Network Working Group
Request for Comments: 5209
Category: Informational

P. Sangster
Symantec
H. Khosravi
Intel
M. Mani
Avaya
K. Narayan
Cisco Systems
J. Tardo
Nevis Networks

June 2008

Оценка конечных точек - обзор и требования

Network Endpoint Assessment (NEA): Overview and Requirements

Статус документа

Этот документ содержит информацию для сообщества Internet и не задает каких-либо стандартов Internet. Документ может распространяться свободно.

Аннотация

В данном документе описана задача, область применения и требования к протоколам взаимодействия компонент эталонной модели NEA[1]. Модель NEA обеспечивает владельцам сетей (например, предприятиям с удаленным доступом в сеть) механизм определения состояния[2] систем. Определение может выполняться в процессе обработки запросов на доступ в сеть и/или позднее в течение сеанса работы в сети. Полученные сведения о состоянии могут использоваться для принятия различных решений, ориентированных на соответствие. Информация о состоянии зачастую оказывается полезной для обнаружения систем с недостаточным уровнем защиты или устаревшими средствами обеспечения безопасности (например, антивирусы или персональные МСЭ). Для обеспечения контекста разработки требований вводится эталонная модель и терминология.

Оглавление

[1]Network Endpoint Assessment - оценка оконечных точек.
[2]В оригинале используется термин «posture». *Прим. перев.*

1. Введение

Оконечные точки, подключенные к сети, могут подвергаться широкому классу угроз. Некоторую защиту от таких угроз можно обеспечить за счет предъявления к таким точкам требований соответствия определенному набору правил (политике). Следовательно, задачей NEA является оценка конечных точек с целью проверки их соответствия политике безопасности для того, чтобы можно было предпринять меры по защите до возникновения угроз. Например, если будет выяснено, что система не соответствует требованиям по причине нехватки средств защиты (типа персональных МСЭ и антивирусных программ) или отсутствия критически важных исправлений ПО, протоколы NEA могут обеспечить механизм детектирования недостаточного уровня защищенности, а также указать требуемые для приведения в соответствие меры. Отметим, что оконечная точка, соответствующая требованиям политики, может оставаться уязвимой для угроз, которые могут присутствовать в сети.

NEA обычно включает использование специальных клиентских программ, работающих на оконечных точках, которые определяют конфигурацию системы и передают информацию в сетевую инфраструктуру. Инфраструктура сети включает соответствующее ПО для проверки валидности конечных точек, способное сравнить данные о конфигурации подключающейся системы с принятой в сети политикой безопасности и передать информацию о результатах сравнения соответствующим элементам, санкционирующим доступ в сеть или к приложениям. На некоторых конечных точках (например, принтерах) может не поддерживаться возможность запуска клиентов NEA, а отдельные клиенты могут отказываться от предоставления сведений о своей конфигурации. Такие ситуации выходят за пределы NEA и должны обрабатываться в соответствии с принятой локальной политикой.

Результат оценки конечной точки может оказывать влияние на принятие решения о предоставлении доступа, которое передается механизмам реализации политики доступа в сеть и/или запрашивающим доступ точкам. Хотя рабочая группа NEA признает возможность наличия связи между оценкой и принятием решения о предоставлении доступа, механизмы и протоколы исполнения этих решений выходят за пределы настоящей спецификации.

Архитектуры, похожие на NEA, используются уже достаточно давно и реализованы в поставляющейся на рынок продукции, но решения разных производителей не обеспечивают должной интероперабельности. Примерами таких архитектур могут служить: Trusted Network Connect [TNC] от Trusted Computing Group, Network Access Protection [NAP] от Microsoft или Cisco Network Admission Control [CNAC]. В этих технологиях оценивается программная и/или аппаратная конфигурация оконечных устройств в целях мониторинга или исполнения требований принятой в организации политики.

Рабочая группа NEA разработала стандартные протоколы, которые могут использоваться для обмена информацией между клиентом (NEA Client) и сервером (NEA Server). В этом документе описывается контекст NEA, включая терминологию, вопросы применимости, постановку задачи, эталонную модель и примеры использования. Далее идентифицируются требования к протоколам, используемым для обмена информацией между клиентами и серверами NEA. В заключительной части документа рассматриваются некоторые потенциальные угрозы безопасности и приватности при использовании NEA. Основная часть данной спецификации представляет собой описание контекста NEA.

1.1. Уровни требований

Выделенные шрифтом уровни требований в данном документе, применяются в указанном ниже смысле:

должно, требуется (MUST) - обязательно к выполнению;

недопустимо (MUST NOT) - полностью запрещено;
следует (SHOULD) - желательно выполнить для достижения желаемого результата;
не следует (SHOULD NOT) - желательно не допускать;
можно (MAY) - выполняется по желанию.

Использование перечисленных слов без шрифтового выделения означает обычную трактовку этих терминов без привязки к приведенным выше определениям.

2. Терминология

В этом разделе приведены определения используемых в документе терминов. В других документах те же термины могут иметь иной смысл, поэтому здесь предпринимается попытка растолковать их в контексте NEA.

Assessment - оценка

Процесс сбора информации о свойствах конечной точки (таких, как наличие персонального МСЭ), которые могут использоваться для проверки соответствия требованиям политики.

Assertion Attributes - подтвержденные атрибуты

Атрибуты, включающие пригодную для дальнейшего использования информацию о результатах предыдущей оценки данной точки. Такие атрибуты могут служить для оптимизации последующих оценок с целью предотвращения ненужных повторов. Например, атрибут такого типа может выделяться специально для конкретной точки с подписью и датой от сервера NEA, подтверждающей на определенный период соответствие этой точки заданному набору правил. Сервер NEA может принимать такой атрибут вместо повторного запроса информации для оценки.

Attribute - атрибут

Элемент данных, включающий любые требуемые метаданные, которые описывают наблюдаемое, ожидаемое или оперативное состояние конечной точки (например, используемые антивирусные программы).
Обмен атрибутами выполняется, как часть протокола NEA (см. параграф 5.2). NEA предполагает множество сценариев, где использование атрибута того или иного типа может показывать:

- предшествующую оценку состояния (Assertion Attributes);
- наблюдаемую конфигурацию или свойство (Posture Attributes);
- запрос данных о конфигурации или свойствах (Request Attributes);
- решение об оценке (Result Attributes);
- инструкции по исправлению ситуации (Remediation Attributes).

Рабочая группа NEA будет стандартизовать подмножество пространства имен атрибутов в качестве стандартных атрибутов. Нестандартизованные атрибуты называются в данной спецификации фирменными (vendor-specific).

Dialog - диалог

Последовательность запросов и откликов в обмене сообщениями.

Endpoint - оконечная точка

Любое компьютерное устройство, которое может быть подключено к сети. С такими устройствами обычно бывает связан некий конкретный адрес канального уровня еще до подключения и может выделяться адрес IP после подключения к сети. Конечными точками могут быть настольные и стационарные компьютеры, серверы, сотовые телефоны и прочие устройства, которые могут поддерживать адрес IP.

Message - сообщение

Самодостаточная единица обмена данными между клиентом и сервером NEA. Например, сообщение с атрибутами может содержать набор атрибутов, описывающих конфигурацию антивирусных программ на конечной точке.

Owner - владелец

Элемент (сущность), являющийся законным и правомочным обладателем актива (например, конечной точки). Владелец имеет право контролировать исполнение политики для устройства даже если это устройство не находится в его распоряжении. Владелец может разрешить пользователю переопределять или усиливать правила, а также может отказаться от исполнения любых правил, ограничивающих использование актива.

Posture - состояние

Конфигурация и/или состояние оборудования и программ на конечной точке применительно к политике безопасности организации.

Posture Attributes - атрибуты состояния

Атрибуты, описывающие конфигурацию или состояние (posture) конечной точки. Например, такие атрибуты могут указывать версию операционной системы, установленной на конечной точке.

Request Attributes - атрибуты запроса

Атрибуты, передаваемые сервером NEA для идентификации данных о состоянии, запрашиваемых у клиента NEA. Такие атрибуты могут включать, например, сообщение с запросом сервера NEA о версии операционной системы на стороне клиента.

Remediation Attributes - атрибуты восстановления

Атрибуты, содержащие инструкции по приведению конечной точки в соответствие одному или нескольким правилам. Рабочая группа NEA не будет определять стандартные атрибуты восстановления, но в данной спецификации описывается использование таких атрибутов в эталонной модели и протоколах.

Result Attributes - атрибуты результата

Атрибуты, описывающие соответствие конечной точки политике NEA. Такие атрибуты обычно создаются сервером NEA в качестве заключения по результатам проверки соответствия. Может использоваться более одного атрибута этого типа для обеспечения гранулярности уровней соответствия в дополнение к общему решению по результатам оценки.

Session - сессия

Соединение с поддержкой информации о состоянии, способное поддерживать обмен множеством сообщений, связанных с оценкой(ами) конкретной конечной точки. В этом документе термин «сессия» определяется на концептуальном уровне, но не описываются свойства сессий и не задаются требования к протоколам NEA по управлению сессиями.

User - пользователь

Персональная роль для лица, пользующегося услугами конечной точки. Пользователь может не быть владельцем конечной точки и к нему могут применяться те или иные ограничения, наложенные владельцем. Например, сотрудники предприятия могут быть пользователями компьютеров, предоставленных организацией (владелец) для выполнения работы.

3. Применимость

В этом разделе описана сфера действия стандартизуемых технологий и рассмотрены сетевые среды, в которых технологии NEA представляются применимыми.

3.1. Сфера действия

Приоритетной задачей группы NEA является разработка стандартных протоколов верхних уровней эталонной модели (см. раздел 5): протокола атрибутов состояния (PA[1]) и протокола брокера (PB[2]). Протоколы PA и PB разрабатываются с учетом передачи информации по разным протоколам транспортного уровня (PT). Рабочая группа NEA будет идентифицировать стандартные протоколы PT, которые явятся обязательными для реализации. Протоколы PT могут определяться другими рабочими группами, поскольку требования могут не относиться к сфере NEA. При работе со стандартными протоколами PT (например, EAP[3], TLS[4] [TLS]) протоколы PA и PB обеспечат интероперабельность между клиентами NEA одного производителя и серверами NEA других компаний. В данной спецификации не рассматриваются другие интерфейсы между функциональными компонентами эталонной модели NEA и требования к их устройству. Включенное в текст рассмотрение этих аспектов предназначено лишь для разъяснения модели и тех или иных требований.

Некоторые смежные области, не показанные в эталонной модели, также выходят за пределы сферы деятельности группы NEA. В результате данная спецификация включает:

- стандартизацию протоколов и механизмов исполнения для организации доступа в сеть с учетом ограничений;
- разработку стандартных протоколов для внесения изменений на конечных точках, не соответствующих требованиям;
- спецификация протоколов, используемых для обмена данными с удаленными компонентами клиентов или серверов NEA (например, удаленные коллекторы или валидаторы состояния);
- поддержка клиентов NEA, обеспечивающих состояние (posture) для других конечных точек (например, клиент NEA на устройстве IDS[5], обеспечивающий состояние для конечных точек без клиента NEA);
- определение набора событий и ситуаций, которые могут инициировать на клиенте или сервере NEA запрос оценки;
- детектирование ложных конечных точек и работа с ними (см. параграф 8.1.1).

3.2. Применимость сред

Поскольку модель NEA основана на специальных программах NEA, присутствующих на клиентах и в сетевой инфраструктуре, а также по самой природе информации, которая будет раскрываться, применение технологий NEA может оказаться невозможным во многих ситуациях, возникающих в сети Internet. Поэтому в данном разделе рассматриваются сценарии, в которых применимость NEA достаточно очевидна, а также некоторые случаи, когда использование этих технологий невозможно. В конечном счете применение NEA не ограничивается описанными здесь сценариями. Решение об использовании NEA всегда остается за тем, кто развертывает систему (например, сетевым провайдером) с учетом предполагаемых отношений с владельцами и потенциальными пользователями конечных точек.

Технологии NEA в основном сфокусированы на сценариях, где владелец конечных точек является и владельцем сети. Это типичный случай для корпоративных сетей, обеспечивающих своих сотрудником оборудованием для выполнения их работы. Такие сотрудники связаны с владельцем контрактными обязательствами, в которых оговаривается использование корпоративных активов и допустимые в рабочее время действия. Контракт может включать установку правил подключения и использования конечных точек.

Подобные ситуации могут наблюдаться и в других средах, обеспечивая там преимущества использования технологий NEA. Примером могут служить среды, где конечные точки принадлежат лицам (возможно, даже пользователям), явно выразившим желание соответствовать политике сети или поставщика услуг в обмен на возможность доступа к его активам. Примером могут также служить сотрудники, не входящие в штат компании и использующие личные компьютеры для доступа в корпоративную сеть в соответствии с правилами оценки NEA, принятыми для штатных сотрудников. Технологии NEA хорошо подходят для таких случаев.

И, напротив, некоторые среды, где применение NEA не ожидается, будут включать среды, в которых конечные точки принадлежат владельцам, не согласным на выполнение правил сетевого провайдера. Примером могут служить ситуации, когда упомянутые выше нештатные сотрудники компаний подключаются к сети в местах общего доступа типа кафе. Использование технологий NEA в кафе не предполагается и переносной компьютер при подключении к сети не может быть оценен. Инвазивная по своей природе технология NEA при проверке конечных точек в таких местах общего доступа может создавать угрозу приватности.

Сложнее определить применимость NEA в других средах, поэтому рабочая группа NEA будет рассматривать эти среды, как выходящие за пределы данной спецификации. Для того, чтобы та или иная среда рассматривалась, как применимая для NEA, владельцы или пользователи конечных точек должны четко понять, что им придется

[1]Posture Attribute.
[2]Posture Broker.
[3]Extensible Authentication Protocol - расширяемый протокол аутентификации.
[4]Transport Layer Security - защита на транспортном уровне.
[5]Intrusion Detection System - система детектирования вторжений.

соответствовать правилам владельца и оператора сети. Соответствие включает также раскрытие некой информации, которая требуется сети для выполнения проверки соответствия.

4. Описание задачи

Технология NEA может быть использована для решения различных задач. В этом разделе описаны основные ситуации, в которых могут быть реализованы преимущества технологии NEA.

Технологию можно использовать для облегчения проверки соответствия конечных точек принятой в организации политике безопасности при подключении этих точек к сети. Организации часто требуют наличия на конечных точках заданной службами IT конфигурации операционной системы (ОС) и наличия некого набора защитных приложений (например, антивирусов, средств обнаружения/предотвращения вторжений, персональных МСЭ, программ контроля обновлений). Конечные точки, не удовлетворяющие требованиям политики, могут быть уязвимыми для различных известных угроз, которые могут существовать в сети.

Без применения технологии NEA обеспечение соответствия конечных точек принятой в компании политике требует много времени и усилий. Не все конечные точки находятся в ведении служб IT компании (например, компьютеры привлекаемых извне специалистов). Даже для контролируемых активов не всегда удается обеспечить своевременную установку обновлений, поскольку не все компьютеры постоянно подключены к корпоративной сети (например, портативные компьютеры). При использовании технологии NEA сеть получает возможность оценки каждой конечной точки при получении от нее запроса на подключение к сети или в любой момент после подключения. Это обеспечивает организации возможность своевременной проверки соответствия заданной политике на всех поддерживающих NEA конечных точках и обеспечивает при необходимости своевременное внесение изменений на конечных точках.

Технологию NEA можно использовать для организации оценки состояния для множества вариантов подключения к сети, включая (но не ограничиваясь) проводные и беспроводные подключения к ЛВС с использованием 802.1X [802.1X], удаленный доступ по протоколам IPsec [IPSEC], SSL[1] VPN, серверы доступа.

Конечные точки, не способные работать с NEA или не предоставляющие достаточный для оценки состояния объем информации, можно подключать в соответствии с другими правилами доступа. Решение о способах обслуживания таких точек может приниматься администратором сети на основе данных от других механизмов защиты в сети (например, аутентификации). Не соответствующим политике конечным точкам могут направляться инструкции по исправлению или предупреждения вместе с предоставлением ограниченного доступа в сеть. Технологии контроля доступа в сети могут использовать результаты NEA для ограничения или блокирования доступа в сеть отдельных точек, что позволяет устранять потенциальные уязвимости до того, как конечная точка станет открытой для атак. Представление результатов оценки NEA и обмен соответствующей информацией с технологиями контроля доступа в сети выходит за пределы этого документа.

Переоценка является другим важным примером использования технологии NEA, когда выполняется новая оценка конечных точек, ранее считавшихся соответствующими политике. Такая проверка может потребоваться в результате смены политики и/или состояния конечной точки, что может произойти в любой момент. Считавшаяся ранее соответствующей правилам конечная точка при подключении ее к сети может показать несоответствие, если политика была сменена. Например, переоценка может потребоваться, если пользователь отключит защитные функции, требуемые политикой (например, персональный МСЭ), или МСЭ перестает соответствовать требованиям политики, связанным с установкой обязательного обновления.

Третьим примером использования технологии NEA может служить проверка или дополнение данных об активах организации, хранящихся в инвентаризационных базах данных.

Технологию NEA можно использовать также для проверки соответствия конечных точек заданной политике и подготовки отчетов о результатах для случаев попыток доступа таких точек к критически важным корпоративным приложениям по инициативе службы персонала.

5. Эталонная модель

В этом параграфе описана эталонная модель оценки конечных точек (NEA). Эта модель разработана для организации контекста обсуждения и может не отражать напрямую тот или оной конкретный протокол или архитектуру развертывания. Модель описывает базовую функциональность клиентов и серверов NEA, связь между ними, а также используемые для коммуникаций на различных уровнях протоколы (например, PA передаётся с помощью протокола PB).

Хотя на рисунке 1 показано 3 протокольных уровня, PA по сути является сообщениями, содержащими набор атрибутов, которые собираются вместе и инкапсулируются в PB. В свою очередь, PB представляет собой упрощенный протокол для передачи множества сообщений, поэтому стек протоколов представляет собой, прежде всего, транспорт (PT[2]). Вертикальные линии на рисунке представляют API и/или протоколы взаимодействия между компонентами внутри клиентов и серверов NEA. Эти интерфейсы выходят за пределы сферы стандартизации рабочей группы NEA.

[1]Secure Socket Layer - уровень защищенного сокета.
[2]Posture Transport.

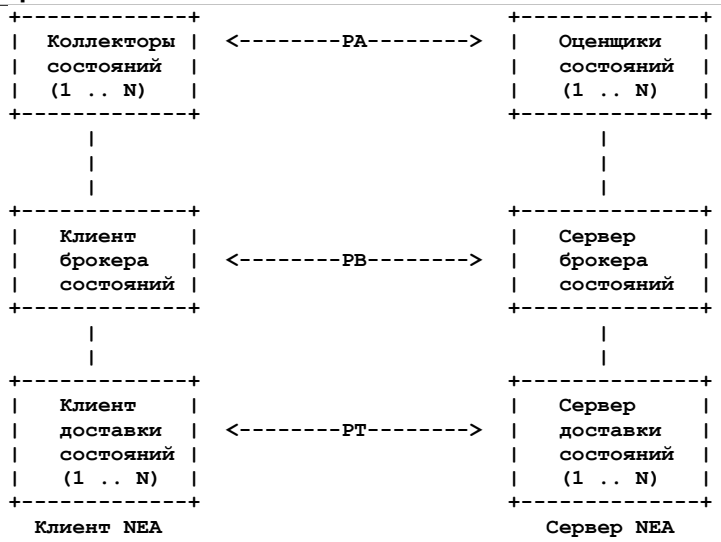

Рисунок 1. Эталонная модель NEA.

Эталонная модель NEA не включает механизмов обнаружения клиентов и серверов NEA. Предполагается, что в конфигурации клиентов и серверов NEA указывается информация, позволяющая им находить друг друга. Методы указания и механизмы организации коммуникационных каналов выходят за пределы эталонной модели NEA и их следует включать в спецификации протоколов, претендующих на роль PT.

5.1. Клиент и сервер NEA

5.1.1. Клиент NEA

Клиент NEA размещается на оконечном устройстве и обеспечивает следующую функциональность:

- сбор состояний (Posture);
- клиент брокера состояний;
- клиент транспортировки состояний.

Клиент NEA отвечает за отклики на запросы атрибутов, описывающих локальную конфигурацию рабочего домена для клиента и обработку результатов оценки, включая выполнение инструкций по приведению в соответствие политике. Клиенты NEA не отвечают за отчеты о состоянии элементов, которые могут присутствовать на конечной точке или доступны через сеть, но находятся за пределами рабочего домена данной конечной точки (например, виртуальные машины другого домена).

Например, устройство трансляции сетевых адресов (NAT) может маршрутизировать соединения для многочисленных устройств, расположенных за ним, но когда NAT-устройство подключается к сети, его клиент NEA будет сообщать только свое (локальное) состояние. Аналогично и конечные точки с поддержкой виртуализации могут иметь множество независимых рабочих доменов (например, экземпляров OS). Каждый клиент NEA отвечает только за информацию о состоянии для своего рабочего домена, но эта информация может агрегироваться теми или иными локальными механизмами для представления состояния множества доменов конечной точки. Такие механизмы агрегирования данных о состоянии выходят за пределы данной спецификации.

Конечные точки без клиента NEA (не входят в область действия NEA) или отказавшиеся от предоставления атрибутов, запрашиваемых сервером NEA, могут рассматриваться, как не соответствующие требованиям. Модель NEA включает для конечных точек возможности обновления их состояний с целью приведения в соответствие.

5.1.1.1. Сборщик состояний

Сборщик состояний (Posture Collector) отвечает за отклики на запросы информации о состоянии, полученных в атрибутах Request Attribute от сервера NEA. Он отвечает также за обработку решений по результатам оценки, полученных с Result Attribute и выполнение инструкций из Remediation Attribute. Клиент NEA может поддерживать несколько сборщиков состояний способных собирать стандартные или фирменные атрибуты состояния (Posture Attribute) для отдельных свойств конечной точки. Типичные примеры сборщиков предоставляют информацию о версии операционной системы (ОС) и уровне обновления (patch level), антивирусных программах и механизмах защиты конечной точки (таких, как IDS или МСЭ).

Каждый сборщик связывается с одним или множеством идентификаторов, позволяющих указывать этот сборщик в качестве получателя сообщений PA. Клиент брокера состояний (Posture Broker Client) использует эти идентификаторы для маршрутизации сообщений соответствующему сборщику. Идентификаторы могут быть динамическими (например, их может генерировать клиент брокера при регистрации), статическими (например, выделяемыми сборщикам на этапе инсталляции и передаваемые брокерам при регистрации) или задаваться, как функция сообщений с атрибутами, которые сборщик желает получать (например, по типу сообщения).

В модели NEA для сборщика состояний выделяются следующие зоны ответственности:

- выяснение из локальной политики приватности и безопасности ограничений, которые могут применяться к раскрытию информации данному серверу NEA;
- прием атрибутов Request Attribute от валидатора и выполнение их локальной обработки, требуемой для отклика; это может включать:

- сбор связанной информации о состояниях для конкретных характеристик конечной точки и возврат этой информации в атрибутах Posture Attribute;
- кэширование и контроль применимости ранее выданных атрибутов, содержащих пригодные для повторного использования оценки, которые могут служить для подтверждения соответствия и возврата атрибутов взамен данных о состоянии;

- прием атрибутов, содержащих инструкции по обновлению функциональности конечной точки; это может потребовать от сборщика взаимодействия с пользователем, владельцем и/или сервером восстановления;
- мониторинг состояния отдельных характеристик конечной точки на предмет изменений, о которых требуется сообщать клиенту брокера состояний;
- выполнение криптографической верификации атрибутов, полученных от валидатора (Validator) с использованием криптозащиты возвращаемых атрибутов.

Приведенный выше список показывает возможные зоны ответственности сборщика состояний с точки зрения модели. Отметим, что этот не задает требований, которым должна соответствовать каждая реализация сборщика состояний, и не является исчерпывающим перечнем того, что сборщик может делать.

5.1.1.2. Клиент брокера состояний

Клиент брокера состояний (Posture Broker Client) представляет собой мультиплексор-демультиплексор сообщений PA. Клиент отвечает за демультиплексирование сообщений PB, получаемых от сервера NEA, и распределение каждого инкапсулированного в нем сообщения PA соответствующему сборщику (Posture Collector). Модель также позволяет на клиентах заранее подготавливать отклики с данными о состоянии, что позволяет клиенту NEA передать свое состояние, не дожидаясь получения запроса для конкретного атрибута от сервера NEA.

Клиент брокера также мультиплексирует отклики от сборщиков состояний и возвращает их серверу NEA. Клиент-брокер создает одно или множество сообщений PB, используя сообщения PA, которые он получил от сборщиков, вовлеченных в оценку. Количество и порядок откликов от сборщиков состояний (сообщения PA), мультиплексируемых в каждое сообщение PB определяется клиентом брокера на основе множества факторов, включая политику и характеристики нижележащего уровня сетевого транспорта (например, MTU). Клиент NEA может иметь одного клиент-брокера.

Клиент-брокер также обслуживает глобальное решение по результатам оценки от серверного брокера ((Posture Broker Server) и может взаимодействовать с пользователем для передачи ему полученного решения и рекомендаций по приведению в соответствие.

Модель NEA возлагает на клиента брокера следующие зоны ответственности:

- поддержка реестра известных сборщиков состояний и обеспечение для них возможности динамической регистрации-дерегистрации;
- мультиплексирование и демультиплексирование сообщений с атрибутами между сервером NEA и соответствующими сборщиками;
- обработка уведомлений об изменении состояния от сборщиков и инициирование переоценки;
- уведомление пользователя о принятом по результатам оценки решении и передача пользователю других сообщений от сервера NEA.

5.1.1.3. Клиент транспортировки состояний

Клиент транспортировки (Posture Transport Client) отвечает за организацию надежного коммуникационного канала с сервером NEA для обмена сообщениями между клиентом и сервером. На одном клиенте NEA может поддерживаться более одного транспортного клиента для работы по разным протоколам (например, 802.1X, VPN). На некоторых транспортных клиентах в конфигурации может быть задан адрес подходящего сервера транспортировки (Posture Transport Server) для использования с конкретной сетью.

Модель NEA выделяет Posture Transport Client две зоны ответственности:

- инициирование и поддержка коммуникационного канала с сервером NEA; транспортный клиент прячет детали взаимодействия с нижележащим уровнем (Layer 2 или Layer 3);
- обеспечение криптографической защиты обмена сообщениями между клиентом и сервером NEA.

5.1.2. Сервер NEA

Сервер NEA обычно наделяется следующей функциональностью:

- валидатор состояний (Posture Validator);
- серверный брокер состояний (Posture Broker Server);
- сервер транспортировки состояний (Posture Transport Server).

Валидаторы состояний могут размещаться на отдельном от серверного брокера сервере и тогда от брокера будет требоваться взаимодействие как с локальными, так и с удаленными валидаторами.

5.1.2.1. Валидатор состояний

Валидатор состояний отвечает за обработку атрибутов Posture Attribute от соответствующих сборщиков состояний. Валидатор может обрабатывать атрибуты состояний от одного или множества сборщиков (и наоборот). Валидатор выполняет оценку состояния для одной или множества характеристик конечной точки (например, анитивирусы) и

генерирует результат, дополняя его при необходимости рекомендациями по приведению в соответствие. По своему усмотрению валидатор может запросить дополнительные атрибуты от одного или нескольких сборщиков.

С каждым валидатором связывается один или множество идентификаторов, которые позволяют указать этот валидатор в качестве получателя сообщений PA. Серверный брокер состояний использует эти идентификаторы для маршрутизации сообщений к валидатору. Идентификатор может быть динамическим (генерируется серверным брокером при регистрации), статическим (присваивается валидатору при инсталляции и передается брокеру в процессе регистрации) или функцией от сообщений с атрибутами, которые валидатор желает принимать (например, тип сообщений).

Валидаторы могут размещаться вместе с сервером NEA или устанавливаться на отдельный сервер. Очевидно, что серверу NEA требуется обслуживать множество валидаторов.

Модель NEA выделяет для валидаторов следующие зоны ответственности:

- запрос атрибутов от сборщиков состояний, который может включать:
  - атрибуты Request Attribute, указывающие сборщику необходимость собрать и представить атрибуты Posture Attributes для конкретной характеристики конечной точки;
- прием атрибутов от сборщиков; отклики сборщика состояний могут включать:
  - атрибуты Posture Attribute, собранные для запрошенной функциональности;
  - атрибуты Assertion Attribute, показывающие результат проверки соответствия из предыдущей оценки;
- оценка состояния характеристик конечной точки на основе полученных от сборщика атрибутов;
- передача результатов оценки состояния серверному брокеру;
- передача результатов оценки состояния сборщику состояний; сообщение может включать:
  - атрибуты Result Attribute, показывающие результат оценки;
  - атрибуты Remediation Attribute с инструкциями по приведению в соответствие для сборщика;
- мониторинг обновлений (по внешним каналам), которые требуют выполнения переоценки и передачи уведомления серверному брокеру;
- обеспечение криптографической защиты для атрибутов, передаваемых сборщику, и криптографической верификации полученных от сборщика атрибутов.

Приведенный выше список показывает зоны ответственности валидатора с точки зрения модели. Перечисленные пункты не являются требованиями, которые должна поддерживать каждая реализация Posture Validator, и не задают полного списка того, что может делать валидатор.

5.1.2.2. Серверный брокер состояний

Серверный брокер состояний (Posture Broker Server) выступает в качестве мультиплексора и демультиплексора сообщений с атрибутами. Серверный брокер разбирает сообщения PB, полученные от клиента NEA и демультиплексирует их в сообщения PA, которые передает соответствующим валидаторам. Серверный брокер также мультиплексирует сообщения PA (например, сообщения с атрибутами Request Attribute от соответствующих валидаторов) в одно или несколько сообщений PB и передает их клиенту NEA с помощью протокола Posture Transport. Количество и порядок откликов валидатора (сообщения PA), а также общее решение по результатам оценки, мультиплексируемые в отклик(и) PB, могут определяться серверным брокером на основе множества факторов, включая политику и характеристики нижележащего сетевого транспорта (например, значение MTU).

Серверный брокер также отвечает за расчет общего решения по результатам оценки на основе отдельных решений по оценке состояний по результатам от разных валидаторов. Общее решение по результатам оценки возвращается клиенту NEA в атрибутах Result Attribute внутри сообщения PB. Конкретный сервер NEA может иметь один серверный брокер, который будет обслуживать все локальные и удаленные валидаторы.

Модель NEA возлагает на серверный брокер следующие зоны ответственности:

- поддержка реестра валидаторов и обеспечение для них возможности регистрации и дерегистрации;
- мультиплексирование и демультиплексирование сообщений, передаваемых валидаторам и принимаемых от них;
- расчет общего решения по результатам оценки на основе результатов оценки состояний от разных валидаторов и проверки соответствия политике; принятое по результатам оценки решение передается клиенту-брокеру в сообщении PB.

5.1.2.3. Сервер транспортировки состояний

Сервер транспортировки (Posture Transport Server) отвечает за надежный канал связи с клиентом NEA для обмена сообщениями между клиентом и сервером NEA. На конкретном сервере NEA может использоваться несколько серверов транспортировки для поддержки разных транспортных протоколов. Конкретный сервер транспортировки обычно будет обслуживать запросы множества транспортных клиентов (Posture Transport Clients) and may require local configuration describing how to reach the NEA Clients.

Модель NEA возлагает на сервер транспортировки несколько зон ответственности:

- организация и поддержка коммуникационного канала с (потенциально) несколькими клиентами NEA;
- обеспечение криптографической защиты обмена сообщениями между клиентом и сервером NEA.

5.2. Протоколы

Эталонная модель NEA включает три протокольных уровня (PA, PB, PT), обеспечивающих обмен атрибутами через сеть. Эти три протокола предназначены для совместного использования и каждый играет в рамках модели свою роль, однако функциональность разных уровней может перекрываться. Например, каждому из этих протоколов следует обеспечивать возможность защиты информации от атак (см. параграф 8.2).

5.2.1. Протокол атрибутов состояний (PA)

PA[1] представляет собой протокол, который служит для переноса одного или множества атрибутов между сборщиком состояний и связанным с ним валидатором (Posture Validator). Протокол PA представляет собой облегченный, ориентированный на сообщений способ сбора в единый блок атрибутов, которые нужно передать. При сборке атрибутов воедино может быть указана цель, которой служат эти атрибуты. К ожидаемым типам сообщений относятся запросы информации о состоянии (Request Attribute), данные о состоянии конечной точки (Posture Attribute), результат оценки (Result Attribute), пригодные для повторного использования оценки состояния (Assertion Attribute), а также инструкции по приведению конечной точки в соответствие политике (Remediation Attribute). Протокол PA также обеспечивает необходимое кодирование и криптографическую защиту атрибутов состояния (Posture Attribute).

5.2.2. Протокол брокера состояний (PB)

PB[2] представляет собой протокол для передачи агрегированных атрибутов между сборщиками состояний на клиенте NEA и соответствующими валидаторами на сервере NEA, вовлеченном в конкретную оценку. Протокол PB обеспечивает поддержку сеанса обмена сообщениями для каждой оценки. Сессия PB используется для множества запросов Posture Attribute и откликов от разных сборщиков состояний и валидаторов, вовлеченных в конкретную оценку. Протокол PB позволяет также передавать общее решение по результатам оценки в атрибуте Result Attribute от серверного брокера к клиент-брокеру. PB можно использовать для передачи дополнительных типов сообщений, используемых брокерами (клиентом и сервером), например, о предпочитаемых пользователем настройках интерфейса (например, языке).

5.2.3. Протокол доставки состояний (PT)

PT представляет собой транспортный протокол, используемый для обмена данными между клиентом и сервером NEA и отвечающий за доставку сообщений, генерируемых протоколом PB. Протокол PT доставляет сообщения PB в процессе запроса на организацию соединения с сетью или после организации такого соединения.

В сценариях, где начальная оценка требуется в процессе подключения к сети, протокол PT (например, EAP в 802.1X) может вносить ограничения на использование сети, поэтому при реализации может быть выбрано ограничение числа и/или размера передаваемых атрибутов. Клиентам и серверам NEA следует поддерживать обнаружение возможности такого ограничения до выполнения оценки на основе свойств нижележащего сетевого протокола. С учетом этой информации политика NEA может задавать аспекты начальной проверки конечных точек и потенциально ограничивать обмен атрибутами в сообщениях PA. За этой процедурой может следовать полная переоценка конечной точки после ее подключения к сети. Можно и не ограничивать объем обмена атрибутами, настроив технологию доступа в сеть на выделение адресов IP из специального блока, которому присущи определенные ограничения, до полной проверки конечной точки и использование полнофункционального IP-транспорта по результатам оценки. Некоторые из ограничений, которые могут быть присущи протоколам на этапе подключения к сети, перечислены ниже:

- ограниченный размер MTU и ограниченная возможность его увеличения;
- невозможность использования множества циклов (roundtrip);
- слабая поддержка «привязывания» (piggybacking) атрибутов для других протоколов;
- малая полоса или значительные задержки, ограничивающие объем передаваемой информации;
- неспособность сервера инициировать обмен сообщениями вне фазы подключения к сети.

В процессе выбора протокола PT требуется учесть влияние конкретного PT и множества нижележащих протоколов на потребности развертывания PA и PB, которые выбираются раньше PT и их потребности уже понятны. Некоторые нижележащие стеки протоколов могут вносить слишком большие ограничения, не позволяющие выполнить адекватные оценки NEA на этапе подключения к сети.

Протокол PT обеспечивает гарантированную доставку сообщений, взаимную аутентификацию и криптографическую защиту для сообщений PB в соответствии с локальной политикой.

5.3. Атрибуты

Протокол PA отвечает за обмен атрибутами между сборщиком состояний и валидатором. Протокол PB может также передавать атрибуты общего результата оценки от серверного брокера. Атрибуты, по сути, являются зарезервированными словами, обозначающими те или иные состояния. Сервер NEA способен запрашивать лишь информацию, для которой имеется соответствующий атрибут, определяющий тип получаемого состояния. Рабочая группа NEA будет определять общий (стандартный) набор атрибутов, которые представляются достаточно широко применимыми для сборщиков состояний, чтобы обеспечить максимальное взаимодействие, однако сборщики могут поддерживать и дополнительные (фирменные) атрибуты.

Назначение обмена атрибутами может меняться в зависимости от сценария развертывания (например, данные о состоянии или оценка соответствия). В этом разделе рассматривается предполагаемое влияние на ситуацию каждого класса атрибутов в сообщениях PA с учетом инициатора. Приведенная классификация не является схемой для определения пространства имен рабочей группой NEA.

[1]Posture Attribute Protocol.
[2]Posture Broker Protocol.

5.3.1. Атрибуты, обычно передаваемые клиентом NEA

- *Posture Attribute (атрибуты состояния)* - атрибуты и значения, передаваемые для обмена информацией о конкретном аспекте системы (на основе семантики атрибута). Такие атрибуты обычно передаются в ответ на атрибуты запроса (Request Attribute) от сервера NEA. Например, набор атрибутов состояния может описывать статус межсетевого экрана на хосте (например, запущен ли он, какова версия и кто производитель). Решение сервера NEA будет базироваться на сравнении данного типа атрибута с политикой.

- *Assertion Attribute (атрибуты оценки)* - атрибуты, содержащие предыдущую оценку соответствия, которые хранятся для предотвращения необходимости повторного запроса состояния и его передачи серверу NEA. Примерами таких атрибутов могут служить (a) предоставленные сервером NEA атрибуты (состояние), описывающие предыдущую оценку (например, непонятные для конечной станции, подписанные и помеченные временем данные, констатирующие тот или иной результат) или (b) идентификационные данные клиента NEA, используемые сервером NEA для поиска информации о предыдущих решениях (например, cookie). Эти атрибуты могут возвращаться взамен атрибутов запроса (Posture Attribute) или в дополнение к ним.

5.3.2. Атрибуты, обычно передаваемые сервером NEA

- *Request Attribute (атрибуты запроса)* - атрибуты, определяющие конкретную информацию о состоянии, которую хочет получить сервер NEA. Эти атрибуты могут формировать шаблон, который сборщик состояний будет заполнять (с учетом ограничений локальной политики) данными, соответствующими каждому атрибуту. В результате будут получены атрибуты состояния (Posture) или оценки (Assertion) от клиента NEA.

- *Result Attribute (атрибуты результата)* - атрибуты, содержащие решение валидаторов (Posture Validator) и/или серверного брокера (Posture Broker Server). Уровень детализации сильно зависит от соответствия или несоответствия отдельных атрибутов.

- *Remediation Attribute (атрибуты реабилитации)* - атрибуты, показывающие клиенту NEA и пользователю, что нужно сделать для приведения конечной точки в соответствие политике сервера NEA. Эти атрибуты передаются в тех случаях, когда принято общее решение о несоответствии конечной точки заданным правилам. Атрибуты Remediation и Result могут передаваться в одном сообщении от сервера NEA.

- *Assertion Attribute (атрибуты оценки)* - атрибуты, содержащие оценку сервером NEA соответствия конечной точки заданной политике для будущего использования клиентом NEA (см. параграф 5.3.1).

6. Варианты использования

В этом разделе рассмотрено несколько ситуаций применения NEA с целью описания и обсуждения рассматриваемой проблемы. Примеры обеспечивают контекст и общее обоснование определяемых здесь требований. Для упрощения понимания вариантов использования и их связи с эталонной моделью каждый вариант применения сопровождается простым примером и обсуждением его связи с протоколами NEA. Следует понимать, что представленные примеры не являются единственными вариантами решения задач и приведены скорей для понимания того, какие потоки могут возникать и как они влияют на протоколы NEA.

Варианты применения будем делить на две широких категории, каждая из которых имеет свой набор событий-триггеров:

- начальная оценка - оценка состояния конечной точки, которая не проверялась раньше (в обозримые сроки) и, таким образом, не имеет каких-либо подтверждений соответствия политике; такая оценка может инициироваться по запросу на подключение к сети, запросу на использование сервиса или по желанию понять состояние системы;

- переоценка - оценка состояния конечной точки, которая оценивалась ранее; такая оценка может выполняться по разным причинам, включая констатацию клиентом или сервером NEA событий, которые могут повысить уровень риска для конечной точки (например, ситуация, когда с момента предыдущей оценки прошло достаточно много времени).

6.1. Начальная оценка

Начальная оценка выполняется в тех случаях, когда на клиента или сервере NEA происходит событие, которое вызывает необходимость проверить состояние конечной точки в первый раз. Конечная точка не относится к этой категории, если она ранее была оценена и клиент или сервер NEA поддерживает информацию о соответствии данной конечной точки и, следовательно, не возникает необходимости оценивать эту точку заново.

6.1.1. Оценка при подключении к сети или по запросу сервера

Этот вариант фокусируется на оценках, выполняемых при попытке подключения конечной точки к сети или начала использования сервиса, который требует оценки состояния. Этот вариант представляет особый интерес, поскольку он позволяет серверу NEA оценить состояние конечной точки до того, как ей будет предоставлен доступ к сети или сервису.

Данная модель может использоваться для обнаружения конечных точек с известными уязвимостями и выполнения корректирующих действий до того, как конечная точка будет допущена в сеть и сможет создать угрозу для нее.

Оценки этого класса могут вызываться самыми разными действиями на конечных точках. Например, оценка может быть инициирована попыткой конечной точки получить доступ к хорошо защищенному сетевому сервису (например, к серверу финансовых или кадровых приложений), где требуется серьезная проверка защищенности. Хорошим примером может служить запрос доступа в сеть, требующую от конечных точек соответствия заданной политике. Более детальное рассмотрение этого случая приведено ниже.

6.1.1.1. Пример

Сотрудник IT, вернувшийся из отпуска, включает свой офисный компьютер, который генерирует запрос на подключение к проводной сети компании. Политика безопасности в сети от системы предоставить информацию о состоянии для проверки того, что функции защиты на компьютере включены и обновлены. Компьютер передает свои сведения об установленных обновлениях, антивирусе, межсетевом экране. Сервер NEA определяет отсутствие на компьютере свежих обновлений защиты, предназначенных для устранения серьезной уязвимости, и система помещается в сеть с ограниченным доступом. Компьютер следует предоставленным инструкциям по загрузке и установке требуемых обновлений. Позднее компьютер снова запрашивает подключение к сети и ему предоставляется полный доступ в сеть компании после полной оценки его состояния.

6.1.1.2. Возможные события и использование протокола

Ниже приведен типичный поток сообщений эталонной модели NEA для описанного выше примера.

1. Стационарный компьютер сотрудника IT подключается к сети через шлюз доступа в проводной сети предприятия.
2. Серверный брокер на сервере NEA получает инструкцию разрешить подключение конечной точки к проводной сети.
3. В соответствии с политикой серверный блокер связывается с компонентами проверки установленных обновлений, локального брандмауэра и антивирусной системы (валидатор) для проверки соблюдения политики доступа. Каждый валидатор создает сообщение, содержащее атрибуты, которые должны быть запрошены для проверки подключаемого компьютера.
4. Серверный блокер агрегирует сообщения PA от валидатора в сообщение PB, а затем передает PB серверу транспорта, который использует протокол PT для отправки сообщения PB клиенту NEA на компьютере.
5. Клиент транспорта получает сообщение от сервера NEA и передает его клиентскому брокеру для доставки.
6. Клиентский брокер демультиплексирует сообщение PB и доставляет сообщения PA сборщикам состояний с запросами атрибутов для межсетевого экрана, исправлений (patch) операционной системы и антивирусной защиты.
7. Каждый вовлеченный сборщик состояний обращается к локальной политике для определения информации, которая может быть раскрыта, и после этого возвращает запрошенные атрибуты, для которых предоставлены полномочия, в сообщении PA клиентскому брокеру.
8. Клиентский брокер агрегирует сообщения PA в одно сообщение PB и передает его серверному брокеру, используя сессию между клиентом и сервером транспорта.
9. Сервер транспорта предоставляет сообщение PB серверному брокеру, который демультиплексирует его и передает атрибуты соответствующим валидаторам.
10. Каждый валидатор сравнивает полученные атрибуты с ожидаемыми значениями, определяемыми его политикой.
11. Для антивируса и межсетевого экрана валидатор возвращает серверному брокеру атрибуты, подтверждающие соответствие компьютера, а для исправлений операционной системы передается несоответствие. Валидатор для исправлений операционной системы создает сообщение PA, которое содержит атрибуты с инструкциями по исправлению в дополнение к атрибутам, показывающим несоответствие.
12. Серверный брокер агрегирует сообщения PA и передает их в сообщении PB клиентскому брокеру через транспортный сервер и клиента.
13. Клиентский брокер доставляет сообщения PA с результатами от разных валидаторов сборщикам состояний, включая сообщение PA, содержащее атрибуты с инструкциями по исправлению для операционной системы. Сборщик состояний для исправлений операционной системы взаимодействует с пользователем для загрузки и установки требуемых обновлений, при этом конечная может оставаться в карантине.
14. После внесения исправлений указанные выше этапы 1-10 повторяются (по инициативе клиента NEA, повторяющего запрос на подключение к сети).
15. С этого момента каждый вовлеченный валидатор (включая проверяющий обновления операционной системы) возвращает статус соответствия и серверный брокер возвращает результат, показывающий общий успех.
16. Клиентский брокер получает результат соответствия и компьютер сотрудника IT подключается к сети.

6.1.1.3. Воздействие на требования

Ниже приведено несколько аспектов примера варианта использования, которые может быть необходимо учесть в требованиях.

- Оценка местоположения до того, как конечная точка будет допущена в сеть.
- Конечная точка передает атрибуты, содержащие данные о местоположении.
- Сервер NEA передает инструкции по исправлению
- Клиент NEA запрашивает переоценку после исправления.

6.1.2. Оценка по инициативе конечной точки

Этот вариант показывает, что конечная точка (возможно, по запросу пользователя) может инициировать оценку своего состояния для проверки работоспособности и своевременности механизмов защиты.

6.1.2.1. Пример

Студент идет в зал терминалов для работы над проектом. В этом зале размещаются терминалы общего пользования, принадлежащие учебному заведению и подключенные к сети. Эти системы ранее использовались другими студентами, поэтому состояние из защиты неизвестно. Студент хочет проверить соответствие защищенности терминала правилам учебного заведения до начала работы, поэтому он запрашивает оценку состояния. Сервер NEA проводит первоначальную оценку системы и определяет ее соответствие, но указывает, что антивирусная защита не применяется. Студен получает консультативное сообщение, указывающее, что антивирусные программы отключены, но все остальное соответствует правилам. Студент включает антивирусную защиту, сканирует систему и по завершении сканирования принимает решение о доверии к системе и начинает работу.

6.1.2.2. Возможные события и использование протокола

Ниже приведен поток сообщений через эталонную модель NEA для студента, использующего общую систему в терминальном зале.

1. Студент запускает клиентский брокер на компьютере терминального зала для инициирования оценки.
2. Брокер организует сессию с серверным брокером, что запускает процесс оценки.
3. Серверный брокер детектирует новую сессию и просматривает правила для определения валидаторов, участвующих в оценке. Брокер принимает решение о выборе нескольких валидаторов, включая антивирусную проверку.
4. Используемые валидаторы создают сообщения PA с запросами конкретных атрибутов, содержащих информацию о компьютере в терминальном зале на основе политики безопасности учебного заведения.
5. Серверный брокер собирает сообщение PB, включающее все сообщения PA от валидаторов.
6. Транспортный сервер передает сообщение PB транспортному клиенту, где оно передается клиентскому брокеру.
7. Клиентский брокер на компьютере студента демультиплексирует сообщения PA и доставляет их соответствующим сборщикам состояний.
8. Сборщики состояний обращаются к политике конфиденциальности для решения вопроса о предоставляемой серверу информации. Если это допустимо, каждый сборщик состояний возвращает сообщение PA с запрошенной оценкой клиентскому брокеру.
9. Клиентский брокер собирает возвращенные сообщения PA в сообщение PB и передает его транспортному клиенту для отправки серверу транспорта.
10. Серверный брокер разделяет и распределяет сообщения PA от сборщика состояний между соответствующими валидаторами.
11. Валидаторы определяют соответствие содержащихся в оценке атрибутов, включенных в сообщение PA, принятым правилам и возвращают оценку состояния серверному брокеру. В данном случае антивирусный валидатор возвратил сообщение PA, указывающее несоответствие по причине отсутствия запущенной антивирусной программы и содержащее рекомендации по активации программы.
12. Серверный брокер принимает общее решение о соответствии на основе результатов оценки всеми валидаторами и передает сообщение PB с атрибутом, выражающим общее решение об оценке и сообщение PA от антивирусного валидатора. В данном случае общая оценка указывает соответствие системы требованиям (несмотря на результат антивирусного валидатора), поскольку политика серверного брокера разрешает работать без антивирусной программы, если в системе установлены исправления и работает межсетевой экран (на основании данных от других валидаторов).
13. Транспортный сервер передает сообщение PB транспортному клиенту, который доставляет его клиентскому брокеру.
14. Клиентский брокер на компьютере в терминальном зале проверяет атрибуты общего решения в сообщении PB и сообщает студенту, что система соответствует требованиям, но имеются дополнительные рекомендации.
15. Клиентский брокер передает сообщение PA с атрибутами рекомендации антивирусному сборщику состояний, который информирует пользователя как включить антивирус для улучшения локальной защиты.
16. Студент запускает антивирусную программу и операции 1-10 повторяются.
17. На этот раз антивирусный валидатор сообщает о работе программы и серверный брокер возвращает решение о положительной общей оценке в сообщении PB.
18. Клиентский брокер получает решение о положительной общей оценке в сообщении PB и студен начинает работу с компьютером.

6.1.2.3. Воздействие на требования

Ниже приведены несколько разных аспектов примера, которые могут быть учтены в требованиях.

- Произвольная конечная точка запросила начальную оценку.
- Положительное общее решение включено в сообщение PB с сообщением PA, содержащим рекомендуемый набор атрибутов для исправления.

6.2. Повторная оценка состояния

Повторная оценка конечной точки может произойти в любой момент после успешной первоначальной оценки NEA. Это может быть вызвано событием, например, обнаруженной клиентом NEA смене местоположения или изменениями,

обнаруженными сетевой инфраструктурой, таким как регистрация подозрительного поведения или обновление сетевой политики на сервер NEA. /то может быть также периодическая (по таймеру) оценка состояния конечной точки.

6.2.1. Переоценка по инициативе клиента NEA

Этот вариант позволяет программам на конечной точке или пользователю определить необходимость в повторной оценке системы. Имеется много причин, по которым такая переоценка может быть полезной, включая изменение сообщенного ранее состояния, обнаружение подозрительного поведения или даже просто возможность системы периодически опрашивать сервер NEA для проверки соответствия свежей политике.

6.2.1.1. Пример

Настольные компьютеры в отделе кадров компании слабо защищены и могут быть взломаны. Администратор отдела кадров решает развернуть на каждом компьютере программы для мониторинга использования защитных механизмов. Однажды сотрудник отдела случайно отключил персональный брандмауэр. Процесс мониторинга обнаруживает это и связывается с сервером NEA для запроса переоценки соответствия брандмауэра. Сервер NEA возвращает решение о необходимости включения брандмауэра для продолжения работы в сети. Клиент NEA доводит это решение до пользователя, указывая способ включения брандмауэра. Сотрудник запускает брандмауэр и инициирует запрос на подключение к сети.

6.2.1.2. Возможные события и использование протокола

Ниже приведен поток сообщений через эталонную модель NEA для сотрудника отдела кадров.

1. Программа мониторинга настольного компьютера, которая обычно может служить сборщиком состояний, запускает Posture Broker Client для инициирования переоценки состояния. Клиентский брокер создает сообщение PB, содержащее сообщение PA с указанием отключенного на настольном компьютере брандмауэра.
2. Клиентский брокер передает сообщение PB серверному брокеру.
3. Транспортный клиент передает сообщение PB серверу транспорта по протоколу PT.
4. Серверный брокер получает сообщение PB и пересылает сообщение PA из него валидатору брандмауэра для оценки.
5. Валидатор брандмауэра определяет, что конечная точка не соответствует требованиям, поскольку брандмауэр отключен.
6. Валидатор создает сообщение PA с атрибутами, указывающими несоответствие при оценке состояния, и рекомендациями по включению брандмауэра.
7. Валидатор передает сообщение PA с результатом оценки серверному брокеру для отклика клиенту NEA.
8. Серверный брокер создает сообщение PB с решением по общей оценке (несоответствие) и сообщением PA от валидатора брандмауэра.
9. Транспортный сервер доставляет сообщение PB клиенту транспорта, а тот передает его клиентскому брокеру.
10. Клиентский брокер обрабатывает атрибут, содержащий решение об общей оценке состояния от сервера NEA и выводит пользователю сообщение о несоответствии.
11. Клиентский брокер пересылает сообщение PA сборщику состояний брандмауэра, который выводит инструкции по включению персонального брандмауэра.
12. Пользователю предлагается инициировать переоценку после включения брандмауэра.
13. После выполнения рекомендаций клиент NEA инициирует переоценку и этапы 1-4 повторяются. На этот раз валидатор брандмауэра определяет соответствие конечной точки требованиям и возвращает положительное решение.
14. Серверный брокер создает сообщение PB с решением об общей оценке (соответствие) и возвращает его клиенту NEA.

6.2.1.3. Воздействие на требования

Ниже приведены несколько разных аспектов примера, которые могут быть учтены в требованиях.

- Произвольная конечная точка (программа) запросила повторную оценку.
- Сервер NEA запросил конкретные атрибуты, связанные с брандмауэром.
- Клиент NEA (сборщик состояний брандмауэра) взаимодействует с пользователем для устранения проблемы.

6.2.2. По инициативе сервера NEA

Во многих случаях (особенно для переоценки) сервер NEA может инициировать определенную или полную переоценку одной или множества конечных точек, в зависимости от:

- времени (периодическая);
- события;
- обновления политики.

6.2.2.1. Пример

Предприятие требует, чтобы сотрудники всегда были в курсе важных обновлений защиты операционной системы. Сотрудник отдела маркетинга подключается к сети и выполняет начальную оценку, которая определяет соответствие

его переносного компьютера требованиям безопасности. Несколько часов спустя крупный производитель операционных систем выпускает комплект исправлений, предотвращающих серьезную уязвимость системы, которая используется в Internet.

Администраторы предприятия делают обновления доступными и меняют политику сети с требованием установить обновления к 17 часам. Это изменение политики заставляет сервер NEA запросить переоценку для определения конечных точек, на которые воздействуют исправления, но те еще не установлены. Переносной компьютер маркетолога оценивается и определяется необходимость установки обновлений. Передаются рекомендации по установке и сотруднику выдается разъяснение о способе получения обновлений и необходимости их установки до 17 часов. Сотрудник незамедлительно загружает и устанавливает обновления, а также получает подтверждение установки всех исправлений.

В 17 часов проводится повторная оценка всех затронутых обновлением конечных точек для определения их соответствия. Компьютер сотрудника маркетингового отдела переоценивается и представляет установленные обновления, подтверждая свое соответствие требованиям.

6.2.2.2. Возможные события и использование протокола

Ниже приведен поток сообщений через модель NEA описанного выше примера.

1. Сотрудник отдела маркетинга подключается к сети и выполняет первоначальную оценку а результате которой принимается решение о соответствии.
2. Администратор предприятия настраивает политику обновления операционных систем, указывающую, что все свежие исправления должны быть установлены к 17 часам для предотвращения серьезных уязвимостей.
3. Валидатор для операционных систем на сервере NEA узнает о смене политики и создает сообщение PA, запрашивающее атрибуты с описанием установленных обновлений операционной системы и указывает серверному брокеру инициировать повторную оценку конечных точек, подключенных к сети.
4. Posture Broker создает сообщение PB, включающее сообщение PA от Posture Validator для проверки обновлений ОС.
5. Серверный брокер постепенно организует сессию с каждым доступным клиентом NEA.
6. Серверный брокер передает сообщение PB клиенту клиентскому брокеру.
7. Сервер транспорта передает сообщение PB транспортному клиенту по протоколу PT.
8. Клиентский брокер получает сообщение PB и пересылает сообщение PA сборщику состояний для обновлений операционной системы.
9. Сборщик состояний для обновлений ОС определяет установленные на конечной точке обновления и, если это разрешено политикой раскрытия информации, создает сообщение PA с атрибутами установленных обновления.
10. Клиентский брокер передает сообщение PB, включающее сообщение PA об установленных обновлениях.
11. Клиент транспорта доставляет сообщение PB транспортному серверу, где оно передается серверному брокеру.
12. Серверный брокер получает сообщение PB и доставляет сообщение PA валидатору для обновлений ОС.
13. Валидатор извлекает атрибуты, описывающие установленные обновления из сообщения PA и использует их для проверки соответствия конечной точки новой политике. Валидатор решает, что конечная точка не соответствует правилам, поскольку на ней не установлены новые исправления.
14. Валидатор генерирует сообщение PA, включающее атрибуты, которые указывают решение о несоответствии и атрибуты, содержащие инструкции по исправлению, позволяющие конечной точке загрузить требуемые обновления ОС.
15. Валидатор сообщает результат оценки серверному брокеру вместе с сообщением PA.
16. Серверный брокер принимает глобальное решение по оценке и передает сообщение PB с этим решением и сообщением PA от валидатора.
17. Сервер транспорта доставляет сообщение PB транспортному клиенту, где оно передается клиентскому брокеру.
18. Клиентский брокер обрабатывает атрибут Result, полученный от сервера NEA, и выводит на экран пользователя сообщение о несоответствии.
19. Клиентский брокер пересылает сообщение PA с инструкциями по исправлению сборщику состояний для обновлений ОС и тот дает пользователю инструкции по обеспечению соответствия, включающие загрузку требуемых обновлений ОС для устранения уязвимости.
20. Сотрудник отдела маркетинга устанавливает требуемые обновления и это обеспечивает соответствие.
21. Клиент NEA инициирует повторную оценку обновлений ОС, при которой повторяются многие из указанных выше этапов. На этот раз на этапе 13 валидатор определяет соответствие компьютера сотрудника заданным требованиям. Он возвращает многократно используемый (например, подписанный и датированный) набор атрибутов, подтверждающий соответствие ОС новой политике. Эта оценка соответствия ОС может использоваться в будущих сообщениях PA от коллектора обновлений ОС вместо новой проверки и предоставления установленного набора обновлений.
22. На этот раз сборщик состояний обновления ОС, получив сообщение PA с многократно используемыми атрибутами, подтверждающее соответствие, кэширует эти атрибуты на будущее.

23. Позднее, в 17 часов, сервер NEA запускает постепенную переоценку для проверки соответствия рекомендациям по установке обновлений. Когда сборщик состояний для обновлений ОС получает запрос информации о положении дел (как в п. 9 выше), он возвращает кэшированный набор подтверждений (вместо информации об исправлениях ОС) для индикации установки обновлений вместо реальной проверки установленных в системе обновлений.

24. Когда валидатор для обновлений ОС получает сообщение PA с этими подтверждениями, он способен проверить их подлинность и пригодность. В результате он возвращает положительное решение по результатам оценки, позволяя компьютеру оставаться в сети.

6.2.2.3. Воздействие на требования

Ниже приведены несколько разных аспектов примера, которые могут быть учтены в требованиях.

- Инициированная сервером переоценка, требуемая доступностью важного обновления.
- Представление клиентом NEA атрибутов оценки вместо подтверждения установки обновления.
- Способность сервера NEA признавать ранее выданные атрибуты оценки достаточными.

7. Требования

В этом разделе описаны требования, которые будут предъявляться рабочей группой NEA при оценке и сравнении протоколов-кандидатов для PA, PB и PT. Эти требования часто выражают функции, которые кандидаты должны поддерживать, чтобы разработчик мог решить вопрос об использовании этой функции. Раздел не содержит требований по реализации функций протоколов. Например, могут быть заданы требования (**должно**, **следует**, **можно**), чтобы функции криптографической защиты были доступны в каждом протоколе, но это не означает для разработчиков необходимости применять все или даже некоторые из этих функций, если он считает, что среда обеспечивает достаточный уровень защиты.

7.1. Общие требования к протоколам

Ниже перечислены требования, применимые к протоколам PA, PB и PT в эталонной модели NEA.

C-1 Протоколы NEA **должны** поддерживать множество обменов между клиентом и сервером NEA в одном процессе оценки.

C-2 Протоколам NEA **следует** обеспечивать клиентам и серверам NEA возможность инициировать оценку и переоценку при возникновении необходимости.

C-3 Протоколы NEA, включающие возможности защиты, **должны** быть способны защитить от активных и пассивных атак на промежуточных и конечных точках, включая защиту от повторного использования (replay).

C-4 Протоколы PA и PB **должны** быть способны работать на основе любого протокола PT. Например, протокол PB должен обеспечивать независимый от транспорта интерфейс, позволяющий протоколу PA работать без изменений в широком диапазоне сетевых сред (EAP/802.1X, TLS, IKEv2[1]).

C-5 Процесс выбора протоколов для NEA **должен** оценивать и предпочитать использование имеющихся открытых стандартов, удовлетворяющих требованиям, перед тем, как разрабатывать новые. Целью NEA является не создание дополнительных протоколов при наличии подходящих решений, которые уже разработаны.

C-6 Протоколы NEA **должны** быть расширяемыми по масштабу развертывания, протоколы **должны** поддерживать множество сборщиков состояний на большом числе клиентов NEA для оценки множеством Posture Validator, размещенных на многих серверах NEA.

C-7 Протоколы NEA **должны** поддерживать эффективную доставку большого числа сообщений с атрибутами между клиентом и сервером NEA.

C-8 Протоколы NEA **должны** эффективно работать на каналах с низкой пропускной способностью и большими задержками.

C-9 Для всех строк, выводимых пользователям протоколы **должны** поддерживать преобразование строк с учетом языковых предпочтений пользователя.

C-10 Протоколы NEA **должны** поддерживать кодирование строк в формате UTF-8 [UTF8].

C-11 В результате различия транспортных характеристик базовых протоколов, являющихся кандидатами в PT клиент и сервер NEA **должны** быть способны узнавать и приспосабливаться к ограничениям доступного протокола PT. Например, некоторые характеристики PT могут влиять на работу протоколов PA и PB, включая ограничения на возможность той или иной стороны инициировать соединение NEA, максимальный объем данных в сообщении или полной оценке, верхнюю границу числа обменов, упорядоченный (дуплексный) обмен сообщениями. Процесс выбора для протоколов PT **должен** учитывать ограничения кандидатов в PT, налагаемые на протоколы PA и PB.

7.2. Требования к протоколу PA

Протокол атрибутов состояния (PA) определяет транспорт и модель данных для доставки информации о состоянии и оценке между конкретным сборщиком состояний, связанным с клиентом NEA, и валидатором, связанным с сервером NEA. Протокол PA передает наборы стандартных и фирменных атрибутов. Сам протокол PA передается протоколом PB.

Приведенные ниже требования задают желаемые свойства, формирующие базу для сравнения и оценки протоколов-кандидатов в PA. Эти требования не задают использование свойств, просто протоколы кандидаты могут предлагать эти свойства при необходимости.

[1]Internet Key Exchange Protocol version 2 - протокол обмена ключами в Internet, версия 2.

PA-1 Протокол PA **должен** поддерживать обмен расширяемым набором стандартных атрибутов NEA. Эти атрибуты будут отличаться от нестандартных.

PA-2 Протокол PA **должен** поддерживать обмен расширяемым набором фирменных атрибутов. Эти атрибуты будут сегментироваться в однозначно определяемые пространства имен производителей.

PA-3 Протокол PA **должен** позволять валидаторам делать один или множество запросов для атрибутов от сборщика состояний в одном процессе оценки. Это позволяет валидатору повторно оценить состояние конкретной конечной точки или запросить другую оценку, в том числе для других частей конечной точки.

PA-4 Протокол PA **должен** быть способен возвращать атрибуты от валидаторов сборщику состояний. Например, это может позволить сборщику состояний узнать конкретную причину негативной оценки и помочь в исправлении ошибок и уведомлении владельца.

PA-5 Протоколу PA **следует** поддерживать защиту подлинности, целостности и конфиденциальности атрибутов, передаваемых между сборщиком состояний и валидатором. Это обеспечивает сквозную защиту системы NEA, которая может включать транзитные среды и переходить через границы доверия.

PA-6 Протокол PA **должен** обеспечивать возможность передачи атрибутов, содержащих двоичные и иные данные, включая шифрованные.

7.3. Требования к протоколу PB

Протокол PB поддерживает мультиплексирование сообщений Posture Attribute (протокол PA) между сборщиками состояний на клиенте NEA и валидаторами на сервере NEA (в обоих направлениях).

Протокол PB передает клиентскому брокеру глобальное решение об оценке, принятое серверным брокером, с учетом результатов валидаторов, участвовавших в оценке.

Протокол PB также агрегирует и доставляет рекомендации и уведомления, такие как инструкции по исправлению(например, ссылки на обновления) от одного или нескольких валидаторов.

Требования к PB приведены ниже

PB-1 Протокол PB **должен** поддерживать передачу атрибутов от серверного брокера клиентскому. Это позволяет клиентскому брокеру получить решение по результатам оценки и, если это применимо, рекомендации и уведомление для владельца конечной точки.

PB-2 Протоколу PB **недопусимо** интерпретировать содержимое передаваемых сообщений PA (т. е. данные в сообщениях должны быть «непрозрачны» для протокола).

PB-3 Протокол PB **должен** передавать уникальный идентификатор, используемый брокерами для маршрутизации (доставки) сообщений PA между сборщиками состояний и валидаторами. Эта маршрутизация сообщений должна способствовать динамической регистрации и дерегистрации сборщиков состояний и валидаторов. Например, динамически регистрируемому антивирусному сборщику состояний следует поддерживать подписку для получения сообщений от соответствующих сборщиков состояний на клиентах NEA.

PB-4 Протокол PB **должен** обеспечивать возможность поддержки полудуплексного протокола PT. Однако это не препятствует работе PB в полнодуплексном режиме при полнодуплексном протоколе PT.

PB-5 Протокол PB **может** поддерживать защиту подлинности, целостности и конфиденциальности атрибутов, передаваемых между клиентским и серверным брокером. Это позволяет защитить обмен группами сообщений с атрибутами между клиентским и серверным брокером. Эта защита независима от защиты PA (которая является сквозной) и позволяет реализовать более простые сборщики состояний и валидаторы, а также консолидировать криптографические операции для улучшения расширяемости и управляемости.

PB-6 Протокол PB **должен** поддерживать группировку сообщений с атрибутами для оптимизации доставки сообщений и снижения числа обменов.

7.4. Требования к протоколу PT

Транспортный протокол PT обеспечивает обмен сообщениями протокола PB между клиентом и сервером Posture Transport. PT отвечает за обеспечение защищенного транспорта для протокола PB. Сам протокол PT может транспортироваться в одной или нескольких объединенных (конкатенация) сессиях протокола нижележащего уровня (например, 802.1X, RADIUS [RADIUS], TLS, IKE).

В этом параграфе приведены требования, которые должны выполнять протоколы, являющиеся кандидатами в PT.

PT-1 Протоколу **недопустимо** интерпретировать содержимое передаваемых сообщений PB (т. е. передаваемые данные должны быть «непрозрачны» для протокола).

PT-2 Протокол PT **должен** обеспечивать возможность поддержки взаимной аутентификации, а также защиту целостности и конфиденциальности сообщений PB между клиентом и сервером Posture Transport.

PT-3 Протокол PT **должен** обеспечивать надежную доставку для протокола PB, включая возможность фрагментации и сборки, обнаружение дубликатов и нарушения порядка, если это требуется.

PT-4 Протоколу PT **следует** обеспечивать возможность работы и имеющимися протоколами доступа в сеть, такими как 802.1X и IKEv2.

PT-5 Протоколу PT **следует** обеспечивать возможность обмена между клиентом и сервером NEA по протоколу TCP или UDP (подобно LDAP[1]).

[1]Lightweight Directory Access Protocol - облегченный протокол доступа к службам каталогов.

8. Вопросы безопасности

Этот документ задает функциональные требования к протоколам PA, PB и PT, используемым при оценке конечных точек (NEA). Поэтому здесь не задан конкретный стек протоколов или набор технологий. В результате данный раздел посвящен вопросам безопасности NEA в целом и отдельных аспектов эталонной модели NEA.

Хотя многие темы выходят за рамки рабочей группы NEA и, следовательно, данной спецификации (см. параграф 3.1), важно обеспечить защиту этих механизмов от атак. Например, методы запуска оценки или переоценки выходят за рамки документа, но они должны быть надежно защищены от атак (например, от сокрытия злоумышленником события, указывающего на изменение политики сервера NEA).

NEA намеревается облегчить обнаружение и исправление взаимодействующих конечных точек в соответствии с принятой в сети политикой. Например, предполагается, что эти правила позволят разработчикам обнаруживать устаревшие, неактивные или отсутствующие механизмы защиты на конечной точке, что может делать ее более уязвимой для известных атак. Если конечная точка более уязвима, рискованно иметь такую точку в сети вместе с другими ценными активами. Заранее оценивая взаимодействующие конечные точки при их подключении к сети, можно существенно повысить их устойчивость к атакам еще до допуска в сеть. Точно так же повторная оценка взаимодействующих конечных точек сети может помочь для обеспечения использования механизмов защиты, соответствующих свежей политике сети.

NEA полностью признает, что не все конечные точки будут взаимодействовать, предоставляя свое реальное состояние (или вообще состояние). Причиной этого могут быть вредоносные программы, влияющие на клиентов NEA или правила, что делает достоверную оценку невозможной. Такая ситуация может привести к допуску в сеть конечной точки, представляющей угрозу для сети и других конечных точек, несмотря на прохождение проверки NEA.

8.1. Доверие

NEA включает оценку состояния конечных точек, входящих или уже находящихся в сети, на предмет соответствия правилам, чтобы убедиться в их адекватной защите. Поэтому конечные точки должны считаться недоверенными, пока нет оснований полагать (на основе данных о состоянии), что они защищены от угроз, устраняемых политикой соответствия, и не будут распространять угроз другим конечным точкам. На стороне сетевого провайдера обычно предполагается, что клиент NEA доверяет сетевой инфраструктуре в части злоупотреблений раскрытой информацией о состоянии (см. раздел 9) и какими-либо инструкциями, предоставляемыми конечной точке. Клиент NEA обычно должен быть уверен в том, что сервер NEA будет запрашивать лишь информацию для определения безопасности разрешения конечной точке доступа к сетевым активам.

Между клиентом и сервером NEA имеется сеть, которая не считается доверенной. Поэтому мало что в этой сети считается заслуживающим доверия, кроме ее готовности и возможности своевременно доставлять сообщения в процессе обмена ими. Уровень доверия к каждому элементу эталонной модели NEA зависит от реализации. Рабочая группа NEA намеревается предоставить механизмы защиты для снижения уровня доверия, который должен предполагаться разработчиком. Эти вопросы более подробно рассмотрены в последующих параграфах.

8.1.1. Конечная точка

Для правильной работы NEA конечные точки должны быть доверенными, чтобы точно представить запрашиваемое состояние защиты серверу NEA. Согласно уставу рабочей группы NEA, эталонная модель NEA не задает явно способ обнаружения или предотвращения ложных конечных точек, намеренно искажающих свое состояние. Точно так же обнаружение вредоносных программ (например, rootkit), которые могут обмануть сборщики состояний, возвращая некорректные данные, является предметом исследований и стандартизации вне IETF (например, в Trusted Computing Group [TCG]) и не рассматривается в модели. Однако при использовании таких механизмов в реализации, эталонная модель NEA должна быть способна приспособить эти технологии, позволяя им взаимодействовать по протоколу PA с валидаторами или работать независимо для защиты клиентов NEA от атак и обеспечения возможности сборщикам видеть корректное состояние.

Помимо необходимости доверять целостности клиента NEA и его способности точно собрать и передать атрибуты состояния конечной точки, мы пытаемся не использовать другое предполагаемое доверие. Большинство моделей использования NEA предполагает отправку информации о состоянии на сервер NEA для оценки и принятия решения. При использовании защиты на уровне PA и/или PT конечная точка должна доверять целостности и возможно конфиденциальности данных привязки доверия (например, сертификатам открытых ключей), используемых сборщиком состояний и/ли транспортным клиентом. Однако реализации NEA могут выбрать отправку или предварительную подготовку неких правил конечной точке для оценки, обеспечивающих повышение доверия. В таких случаях сервер NEA должен верить, что механизмы хранения, оценки и информирования в конечной точке не фальсифицируют результаты оценки соответствия.

Как правило, конечной точке не следует доверять сетевым коммуникациям (например, входящим запросам на соединение), пока это доверие не было специально разрешено пользователем или владельцем (через политику или действие). Эталонная модель NEA предполагает размещение клиента NEA целиком на конечной точке. Незапрошенные соединения из сети должны проверяться обычными механизмами защиты хоста (например, брандмауэр, протоколы защиты IDS/IPS[1] и т. п.). Коммуникации, связанные с оценкой или переоценкой NEA, требуют некоторого уровня доверия особенно при их инициировании сервером NEA (переоценка). Уровень доверия моет быть ограничен за счет применения строгой защиты сообщений в соответствии с требованиями сети и политикой конечной станции/пользователя.

8.1.2. Сетевые коммуникации

Между клиентом и сервером NEA может присутствовать много разнотипных устройств, обеспечивающих коммуникационный путь. Некоторые из промежуточных устройств (например, простые коммутаторы L2), которые способны наблюдать и изменять передаваемые сообщения. Промежуточные устройства можно разделить на несколько категорий по влиянию на уровень доверия к операциям.

[1]Intrusion Detection/Prevention System - система обнаружения/предотвращения вторжений.

Во-первых, некоторые промежуточные устройства участвуют в пересылке сообщение или поддержке PT (например, коммутаторы L2, маршрутизаторы L3). Предполагается, что эти устройства не отбрасывают сообщений и не предпринимают попыток активно препятствовать (например, DoS-атака[2]) развертыванию NEA.

Во-вторых, некоторые промежуточные устройства могут быть частью уровня управления доступом в сеть т поэтому им доверяется исполнение политики, включая исправление, изоляцию и контроль доступа, предоставляемые им по результатам оценки NEA. Эти устройства могут также играть другие роли, описанные в этом разделе.

В-третьих, некоторые устройства могут служить точкой завершения или прокси для транспортного протокола PT. Часто предполагается, что базовый протокол для PT завершается на клиенте и сервере NEA, которые оказываются точками завершения PT. Если в реализации это не выполняется, приходится доверять устройствам завершения в части аккуратной и точной передачи сообщений PT следующему протоколу оператора (например, при переходе внутренних сообщений метода EAP [EAP] из туннеля EAP в сессию RADIUS).

В-четвертых, инфраструктура многих сетей включает такие устройства, как IDS/IPS, которые отслеживают и исправляют подозрительное поведение в сети. Эти устройства могут быть связаны с сервером NEA, но этот вопрос выходит за рамки спецификации. Устройства, которым сервер NEA доверяет предоставление данных о защите, которые могут влиять на принимаемое сервером решение, предполагаются доверенными и не вынуждающими сервер NEA принимать некорректные решения.

Кроме того, между клиентом и сервером NEA могут размещаться другие типы сетевых устройств для обслуживания задач, выходящих за пределы NEA. Эти устройства могут быть способны пассивно перехватывать трафик, архивировать данные для последующего применения (например, повторное использование - replay или нарушение конфиденциальности), а также активно влиять на работу протоколов NEA. Поскольку эти устройства напрямую не участвуют в работе NEA, важно при развертывании NEA не доверять слепо таким устройствам в части обеспечения корректной работы NEA. Поэтому протоколы NEA должны обеспечивать защиту, чтобы такие устройства не могли украсть, изменить, подделать данные или иным способом воздействовать на обмен сообщениями.

8.1.3. Сервер NEA

Серверу NEA (включая возможные удаленные системы, обеспечивающие услуги проверки состояния) обычно доверяют исполнение заданных правил состояния, поэтому он должен быть защищен. Важно обеспечить для серверов NEA надежную защиту от различных атак со стороны сети и конечных точек.

Хотя приходится в той или иной степени доверять работе сервера NEA, нужна строгая защита, анализ и мониторинг сети и внутренних процессов сервера. Сетевые коммуникации могут быть подвержены таким атакам на предоставление политики из систем управления правилами, а также базовые протоколы защиты и управления сетью. Примерами защиты внутренних процессов могут служить защита от вредоносных программ на сервере NEA, защита внутренней логики сервера, а также хранилища данных (особенно в части, способной влиять на принимаемые решения и их исполнение). Сервер NEA должен доверять базовым протоколам NEA и сетевым протоколам нижележащих уровней в части корректного поведения и надлежащей защиты обмена сообщениями с конечными точками. Эталонная модель NEA не пытается решать вопросы защиты целостности операционной системы и других программ, поддерживающих работу сервера NEA.

Интересным примером является физическое разделение сервера NEA между разными системами. Это может происходить в тех случаях, когда валидатор (или используемый им удаленный сервер) размещается отдельно от серверного брокера. Точно так же серверный брокер может быть физически отделен от сервера транспорта. При наличии такого физического разделения коммуникации между удаленными компонентами сервера NEA должны гарантировать устойчивость сессий PB и обмена сообщениями PA к активным и пассивным атакам, в частности от перехвата, поддержки и повторного использования. Аналогично, для валидаторов может быть желательно минимизировать свое доверие к серверному брокеру помимо его способности должным образом передавать и доставлять сообщения PA. Валидаторы могут реализовать сквозную защиту PA с проверкой подлинности, целостности и конфиденциальности обмена сообщениями PA. При использовании защиты PA каждый валидатор должен иметь возможность доверять целостности и (возможно) конфиденциальности своих правил привязки доверия.

8.2. Механизмы защиты на разных уровнях

Неотъемлемой частью требований является стремление к тому, чтобы все протоколы-кандидаты для NEA в эталонно модели были способны обеспечить механизмы строгой защиты, требуемые конкретным развертыванием. В некоторых случаях может показаться, что эти механизмы дублируют друг друга. Такие очевидные наложения могут служить для обеспечения более эшелонированной защиты. Однако многоуровневая структура протоколов позволяет реализовать несколько различающиеся возможности защиты и уровни детализации.

Например, разработчик может шифровать трафик на уровне PT для защиты от некоторых форм анализа или перехвата. Дополнительно могут также шифроваться некоторые сообщения, содержащие оценку конечных точек, для обеспечения сквозной защиты конфиденциальности соответствующих валидаторов. В частности, это может быть желательно при размещении валидаторов отдельно от сервера NEA, когда информация передается через дополнительные сегменты сети, а также для обеспечения валидаторам возможности проверить подлинность сборщика состояний (и наоборот).

Разные варианты и среды применения технологий NEA будут вероятно влиять на выбор механизмов защиты. Целью требований NEA является поощрение выбора технологий и протоколов, способных обеспечить требуемый уровень защиты для самых разных вариантов оценки состояния.

8.3. Классы атак

Возможно множество разных атак для протоколов и технологий оценки NEA. В этом параграфе не приводится полного анализа безопасности, но рассмотрено несколько типов атак, которые повлияли на выбор требований и должны учитываться при развертывании путем выбора подходящих механизмов защиты в рамках эталонной модели NEA.

[2]Denial of service - отказ в обслуживании.

Как уже говорилось, имеется множество защитных механизмов, включенных в требования для протоколов-кандидатов в NEA. Различные среды и варианты применения могут вынудить разработчиков к отказу от использования некоторых механизмов, однако это следует делать с осознанием того, что отказ может открывать уязвимость для некоторых типов атак. Как всегда, следует учитывать баланс между риском, производительностью, удобством использования, управляемостью и другими факторами.

Ниже описаны типы атак, применимых к сетевым протоколам, которые определены в эталонной модели. Эти атаки следует учитывать при разработке.

8.3.1. Перехват с участием человека (MITM)

MITM[1]-атаки на сетевой протокол возникают в тех случаях, когда посторонние могут подключиться к сетевой среде между отправителем и получателем, перехватывая и изменяя трафик между ними. Например, зараженная вредоносным кодом система может подключиться к сети и повторно использовать пакеты оценки состояния, перехваченные от чистой системы, подключающейся к сети. Это может произойти, когда система включается в диалог и выступает в качестве активного посредника в диалоге сообщений. Воздействие MITM-атак можно предотвратить или ослабить путем выбора подходящих методов защиты протоколов.

Например, требования для PT поддерживать взаимную аутентификацию до начала диалога с конечной точкой не позволит злоумышленнику незаметно включиться в качестве активного участника (прокси), если у него нет учетных данных участников диалога, позволяющих представиться легитимным участником. Многократно используемые учетные данные не следует раскрывать в сети, чтобы организаторы MITM-атак не могли ими воспользоваться для обмана. Требование к PT обеспечивать защиту конфиденциальности (шифрование) вместе с упомянутой выше проверкой подлинности предотвращает пассивные MITM-атаки за счет перехвата и сохранения значений проверки состояния для последующего использования. Требование к PT в части предотвращения повторного использования (replay) предотвращает пассивные MITM-атаки путем организации новых сессий (или захвата имеющейся) и использования ранее перехваченного обмена сообщениями.

С помощью активной MITM-атаки злоумышленник может прикинуться «чистой» конечной точкой и представить ее данные оценки состояния серверу NEA. Например, злоумышленник может подключиться к серверу NEA и корректно представиться ему, а когда сервер запросит данные состояния, злоумышленник может запросить эти данные у чистой конечной точки. Если такая точка доверяет атакующему в плане запроса переоценки и готова поделиться запрошенными данными, злоумышленник может получить требуемую оценку состояния и передать ее серверу NEA. Для предотвращения этой формы MITM-атак протоколам NEA следует обеспечивать строгую (криптографическую) привязку данных оценки состояния к аутентифицированной сессии с сервером NEA, чтобы сервер знал, что сведения получены от проверенной конечной точки. Такая строгая привязка вполне возможна и рабочей группе NEA следует предпочитать ее.

8.3.2. Изменение сообщений

Без защиты целостности сообщений злоумышленники, способные перехватывать сообщения, смогут менять их содержимое и вынуждать к принятию некорректных решений. Например, атакующий может изменить атрибуты оценки состояния, указав в них некорректные значения, что не позволит соответствующей требованиям системе подключиться к сети. Если сервер NEA не сможет обнаружить такую подмену, атакующему удастся заблокировать доступ в сеть большому числу «чистых» систем. И наоборот, злоумышленник может обеспечить подключение к сети системы, зараженной вредоносными программами, изменяя передаваемые атрибуты оценки состояния для сокрытия вредоносных программ от валидаторов. Злоумышленник может также заразить вредоносными программами «чистые» системы путем передачи инструкций по установке вредоносного кода или отключению механизмов защиты.

Для защиты от таких атак в PT включено требование строгой защиты целостности (например, с помощью защищенных хэш-значений, таких как HMAC[2] [HMAC]), чтобы любое изменение сообщения можно было заметить. В PA включено аналогичное требование для обеспечения сквозной защиты целостности атрибутов, расширяющей защиту на весь путь до валидаторов даже при их размещении отдельно от серверов NEA.

Важно применять в схемах защиты целостности свежую секретную информацию (неизвестную злоумышленникам), которая привязана к аутентифицированной сессии. Это может быть, например, HMAC с использованием производного свежего секрета, связанного с сессией. Включение информации о свежести позволяет участникам защититься от некоторых атак с повтором сообщений, использующих секретную информацию из прежних сессий.

8.3.3. Повторное использование сообщений или кража атрибутов

Злоумышленник может прослушивать сеть, записывать сообщения или атрибуты от соответствующих правилам конечных точек для последующего использования с тем же сервером NEA или просто «инвентаризации» программ на других системах с целью поиска уязвимостей в них. Сервер NEA должен быть способен обнаружить попытки повторного использования данных состояния и/или модель должна обеспечивать защиту такой информации от перехвата. Поэтому протокол PT должне защищать конфиденциальность и предотвращать повторное использование.

Криптографическая защита от раскрытия сообщений PT, PB, PA не позволяет при пассивной атаке видеть содержимое сообщений, а также препятствует их последующему повторному использованию. Однако активный атакующий может повторно использовать шифрованное сообщение, если оно не связано надежно с создавшей его стороной или сеансом обмена. Привязка обмена зашифрованными сообщениями к проверке подлинности или использование свежей информации в каждой сессии и обмена ключами предотвращает возможность повторного использования сообщений.

8.3.4. Другие типы атак

В этом параграфе не представлен полный список возможных атак для эталонной модели NEA. Некоторые типы атак будет проще понять и проанализировать после того, как рабочая группа NEA выпустит спецификации выбранных технологий и протоколов для применения в NEA. Одним из таких типов являются DoS-атаки. В данный момент не

[1]Man-in-the-Middle.
[2]Hashed Message Authentication Code - хэшированный код проверки подлинности сообщения.

имеет смысла пытаться определить все возможные воздействия на протоколы NEA, поэтому такой анализ следует включать в раздел «Вопросы безопасности» выбираемых протоколов NEA.

Важно обеспечить устойчивость сервера NEA к DoS-атакам, поскольку такие атаки могут воздействовать на большое число конечных точек, желающих подключиться или остаться в сети. Эталонная модель NEA предполагает, что протокол PT будет обеспечивать ту или иную степень устойчивости к DoS-атакам, а протоколы PA и PB будут опираться на нее и использовать свою защиту. Для снижения фронта возможных атак неуполномоченных сторон предполагается использованием серверами NEA протоколов PT с упреждающей взаимной аутентификацией запрашивающих конечных точек как одного из механизмов фильтрации атак.

Для происходящих после проверки подлинности атак известно по меньшей мере то, что их источники владеют действующими свидетельствами и могут быть привлечены к ответственности. Точно так же протоколам NEA следует обеспечивать строгую защиту от повторного использования для предотвращения DoS-атак на основе таких сессий и сообщений. Оценки соответствия следует строго привязывать к транспортной аутентификации, чтобы гарантировать происхождение данных оценки от полномочной стороны. Следует применять криптографические механизмы и иные ресурсоемкие средства с осторожностью, пока не будет подтверждена достоверность запроса. Эти и другие атаки на протоколы и ресурсы можно будет оценить точнее после выбора технологий NEA и применяемой ими криптографии.

9. Приватность

Несмотря на многочисленные преимущества применения технологий NEA для организаций и сетевых операторов, владеющих сетями, которые предоставляют услуги конечным точкам, эти же технологии могут быть использованы для злоупотреблений и вторжения в частную жизнь в случаях неподобающего применения. В этом разделе рассматриваются несколько возможных проблем нарушения приватности в результате развертывания технологии и даны некоторые рекомендации для разработчиков.

Технология NEA позволяет видеть конфигурацию конечной точки из сети. Такая «прозрачность» позволяет сети учитывать надежность защитных механизмов конечной точки при решении вопроса о ее доступе к сетевым ресурсам. Однако это можно использовать также для обеспечения ограничительных правил в ущерб пользователям, ограничивая им выбор программ или пытаясь изучить прошлое и настоящее использование конечной точки.

Область действия рабочей группы NEA была ограничена спецификацией протоколов, нацеленных на варианты использования, где конечные точки и сеть принадлежат одной организации или владельцы конечных точек четко указали согласие с раскрытием информации владельцу сети. Это знакомая модель работы для правительственных организаций, учреждений и многочисленных предприятий, предоставляющих оборудование (конечные точки) для выполнения работы своим сотрудникам. В большинстве этих случаев конечная точка приобретается организацией и принадлежит ей, которое часто оставляет за собой право аудита конечных точек и указания правил использования этих устройств. Технологии NEA позволяют автоматизировать проверку содержимого конечной точки и эти данные могут быть привязаны к механизмам управления доступом в сеть для ограничения использования конечной точки в соответствии правилами соответствия.

В таких средах уровень защиты приватности сотрудников может быть существенно снижен локальными правилами и обычаями. Однако в ситуациях, когда конечная точка принадлежит пользователю или местное законодательство защищает права пользователей даже при использовании чужих конечных точек, важно, чтобы реализация NEA позволяла пользователям контролировать распространение данных конечной точки по сети. Такие меры контроля, организованные пользователем могут блокировать или ограничивать доступ к некоторым ресурсам сети или защищенным ресурсам, но это должно быть выбором пользователя.

9.1. Вопросы реализации

Рабочая группа NEA не задает стандарты содержимого правил для клиентов NEA и не определяет требований к аспектам реализации сверх сетевых протоколов, однако приведенные ниже рекомендации помогут реализовать сохраняющие приватность системы для более широкого использования, чем рассмотренная выше корпоративная реализация.

Реализациям клиентов NEA рекомендуется предоставлять пользователю возможность согласиться с политикой подключения до предоставления в сеть данных с оценкой состояния конечной точки. Механизм согласия следует делать селективным для каждого пользователя и сервера NEA, чтобы пользователь мог контролировать, какие сети могут получить доступ к информации о его системе. Для сетей, которым открыт доступ к конечной точке, пользователю следует предоставить возможность задать ограничения для раскрываемых данных и атрибутов. Реализациям валидаторов не рекомендуется использовать принятое по умолчанию поведение на основе шаблонных запросов, которые могут приводить к избыточному раскрытию информации (9.2. Минимизация раскрытия атрибутов). Вместо этого валидаторам рекомендуется по умолчанию запрашивать лишь конкретные атрибуты, требуемые для оценки системы.

Запросы атрибутов, которые не разрешены явно (или запрещены) для передачи в сеть, должны приводить к уведомлению пользователя и/или записи в системный журнал, чтобы пользователь мог оценить, делает ли служба что-либо нежелательное т хочет ли он делиться запрашиваемой информацией через сеть для получения доступа. В некоторых решениях могут применяться (на основе правил) приглашения пользователям на предоставление запрашиваемой сервером информации для оценки состояния конечной точки (с описанием этих данных) еще до отправки серверу NEA.

Предполагается, что владелец конечной точки имеет возможность задать правила раскрытия информации, которые могут переопределять или изменять политику пользователя в части раскрытия атрибутов в сеть. Если политика раскрытия информации от владельца позволяет передать больше информации, нежели политика пользователя, реализации следует обеспечивать механизм обратной связи, позволяющий пользователю понять ситуацию и принять решение об использовании конечной точки в таких обстоятельствах.

В таких системах важно обеспечить для пользовательского интерфейса управления политикой простоту понимания и четкость формулировок в правилах раскрытия информации, включая учет политики владельца конечной точки. Пользователь должен быть в состоянии понять, какое состояние приемлемо для сети и какое влияние может иметь раскрытие этих данных. Для уменьшения списка перечисляемых ограничений следует использовать по умолчанию

консервативную политику раскрытия, такую как «запрещено раскрытие чего-либо, не разрешенного явно». Это позволит избежать непреднамеренной утечки информации.

Реализациям серверов NEA следует предоставлять новым абонентам (пользователям конечных точек) заявление о раскрытии информации, в котором четко указаны:

- требуемая для доступа в сеть информация;
- использование и защита предоставленных данных;
- применимые локальные правила защиты приватности.

Эта информация позволит абонентам принять решение о приемлемости раскрытия запрашиваемой информации с учетом местных законов и обычаев.

9.2. Минимизация раскрытия атрибутов

Одним из важных вопросов при разработке эталонной модели и протоколов NEA является предоставление конечным точкам возможности минимального раскрытия информации, требуемой в соответствии с политикой сети. Можно рассмотреть несколько моделей организации набора раскрываемых атрибутов, каждая из которых имеет свои преимущества и недостатки в части приватности пользователей, разработчикам следует принимать их во внимание. В этом параграфе кратко описаны три возможных модели раскрытия атрибутов в NEA и некоторые последствия такого раскрытия для приватности в рамках каждой модели.

Первая модель проста в реализации и развертывании, но в ней есть проблемы конфиденциальности и могут также возникать проблемы с задержками и расширяемостью. В этой модели по умолчанию локальная политика диктует отправку всех известных атрибутов NEA Posture при оценке конечной точки. Это может упростить развертывание, но ведет к передаче большого объема информации, которая может быть не связана с оценкой состояния защиты в системе и даже раскрывать те или иные приватные сведения. Например, нужно ли предприятию при оценке защищенности системы знать об использовании в системе Firefox, а не иного браузера?

Во второй модели используется предоставление всем конечным точкам политики раскрытия информации по отдельному каналу до подключения к сети. Эта модель может включать заданную предприятием политику, в соответствии с которой нужно предоставить определенный набор атрибутов в процессе обмена NEA. Правила конфиденциальности конечной точки могут фильтровать этот список атрибутов, но отказ от предоставления того или иного атрибута может воспрепятствовать получению конечной точкой доступа в сеть или к определенным ресурсам. Эта модель упрощает сетевой обмен, поскольку конечные точки всегда передают отфильтрованный набор атрибутов при подключении к сети. Однако для реализации модели требуется дополнительный протокол управления без использования сети, позволяющий организовать и поддерживать правила раскрытия информации NEA для всех систем.

В третьей модели исключена необходимость предварительной передачи политики раскрытия за счет использования серверами NEA специальных запросов с указанием требуемых атрибутов. Это напоминает политику, используемую в процессе обмена сообщениями NEA, которой достаточно просто управлять. Модель позволяет серверу NEA итеративно запрашивать атрибуты на основе значений предыдущих атрибутов. Отметим, что даже в этой модели от протоколов NEA не ожидается поддержки языка запросов общего назначения. Она скорее позволяет серверу NEA запрашивать конкретные атрибуты по заданному политикой списку. Например, предприятие может запрашивать версию ОС в первом сообщении диалога и после получения ответа об использовании ОС Linux запрашивать один набор атрибутов, в для Windows - другой. Предполагается, что это позволит минимизировать набор передаваемых через сеть атрибутов, если оценивается достаточно сложная система (например, определяется набор установленных обновлений ОС).

В каждой модели пользователь может создать набор правил фильтрации, применяемых клиентом NEA для предотвращения раскрытия атрибутов, которые являются приватными по своей природе или не относятся к конкретной сети. Такие фильтры будут защищать приватность пользователя, но могут приводить к ограничению доступа в сети или к определенным ресурсам.

10. Литература

10.1. Нормативные документы

[UTF8] Yergeau, F., "UTF-8, a transformation format of ISO 10646", STD 63, RFC 3629, November 2003.

10.2. Дополнительная литература

[802.1X] IEEE Standards for Local and Metropolitan Area Networks: Port based Network Access Control, IEEE Std 802.1X-2001, June 2001.

[CNAC] Cisco, Cisco's Network Admission Control Main Web Site, http://www.cisco.com/go/nac

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

[HMAC] Krawczyk, H., Bellare, M., and R. Canetti, "HMAC: Keyed-Hashing for Message Authentication", RFC 2104, February 1997.

[IPSEC] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, December 2005.

[NAP] Microsoft, Network Access Protection Main Web Site, http://www.microsoft.com/nap

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

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

[TCG] Trusted Computing Group, Main TCG Web Site, http://www.trustedcomputinggroup.org/

[TNC] Trusted Computing Group, Trusted Network Connect Main Web Site, https://www.trustedcomputinggroup.org/groups/network/

11. Благодарности

Авторы документа благодарят членов рабочей группы NEA, внесших свой вклад в подготовку предшествующих документов в части идентификации проблемы и разработки требований, оказавших влияние на данную спецификацию, Kevin Amorin, Parvez Anandam, Diana Arroyo, Uri Blumenthal, Alan DeKok, Lauren Giroux, Steve Hanna, Thomas Hardjono, Tim Polk, Ravi Sahita, Joe Salowey, Chris Salter, Mauricio Sanchez, Yaron Sheffer, Jeff Six, Susan Thompson, Gary Tomlinson, John Vollbrecht, Nancy Winget, Han Yin, Hao Zhou.

Адреса авторов

Paul Sangster
Symantec Corporation
6825 Citrine Dr
Carlsbad, CA 92009 USA
Phone: +1 760 438-5656
EMail: Paul_Sangster@symantec.com

Hormuzd Khosravi
Intel
2111 NE 25th Avenue
Hillsboro, OR 97124 USA
Phone: +1 503 264 0334
EMail: hormuzd.m.khosravi@intel.com

Mahalingam Mani
Avaya Inc.
1033 McCarthy Blvd.
Milpitas, CA 95035 USA
Phone: +1 408 321-4840
EMail: mmani@avaya.com

Kaushik Narayan
Cisco Systems Inc.
10 West Tasman Drive
San Jose, CA 95134
Phone: +1 408 526-8168
EMail: kaushik@cisco.com

Joseph Tardo
Nevis Networks
295 N. Bernardo Ave., Suite 100
Mountain View, CA 94043 USA
EMail: joseph.tardo@nevisnetworks.com

Перевод на русский язык

Николай Малых

nmalykh@protokols.ru

Полное заявление авторских прав

или пользователями этой спецификации, можно получить из сетевого репозитория IETF IPR по ссылке http://www.ietf.org/ipr.

IETF предлагает любой заинтересованной стороне обратить внимание на авторские права, патенты или использование патентов, а также иные права собственности, которые могут потребоваться для реализации этого стандарта. Информацию следует направлять в IETF по адресу ietf-ipr@ietf.org.