
architecture. Examples of the parameters being exchanged include, but are not limited to, state change notifications between the Client broker and Posture collector, state change notifications between the Server broker and Posture validator, the parameters and messages exchanged between two peer entities (on the NEA client and NEA Server respectively) across IF-PA and IF-PB, and in general parameters and messages exchanged across interfaces IF-PT, and IF-NAE.

9.5. Identity authentication of communicating end-points

In order for the NEA Server to accept access requests and posture information being reported to by the NEA client, the NEA Server may need to authenticate the NEA client in some manner. Similarly, within some network environments there may be the requirement that the NEA client also authenticate the NEA Server with whom it is communicating. Although the process of evaluating an access request may combine together the notion of authentication and integrity state evaluation (through posture information), it is important from a security perspective and useful from a good engineering practices perspective to be able to separate end-point authentication (including both machine and user authentication) from end-point posture assessment.

10. Acknowledgements

We acknowledge the contributions from members of the NEA mailing list.

11. References

11.1. Normative References


11.2. Informative References


Authors’ Addresses

Steve Hanna
Juniper Networks
35 Forest Ridge Road
Concord, MA  01742
U.S.A.

Phone: 781-729-9559
Email: shanna@juniper.net

Thomas Hardjono
Signacert Inc
115 SW Ash Street
Suite 430
Portland, OR  97204
U.S.A.

Phone: 781-729-9559
Email: thardjono@signacert.com

Susan Thomson
Cisco Systems
499 Thornall Street, 8th floor
Edison, NJ  08837
U.S.A.

Phone: 732-635-3086
Email: sethomso@cisco.com
Intellectual Property Statement

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Disclaimer of Validity

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Copyright Statement

Copyright (C) The Internet Society (2006). This document is subject to the rights, licenses and restrictions contained in BCP 78, and except as set forth therein, the authors retain all their rights.

Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.