Международный союз электросвязи

МСЭ-Т X.1210

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

(01/2014)

СЕРИЯ X: СЕТИ ПЕРЕДАЧИ ДАННЫХ,
ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ
И БЕЗОПАСНОСТЬ

Безопасность киберпространства – Кибербезопасность

Обзор механизмов диагностики нарушений безопасности на основе источника для сетей на базе протокола Интернет

Рекомендация МСЭ-Т X.1210

ITU-T

Международный союз электросвязи

РЕКОМЕНДАЦИИ МСЭ-Т СЕРИИ X

СЕТИ ПЕРЕДАЧИ ДАННЫХ, ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ И БЕЗОПАСНОСТЬ

СЕТИ ПЕРЕДАЧИ ДАННЫХ ОБЩЕГО ПОЛЬЗОВАНИЯ	X.1–X.199
ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ	X.200–X.299
ВЗАИМОДЕЙСТВИЕ МЕЖДУ СЕТЯМИ	X.300–X.399
СИСТЕМЫ ОБРАБОТКИ СООБЩЕНИЙ	X.400–X.499
СПРАВОЧНИК	X.500–X.599
ОРГАНИЗАЦИЯ СЕТИ ВОС И СИСТЕМНЫЕ АСПЕКТЫ	X.600–X.699
УПРАВЛЕНИЕ В ВОС	X.700–X.799
БЕЗОПАСНОСТЬ	X.800–X.849
ПРИЛОЖЕНИЯ ВОС	X.850–X.899
ОТКРЫТАЯ РАСПРЕДЕЛЕННАЯ ОБРАБОТКА	X.900–X.999
БЕЗОПАСНОСТЬ ИНФОРМАЦИИ И СЕТЕЙ	
Общие аспекты безопасности	X.1000–X.1029
Безопасность сетей	X.1030–X.1049
Управление безопасностью	X.1050–X.1069
Телебиометрия	X.1080–X.1099
БЕЗОПАСНЫЕ ПРИЛОЖЕНИЯ И УСЛУГИ	
Безопасность многоадресной передачи	X.1100–X.1109
Безопасность домашних сетей	X.1110–X.1119
Безопасность подвижной связи	X.1120–X.1139
Безопасность веб-среды	X.1140–X.1149
Протоколы безопасности	X.1150–X.1159
Безопасность одноранговых сетей	X.1160–X.1169
Безопасность сетевой идентификации	X.1170–X.1179
Безопасность IPTV	X.1180–X.1199
БЕЗОПАСНОСТЬ КИБЕРПРОСТРАНСТВА	
Кибербезопасность	**X.1200–X.1229**
Противодействие спаму	X.1230–X.1249
Управление определением идентичности	X.1250–X.1279
БЕЗОПАСНЫЕ ПРИЛОЖЕНИЯ И УСЛУГИ	
Связь в чрезвычайных ситуациях	X.1300–X.1309
Безопасность повсеместных сенсорных сетей	X.1310–X.1339
ОБМЕН ИНФОРМАЦИЕЙ, КАСАЮЩЕЙСЯ КИБЕРБЕЗОПАСНОСТИ	
Обзор кибербезопасности	X.1500–X.1519
Обмен информацией об уязвимости/состоянии	X.1520–X.1539
Обмен информацией о событии/инциденте/эвристических правилах	X.1540–X.1549
Обмен информацией о политике	X.1550–X.1559
Эвристические правила и запрос информации	X.1560–X.1569
Идентификация и обнаружение	X.1570–X.1579
Гарантированный обмен	X.1580–X.1589
БЕЗОПАСНОСТЬ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ	
Обзор безопасности облачных вычислений	X.1600–X.1601
Проектирование безопасности облачных вычислений	X.1602–X.1639
Передовой опыт и руководящие указания в области облачных вычислений	X.1640–X.1659
Обеспечение безопасности облачных вычислений	X.1660–X.1679
Другие вопросы безопасности облачных вычислений	X.1680–X.1699

Для получения более подробной информации просьба обращаться к перечню Рекомендаций МСЭ-Т.

Рекомендация МСЭ-Т X.1210

Обзор механизмов диагностики нарушений безопасности на основе источника для сетей на базе протокола Интернет

Резюме

В Рекомендации МСЭ-Т X.1210 представлены механизмы диагностики нарушений безопасности на основе источника, а также критерии выбора и базовые руководящие принципы безопасности механизмов диагностики нарушений.

Диагностика нарушений безопасности на основе источника в сетях на базе протокола Интернет включает методы, используемые для обнаружения технической информации о точках входа, трактах, частичных трактах или источниках пакета или пакетов, являющихся причиной вызывающего проблему сетевого события, как правило, для целей применения мер по смягчению последствий.

Хронологическая справка

Издание	Рекомендация	Утверждение	Исследовательская комиссия	Уникальный идентификатор*
1.0	МСЭ-Т X.1210	24.01.2014 г.	17-я	11.1002/1000/12043

* Для получения доступа к Рекомендации наберите в адресном поле вашего браузера URL: http://handle.itu.int/, после которого следует уникальный идентификатор Рекомендации. Например, http://handle.itu.int/11.1002/1000/11830-en.

ПРЕДИСЛОВИЕ

Международный союз электросвязи (МСЭ) является специализированным учреждением Организации Объединенных Наций в области электросвязи и информационно-коммуникационных технологий (ИКТ). Сектор стандартизации электросвязи МСЭ (МСЭ-Т) – постоянный орган МСЭ. МСЭ-Т отвечает за изучение технических, эксплуатационных и тарифных вопросов и за выпуск Рекомендаций по ним с целью стандартизации электросвязи на всемирной основе.

На Всемирной ассамблее по стандартизации электросвязи (ВАСЭ), которая проводится каждые четыре года, определяются темы для изучения исследовательскими комиссиями МСЭ-Т, которые, в свою очередь, вырабатывают Рекомендации по этим темам.

Утверждение Рекомендаций МСЭ-Т осуществляется в соответствии с процедурой, изложенной в Резолюции 1 ВАСЭ.

В некоторых областях информационных технологий, которые входят в компетенцию МСЭ-Т, необходимые стандарты разрабатываются на основе сотрудничества с ИСО и МЭК.

ПРИМЕЧАНИЕ

В настоящей Рекомендации термин "администрация" используется для краткости и обозначает как администрацию электросвязи, так и признанную эксплуатационную организацию.

Соблюдение положений данной Рекомендации осуществляется на добровольной основе. Однако данная Рекомендация может содержать некоторые обязательные положения (например, для обеспечения функциональной совместимости или возможности применения), и в таком случае соблюдение Рекомендации достигается при выполнении всех указанных положений. Для выражения требований используются слова "следует", "должен" ("shall") или некоторые другие обязывающие выражения, такие как "обязан" ("must"), а также их отрицательные формы. Употребление таких слов не означает, что от какой-либо стороны требуется соблюдение положений данной Рекомендации.

ПРАВА ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

МСЭ обращает внимание на вероятность того, что практическое применение или выполнение настоящей Рекомендации может включать использование заявленного права интеллектуальной собственности. МСЭ не занимает какую бы то ни было позицию относительно подтверждения, действительности или применимости заявленных прав интеллектуальной собственности, независимо от того, доказываются ли такие права членами МСЭ или другими сторонами, не относящимися к процессу разработки Рекомендации.

На момент утверждения настоящей Рекомендации МСЭ не получил извещения об интеллектуальной собственности, защищенной патентами, которые могут потребоваться для выполнения настоящей Рекомендации. Однако те, кто будет применять Рекомендацию, должны иметь в виду, что вышесказанное может не отражать самую последнюю информацию, и поэтому им настоятельно рекомендуется обращаться к патентной базе данных БСЭ по адресу: http://www.itu.int/ITU-T/ipr/.

СОДЕРЖАНИЕ

Рекомендация МСЭ-Т X.1210

Обзор механизмов диагностики нарушений безопасности на основе источника для сетей на базе протокола Интернет

1 Сфера применения

В настоящей Рекомендации представлен обзор механизмов диагностики нарушений безопасности на основе источника, критерии оценки и базовые руководящие принципы безопасности механизмов диагностики нарушений.

Специалисты по применению и пользователи настоящей Рекомендации МСЭ-Т должны соблюдать все применимые национальные и региональные законы, нормативные акты и стратегии.

2 Справочные документы

Отсутствуют.

3 Определения

3.1 Термины, определенные в других документах

В настоящей Рекомендации используются следующие термины, определенные в других документах:

3.1.1 отказ в обслуживании [b-ITU X.800]: Недопущение санкционированного доступа к ресурсам или задержка выполнения операций, критических по времени.

3.1.2 домен безопасности (security domain) [b-ITU-T T.411]**:** набор ресурсов, в отношении которых действует одна стратегия безопасности

3.1.3 угроза [b-ITU-T X.800]: Потенциальное нарушение безопасности.

3.2 Термины и определения в настоящей Рекомендации

Отсутствуют.

4 Аббревиатуры и акронимы

В настоящей Рекомендации используются следующие аббревиатуры и акронимы:

AS	Autonomous System		Автономная система
BGP	Border Gateway Protocol		Протокол граничных шлюзов
DoS	Dental of Service		Отказ в обслуживании
ICMP	Internet Control Message Protocol		Протокол межсетевых управляющих сообщений
IP	Internet Protocol		Протокол Интернет
IPFIX	IP Flow Information Export		Экспорт информации о потоках IP
IPv4/v6	Internet Protocol version 4/version 6		Протокол Интернет версии 4/версии 6
ISP	Internet Service Provider	ПУИ	Поставщик услуг интернета
RID	Real-time Inter-network Defense		Межсетевая защита в реальном времени
TCP	Transmission Control protocol		Протокол управления передачей

5 Условные сокращения

Отсутствуют.

6 Общий обзор механизмов диагностики нарушений безопасности на основе источника

Диагностика нарушений безопасности на основе источника в сетях, базирующихся на протоколе Интернет (IP), включает, как правило, технический и/или административный процесс, необходимый для надежного определения источника IP-пакета или IP-пакетов, которые могут содержать или не содержать правильный IP-адрес отправителя или тракты либо части трактов, которые вносят нарушения безопасности.

Механизмы диагностики нарушений безопасности на основе источника могут использоваться для определения физического или логического местоположения таких событий нарушения безопасности в реальном времени с помощью сетевых элементов, например маршрутизаторов или главных компьютеров в сети.

Ниже описаны механизмы диагностики нарушений безопасности в базирующихся на IP сетях.

6.1 Диагностика нарушений безопасности на основе источника с тестированием линии

Диагностика нарушений может выполняться начиная от маршрутизатора, ближайшего к затронутому элементу, путем интерактивного тестирования его линий в восходящем направлении, до тех пор пока поставщики услуг интернета, не смогут определить, какая именно из этих линий используется для передачи проблемного трафика. В оптимальном случае эта процедура повторяется рекурсивно на восходящем маршрутизаторе до определения источника нарушения безопасности.

В рамках этого способа предполагается, что нарушение безопасности остается активным до завершения процедуры диагностики нарушения. Таким образом, этот метод непригоден для атак, обнаруживаемых после факта атаки, для атак, которые происходят периодически, или для атак, которые изменяют свои режимы в ответ на диагностику нарушений безопасности.

Одним из способов реализации механизма тестирования линии является отладка на входе. Это функция, которая уже имеется во многих маршрутизаторах, позволяет администратору анализировать входящие сетевые линии на наличие конкретных пакетов. Если оператор маршрутизатора знает конкретные характеристики трафика атаки (называемые "сигнатуры атаки"), то возможно выполнить анализ входящей сетевой линии на маршрутизаторе.

6.2 Диагностика нарушений безопасности на основе источника с наложенной сетью

Механизм вывода в "черную дыру" [b-IETF RFC 3882] это эксплуатационный способ, в котором используется туннель-колодец, реализуемый во всех возможных точках входа, которые могут использоваться для проникновения при атаке на целевую/атакуемую автономную систему (AC). Используя протокол граничных шлюзов (BGP) [b-IETF RFC 4271], трафик, предназначенный для атакуемого/целевого главного компьютера, может быть устранен из сети или перенаправлен в специальный тракт (туннель), где какое-либо устройство может собирать этот трафик для анализа и затем устранять его.

6.3 Диагностика нарушений безопасности на основе источника с зондированием

Протокол межсетевых управляющих сообщений (ICMP) как для протокола Интернет версии 4 (IPv4) [b-IETF RFC 792], так и для протокола Интернет версии 6 (IPv6) [b-IETF RFC 4443], являлся и будет оставаться одним из наиболее эффективных механизмов диагностики для сетей на базе IP. Ряд инструментов, включая эхо-запросы и трассировку трактов, предоставляются в пакете с широко распространенными операционными системами, которые используют ICMP для выполнения сквозной диагностики или диагностики на уровне линии.

6.4 Диагностика нарушений безопасности на основе источника с регистрацией и дискретизацией

Дискретизация потока может быть полезным механизмом диагностики нарушений безопасности в базирующихся на IP сетях. Операторы могут использовать экспорт информации о потоках sFlow [b-IETF RFC 3176], NetFlow [b-IETF RFC 3954] или IP-потоке (IPFIX) [b-IETF RFC 5655], учитывая при этом поддерживающие стандарты дискретизации потока, используемые в маршрутизаторах.

6.5 Диагностика нарушений безопасности на основе источника в рамках нескольких автономных сетей

В случае крупного нарушения безопасности, охватывающего несколько автономных систем, операторы могут использовать инструменты диагностики на основе зондирования (см. пункт 6.3) и онлайновые зонды, доступные в интернете, например Looking Glass [b-LG]. В будущем операторы возможно смогут упростить обмен информацией с помощью более совершенных инструментов диагностики в рамках нескольких автономных систем, например посредством использования межсетевой защиты в реальном времени (RID) [b-IETF RFC 6045].

7 Базовые руководящие принципы безопасности механизмов диагностики нарушений безопасности на основе источника

Представлены следующие базовые руководящие принципы безопасности для диагностики нарушений безопасности на основе источника.

- Механизмы диагностики нарушений безопасности на основе источника должны в силу проектного решения быть масштабируемыми, устойчивыми и надежными.
- Механизмы диагностики нарушений безопасности на основе источника следует использовать и эксплуатировать в рамках нескольких доменов, каждый из которых управляется ответственным за безопасность администратором (то есть диагностика нарушений в рамках нескольких автономных систем).
- Механизмы диагностики нарушений безопасности на основе источника должны реализовываться в соответствии с моделями развертывания двух типов: модель централизованного развертывания и модель распределенного развертывания.
- Механизмы диагностики нарушений безопасности на основе источника должны обеспечивать обнаруживаемую техническую информацию о точках входа, трактах, частичных трактах или источниках пакета или пакетов, являющихся причиной вызывающего проблему сетевого события, как правило, для целей применения мер по смягчению последствий.
- Для выбора подходящего механизма диагностики нарушений безопасности на основе источника следует оценивать эти механизмы по критериям, приведенным в разделе 8.
- Интерфейс механизмов диагностики нарушений безопасности на основе источника в рамках нескольких автономных систем должен обеспечивать конфиденциальность, аутентификацию источника данных и целостность информации, участвующей в обмене между разными доменами безопасности, и может обеспечивать доступность механизма диагностики нарушений.

8 Критерии оценки механизмов диагностики на основе источника

Определены следующие критерии, которые могут использоваться для оценки механизмов диагностики нарушений:

- Степень участия поставщика услуг интернета (ПУИ): степень участия ПУИ при выполнении диагностики нарушений определяется администратором ПУИ. В большинстве механизмов диагностики нарушений предполагается, что ПУИ обеспечивает ограниченные технические средства, позволяющие провести диагностику нарушений. Оптимальной схемой диагностики является схема, требующая незначительного участия ПУИ.
- Число пакетов, требуемых для диагностики нарушений: число используемых администратором пакетов для определения источника нарушения безопасности после обнаружения нарушения безопасности.
- Эффективность частичного развертывания: степень эффективности диагностики нарушений, когда схемы диагностики развернуты частично в рамках одного ПУИ. Эффективность определяется в диапазоне от невозможности выполнения идентификации до выполнения значащей идентификации.
- Затраты ресурсов на диагностику нарушений: объем затрат ресурсов на обработку в промежуточном сетевом элементе или являющемся потенциальным объектом атаки главном компьютере. Предпочтительна оптимальная схема диагностики нарушений с минимальным объемом ресурсов, затрачиваемых на обработку, для промежуточного сетевого элемента или главного компьютера, являющегося потенциальным объектом атаки.

- Степень увеличения ширины полосы: дополнительный объем трафика, необходимого для диагностики нарушений. Желательный механизм диагностики нарушений должен характеризоваться минимальным увеличением ширины полосы или не увеличивать ширину полосы.
- Требования к памяти: объем дополнительной памяти, требуемой в сетевых элементах или выделенном сервере диагностики. Дополнительная память в сетевом элементе нежелательна, а дополнительная память в выделенных серверах допустима. Оптимальный механизм диагностики нарушений требует ограниченного объема дополнительной памяти в выделенном сервере и не требует дополнительной памяти в сетевой элементе.
- Устойчивость диагностики нарушений: способность механизма диагностики нарушений выдавать значащие результаты работы, даже если некоторые сетевые элементы, участвующие в диагностике, были нарушены. Нарушения возникают вследствие ошибок в результате неправильной конфигурации сетевого элемента или ненадлежащих программных корректировок.
- Масштабируемость: объем дополнительной конфигурации, которую необходимо выполнить на других сетевых элементах для добавления одного сетевого элемента. Это показывает, насколько просто может быть расширена схема диагностики. Масштабируемость рассматривается как удовлетворительная, если конфигурация требуется только на новом добавленном элементе, и как неудовлетворительная, если добавление одного сетевого элемента требует выполнения полной конфигурации остальных сетевых элементов. Оптимальный механизм диагностики должен быть масштабируемым.
- Число функций, необходимых для выполнения диагностики: объем дополнительных функций, требуемых для реализации данной схемы диагностики.
- Способность обрабатывать массированные нарушения безопасности сетевого уровня: способность схемы диагностики отражать эффективность идентификации схемой диагностики нарушений безопасности сетевого уровня. Оптимальная схема диагностики должна идентифицировать любое нарушение безопасности, включая атаки типа распределенного отказа в обслуживании (DDoS).
- Способность диагностики преобразованных пакетов: способность схемы диагностики идентифицировать источник проблем, даже в случае проведенного преобразования пакетов. Преобразование пакетов означает внесение в пакет изменений при пересылке пакета. К наиболее распространенным преобразованиям относится трансляция сетевых адресов, при которой изменяется адрес источника и/или назначения пакетов или пакета.

Библиография

[b-ITU-T X.800] Рекомендация МСЭ-Т X.800 (1991 г.), *Архитектура безопасности для взаимосвязи открытых систем для приложений МККТТ*.

[b-ITU-T T.411] Recommendation ITU-T T.411 (1993), *Information technology – Open Document Architecture (ODA) and interchange format: Introduction and general principles*.

[b-IETF RFC 792] IETF RFC 792 (1981), *Internet Control Message Protocol*.

[b-IETF RFC 3176] IETF RFC 3176 (2001), *InMon Corporation's sFlow: A Method for Monitoring Traffic in Switched and Routed Networks*.

[b-IETF RFC 3882] IETF RFC 3882 (2004), *Configuring BGP to Block Denial-of-Service Attacks*.

[b-IETF RFC 3954] IETF RFC 3954 (2004), *Cisco Systems NetFlow Services Export Version 9*.

[b-IETF RFC 4271] IETF RFC 4271 (2006), *A Border Gateway Protocol 4 (BGP-4)*.

[b-IETF RFC 4443] IETF RFC 4443 (2006), *Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification*.

[b-IETF RFC 5655] IETF RFC 5655 (2009), *Specification of the IP Flow Information Export (IPFIX) File Format*.

[b-IETF RFC 6045] IETF RFC 6045 (2010*), Real-time Inter-network Defense (RID)*.

[b-LG] BGP Looking Glass, http://www.lookinglass.org/

СЕРИИ РЕКОМЕНДАЦИЙ МСЭ-Т

Серия A	Организация работы МСЭ-Т
Серия D	Общие принципы тарификации
Серия E	Общая эксплуатация сети, телефонная служба, функционирование служб и человеческие факторы
Серия F	Нетелефонные службы электросвязи
Серия G	Системы и среда передачи, цифровые системы и сети
Серия H	Аудиовизуальные и мультимедийные системы
Серия I	Цифровая сеть с интеграцией служб
Серия J	Кабельные сети и передача сигналов телевизионных и звуковых программ и других мультимедийных сигналов
Серия K	Защита от помех
Серия L	Конструкция, прокладка и защита кабелей и других элементов линейно-кабельных сооружений
Серия M	Управление электросвязью, включая СУЭ и техническое обслуживание сетей
Серия N	Техническое обслуживание: международные каналы передачи звуковых и телевизионных программ
Серия O	Требования к измерительной аппаратуре
Серия P	Оконечное оборудование, субъективные и объективные методы оценки
Серия Q	Коммутация и сигнализация
Серия R	Телеграфная передача
Серия S	Оконечное оборудование для телеграфных служб
Серия T	Оконечное оборудование для телематических служб
Серия U	Телеграфная коммутация
Серия V	Передача данных по телефонной сети
Серия X	**Сети передачи данных, взаимосвязь открытых систем и безопасность**
Серия Y	Глобальная информационная инфраструктура, аспекты протокола Интернет и сети последующих поколений
Серия Z	Языки и общие аспекты программного обеспечения для систем электросвязи

Отпечатано в Швейцарии
Женева, 2014 г.