(19) Евразийское патентное ведомство

(11) 037617 (13) B1

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ЕВРАЗИЙСКОМУ ПАТЕНТУ

(45) Дата публикации и выдачи патента
2021.04.22

(21) Номер заявки
201490333

(22) Дата подачи заявки
2012.07.26

(51) Int. Cl. *H04L 29/06* (2006.01)

(54) СПОСОБ И СИСТЕМА ДЛЯ ОБНАРУЖЕНИЯ НЕСАНКЦИОНИРОВАННОГО ВТОРЖЕНИЯ В ТРАФИК ДАННЫХ В СЕТИ ПЕРЕДАЧИ ДАННЫХ

(31) **2007180; 61/511,685**
(32) **2011.07.26**
(33) **NL; US**
(43) **2014.06.30**
(86) **PCT/NL2012/050537**
(87) **WO 2013/015691 2013.01.31**

(71)(73) Заявитель и патентовладелец:
СЕКЬЮРИТИ МЭТТЕРС Б.В. (NL)

(72) Изобретатель:
Цамбон Эммануэле (NL)

(74) Представитель:
Медведев В.Н. (RU)

(56) US-A1-2011167493
WO-A2-2005047862
US-A1-2007239999

(57) Способ и электронно-вычислительное устройство для обнаружения несанкционированного вторжения в трафик данных сети передачи данных, при этом способ содержит этапы, на которых синтаксически анализируют трафик данных для извлечения по меньшей мере одного поля протокола сообщения протокола трафика данных; ассоциируют извлеченное поле протокола с моделью для данного поля протокола, причем модель выбирают из набора моделей; оценивают, находится ли содержимое извлеченного поля протокола в безопасной области, как определено моделью; и генерируют сигнал обнаружения вторжения в случае, когда установлено, что содержимое извлеченного поля протокола находится за пределами безопасной области. Набор моделей может содержать соответствующую модель для каждого поля протокола из набора полей протокола.

037617 B1

037617 B1

Область техники, к которой относится изобретение

Изобретение относится к области сетей передачи данных, в частности к области классифицирования сообщений в сетях передачи данных, например для обнаружения вредоносных вторжений в таких сетях передачи данных.

Уровень техники

Во многих сетях передачи данных разворачиваются системы обнаружения для обнаружения вредоносных вторжений. Такие вторжения содержат данные источника атаки или зараженных компьютеров, которые могут оказать воздействие на работу серверов, компьютеров или иного оборудования.

Существует два основных типа таких систем обнаружения вторжения: системы обнаружения вторжения, основанные на сигнатуре и основанные на аномалии.

Основанные на сигнатуре системы обнаружения вторжения (SBS) основываются на методиках сопоставления с образцом. Система содержит базу данных сигнатур, т.е., последовательности данных, которые известны по атакам в прошлом. Эти сигнатуры сопоставляются с тестируемыми данными. Когда найдено совпадение, вызывается оповещение о тревоге. Требуется обновление базы данных сигнатур экспертами после идентификации новой атаки.

В отличие от этого, основанная на аномалии система обнаружения вторжения (ABS) сначала строит статистическую модель, описывающую нормальный сетевой трафик во время так называемой "фазы обучения". Затем, во время так называемой "фазы тестирования" система анализирует данные и классифицирует любой трафик или действие, которое значительно отличается от модели, как атаку. Преимущество основанной на аномалии системы состоит в том, что она может обнаружить атаки нулевого дня, т.е. атаки, которые как таковые еще не были идентифицированы экспертами. Для обнаружения наибольшего количества атак, ABS требуется инспектировать полезную нагрузку сетевого трафика.

Существующие способы основаны на анализе n-грамм, который либо применяется к (необработанной) полезной нагрузке пакета, либо к ее частям.

Тем не менее, в некоторых сетях передачи данных вредоносные данные очень похожи на допустимые данные. Это может иметь место в так называемой сети SCADA (Диспетчерское Управление и Сбор Данных) или другой Сети Управления Производственным Процессом. В SCADA или сети Управления Производственным Процессом осуществляется обмен сообщениями протокола между компьютерами, серверами и иным оборудованием на прикладном уровне сети передачи данных. Эти сообщения протокола могут содержать инструкции для управления машинами. Сообщение протокола с вредоносной инструкцией ("установить частоту вращения равной 100 об/мин") может быть очень похоже на допустимую инструкцию ("установить частоту вращения равной 10 об/мин").

Когда вредоносные данные очень похожи на допустимые данные, вредоносные данные могут быть классифицированы основанной на аномалии системой обнаружения вторжения как нормальные или допустимые данные, что может подвергать опасности работу компьютеров, серверов и иного оборудования в сети.

Сущность изобретения

Цель изоб**р**етения может состоять в предоставлении усовершенствованной системы и/или способа обнаружения вторжения.

В соответствии с аспектом изобретения, предоставляется способ обнаружения вторжения для обнаружения вторжения в трафике данных сети передачи данных, при этом способ содержит этапы, на которых

синтаксически анализируют трафик данных для извлечения по меньшей мере одного поля протокола сообщения протокола трафика данных;

ассоциируют извлеченное поле протокола с соответствующей моделью для данного поля протокола, причем модель выбирается из набора моделей;

оценивают, находится ли содержимое извлеченного поля протокола в безопасной области, как определяется моделью; и

генерируют сигнал обнаружения вторжения в случае, когда установлено, что содержимое извлеченного поля протокола находится за пределами безопасной области.

Синтаксический анализ трафика данных позволяет различать отдельные поля протокола ("именуемые как "поля протокола"), в соответствии с которыми имеет место передача данных по сети данных. Затем создается ассоциация (если успешно) между этим полем ("полем протокола") и моделью. Для этой цели предоставляется набор моделей. Выбирается подходящая модель для извлеченного поля протокола, как будет более подробно объяснено ниже. Затем поле протокола оценивается с использованием модели, чтобы установить, находится ли содержимое поле протокола в нормальной, безопасной, приемлемой области или нет. В последнем случае, может быть выполнено подходящее действие. Посредством синтаксического анализа сообщения протокола можно различать отдельные поля протокола трафика данных, и может быть выбрана подходящая модель для оценки данного конкретного поля протокола. Тем самым, может быть выполнена адекватная оценка, поскольку разные поля протокола могут быть оценены с применением разных моделей, например каждое поле протокола - с применением соответствующей модели, которая приспособлена для данного конкретного поля протокола, например с применением модели, ко-

торая приспособлена для типа поля протокола и/или содержимого. Способ обнаружения вторжения в соответствии с изобретением может быть реализуемым компьютером способом обнаружения вторжения. Блок синтаксического анализа (т.е. синтаксический анализ) может использовать предварительно определенную спецификацию протокола. Также, например, в случае, когда протокол неизвестен, протокол может быть изучен посредством отслеживания трафика данных в сети и извлечения из него спецификации протокола.

В контексте данного документа, под понятием "протокол" может пониматься набор правил, который определяет содержимое некоторых или всех сообщений, передаваемых по сети данных.

Сетевой протокол может содержать определение сообщений протокола, также известных как Протокольные Единицы Данных (PDU). Сообщение протокола (PDU) в свою очередь может содержать одно или более полей. Может существовать много типов полей. Поле может содержать либо другую PDU, либо "элементарный" объект данных (например, число, строку или двоичный непрозрачный объект). Как будет более подробно описано ниже, сетевой протокол может быть организован в виде дерева, в котором узлами являются PDU, а листьями дерева являются элементарные объекты данных (поля). Для каждого поля (или каждого существенного поля) может быть предусмотрена отдельная модель. В качестве примера, предположим, что сообщение протокола содержит персональные данные человека (содержащие, например, имя, адрес и персональные установки): тогда сообщение протокола, которое передает персональные данные, может содержать поля: "имя", "адрес", и "персональные установки". Поле "имя" может, например, в свою очередь содержать поля: "фамилия", "имя", "имя входа в систему" и т.д. Поле "адрес" может, например, содержать поля: "домашний адрес" и "рабочий адрес". Поле "домашний адрес" может, например, содержать "улицу домашнего адреса", "номер домашнего адреса", "почтовый индекс домашнего адреса", "город домашнего адреса", тогда как поле "рабочий адрес" может, например, содержать поля "улица рабочего адреса", "номер рабочего адреса", "почтовый индекс рабочего адреса", "город рабочего адреса" и т.д. Отдельная модель может быть построена для каждого поля. Например, отдельная, соответствующая модель может быть предусмотрена для каждого из полей. В варианте осуществления, одна и та же модель может применяться для подмножества полей, например, к полям "город рабочего адреса" и "город домашнего адреса" может применяться одна и та же модель.

Понятие "трафик данных" может пониматься таким образом, что оно содержит любые данные, передача которых осуществляется через сеть, такие как поток данных, пакеты данных и т.д. Понятие "сеть данных" может пониматься таким образом, что оно содержит любую организацию для передачи данных, которая обеспечивает передачу (например, цифровых) данных. Сеть может содержать или быть связана с открытой сетью, такой как Интернет, и/или может содержать частную сеть или виртуальную частную сеть, доступ к которой разрешен только авторизованным пользователям или авторизованному оборудованию. Передача может осуществляться через проводное соединение, оптоволоконное соединение, беспроводное соединение и/или любое другое соединение. Понятие "модель" может пониматься таким образом, что оно содержит правило или набор правил, который применяется к полю протокола, для того чтобы оценить это поле протокола. Модель может описывать, нормальные, допустимые или свободные от вторжения сообщения протокола. Следует понимать, что чем большее количество сообщений протокола используется на фазе обучения, тем лучше модель может описывать нормальные, допустимые или свободные от вторжения сообщения протокола.

Понятие "вторжение" может пониматься таким образом, что оно содержит любые данные, которые могут быть нежелательными, возможно вредными для компьютерной системы, которая принимает данные, возможно вредными для приложения, запущенного на компьютерной системе, соединенной с сетью данных, или возможно вредными для работы устройства, инсталляции, аппаратуры, и т.д., соединенной с сетью данных.

В варианте осуществления набор моделей содержит соответствующую модель для каждого поля протокола из набора полей протокола. Таким образом, могут быть получены более точные результаты, поскольку для каждого поля протокола может применяться специально подогнанная для этого поля протокола модель.

В варианте осуществления набор моделей содержит две модели для одного поля протокола, причем конкретная одна из двух моделей для одного поля протокола выбирается на основании значения другого поля, так чтобы возможно дополнительно увеличить точность моделей.

Аналогичным образом, в варианте осуществления может выполняться анализ временной последовательности по полю протокола, при этом набор моделей, содержит по меньшей мере две модели для одного поля протокола, причем первая одна из двух моделей ассоциируется с первым временным интервалом, в который наблюдается трафик данных, а вторая одна из моделей ассоциируется со вторым временным интервалом, в который наблюдается трафик данных, причем второй временной интервал, например, не накладывается с первым временным интервалом.

В варианте осуществления модель для поля определяется в фазе обучения, причем фазе обучения, содержащей

синтаксический анализ трафика данных для извлечения по меньшей мере одного поля протокола для протокола, применяемого в трафике данных;

ассоциирование извлеченного поля протокола с моделью для данного поля протокола, причем модель выбирается из набора моделей; и

обновление модели для извлеченного поля протокола с использованием содержимого извлеченного поля протокола.

Таким образом, наблюдение за трафиком данных может осуществляться на фазе обучения, и содержимое извлеченных полей протокола может быть применено для обновления соответствующих моделей, с которыми ассоциированы поля протокола. Если между извлеченным полем протокола и одной из моделей ассоциация не может быть создана, то для извлеченного поля протокола может быть создана и добавлена в набор моделей новая модель.

Следовательно, могут быть выделены две фазы: фаза обучения, на которой строится модель сообщений протокола. Эти сообщения протокола на фазе обучения могут быть созданы на основании протокола связи или могут быть извлечены из трафика данных в сети передачи данных.

Поскольку сообщения протокола могут быть описаны посредством их структуры и значения полей протокола, то модель может касаться полей протокола на фазе обучения и их значений. Разные поля протокола на фазе обучения могут иметь разные типы данных, т.е. их значение может быть числом (таким как целое число, число с плавающей точкой, и т.д.), строкой, логическим или двоичным значением. Это может быть определено протоколом связи. Модель может строиться в соответствии с типом данных, по меньшей мере одного поля протокола.

Определенное поле протокола и/или определенное значение упомянутого поля протокола сравнивается с моделью и классифицируется на основании сравнения. Сообщение протокола может быть классифицировано как аномалия, т.е., находящееся за пределами безопасной области, которая определяется моделью (и, следовательно, в качестве возможной опасности) на основании сравнения.

На фазе обучения сообщения протокола, которые применяются для обучения модели, могут быть получены из трафика данных в сети. Альтернативно, или в дополнение к этому, могут быть применены данные симуляции. На фазе обучения сообщения протокола с возможным вторжением могут выявляться статистическими способами, т.е., нечасто используемые сообщения протокола или сообщения протокола с редким содержимым могут удаляться перед использованием сообщений протокола для обучения модели(ей). В дополнение, или вместо этого, оператор может идентифицировать некоторые сообщения протокола как являющиеся вторжением, и такие сообщения протокола могут либо удаляться до обучения, либо модели соответствующим образом корректируются.

Могут применяться альтернативы обучению (т.е., обучению) модели (ей), отличные от вышеописанной фазы обучения. Например, модель может быть получена посредством инспектирования протокола и приложения, создания набора, например ожидаемых сообщений протокола, их полей и/или значений полей, из него и построения модели, или набора моделей, из него. Также может применяться сочетание такого построения модели(ей) посредством инспектирования, с обучением модели(ей): например, сначала обучение модели(ей) на фазе обучения и затем адаптация полученной в результате обучения модели(ей) на основании знаний об известном поведении и косвенном явлении и/или содержимом сообщений протокола, их полей и/или значений полей.

В варианте осуществления сигнал обнаружения вторжения дополнительно генерируется, когда синтаксический анализ не может установить поле как согласующееся с протоколом, так что действие может быть также выполнено в том случае, когда обнаруживается поле, которое не согласуется с протоколом (например, деформированное сообщение протокола).

В варианте осуществления сигнал обнаружения вторжения дополнительно генерируется, когда извлеченное поле не может быть ассоциировано ни с одной моделью из набора моделей, так что действие может быть также выполнено в случае, когда извлеченное поле возможно согласуется с протоколом, но для которого не предусмотрена подходящая модель. Часто, используется только подмножество возможных полей протокола, например, в приложениях управления, что позволяет, например, вызывать оповещение о тревоге тогда, когда извлечено поле протокола, которое согласуется с протоколом, но которое обычно не применяется.

Способ может быть применен к разнообразным уровням протокола. Например, протокол может быть по меньшей мере одним из протоколов: протоколом прикладного уровня, протоколом уровня сеанса, протоколом транспортного уровня или даже протоколом более низких уровней из стека протоколов. Прикладной уровень сети передачи данных может быть определен моделью Взаимодействия Открытых Систем (модель OSI), которая была определена Международной Организацией по Стандартизации. На прикладном уровне программное обеспечение, запущенное на компьютерах или серверах, может осуществлять связь друг с другом посредством отправки сообщений протокола. Сообщения протокола могут быть сообщениями протокола сетей SCADA или Управления Производственным Процессом, Windows, сообщениями протокола сетей автоматизации делопроизводства, сообщениями протокола HTTP, и т.д.

Осуществление связи между программным обеспечением может придерживаться некоторого протокола связи, в котором определены структура и возможные значения (части) сообщений протокола. Структура сообщения протокола может быть дополнительно описана полями протокола в сообщениях протокола. Программное обеспечение может быть выполнено неспособным обрабатывать сообщения

протокола, которые созданы не в соответствии с протоколом связи.

В варианте осуществления, в ответ на генерирование сигнала обнаружения вторжения, способ дополнительно содержит по меньшей мере один из этапов, на которых

удаляют поле протокола или пакет данных, содержащий поле протокола; и

вызывают и выводят сообщение оповещения о вторжении. Может быть применено любое другое действие обнаружения вторжения, такое как, например, изолирование поля протокола или пакета данных, содержащего поле протокола, и т.д.

В варианте осуществления модель для поля протокола содержит по меньшей мере одно из следующего:

набор приемлемых значений поля протокола и

определение диапазона приемлемых значений поля протокола. В случае, когда поле протокола содержит численное значение, то в связи с этим может быть предусмотрена простая модель, которая может позволить обеспечить тестирование поля протокола с низкой нагрузкой по обработке данных.

В варианте осуществления модель для поля протокола содержит определение приемлемых букв, цифр, символов, и сценариев. В случае, когда поле протокола содержит знак или строку, то в связи с этим может быть предусмотрена простая модель, которая может позволить обеспечить тестирование поля протокола с низкой нагрузкой по обработке данных.

В варианте осуществления модель для поля протокола содержит набор предварительно определенных сигнатур вторжения, таким образом, что могут учитываться знания об известных атаках. Сочетание модели, как описано выше (содержащей, например, набор приемлемых значений поля протокола, определение диапазона приемлемых значений поля протокола, определение приемлемых букв, цифр, символов, и сценариев) с набором предварительно определенных сигнатур вторжения может быть высоко эффективным, поскольку для каждого конкретного поля может применяться модель со своим нормальным содержимым в сочетании с одной или более конкретными сигнатурами вторжения для данного поля.

В варианте осуществления протокол содержит примитивные поля протокола и составные поля протокола, причем составные поля протокола в свою очередь содержат по меньшей мере одно примитивное поле протокола, при этом соответствующая модель предусмотрена в наборе моделей для каждого примитивного поля протокола. Следовательно, может быть обеспечено эффективное обнаружение вторжения, поскольку поля протокола, которые являются составными (т.е., поля протокола, которые сами по себе содержат поля протокола, как например "адрес", содержащий "название улицы", "номер", "почтовый индекс" и "город"), могут быть разбиты на их элементарные (примитивные) поля протокола, позволяя применять подходящую модель для каждого примитивного поля протокола.

Поскольку модель по меньшей мере для одного поля протокола на фазе обучения и/или для значения по меньшей мере одного поля протокола на фазе обучения может быть построена в соответствии с типом данных по меньшей мере одного поля протокола на фазе обучения, то модель может быть более точной при описании нормальных, допустимых или свободных от вторжения сообщений протокола, чем модель, которая не учитывает тип данных полей протокола.

Может быть так, что модель, оптимизированная для описания поля протокола с числовым типом данных, может быть менее точна (или не применима) для описания поля протокола со строковым или двоичным типом данных. Подобным образом модель, оптимизированная для описания поля протокола со строковым типом данных, может быть менее точна при описании поля протокола с числовым или двоичным типом данных. Вследствие этого точность модели может быть повышена посредством учета типа данных поля протокола при построении модели.

В варианте осуществления предоставляется множество типов модели, при этом тип модели для извлеченного поля протокола выбирается на фазе обучения из множества типов модели на основании характеристики извлеченного поля протокола и на основании выбранного типа модели строится модель для извлеченного поля протокола.

Для того чтобы получить модель для конкретного поля протокола, может быть выполнено несколько этапов. Как объяснено выше, может применяться множество разных типов модели. Сначала должен быть выбран некоторый тип модели из набора доступных типов модели для конкретного поля протокола. Как только определен тип модели для некоторого поля протокола, для данного поля протокола может быть построена модель. Как описано в данном документе, модель может быть построена, например, с использованием анализа трафика данных на фазе обучения. Характеристика поля протокола может быть любой подходящей характеристикой данных в самом поле протокола, его смыслом в контексте протокола и т.д. Некоторые примеры будут описаны ниже. Посредством использования разных типов модели можно как применять методики моделирования, которые являются конкретными для типа разных значений поля, так и использовать безопасную область значений таким образом, при котором она является ограничивающей в большей или меньшей степени в соответствии со смыслом, ролью и важностью поля протокола в протоколе или контексте, в котором применяется протокол. В целом, разные типы модели могут применять разные типы критерия для того чтобы установить, может или нет конкретное значение поля протокола являться вторжением. Например, разные типы моделей могут применять один из критериев: диапазон значений, числовое распределение значений, набор значений, набор операторов, набор

текстовых значений, набор описаний состояния, набор или диапазон текстовых знаков, набор/диапазон текстовых кодировок и т.д. Следовательно, под понятием "тип модели" может пониматься набор операций, который разрешен над конкретным типом значения, совместно с эвристическим правилом для определения безопасной области для значений некоторого типа и критерием для определения того, находится ли некоторое значение в пределах безопасной области.

Выбор типа модели может выполняться в любой момент времени: во время фазы обучения, как впрочем, и во время отслеживания и обнаружения вторжения. Во время фазы обучения тип модели может быть выбран как часть процесса построения модели для конкретного поля протокола. Во время обнаружения, если выявляется, что модель для конкретного поля протокола не обеспечивает не противоречащего результата, может быть выбран другой тип модели.

Выбор типа модели может быть выполнен, с использованием типа данных значения(ий) поля протокола и/или семантики синтаксически проанализированного поля(ей) протокола. В варианте осуществления характеристика поля протокола содержит тип данных поля протокола, причем способ содержит этапы, на которых

определяют тип данных извлеченного поля протокола и

выбирают тип модели с использованием определенного типа данных.

Тип данных значений поля протокола (такой как "число", "строка", "массив", "набор" и т.д.) может, например, быть извлечен из спецификаций протокола. В качестве альтернативы, тип данных значений поля протокола может, например, предполагаться из наблюдения за сетевым трафиком. В одном варианте осуществления, значения поля предполагается посредством регулярных выражений. Например, регулярное выражение ^[0-9]+$ может быть использовано для идентификации числовых целых значений поля. Посредством выбора соответствующего типа модели для сопоставления типа данных значений поля протокола, может быть получена модель, которая может привести к более достоверным результатам обнаружения.

Выбор типа модели может дополнительно быть или вместо того чтобы быть основанным на типе данных значения поля протокола, быть основан на семантике синтаксически проанализированного поля протокола. Следовательно, в варианте осуществления характеристика поля протокола содержит семантику поля протокола, при этом способ содержит этапы, на которых

определяют семантику извлеченного поля протокола и

выбирают тип модели с использованием определенной семантики.

Семантика может быть назначена синтаксически проанализированному полю протокола. Назначение семантики может выполняться разнообразными способами: вручную во время фазы обучения, предполагая по наблюдаемым сетевым данным, посредством извлечения информации из спецификации протокола и т.д. Семантика может применяться для выбора наиболее соответствующего типа модели, например в случае, когда несколько типов модели доступно для некоторого типа значения поля протокола. Например, для значения поля протокола числового типа, можно воспользоваться типом модели, которая содержит диапазон таких значений поля протокола, типом модели, которая содержит набор значений поля протокола, и т.д. Учет семантики, при этом предпочтительно учет как типа значения поля протокола, так и семантики, может позволить осуществлять назначение соответствующего типа модели, который больше всего подходит для данного конкретного поля протокола.

Примером использования семантики может служить случай определения того, каким образом задать "строгий" числовой диапазон на основании важности поля. Другими словами, если семантика поля протокола предполагает, что данное поле является важным с точки зрения безопасности, то может применяться более строгий числовой диапазон, чем в противоположном случае, при котором будет применяться более свободный диапазон (например, удвоенное максимальное значение и половина минимального значения, наблюдаемого во время фазы обучения).

Посредством назначения полю протокола типа модели в соответствии с типом значения поля протокола и/или семантики протокола, тип модели может быть назначен таким образом, что он учитывает содержимое данных в поле протокола, и, следовательно, позволяет подогнать модель в соответствии с содержимым поля протокола. Например, если типом поля является числовой целый тип, а семантика говорит о том, что данное поле содержит длину другого поля, то может быть выбрана модель типа числового распределения. С другой стороны, если типом поля является числовой целый тип, а семантика говорит о том, что поле является полем типа сообщения, тогда может быть выбрана модель типа числового набора. В качестве третьего примера, если типом поля является числовой целый тип, а семантика говорит о том, что поле является частотой вращения двигателя, тогда может быть применена модель типа строгого числового диапазона.

В варианте осуществления набор моделей содержит модель для поля протокола оператора и модель для поля протокола аргумента, причем ассоциирование и оценка выполняются для поля протокола оператора и поля протокола аргумента. Протокол может содержать поля протокола, содержащие операторы (такие как инструкции, вызовы и т.д.), и поля протокола, содержащие операнды (т.е., аргументы), к которым применяются операторы. Следует отметить, что в соответствии с вариантом осуществления изобретения соответствующая модель может быть ассоциирована с полями протокола, содержащими операто-

ры, как впрочем, и с полями протокола, содержащими аргументы. Таким образом, с одной стороны, могут быть распознаны не только являющиеся вторжением значения аргументов, но также возможно являющиеся вторжением операторы. Также учет оператора позволяет назначать наиболее соответствующий тип модели, тем самым позволяя повысить точность обнаружения вторжения, поскольку, как правило, за оператором будет следовать один или более аргументов, содержащих некоторый предварительно определенный тип данных.

Кроме того, под сообщением протокола может подразумеваться спецификация операции, которая должна быть выполнена на стороне принимающего сетевого узла(ов), как того требует отправляющий сетевой узел. Соответственно сообщение протокола может содержать поля оператора (т.е. спецификацию того, какая требуется операция), поля аргумента (т.е., спецификацию того, каким образом должна выполняться операция) и поля маршалинга (т.е., поля, которые непосредственно не относятся к требуемой операции, однако содержат параметр, который требуется сетевым узлам для корректного приема и интерпретации сообщения или, в общем, для обработки сетевой связи). Под маршалингом может пониматься процесс преобразования представления в памяти объектов в формат данных, подходящий для хранения или передачи, и он, как правило, используется, когда данные должны перемещаться между разными частями компьютерной программы или от одной программы другой.

Например, запрос HTTP содержит: поле способа (например, GET, POST, PUT и т.д.), указывающее оператор; поле URL, которое содержит аргументы для способа (например,/index.php?id=3) и некоторое количество полей заголовка (например, Content-length: 100), которые содержат информацию, которая не относится к самой операции, однако используется сетевыми узлами для осуществления связи (например, заголовок Content-length: 100 указывает на то, что тело сообщения запроса составляет в длину 100 байт).

В качестве другого примера сообщение запроса Modbus/TCP содержит поле кода функции, идентифицирующее то, какая операция должна быть выполнена на принимающем PLC/RTU устройстве, доступное количество регистров данных, указывающее аргументы требуемой операции, и некоторое количество других полей, которые непосредственно не относятся к операции (например, поле счета регистра, поля длины данных и т.д.), которые требуются принимающему сетевому узлу для понимания того, каким образом синтаксически анализировать сообщение (например, какое количество регистров было отправлено).

Атаки или попытки вторжения могут выполняться посредством внедрения вредоносных данных в каждое из этих разных полей. Аналогичным образом, такие атаки или попытки вторжения могут быть обнаружены благодаря тому, что значения разных полей отличаются от нормальных. Инспектирование полей оператора и маршалинга может повысить точность при обнаружении атак или попыток вторжения. Соответственно, в варианте осуществления, набор моделей дополнительно содержит модель для поля протокола маршалинга, причем ассоциирование и оценка, кроме того, выполняются для поля протокола маршалинга.

Например, атака, направленная на переполнение буфера, может быть выполнена посредством внедрения в строковое поле большего количества знаков, чем то, на которое выделяется буфер принимающего сетевого узла. Такая атака может быть обнаружена благодаря тому, что строковое поле содержит необычные значения знака. С другой стороны, может быть выполнена успешная атака, которая использует только совершенно действительные текстовые знаки в качестве вредоносной полезной нагрузки. Та же атака тогда может быть обнаружена благодаря другому полю, указывающему на то, что длина строки больше нормальной: это обязательно должно быть истинным, поскольку максимальное разрешенное значение для допустимой длины строки будет размером буфера, который выделяется принимающим сетевым узлом.

Дополнительно, разные, конкретные типа модели могут быть использованы для полей оператора, полей аргумента и полей маршалинга для того, чтобы дополнительно повысить точность обнаружения или сократить количество нерелевантных генерируемых оповещений о тревоге. Для разных полей оператора могут использоваться разные модели (одинаковых или разных типов модели). Для разных полей аргумента могут использоваться разные модели (одинаковых или разных типов модели). Для разных полей маршалинга могут использоваться разные модели (одинаковых или разных типов модели). Типы модели могут быть выбраны на основании, например, типа данных и семантики, как описано выше.

Следует отметить, что система и способ обнаружения вторжения в соответствии с изобретением могут применяться к любому типу трафика данных, такому как текстовый трафик данных (т.е., текстовый протокол) или двоичный трафик данных (т.е., Двоичный протокол). В целом, спецификация текстовых протоколов не несет в себе описание типа большей части его значений полей. Например, спецификация протокола HTTP не ассоциирует тип со значениями заголовка или значениями параметра, которые должны синтаксически анализироваться в качестве текстовых строк. В таких случаях может потребоваться строить предположение о типе поля посредством инспектирования трафика. С другой стороны, данное поведение не присутствует в двоичных протоколах, в которых спецификациям требуется включать тип всех полей протокола для того чтобы обеспечить правильный синтаксический анализ. По этой причине, применение настоящей методики к двоичному протоколу может давать даже более точный результат, чем применение ее к текстовому протоколу, поскольку для двоичных протоколов отсутствует

неопределенность предположения значения поля. В частности, когда учитывается тип данных и семантика синтаксически проанализированного поля протокола, то потоку двоичных данных может придаваться смысл, в том смысле, что синтаксический анализ и выбор подходящего типа модели для каждого поля протокола, основанный на типе данных и/или семантике, позволяет учитывать содержимое двоичных данных. В двоичном протоколе, под понятием "тип данных поля протокола" должно пониматься то, какие данные представлены (двоичными) данными в поле протокола: двоичные данные, например, представляющие собой другой тип данных, такой как число, строка, и т.д.

В целом, сообщение протокола может содержать примитивные поля протокола и составные поля протокола. Составное поле протокола содержит два или более подполя протокола, каждое из которых может быть примитивным полем протокола или составным полем протокола. Модель для составных полей протокола может содержать счетчик экземпляров поля протокола, наблюдаемых на фазе обучения. В случае, когда поле наблюдалось меньше заданного количества раз (порогового значения), наблюдение составного поля протокола во время фазы обнаружения может вызывать генерирование сигнала обнаружения вторжения. В соответствии с семантикой составного поля протокола, его важность в отношении безопасности может меняться. Вследствие этого, семантика может использоваться для указания другого типа модели или другой чувствительности модели в соответствии с, например, важностью поля в отношении безопасности. Например, в случае составного поля, которое не имеет отношения к безопасности, пороговое значение наблюдаемых экземпляров может быть изменено, чтобы ограничить объем нерелевантных генерируемых сигналов обнаружения вторжения, и, следовательно, повышена простота использования. Кроме того, семантика составного поля может распространяться на его подполя, чтобы обеспечить более точный выбор типов модели и настроек модели. Например, базовое поле числового типа, которое содержится в составном поле, которое очень актуально для безопасности, может быть ассоциировано с типом числового набора, который может определять более строгую безопасную область значений, чем модель типа численного диапазона, и, следовательно, повышать точность обнаружения вторжения.

В соответствии с другим аспектом изобретения, предоставляется система обнаружения вторжения для обнаружения вторжения в трафик данных в сети передачи данных, причем система содержит

блок синтаксического анализа для синтаксического анализа трафика данных для извлечения по меньшей мере одного поля протокола сообщения протокола трафика данных;

машину для ассоциирования извлеченного поля протокола с соответствующей моделью для данного поля протокола, причем модель выбирается из набора моделей;

блок обработки модели для анализа того, находится ли содержимое извлеченного поля протокола в безопасной области, как определяется моделью; и

исполнительный блок для генерирования сигнала обнаружения вторжения в случае, когда установлено что содержимое извлеченного поля протокола, находится за пределами безопасной области.

С помощью системы в соответствии с вариантом осуществления могут быть получены точно такие же или подобные эффекты, как с помощью способа в соответствии с изобретением. Также могут быть предоставлены точно такие же или подобные варианты осуществления, как те, что описаны со ссылкой на способ в соответствии с изобретением, при достижении точно таких же или подобных эффектов. Блок синтаксического анализа, машина, блок обработки модели и исполнительный блок могут быть реализованы посредством подходящих инструкций программного обеспечения, которые должны исполняться устройством обработки данных. Они могут быть реализованы в той же самой программе программного обеспечения, которая должна исполняться тем же самым устройством обработки данных, или может исполняться двумя или более отличными устройствами обработки данных. Например, блок синтаксического анализа может исполняться локально в местоположении, где проходит трафик данных, в то время как машина, блок обработки модели и исполнительный блок могут быть расположены удаленно, например, в безопасном местоположении. Также могут отслеживаться данные с различных сайтов, и таким образом, блок синтаксического анализа может быть предусмотрен на каждом сайте, причем выходные данные от каждого блока синтаксического анализа отправляются одной машине, блоку обработки модели и исполнительному блоку.

Следует отметить, что описанный выше способ и система могут применяться не только для обнаружения вторжения. Вместо этого, или в дополнение к данной цели, описанный способ и система могут применяться в целях отслеживания. Например, может отслеживаться трафик данных в сети данных объекта, такого как предприятие, центр обработки данных и т.д. Для каждого или для некоторых полей протокола может быть определена модель, которая представляет собой безопасное и требуемое рабочее состояние. Альтернативно, вместо определения безопасного или требуемого рабочего состояния заранее, система и/или способ, как описано в данном документе, может применяться на фазе обучения, таким образом, модели, полученные на фазе обучения, позволяют получить описание работы, в соответствии с тем, как она отслеживается. Пересылаемые данные могут содержать информацию, из которой может быть получено рабочее состояние, при этом такие данные применяются для обучения моделей для соответствующих полей протокола. Например, в сети данных предприятия, может пересылаться информация управления, которая относится к частоте вращения двигателей, температуре реакторов, гидравлическому давлению, как впрочем и сообщения об ошибках, вызовы процедуры и т.д. Такие данные могут быть ис-

пользованы, либо для сравнения с предварительно определенными моделями, которые определяют требуемое или безопасное рабочее состояние, либо для обучения моделей, и отсюда получения статуса из моделей по мере обучения. Отслеживание может содержать проверку состояния "работоспособности" промышленного предприятия или компьютерной сети посредством наблюдения за значениями некоторых полей протокола (или сочетанием полей протокола), которые являются важными для администраторов системы/сети, и может определять интересные события компьютерной сети или процесса промышленного производства, и т.д. Следовательно, там, где в данном документе применяется понятие "обнаружения вторжения", оно также может пониматься как относящееся к отслеживанию.

Краткое описание фигур

Дополнительные эффекты и признаки изобретения будут описаны лишь в качестве примера, со ссылкой на представленное ниже описание и сопроводительные схематичные чертежи, в которых раскрываются не накладывающие ограничений варианты осуществления, при этом

фиг. 1 схематично изображает пример сети передачи данных, содержащей систему обнаружения вторжения в соответствии с вариантом осуществления изобретения;

фиг. 2 схематично изображает общий вид системы обнаружения вторжения в соответствии с вариантом осуществления изобретения;

фиг. 3 схематично изображает общий вид фазы обучения способа в соответствии с вариантом осуществления изобретения;

фиг. 4 схематично изображает общий вид фазы обнаружения вторжения способа в соответствии с вариантом осуществления изобретения;

фиг. 5 схематично изображает структурную схему, для того чтобы проиллюстрировать систему и способ обнаружения вторжения в соответствии с вариантом осуществления изобретения.

Подробное описание изобретения

На фиг. 1 изображен схематичный общий вид примера сети передачи данных с системой обнаружения вторжения для классифицирования сообщения протокола в соответствии с вариантом осуществления изобретения. В данной сети персональные компьютеры 14 и 15 (или рабочие станции) соединены с сервером 13. Сеть может быть соединена с интернет 16 через межсетевой экран 17.

В сети передачи данных вторжение или атака может исходить от Интернет 16 или от персонального компьютера 14, когда он инфицирован вредоносным программным обеспечением.

Сеть передачи данных может быть сетью SCADA или иной сетью Управления Производственным Процессом. В такой сети управление машинным оборудованием 12 может осуществляться посредством программного обеспечения, запущенного на удаленном терминальном блоке 11 (RTU), или на программируемом логическом контроллере (PLC). Программное обеспечение, запущенное на сервере 13, может отправлять сообщения протокола программному обеспечению, запущенному на RTU 11. Программное обеспечение на RTU 11 может отправлять сообщения протокола машинному оборудованию, на котором также может быть запущено программное обеспечение.

Пользователь может осуществлять связь с сервером 13 через программное обеспечение, запущенное на персональном компьютере 14 или рабочей станции 15 посредством осуществления обмена сообщениями протокола между программным обеспечением, запущенным на персональном компьютере 14 или рабочей станции 15, и программным обеспечением, запущенным на сервере 13.

Система 10 обнаружения вторжения может быть размещена между RTU 11 и оставшейся частью сети, как показано на фиг. 1, или между RTU 11 и машинным оборудованием 12 (не показано). Система 10 обнаружения вторжения может извлекать сообщения протокола из сети передачи данных, обмен которыми может осуществляться между программным обеспечением, запущенным на персональном компьютере 14 или рабочей станции 15, и программным обеспечением, запущенным на сервере 13, между программным обеспечением, запущенным на сервере 13 и программным обеспечением, запущенным на RTU 11, или между программным обеспечением, запущенным на RTU 11 и программным обеспечением, запущенным на устройстве обработки данных машинного оборудования 12.

Протокол связи может быть определен в качестве формального описания цифровых форматов сообщения протокола и правил для обмена этими сообщениями в или между (программным обеспечением, запущенным на) вычислительными системами. Протокол связи может включать в себя описания для синтаксиса, семантики, и синхронизации связи. Сообщения протокола на прикладном уровне в сети передачи данных могут содержать одно или более поля, которые могут характеризоваться их типами данных. Например, поле может представлять собой всю длину сообщения, с числовым значением или строковым значением.

Чем больше информации о сообщениях протокола, тем модель, описывающая нормальное, допустимое или свободное от вторжения сообщение протокола, может включать в себя больше информации о нормальных или допустимых значениях каждого поля протокола каждого сообщения протокола, обмен которым осуществляется в сети передачи данных. Затем модель может быть использована (например, в режиме реального времени) для классифицирования сообщений протокола из живого трафика данных в сети передачи данных для обнаружения аномалий, т.е., чего-нибудь, что отклоняется от нормального поведения сети передачи данных, как оно описывается моделью.

Фиг. 2 показывает схематичный общий вид варианта осуществления системы 10 обнаружения вторжения в соответствии с вариантом осуществления изобретения. Система 10 обнаружения вторжения содержит блок 21 синтаксического анализа сетевого протокола, выполненного с возможностью извлечения по меньшей мере одного поля протокола из сообщения протокола (например) прикладного уровня сети передачи данных. На фазе обучения сообщения протокола могут быть получены из сети через ввод 25. Блок 21 синтаксического анализа сетевого протокола может быть использован во время опциональной фазы обучения, как впрочем, и во время обычной работы системы обнаружения вторжения. Информация об извлеченном сообщении протокола может быть переслана машине 23.

Система обнаружения вторжения дополнительно содержит машину 23, набор 26 моделей и блок 25 обработки модели. Машина 23 выполнена с возможностью ассоциирования извлеченного поля протокола с моделью некоторого типа модели, выбранной на основании типа данных и/или семантики поля протокола. Для этой цели, машина содержит или имеет доступ к набору 26 моделей. Машина ассоциирует извлеченное поле протокола с моделью, которая является конкретной для данного поля протокола, например, конкретной для типа поля данных и/или семантики. С этой целью набор 26 моделей содержит разные модели, причем каждая модель для конкретного одного (или более) из полей протокола. На фазе обучения машина может, в случае, когда для извлеченного поля протокола еще отсутствует доступная модель, создавать модель для извлеченного поля протокола и добавлять ее в набор моделей. Информация об извлеченном поле протокола может быть переслана блоку 24 обработки.

Блок 24 обработки затем делает оценку того, согласуется или нет извлеченное поле протокола с моделью, с тем, чтобы оценить, может или нет считаться вторжением содержимое извлеченного поля протокола. На фазе обучения, модель может быть обновлена с использованием содержимого извлеченного поля протокола. Блок обработки может выводить сообщения через выход 27.

Система обнаружения вторжения может дополнительно содержать исполнительный блок 22 для генерирования сигнала обнаружения вторжения в случае, когда (значение) поле протокола было идентифицировано в качестве вторжения, т.е. как находящееся за пределами безопасной области, определяемой ассоциированной моделью. В ответ на генерирование сигнала обнаружения вторжения, может быть выполнено действие обнаружения вторжения, например, содержащее вызов оповещения о тревоге, фильтрацию пакета данных или поля протокола (тем самым, например, удаляя пакет данных или поле протокола). Сигнал обнаружения вторжения также может быть сгенерирован в случае, когда блок синтаксического анализа не может идентифицировать поле протокола (что подразумевает, что пакет данных не согласуется с протоколом), и/или в случае, когда блок обработки модели во время операции обнаружения вторжения не может ассоциировать извлеченное поле протокола с моделью из набора (что предполагает, что пакет данных не содержит поля протокола, которые передаются нормальным образом).

Для каждого поля протокола используется конкретная модель, предпочтительно с использованием отличной модели для каждого отличного поля протокола, таким образом, что наиболее оптимальная оценка может быть выполнена для каждого поля протокола, так что модель, которая специально предназначена для данного поля протокола, может быть использована для оценки поля протокола.

В варианте осуществления модели были построены с использованием по меньшей мере двух типов модели, при этом первый тип модели по меньшей мере из двух типов модели оптимизирован для (или работает только для) поля протокола с первым типом данных и при этом второй тип модели по меньшей мере из двух типов модели оптимизирован для поля протокола со вторым типом данных. Это может быть случаем, когда первый тип модели оптимизирован для поля протокола с одним из типов: числовой тип данных, строковый тип данных или двоичный тип данных, а второй тип модели оптимизирован для поля протокола с другим из типов: числовым типом данных, строковым типом данных или двоичным типом данных.

Например, для значения поля A1 протокола с числовым типом данных может быть построена модель M-I-A1, которая предназначена для описания числовых значений. Для значения поля A2 протокола с числовым типом данных может быть построена модель M-I-A2, которая подобным образом предназначена для описания числовых значений. Для значения поля A3 протокола со строковым типом данных может быть построена модель M-S-A3, которая оптимизирована для или подогнана для описания строковых значений. Модели для разных полей протокола, которые имеют одинаковый тип данных, например модели M-I-A1 и M-I-A2, могут быть построены, с использованием одинаковой архитектуры модели, но с разным содержанием (например, другой допустимый диапазон, другой набор или набор допустимых значений, и т.д.), с тем чтобы выразить различия между полями A1 и A2 протокола.

Следует понимать, что модель с типом модели для описания числовых значений и модель с типом модели, описывающим строковые значения, могут быть лучше или более точны при описании значений сообщения протокола, содержащего как числовые значения, так и строковые значения в своих полях протокола, чем единая модель, которая будет оптимизирована для описания всех значений, как числовых значений, так и строковых значений, сообщения протокола.

Система 10 обнаружения вторжения может быть выполнена с возможностью построения модели во время фазы обучения. Работа системы 10 обнаружения вторжения и способ в соответствии с вариантами осуществления изобретения будут дополнительно описаны со ссылкой на фиг. 3 и 4. Фиг. 3 схематично

иллюстрирует фазу обучения, а фиг. 4 схематично иллюстрирует фазу обнаружения вторжения.

На фиг. 3 были схематично изображены этапы фазы обучения:

Этап a1: синтаксический анализ трафика данных для извлечения, по меньшей мере, одного поля протокола для протокола, применяемого в трафике данных.

Этап a2: ассоциирование извлеченного поля протокола с моделью для поля протокола, причем моделью выбранной из набора моделей,

Этап a3: в случае, когда невозможно выполнить ассоциирование с существующими моделями из набора моделей, создание новой модели для извлеченного поля протокола и добавление новой модели в набор моделей.

Этап a4: обновление модели для извлеченного поля протокола с использованием содержимого извлеченного поля протокола.

В целом, сообщение протокола может содержать примитивные поля протокола и составные поля протокола. Составное поле протокола содержит два или более подполя протокола, каждое из которых может быть примитивным полем протокола или составным полем протокола. Таким образом, можно сказать, что сообщение протокола содержит древовидную структуру полей протокола. Например, в сообщении протокола составное поле протокола "msg_body" (тело сообщения) содержит примитивное поле протокола "msg_len" (длина сообщения) и составное поле протокола "msg_data" (данные сообщения). Составное поле протокола "msg_data" может содержать примитивные поля протокола "msg_typeA" (сообщение типа A) и "msg_typeB" (сообщение типа B). В данном документе понятие "поле протокола" может относиться к любому примитивному полю протокола на любом уровне такой древовидной структуры.

Разные типы модели могут быть использованы. Например, тип модели поля протокола может, например, быть одним из типов: числовым типом модели, строковым типом модели или двоичным типом модели. В случае, когда обнаруживается, что извлеченное поле протокола содержит числовое значение, числовой тип модели может быть применен для поля протокола. В случае, когда обнаруживается, что извлеченное поле протокола содержит строковое значение, строковой тип модели может быть применен для данного поля протокола. Возможен случай, что (например, в текстовом протоколе), когда на фазе обучения блок синтаксического анализа сетевого протокола не способен установить, каким типом данных является поле протокола, числовым типом данных или строковым типом данных, то модель двоичного типа данных применяется в качестве более универсального типа модели.

Как объяснено выше, набор моделей может содержать соответствующую модель для каждого поля протокола. Модель для поля протокола с числовым типом данных может быть построена по-другому (т.е. может быть другого вида или с другой архитектурой модели), чем модель для поля протокола со строковым типом данных. Поскольку модели могут быть оптимизированы для каждого типа данных, то модель может быть более точной при описании нормальных, допустимых или свободных от вторжения сообщений протокола, чем модели, которые не учитывают тип данных полей протокола.

Примеры разных видов типов модели для разных видов типов данных объясняются ниже. Для числовых типов данных могут быть применены два типа модели, первый для полей протокола, представляющих собой длинны, а второй для полей протокола, представляющих собой перечисления.

Если поле протокола представляет собой перечисление (например, набор значений), то модель может содержать набор S со всеми значениями поля протокола, которые были извлечены на фазе обучения. После начала с пустым набором, во время фазы обучения, каждое значение, которое идентифицировано для поля протокола, может быть добавлено в набор. На фазе обнаружения вторжения сообщение протокола может быть классифицировано в качестве аномального, когда значение соответствующего определенного поля протокола не является, например, частью набора S.

Если поле протокола представляет собой длину, то модель может быть построена на аппроксимации распределения значений поля протокола во время фазы обучения. Во время фазы обучения среднее μ и дисперсия σ^2 аппроксимации распределения могут быть вычислены на основании выборочного среднего или выборочной дисперсии из всех значений, которые были определены в качестве содержимого данного поля протокола. С помощью среднего μ и дисперсии σ^2 аппроксимации распределения, может быть вычислена вероятность для всех значений. Во время фазы обнаружения вторжения, когда вероятность определенного значения поля протокола меньше заданного порогового значения, сообщение протокола с данным значением может быть классифицировано как аномальное.

Модуль для поля протокола логического типа может, например, отслеживать логическое значение, усредненное по некоторому количеству образцов и сравнивать усредненное значение с предварительно определенным пороговым значением. Пример такой модели описывается ниже:

Во время фазы обучения вычисляется вероятность Pt того, что значение поля соответствует значению "истина", и вычисляется вероятность Pf(1-Pt) того, что значение поля соответствует значению "ложь".

2 - Во время обнаружения вторжения рассматривается последовательность из n образцов для значения поля и затем вычисляется биноминальная вероятность наблюдения такой последовательности значений для заданного Pt и Pf. Затем вероятность сравнивается с некоторым пороговым значением t, и вызы-

вается оповещение о тревоге, если p_образца <t. Например, предположим, что во время фазы обучения мы наблюдали одинаковое количество значений "истина" и "ложь". Тогда Pt ~1/2 и Pf ~1/2. Мы установили пороговое значение вероятности для последовательностей из 5 значений равной 0,1. Теперь предположим, что во время фазы обнаружения вторжения мы наблюдаем последовательность [ложь, ложь, ложь, ложь, ложь]. Биноминальная вероятность P_образец= P(истина=0) = 0 03125<0,1. В данном случае мы вызываем оповещение о тревоге. Пример типа модели для строк, который может обрабатывать строки ASCII и Юникод описываются ниже. Сначала, описывается тип модели для строк ASCII.

Тип модели для строки ASCII содержит два логических значения и список. Первое логическое значение $^{(\text{буквы})}$ принимает значение "истина", если мы видим буквы, второе логическое значение $^{(\text{цифры})}$ принимает значение "истина", если мы видим цифры, а набор $^{(\text{символы})}$ следит за всеми символами, которые мы видим. Для заданного строкового поля s определяется функция f(s), которая дает ответ на то, содержит ли строка буквы, числа и какие символы. Например, для строки "пользователяИмя?#!" мы имеем:

$$f(\text{"пользователяИмя?\#!"}) = \begin{Bmatrix} \text{буквы} & \text{истина} \\ \text{цифры} & \text{ложь} \\ \text{символы} & \{!,\#,?\} \end{Bmatrix}$$

Во время фазы обучения, заданная строка s модели M обновляется следующим образом:

$$M = \begin{Bmatrix} \text{буквы} & M\,\text{буквы} \vee f(s)\,\text{буквы} \\ \text{цифры} & M\,\text{цифры} \vee f(s)\,\text{цифры} \\ \text{символы} & M\,\text{символы} \cup f(s)\,\text{символы} \end{Bmatrix}$$

Знаки строки оцениваются один за другим. Для каждого знака машина проверяет тип, и в случае, когда знак является либо буквой, либо цифрой, машина обновляет модель соответствующим образом посредством установки соответствующего флага в значение "истина". В случае, когда текущий знак является символом, он добавляется в текущий набор символов. В случае, когда символ уже присутствует, он дважды не добавляется.

Во время фазы обнаружения вторжения для заданной строки s может вызываться оповещение о тревоге, если:

$$\begin{array}{l} (f(s)\,\text{буквы} \wedge \neg M\,\text{буквы}) \vee \\ (f(s)\,\text{цифры} \wedge \neg M\,\text{цифры}) \vee \\ (f(s)\,\text{символы} \underline{\subset} M\,\text{символы}) \end{array}$$

Знаки строки вновь оцениваются один за другим. Процесс проверки является прямым. Если текущий знак является либо буквой (либо цифрой), машина проверяет, наблюдались ли ранее знаки буквы (или цифры) для заданного поля. Когда проверка проваливается, вызывается оповещение о тревоге. В случае, когда знаком является символ, машина проверяет, что заданный символ наблюдался до этого. Когда данная проверка проваливается, вызывается оповещение о тревоге.

В начале, модель M определяется следующим образом:

$$M = \begin{Bmatrix} \text{буквы} & \text{ложь} \\ \text{цифры} & \text{ложь} \\ \text{символы} & \varnothing \end{Bmatrix}$$

Другой пример типа модели для строк, которая может быть использована для строк Юникод, описывается ниже. Для строк Юникод методика моделирования и обнаружения может быть аналогична моделированию для строк ASCII. Знаки Юникод, которые не являются ASCII, рассматриваются как буквы ASCII, т.е. если строка содержит знак Юникод, логическое значение "буквы" устанавливается в значение "истина". В дополнение запоминается набор сценариев Юникод (например, Латинский, Кириллический, Арабский) как видно во время фазы обучения. С помощью данной дополнительной информации обнаруживается, например, присутствуют ли в строке странные знаки Юникод (которые возможно принадлежат к другому сценарию, чем те, которые видели на фазе обучения).

Более подробно, для заданного строкового поля s Юникод, мы определяем функцию f'(s), которая говорит о том, содержит ли строка буквы, цифры, какие символы и какие сценарии Юникод. Например, для строки "mu3sòafà?#!" мы имеем

$$f'(\text{"mu3s\`oaf'a?\#!"}) = \begin{Bmatrix} \text{буквы} & \text{истина} \\ \text{цифры} & \text{ложь} \\ \text{символы} & \{!,\#,?\} \\ \text{сценарии} & \{\text{латинский}\} \end{Bmatrix}$$

Для строк Юникод модель M инициализируется и обновляется посредством выполнения точно таких же или подобных операций, что и для строк ASCII и посредством обработки дополнительного поля "сценарии", подобно полю "символы".

Некоторый дополнительный пример для типа модели двоичных полей протокола предоставляется ниже:

Для двоичного типа данных может быть применена модель из известных, основанных на аномалии систем обнаружения вторжения, основанная на анализе полезной нагрузки.

Пример двоичной модели основан на анализе 1-грамм. n-грамм является последовательностью n

последовательных байт.

Для заданного двоичного поля b длиной l байт мы сначала вычисляем вектор f, содержащий частоту каждого байта. Другими словами, для заданного значения ν байта элемент f, соответствующий ν, имеет вид

$$\bar{f}[\nu] = \frac{\sum_{i=1}^{l} 1, если \quad b[i] = \nu}{l}$$

Во время фазы обучения, вектор частоты применяется для вычисления среднего и стандартного отклонения каждого значения байта. С этой целью, для заданной последовательности из n двоичных полей b1..bn, и их ассоциированных векторов частоты байта (f1..fn), вычисляются два вектора μ и σ, которые содержат соответственно среднее и стандартное отклонение каждого значения байта (от 0 до 255). Эти два вектора в данном примере образуют двоичную модель.

Во время фазы тестирования для заданного значения s двоичного поля сначала вычисляется ассоциированный вектор из частот fs. Затем применяется соответствующая функция F (например, нормализованное евклидово расстояние) для определения расстояния между fs и моделью, построенной во время фазы обучения. Если результирующее расстояние превышает предварительно определенное пороговое значение, то может быть вызвано оповещение о тревоге.

Более точная версия описанной выше модели может быть получена посредством разбиения набора значений обучения b1..bn на подмножества. Для разбиения набора обучения на подмножества может быть применен алгоритм кластеризации, такой как Самоорганизующаяся Карта (SOM), к входным значениям (b1..bn). Затем для каждого подмножества может быть построена отдельная модель (т.е., пара массивов μ, σ).

Во время фазы обнаружения вторжения, алгоритм кластеризации работает по значению (s) двоичного поля. Тест, как описано выше, затем может быть применен к модели, ассоциированной с результирующим кластером.

Третьим примером двоичной модели является так называемый эмулятор сети. Эмулятор сети является алгоритмом, который выполнен с возможностью определения того, содержатся ли опасные исполняемые инструкции внутри набора байтов. Для заданной последовательности байтов, алгоритм сначала переводит существующие значения байта в соответствующие инструкции по сборке (трансляция на язык ассемблера). Затем, он пытается найти последовательности инструкций, которые могут быть распознаны в качестве опасных или подозрительных (например, длинные последовательности инструкций NOP, которые, как правило, обнаруживаются внутри вредоносных кодов запуска оболочки известных атак). В случае, когда такие последовательности найдены, вызывается оповещение о тревоге. Следует отметить, что для данного типа двоичной модели фаза обучения не требуется.

В случае, когда двоичное поле содержит так называемый Большой Двоичный Объект (BLOB), в котором данные организованы в соответствии со структурой, которая не указана в спецификации сетевого протокола, тот же подход, который описан в данном документе, может быть применен для дальнейшего разделения BLOB на составляющие его поля, до тех пор, пока не будут извлечены и обработаны базовые поля (например, числовые поля, строковые поля, логические поля и т.д.). Например, двоичное поле протокола может содержать изображение GIF или JPEG, для которого существует спецификация, однако такая спецификация не является частью самой спецификации сетевого протокола. В данном случае, может быть использована спецификация изображения GIF или JPEG для дальнейшего разделения значения поля на его базовые составляющие поля. Затем модель может быть выбрана и соответствующим образом построена для составляющих полей объекта. Другой такой случай возникает, когда двоичное поле содержит целую область памяти одного из сетевых узлов, осуществляющих связь (например, карты распределения памяти PLC, обмен которыми является частью протокола Modbus). Структура данной области памяти может быть определена в других документах (например, в спецификациях поставщика PLC), или может быть получена в результате предположения на основании наблюдения за достаточным количеством образцов данных. Такая информация может быть использована для дальнейшего разделения области памяти на ее базовые поля, которые затем могут быть обработаны в соответствии с проиллюстрированными в данном документе методиками.

Кроме того, для строкового типа данных может быть применена модель, как описывается в документе "Bolzoni D. and Etalle, S. (2008), Boosting Web Intrusion Detection Systems by Inferring Positive Signatures. In: Confederated International Conferences On the Move to Meaningful Internet Systems (OTM)". Для двоичного типа данных может быть применена суб-модель из известных основанных на аномалии систем обнаружения вторжения, основанная на анализе полезной нагрузки. Пример может быть найден в документе "Anomalous payload-based network intrusion detection" (RAID, стр. 203-222, 2004) под авторством Ke Wang и Salvatore J. Stolfo. В данной работе авторы представляют систему, именуемую PAYL, которая использует n-грамм анализ для обнаружения аномалий. n-грамм является последовательностью n последовательных байт. Частота и стандартное отклонение 1-грамм (последовательностей из 1 байта) анализируются и сохраняются в моделях обнаружения, которые строятся во время фазы обучения. Затем на фазе обнаружения вторжения, выбирается соответствующая модель (с использованием значение дли-

ны полезной нагрузки) и используется для сравнения входящего трафика.

Другой пример может быть найден в работе "POSEIDON: a 2-tier Anomaly-based Network" (IWIA, страницы 144-1 56. IEEE Computer Society, 2006) под авторством Damiano Bolzoni, Emmanuele Zambon, Sandro Etalle, и Pieter Hartel. В данном труде авторы строят поверх PAYL улучшенную систему посредством игнорирования длины полезной нагрузки для выбора (и построения) моделей обнаружения, и использования вместо этого нейронной сети, которая осуществляет предварительную обработку данных полезной нагрузки и выход которой используется для выбора соответствующего режима обнаружения.

Еще один пример может быть найден в документе под авторством Michalis Polychronakis, Kostas C. Anagnostakis, и Evangelos P. Markatos. Comprehensive Shellcode Detection using Runtime Heuristics. In Proceedings of the 2 6th Annual Computer Security Applications Conference (ACSAC). Декабрь 2010, Остин, Техас, США. В данном труде авторы представляют "эмулятор сети". Данный компонент программного обеспечения реализует эвристику и симулирует посредством программного обеспечения физический CPU. Эмулятор сети может тестировать, содержат ли входные данные исполняемый (и вредный) код. В варианте осуществления, процесс синтаксического анализа может содержать этапы, на которых:

i) собирают пакеты данных из сети передачи данных;

ii) дефрагментируют IP пакеты;

iii) пересобирают сегменты TCP;

iv) извлекают данные приложения и

v) извлекают сообщения протокола.

Как было сказано выше, существует возможность выбора разных типов модели в соответствии с семантикой поля, с которым ассоциируется модель. Также можно регулировать один или более параметры модели (конкретные для каждого типа модели) в соответствии с семантикой для расширения или сужения безопасной области, определяемой моделью. Здесь даны некоторые примеры использования семантики поля для выбора типа модели или регулировки параметров модели.

В случае числового поля, которое представляет тип сообщения протокола, может быть использована модель типа числового перечисления. Такой тип модели позволяет гарантировать то, что только типы сообщения, перечисленные в модели, определены в качестве безопасной области. В случае, когда модель строится автоматически во время фазы обучения, все наблюдаемые типы сообщения рассматриваются в качестве безопасных. В случае, когда модель строится вручную, набор разрешенных сообщений может быть построен в соответствии с конкретными политиками безопасности. Например, политика безопасности может предписывать то, что только операции чтения выполняются на некотором сетевом узле. В данном случае набор разрешенных сообщений будет содержать только сообщения чтения.

В случае числового поля, которое представляет частоту вращения двигателя, в контексте производственного процесса может быть использована модель числового диапазона. Такой тип модели позволяет гарантировать то, что частота вращения двигателя не будет установлена ниже или выше значения, которое считается безопасным. В случае, когда модель строится автоматически во время фазы обучения, минимальные/максимальные разрешенные значения могут быть установлены равными минимальной/максимальной частотам вращения, наблюдаемым во время фазы обучения (точный диапазон). В случае, когда модель строится вручную, минимальное и максимальное значения диапазона могут быть установлены на основании технической спецификации двигателя, чтобы гарантировать то, что частота оборотов остается в допустимых рабочих условиях.

В случае, когда числовое поле, которое представляет собой длину связанного с безопасностью поля (например, длину строкового буфера), может быть использована модель типа числового распределения. Более того, поскольку поле очень существенно в плане безопасности, поскольку оно может быть целью атаки, направленной на переполнение буфера, то может быть установлено пороговое значение высокой вероятности. Таким образом, зона безопасности, определяемая моделью, ограничивается значениями, которые с высокой вероятностью генерируются точно таким же числовым распределением, которое наблюдается во время фазы обучения. Другими словами, если длина значения поля слишком большая по отношению к той, которая ранее наблюдалась во время фазы обучения, то значение рассматривается как аномальное и вследствие этого как возможная атака. Например, код запуска оболочки, используемый для переноса атаки, направленной на переполнение буфера, может быть больше нормального содержимого буфера, тем самым генерируя аномальное значение для поля длины буфера.

В случае строкового поля, которое представляет собой имя человека, может быть выбрана модель строкового типа и пороговое значение по умолчанию для количества символьных знаков, не включенных в модель, может быть установлено на очень низком уровне. Поскольку не ожидается, что имя человека содержит много символов, то установка порогового значения по умолчанию равного очень низкому уровню гарантирует то, что сигнал обнаружения вторжения генерируется сразу в случае, когда наблюдаемое значение содержит символы, которые представлены в модели. Это может быть случаем так называемой атаки по внедрению SQL, которая использует специальные знаки, такие как одинарные или двойные кавычки, запятые и т.д.

Фиг. 4 схематично изображает этапы процесса обнаружения вторжения:

этап b1: синтаксический анализ трафика данных для извлечения по меньшей мере одного поля про-

токола сообщения протокола трафика данных,

этап b2: ассоциирование извлеченного поля протокола с моделью для данного поля протокола, причем модель выбирается из набора моделей,

этап b3: оценка того, находится ли содержимое извлеченного поля протокола в безопасной области, как определяется моделью, и

этап b4: генерирование сигнала обнаружения вторжения (например, сопровождаемое фильтрацией извлеченного поля протокола или сообщения протокола, содержащего поле протокола, генерированием оповещения тревоги для пользователя, или любым другим действием обнаружения вторжения) в случае, когда установлено, что содержимое извлеченного поля протокола находится за пределами безопасной области.

В варианте осуществления сигнал обнаружения вторжения может дополнительно генерироваться, когда синтаксический анализ не может установить поле как согласующееся с протоколом или когда извлеченное поле не может быть ассоциировано ни с одной из моделей из набора моделей.

Фиг. 5 схематично изображает в качестве примера общий вид концепций, предлагаемых в данной патентной заявке. Процесс начинается с синтаксического анализа (500) сетевого трафика для извлечения по меньшей мере одного поля протокола сообщения протокола. Второй этап содержит ассоциирование (501) извлеченного поля протокола с моделью для данного поля протокола, причем модель выбирается из набора моделей. Набор моделей может содержать разные типы модели, при этом набор моделей представлен на фиг. 5 обозначением 513. Выбор типа модели для извлеченного поля протокола может быть обусловлен как типом значения поля протокола (представлен обозначением 511), так и семантикой, связанной с полем протокола (представлена обозначением 512). Набор (513) разных типов модели также предоставляется в качестве входных данных, причем разные типы модели могут включать в себя: модель числового диапазона, модель числового набора (перечисления), модель числового распределения, модель строки ASCII, модель строки Юникод, логическая модель, двоичная модель, основанная на п-грамм, эмулятор сети, набор сигнатур обнаружения вторжения и т.д. Процесс ассоциирования синтаксически проанализированного поля протокола с его соответствующей моделью (некоторым типом модели) также может быть усовершенствован посредством учета зависимости поля, которое описывает операцию, с полем, которое описывает аргумент такой операции (как представлено обозначением 509). В более общем плане, любая зависимость одного значения поля от другого значения поля (как представлено обозначением 510) может учитываться при ассоциировании синтаксически проанализированного поля протокола с его соответствующей моделью, таким образом, что несколько моделей строится для одного и того же поля в соответствии со значением другого поля в том же самом сообщении. На фазе обучения в случае, когда модель выбранного типа модели не существует для синтаксически проанализированного поля протокола, такая модель может быть создана (этап 515). Подобным образом, в случае, когда модель уже существует, модель может быть обновлена (этап 516) на фазе обучения, чтобы включать в себя текущее значение синтаксически проанализированного поля в безопасной области, определяемой моделью. В случае, когда синтаксический анализ не может установить поле, наблюдаемое в сетевых данных, как согласующееся со спецификацией протокола, может быть сгенерирован (этап 508) сигнал обнаружения вторжения. Во время фазы обнаружения, в случае, когда невозможно ассоциировать с синтаксически проанализированным полем существующую модель выбранного типа модели, может быть сгенерирован (этап 504) сигнал обнаружения вторжения. С другой стороны, в случае, когда возможно ассоциировать с синтаксически проанализированным полем существующую модель выбранного типа модели, значение поля оценивается (этап 503) по отношению к безопасной области, определяемой моделью. В случае, когда значение синтаксически проанализированного поля протокола не находится в рамках безопасной области, определяемой моделью, может быть сгенерирован (этап 505) сигнал обнаружения вторжения. В заключении, в случае, когда сигнал обнаружения вторжения генерируется по любой причине из рассмотренных выше, могут быть предприняты дополнительные этапы, такой как удаление (этап 506) из сетевого трафика сообщения протокола, ассоциированного с полем протокола с аномальным значением, или вызов (этап 507) и вывод сообщения оповещения о вторжении.

Следует понимать, что раскрытые варианты осуществления являются лишь примерными для изобретения, которое может быть воплощено в различных формах. Вследствие этого конкретные раскрываемые здесь структурные и функциональные подробности не должны интерпретироваться как накладывающие ограничение, а лишь как основа для формулы изобретения и в качестве репрезентативной основы для обучения специалистов в соответствующей области техники по различному использованию настоящего изобретения практически в любой соответствующем образом детализированной структуре. Кроме того, использованные здесь понятия и фразы не предназначены для ограничения, а, наоборот, для предоставления понятного описания изобретения.

Элементы вышеупомянутых вариантов осуществления могут быть объединены для создания других вариантов осуществления.

Использованные здесь формы единственного числа определяются как одно или более одного. Используемое здесь понятие "другой" определяется как, по меньшей мере, второй или более. Используемые здесь понятия "включающий в себя" и/или "обладающий" определены как содержащий (т.е., не исклю-

чающий другие элементы или этапы). Любые ссылочные обозначения в формуле изобретения не должны толковаться как накладывающие ограничение на объем формулы изобретения или изобретения. Тот лишь факт, что некоторые меры размещены во взаимно разных зависимых пунктах формулы изобретения не указывает на то, что сочетание этих мер не может быть использовано для получения преимущества. Объем изобретения ограничивается только нижеследующей формулой изобретения.

ФОРМУЛА ИЗОБРЕТЕНИЯ

1. Способ обнаружения несанкционированного вторжения в трафик данных в сети передачи данных, реализуемый посредством электронно-вычислительной машины, при этом способ содержит этапы, на которых

синтаксически анализируют посредством блока синтаксического анализа трафик данных для извлечения по меньшей мере одного поля протокола из сообщения протокола из трафика данных, причем протокол является сетевым протоколом передачи, причем сообщение протокола является Протокольной Единицей Данных;

причем на фазе обучения модель строят для извлеченного поля протокола, при этом фаза обучения содержит этапы, на которых

определяют тип данных извлеченного поля протокола;

выбирают тип модели для извлеченного поля протокола из множества типов модели на основании характеристики извлеченного поля протокола, причем характеристика содержит определенный тип данных, и

строят модель для извлеченного поля протокола на основании выбранного типа модели,

при этом способ также содержит этапы, на которых

ассоциируют посредством блока ассоциирования извлеченное поле протокола с соответствующей построенной моделью для извлеченного поля протокола, причем построенную модель выбирают из набора моделей, причем набор моделей содержит разные модели для разных полей протокола;

определяют посредством блока обработки модели, используя модель для извлеченного поля протокола, находится ли содержимое извлеченного поля протокола в безопасной области, в соответствии с моделью для извлеченного поля протокола, причем безопасная область указывает, что содержимое поля протокола не подвержено вторжению; и

генерируют посредством исполнительного блока сигнал обнаружения вторжения в случае, когда установлено, что содержимое извлеченного поля протокола находится за пределами безопасной области.

2. Способ обнаружения вторжения по п.1, при этом набор моделей содержит модель для поля протокола оператора и модель для поля протокола операнда, причем этапы, на которых ассоциируют и определяют, выполняют для поля протокола оператора и поля протокола операнда.

3. Способ обнаружения вторжения по п.2, в котором набор моделей дополнительно содержит модель для поля протокола маршалинга, причем этапы, на которых ассоциируют и определяют, дополнительно выполняют для поля протокола маршалинга.

4. Способ обнаружения вторжения по любому из предшествующих пунктов, при этом характеристика поля протокола содержит семантику поля протокола, причем способ содержит этапы, на которых

определяют семантику извлеченного поля протокола и

выбирают тип модели с использованием определенной семантики.

5. Способ обнаружения вторжения по любому из предшествующих пунктов, при этом набор моделей содержит соответствующую модель для каждого поля протокола из набора полей протокола.

6. Способ обнаружения вторжения по любому из предшествующих пунктов, при этом модель для поля определяют на фазе обучения, причем фаза обучения содержит этапы, на которых

синтаксически анализируют трафик данных для извлечения по меньшей мере одного поля протокола для протокола, применяемого в трафике данных;

ассоциируют извлеченное поле протокола с моделью для этого поля протокола, при этом модель выбирают из набора моделей; и

обновляют модель для извлеченного поля протокола с использованием содержимого извлеченного поля протокола.

7. Способ обнаружения вторжения по п.6, при этом, если ассоциирование не может быть выполнено между извлеченным полем протокола и одной из моделей, то способ содержит этап, на котором создают новую модель для извлеченного поля протокола и добавляют новую модель в набор моделей.

8. Способ обнаружения вторжения по любому из предшествующих пунктов, при этом дополнительно генерируют сигнал обнаружения вторжения, когда синтаксический анализ не может установить поле как согласующееся с протоколом.

9. Способ обнаружения вторжения по любому из предшествующих пунктов, при этом дополнительно генерируют сигнал обнаружения вторжения, когда извлеченное поле не может быть ассоциировано ни с одной из моделей из набора моделей.

10. Способ обнаружения вторжения по любому из предшествующих пунктов, при этом протокол

является по меньшей мере одним из протокола прикладного уровня, протокола уровня сеанса, протокола транспортного уровня или протокола более низкого уровня из стека протоколов.

11. Способ обнаружения вторжения по любому из предшествующих пунктов, при этом способ дополнительно содержит, в ответ на генерирование сигнала обнаружения вторжения, по меньшей мере один из этапов, на которых

удаляют упомянутое поле протокола или пакет данных, содержащий упомянутое поле протокола; и

вызывают и выводят сообщение оповещения о вторжении.

12. Способ обнаружения вторжения по любому из предшествующих пунктов, при этом модель для поля протокола, содержит по меньшей мере одно из:

набор значений поля протокола, которые считаются не подвергавшимися вторжению;

числовое распределениея значений поля протокола, причем числовое распределение образует функцию вероятности числовых значений поля протокола; и

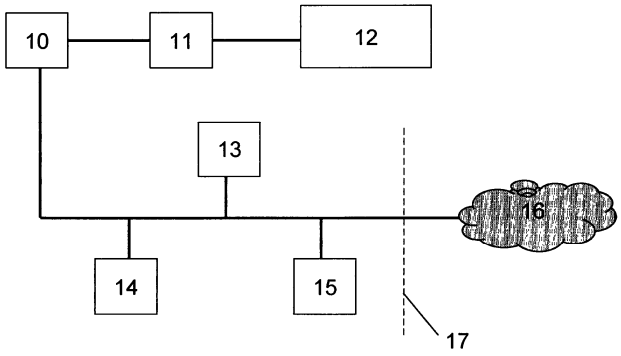
определение диапазона значений поля протокола, которые считаются не подвергавшимися вторжению.

13. Способ обнаружения вторжения по любому из предшествующих пунктов, при этом модель для поля протокола содержит определение букв, цифр, символов и сценариев, которые считаются не подвергавшимися вторжению.

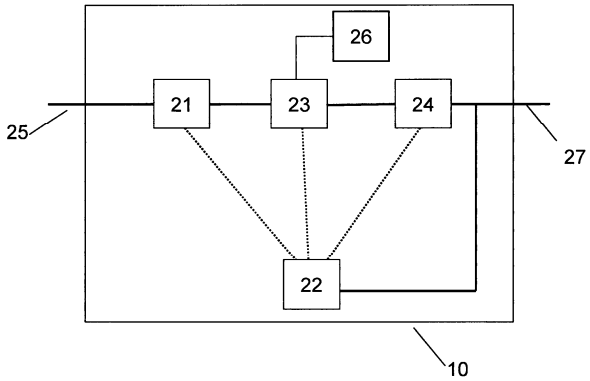
14. Способ обнаружения вторжения по любому из предшествующих пунктов, при этом модель для поля протокола содержит набор предварительно определенных сигнатур вторжения.

15. Способ обнаружения вторжения по любому из предшествующих пунктов, при этом набор моделей содержит две модели для одного поля протокола, причем конкретная одна из двух моделей ассоциирована с одним полем протокола на основании значения другого поля протокола.

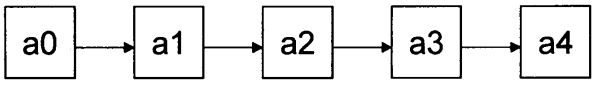
16. Электронно-вычислительное устройство для обнаружения несанкционированного вторжения в трафик данных в сети передачи данных, содержащее процессор и память для исполнения программных команд управления для осуществления способа по пп.1-15.



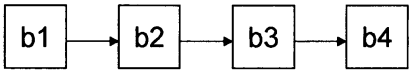
Фиг. 1



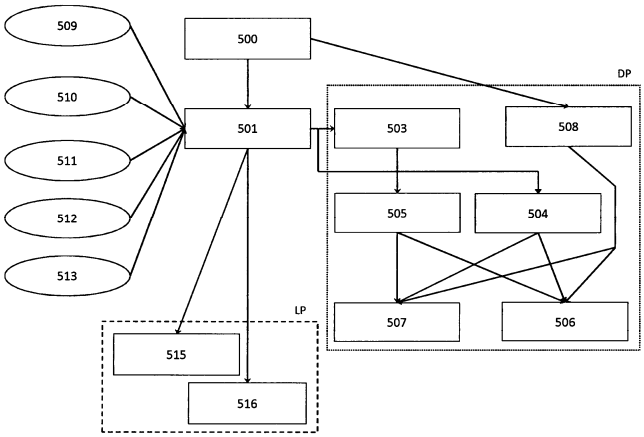
Фиг. 2



Фиг. 3


b1
b2
b3
b4

Фиг. 4


509
510
511
512
513
500
501
DP
503
508
505
504
507
506
LP
515
516

Фиг. 5