УДК 004.772 DOI: 10.34759/trd-2020-115-12

Методы оценки эффективности вуалирующих преобразований интернет-протоколов

Неволин А.О.

Московский авиационный институт (национальный исследовательский университет), МАИ, Волоколамское шоссе, 4, Москва, А-80, ГСП-3, 125993, Россия

e-mail: nevolin.ao@yandex.ru

Статья поступила 10.11.2020

Аннотация

В статье описываются современные способы анализа сетевого трафика. Проводится анализ эффективности мер по защите передаваемых данных без использования шифрования. Описываются модели системы в целом, передающей и принимающей сторон, злоумышленника. Предлагаются способы анализа завуалированного трафика атакующим. Проводится оценка эффективности конкретных преобразований протоколов, основанных на XML.

Ключевые слова: передача данных, информационная безопасность, шифрование, скрытый информационный обмен, маскирующие преобразования, человек посередине.

Введение

Сегодня объемы трафика в авиационно-космической технике достаточно велики. Передаваемая информация относится к самым разным категориям: данные метрологии, команды управления, мониторинг состояния устройств (как во время испытательных полетов, так и во время рядовой эксплуатации) и другие [1, 2, 3]. При этом зачастую трафик проходит через множество узлов, коммутаторов и каналов связи [4], и у злоумышленников возникает стабильно высокий интерес к попытке перехвата данных в этой среде.

В качестве инструментов исследования долгое время использовались т.н. сетевые экраны (брандмауэры, или firewall в англоязычной литературе). Все эти инструменты используют достаточно простой принцип блокирования или анализа информации, основанный на разделении каналов данных по адресам или портам.

Следующее поколение сетевых экранов позволяло анализировать не только сетевые адреса, но и заголовки передаваемой информации. Так, на основе такого анализа определялись протоколы и, иногда, некоторые шаблоны взаимодействия клиента и сервера [5, 6].

Сегодня функционал данных инструментов значительно эволюционировал и позволяет «заглянуть» не только в заголовки пакетов, но и в их содержимое. При этом может использоваться как эвристический анализ (поиск по шаблону), так и исследование статистических характеристик (задержки между пакетами, средняя длина пакета и др.). Такие средства получили название DPI (Deep Packet Inspection) [7]. Их целью может являться:

- определение реального типа трафика (протокола);
- поиск определенных данных в трафике.

Одним из распространенных подходов к защите информации стало использование шифрования. Однако в целом ряде случае его применение невозможно или нецелесообразно. Например, сам факт применения шифрования неизбежно влечет интерес к системе в целом, и в ряде случаев злоумышленнику не нужно пытаться декодировать данные – он просто произведет атаку типа «отказ в обслуживании» [8, 9, 10], что приведет систему к неработоспособности.

В [17] был предложен общий подход к защите от определения реального типа трафика путем вуалирования передаваемых данных (маскировки одного протокола под другой). Данный подход не требует использования шифрования и основан на «запутывании» атакующей стороны.

Однако до сих пор не было предложено никаких мер и методик оценки эффективности защиты информации таким образом. Между тем, наличие подобного инструментария необходимо как для принятия проектных решений (об использовании или неиспользовании такого подхода), так и для выбора конкретных протоколов (исходных и маскирующих).

В статье впервые предлагаются способы оценки эффективности подобных преобразований с точки зрения защищенности передаваемых данных.

Для того, чтобы описать соответствующий метод, опишем сначала модель системы.

Модель системы в целом

Пусть имеется информационная система, в которой присутствуют две стороны, обменивающиеся данными. Передача данных осуществляется через открытый канал связи без использования шифрования. В системе используется XML-образный протокол на базе XML [11, 12, 13].

Предположим, что есть N возможных протоколов: Pr1, Pr2, …, PrN.

Любой из этих протоколов содержит теги, имеющие название *Tg1, Tg2, …, Tg_r*. Эти теги совместно образуют коллекцию (алфавит) тегов с названием *A_tg*. Данный алфавит состоит из *r* элементов. Также в протоколе имеется множество атрибутов с названием *At1, At2, …, At_s*, совместно образующих алфавит названий *A_at*, состоящий из *s* элементов.

Как тег, так и атрибут, имеющие одно и то же название, могут встречаться в протоколе более, чем один раз. Каждый протокол, таким образом, имеет определенные статистические свойства:

- вероятность появления атрибутов P_{ATTR1}, P_{ATTR2}, …, P_{ATTRs};
- вероятность появления тегов P_{T1}, P_{T2}, …, P_{Tr}.

Предположим, что для телекоммуникационного обмена используется произвольно выбранный (из общего множества) протокол.

Защищающейся стороной будем называть как отправителя, так и получателя. Злоумышленником будем называть атакующую сторону. Его цель – перехват пакетов с данными в процессе их передачи от отправителя к получателю.

Будем считать, что в информационном обмене используется канал, не вносящий искажения в сообщения.

Цель защищающейся стороны – завуалировать передаваемую информацию таким образом, чтобы злоумышленник не смог определить, какой из протоколов реально используется для передачи.

Модель защищающегося

Пусть передающая сторона для защиты отправляемой информации выполняет вуалирующие преобразования информации, передаваемой по выбранному протоколу. Принимающая сторона выполняет обратные преобразования. Алгоритм вуалирования и его параметры известны только защищающейся стороне.

Вуалирующем преобразованием будем называть такое обратимое преобразование Q, которое преобразует исходную информацию X в информацию X` (X -> X`).

Данное преобразование меняет статистические характеристики протокола, к которому оно применяется:

- Вероятности появления уже существующий параметров могут поменяться. Причем такое изменение может привести к «исчезновению» параметра – т.е. к тому, что вероятность сведется к нулю;
- Также могут образоваться новые параметры. Это можно интерпретировать как параметры, присутствовавшие изначально, но имеющие нулевую вероятность появления.

Список возможных преобразований описан в [4].

Цель защищающейся стороны – выбрать такие вуалирующие преобразования (и их параметры), которые обеспечили бы максимальную защищенность передаваемых данных от обнаружения вида используемого протокола. Выбор тех или иных параметров алгоритмов (равно как и самих алгоритмов) возможен только наличии модели действий атакующего, поскольку необходимо строить меру защищенности на основе оценки вероятности успешной атаки. В связи с этим дальнейшие исследования параметров модели отправителя и получателя (относительно алгоритмов выбора оптимальных способов вуалирования) возможны после изучения модели злоумышленника (методов атаки, их эффективности и т.п.).

Модель атакующего

Злоумышленник не знает, какой из N протоколов используется в системе, однако ему известны все N протоколов, в том числе и их статистические характеристики. Злоумышленника начинает перехват сообщений параллельно с началом функционирования системы.

В роли злоумышленника может выступать либо человек, либо автоматизированные программные средства и комплексы. В случае работы человека решения могут приниматься за счет «интуиции». Такая модель в работе не рассматривается, так как пока не существует аппарата для формализации человеческой логики. Если применяются программные автоматизированные комплексы, то атака может возможна только при наличии четко заданного эффективного алгоритма действий – такая модель будет рассмотрена далее.

Задача злоумышленника – определить используемый протокол передачи данных.

В реальности злоумышленнику необходимо выполнить два действия:

- Установить факт применения вуалирующих преобразований;
- Определить реально используемый протокол;

Установление факта вуалирования

Будем считать, что злоумышленник должен установить факт вуалирования (или его отсутствия) без знания конкретного протокола. Рассмотрим способ, которым он может это выполнить.

Как упоминалось ранее, отправитель и получатель применяют алгоритм вуалирования. Такой алгоритм неизбежно изменяет статистические свойства протокола. При этом конкретный алгоритм вуалирования меняется с определенным временным интервалом. Следовательно, с тем же интервалом меняются и статистические свойства перехватываемых атакующим сообщений. Из этого вытекает, что если атакующий будет иметь две выборки – одну до момента смены алгоритма вуалирования, вторую – после – и установит, что они не принадлежат одному и тому же закону распределения с одинаковыми значениями, то для него будет очевиден факт изменения алгоритма вуалирования. Следовательно, очевиден и факт использования такого алгоритма.

Для выявления меры соответствия разных серий перехваченных данных одному и тому же закону распределения со схожими параметрами злоумышленник может воспользоваться методами математической статистики – например, *критерием*

согласия. Наиболее часто используется критерий Пирсона (Хи-квадрат). Этот критерий применяется как для проверки гипотезы о принадлежности результатов эксперимента какому-либо знакомому распределению, так и для проверки гипотезы о соответствии результатов одной выборки данных результатам другой выборки.

Определим меру расхождения R между двумя распределениями. Применим критерий Хи-квадрат. При этом берется сумма квадратов отклонений $p_{i1} - p_{i2}$ статистических вероятностей в каждой из выборок, взятых с определенными «весами» (1):

$$R = \sum_{i=1}^{r} c_i \cdot \left(p_{i1} - p_{i2}\right)^2 \qquad (1)$$

где R – степень несоответствия между распределениями, p_{i1}, p_{i2} – вероятности i-го события в каждой выборке, c_i – весовые коэффициенты.

В связи с тем, что отклонения, относящиеся к разным значениям p_i, нельзя считать равноправными по значимости, вводятся коэффициенты c_i: одно и то же по абсолютной величине отклонение может быть незначительным, если сама вероятность p_i велика, и, наоборот, очень весомым, если p_i мала.

Пирсоном доказано: если положить (2)

$$c_i = \frac{n}{p_i}, \qquad (2)$$

где n – общее число опытов, p_i – вероятность i-го события,

то при достаточном числе экспериментов закон распределения величины R близок к распределению Хи-квадрат [18].

Предположим, что атакующий перехватил s серий (выборок) сообщений системы (в нашем случае s = 2), по n_j, j = (1, r) тегов в каждой серии. На основе перехваченных сообщений злоумышленник находит частоты появления каждого из тегов p*j = n_j/n (n_j – число появлений тега, n – общее число тегов в серии) в каждой из серий.

Необходимо подтвердить или опровергнуть гипотезу H_0 о том, что во всех множествах наблюдалась одна и та же совокупность вероятностей p*j.

1) Для каждой i-й серии, i = (1, s), подсчитываются числа n_{ji} появлений тегов T_j, j = (1, r).

2) Подсчитывается суммарное число Nj (4) появлений тега Tj, j=(1, r), во всех сериях, а также числа n_i, i=(1, s) (5) и n (6)

$$N_j = \sum_{i=1}^{s} n_{ji} \tag{4}$$

$$n_i = \sum_{j=1}^{r} n_{ji} \tag{5}$$

$$n = \sum_{i=1}^{s} \sum_{j=1}^{r} n_{ji} \, . \tag{6}$$

3) Вычисляется значение z статистики критерия Хи-квадрат по формуле (7)

$$z = \varphi(z_n) = n \cdot \left(\sum_{i=1}^{s} \sum_{j=1}^{r} \frac{n_{ji}^{\,2}}{n_i \cdot N_j} - 1 \right) . \tag{7}$$

4) Как было сказано выше, при больших n распределение статистики z хорошо аппроксимируется с распределением Хи-квадрат $X_2(m)$ с m = (s – 1)*(r – 1) степенями свободы.

Формируется критическая область (8)

$$\overline{G} = (x_{1-\alpha}(m), +\infty), \quad (8)$$

где $x_{1-\alpha}(m)$ – квантиль уровня 1- α распределения $X_2(m)$, α – вероятность ошибки первого рода.

5) Принимается статистическое решение: отклонить гипотезу H_0, если $\varphi(z_n) \in \overline{G}$, и принять гипотезу H_0, если $\varphi(z_n) \in G$ [19].

Рассмотрим более подробно вероятности ошибки. При принятии решения существует определенная вероятность появления одной из двух ошибок: ошибку 1-го рода («false positive» – отклонение гипотезы при том, что она верна) и 2-го рода («false negative» – принятие гипотезы при том, что она ложна). При этом на основе сравнения полученного значения статистики z с некоторым порогом атакующим принимается решение о принятии или непринятии гипотезы. В соответствии с п. 4 порог сравнения может быть выбран исходя из требуемой вероятности ошибки первого рода.

Из математической статистики известно [19], что с понижением порога (сужением доверительной области) повышается вероятность ошибки первого рода (фактически критерий становится более «строгим»), а с повышением порога (расширением доверительной области) – повышается вероятность ошибки второго рода (критерий может получиться слишком «мягким»).

В таком случае злоумышленник может применить критерий Неймана-Пирсона, который предполагает выбор такого оптимального решения, которое позволяет обеспечить минимальное значение вероятности ошибки второго рода (P2) при условии, что вероятность ошибки первого рода будет не больше определенного заданного значения. Будучи примененным к текущей задаче, этот критерий предполагает, что атакующий выбирает максимально допустимую для него вероятность ошибки первого рода и устанавливает порог в соответствии с этой вероятностью. Понижение порога вызовет превышение приемлемой вероятности false positive, а повышение порога будет неоптимальным, так как повысится вероятность false negative (при том, что вероятность P1 по-прежнему устраивает атакующего).

Определение используемого протокола

Как было сказано ранее, злоумышленник имеет сведения обо всех применяемых протоколах, равно как и об их статистических характеристиках. При этом он не знает, какой конкретно сейчас протокол используется в процессе телекоммуникационного обмена. Одновременно с этим он имеет перехваченную серию данных, обладающую некоторыми статистическими свойствами. Поскольку известно, что эта выборка обязательно должна принадлежать к одному из существующих (используемых) протоколов, то злоумышленнику необходимо сверить статистические данные перехваченной серии сообщений с известными ему данными обо всех протоколах, а далее – предположение о том, какой именно протокол используется в настоящий момент.

В предложенной выше модели для сопоставления статистических данных злоумышленник применяет тот же критерий согласия, что и при установлении факта вуалирования. Он находит меру несоответствия пепрехваченных данных с каждым из известных ему образцов, после чего делает предположение, что используется именно тот протокол, который обеспечил наименьшее расхождение. В оптимальном приемнике используется такой же подход: фактически, принимается решение о получении сигнала, имеющего максимальный коэффициент корреляции («похожести») с имеющимися эталонами.

Допустим, перехвачена серия сообщений информационного обмена. Для сопоставления статистических данных с имеющимися протоколами злоумышленнику необходимо сделать следующее для каждого из протоколов:

1) Подсчитать nj_прот и nj_перехв – числа появлений тегов в образце протокола и перехваченной серии.

2) Найти суммарное число N_j появлений тега T_j, j=(1, r) в образце протокола и перехваченной серии (9)

$$N_j = n_{j\_прот} + n_{j\_перехв}. \quad (9)$$

3) Найти общее число тегов в образце протокола (10) и перехваченной серии (11):

$$n_{прот} = \sum_{j=1}^{r} n_{j\_прот}, \quad (10)$$

$$n_{перехв} = \sum_{j=1}^{r} n_{j\_перехв}. \quad (11)$$

4) Найти общее число тегов (12)

$$n = n_{прот} + n_{перехв} . \quad (12)$$

5) Вычислить значение z статистики критерия Хи-квадрат (13)

$$z = \varphi(z_n) = n \cdot \left(\sum_{j=1}^{1} \frac{n_{j\_прот}^{2}}{\mathrm{n}_{\text{прот}} \cdot \mathrm{N}_{\mathrm{j}}} + \sum_{j=1}^{1} \frac{n_{j\_перехв}^{2}}{\mathrm{n}_{\text{перехв}} \cdot \mathrm{N}_{\mathrm{j}}} - 1 \right) . \quad (13)$$

Таким образом, для каждого из имеющихся протоколов будет найдено значение z, которое фактически будет означать меру расхождения перехваченной выборки с тем или иным протоколом. Злоумышленник принимает решение о том, что используется тот протокол, мера расхождения с которым была наименьшей (наименьшее значение z).

Оценка эффективности алгоритмов вуалирования XML-подобных протоколов передачи данных

В [20] предложены конкретные алгоритмы вуалирования, схожие с методами обфускации программного кода [14, 15, 16]. Исследуем их эффективность.

Переименование тегов и атрибутов

С точки зрения статистики именно этот метод будет в максимальной степени изменять документы. Это вызвано тем, что переименование равнозначно исчезновению одних тегов, но появлению других. Другими словами, вероятность появления у переименованных тегов станет нулевой, а у других – наоборот, из нулевой станет ненулевой.

Доверительная вероятность (по сути – конкретные значения статистики Хи-квадрат) будут изменяться при изменении некоторых параметров вуалирования. Например, можно переименовывать не все теги, а только их часть. Кроме этого,

допустимо делать такие преобразования таким образом, чтобы получать не новые имена, а обмениваться ими между собой.

Изменение местоположения ветвей и листьев в XML-дереве

Величина различия исходного пакета данных от завуалированного при использовании данного метода будет зависеть от выбранной стратегии преобразований. Если перестановки дополняются добавлением информации о прежнем местоположении элемента, то это равносильно появлению новых тегов в документе. Следовательно, изменятся и его статистические характеристики. Однако если получатель имеет информации о перестановках в ином виде (например, в виде секрета), то статистические свойства останутся неизменными.

Вертикальная перестановка тегов в XML-дереве

Выводы по данному способу вуалирования в целом аналогичны сделанным для предыдущего метода: перестановки тегов не изменяют статистических свойств документа. Однако если меняются местами уровни, имеющие разное число элементов, то такая ситуация по сути будет исключением. Допустим, если есть уровень, имеющий пять потомков, то перестановка имен тегов в данном случае повлияет на статистические свойства – ведь в документе получится пять тегов с именем родителя и один тег с именем потомка.

Горизонтальное движение элементов в XML-дереве

Ситуация полностью аналогично той, что была описана в предыдущем преобразовании (вертикальная перестановка тегов).

Синтезирование элементов в XML-дереве

В данном способе вуалирования некоторые теги становятся атрибутами другого тега. В связи с этим статистические свойства завуалированного пакета данных, становятся отличными от исходного. Как и в случае с переименованием тегов, степень изменения статистических свойств зависит от «глубины» вуалирования, т.е. количества тегов, которые затрагиваются преобразованием.

Выводы

В статье предложена модель системы (в целом и в частности – модель злоумышленника и защищающегося). Описаны метрики оценки эффективности защиты данных при применении вуалирующих преобразований поток данных.

В случаях, когда необходимо не только защитить передаваемые данные, но и скрыть факт обмена, маскирующие преобразования имеют гораздо большую эффективность, нежели традиционные алгоритмы шифрования. Так, например, для XML-образных протоколов применение шифрующей технологии XML Security значительно повышает вероятность обнаружения в виду явного искажения статистических характеристик данных внутри тегов.

Библиографический список

1. Гуревич О.С., Кессельман М.Г., Трофимов А.С., Чернышов В.И. Современные беспроводные технологии: проблемы применения на авиационном борту // Труды МАИ. 2017. № 94. URL: http://trudymai.ru/published.php?ID=81143

2. Титов А.Г., Неретин Е.С., Дудкин С.О., Брусникин П.М. Разработка архитектуры бортового сервера данных для применения в составе комплекса радиоэлектронного

оборудования с применением концепции интегрированной модульной авионики // Труды МАИ. 2019. № 105. URL: http://trudymai.ru/published.php?ID=104257

3. Романов А.М., Гринголи Ф., Сикора А. Беспроводная синхронизация бортовых вычислительных устройств при помощи WiFi // Труды МАИ. 2019. № 108. URL: http://trudymai.ru/published.php?ID=109522. DOI: 10.34759/trd-2019-108-13

4. Шихин С.М. Задача контроля данных системы управления работой космического аппарата с охватом проблемной области // Труды МАИ. 2019. № 109. URL: http://trudymai.ru/published.php?ID=111442. DOI: 10.34759/trd-2019-109-28

5. Khummanee S., Khumseela A., Puangpronpitag S. Towards a new design of firewall: Anomaly elimination and fast verifying of firewall rules // 2013 10th International Joint Conference on Computer Science and Software Engineering (JCSSE), 29 - 31 May 2013, Thailand. DOI:10.1109/JCSSE.2013.6567326

6. Sheng H., Wei L., Zhang C., Zhang X. Privacy-Preserving Cloud-Based Firewall for IaaS-based Enterprise // 2016 International Conference on Networking and Network Applications (NaNA), 23 - 25 July 2016, Hakodate, Japan. DOI: 10.1109/NaNA.2016.37

7. Wei L., Hongyu L., Xiaoliang Z. A network data security analysis method based on DPI technology // 2016 7th IEEE International Conference on Software Engineering and Service Science (ICSESS), 26 - 28 August 2016, Beijing, China, DOI: 10.1109/ICSESS.2016.7883228

8. Nagpal B., Sharma P., Chauhan N., Panesar A. DDoS tools: Classification, analysis and comparison // 2015 2nd International Conference on Computing for Sustainable Global Development (INDIACom), 11 - 13 March 2015, New Delhi, India.

9. Wu Z., Wang C., Zeng H. Research on the comparison of Flood DDoS and Low-rate DDoS // 2011 International Conference on Multimedia Technology, 26 - 28 July 2011, Hangzhou, China. DOI: 10.1109/ICMT.2011.6002141

10. Зеленский М.Д. DDOS-атаки: типы атак, устранение DDOS-атак // IV Всероссийская научно-техническая конференция «Студенческая наука для развития информационного общества»: сборник материалов (Ставрополь, 28 - 30 апреля 2016). - Ставрополь: Северо-Кавказский федеральный университет, 2016, С. 241 - 243.

11. Davis S., Burnett I. Collaborative Editing using an XML Protocol. TENCON 2005 // 2005 IEEE Region 10 Conference, pp. 1-5. DOI: 10.1109/TENCON.2005.300936.

12. Абрамов М.В., Шек В.М. Применение открытых протоколов обмена данными на основе XML в автоматизированной системе жилищной организации // Горный информационно-аналитический бюллетень. 2004. № 4. С. 134 - 137.

13. Бражук А.И. Создание семантической модели атак и уязвимостей программного обеспечения на основе публичных источников знаний // II Всероссийская научная конференция с международным участием «Информационные технологии в моделировании и управлении: подходы, методы, решения: сборник трудов (Тольятти, 22 - 24 апреля 2019). - Тольятти: Издатель Качалин Александр Васильевич, 2019. С. 435 - 442.

14. Peng Y., Chen Y., Shen B. An Adaptive Approach to Recommending Obfuscation Rules for Java Bytecode Obfuscators // 2019 IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC), 15 - 19 Jul 2019, Milwaukee, USA. DOI: 10.1109/COMPSAC.2019.00023

15. Сипаков Д.С., Губенко Н.Е. Сравнительный анализ методов обфускации программного кода // Всеукраинская научно-техническая конференция аспирантов и молодых ученых «Информационно-управляющие системы и технологии» - Донецк: ДонНТУ, 2014. С. 37 - 42.

16. Иванов П.С. Обфускация и защита программных продуктов. URL: http://citforum.ru/security/articles/obfus

17. Неволин А.О. Перспективные способы вуалирования интернет-протоколов // Электросвязь. 2019. № 8. С. 49 - 52.

18. Вентцель Е.С., Овчаров Л.А. Теория вероятностей и ее инженерные приложения. – М.: Наука, 1988. – 480 с.

19. Кибзун А.И., Горяинова Е.Р., Наумов А.В., Сиротин А.Н. Теория вероятностей и математическая статистика: базовый курс с примерами и задачами. – М.: Физматлит, 2002. – 224 с.

20. Неволин А.О. Эффективные методы интерпретации информационных потоков для обеспечения безопасности информационного взаимодействия // VIII Международная научно-техническая конференция «Гражданская авиация на современном этапе развития науки, техники и общества: тезисы докладов (Москва, 26 - 27 апреля 2008). - М.: Изд-во МГТУ ГА, 2008. С. 70 – 71.

Internet-protocols obfuscating encoding algorithms effectiveness measurement methods

Nevolin A.O.

Moscow Aviation Institute (National Research University), MAI,

4, Volokolamskoe shosse, Moscow, A-80, GSP-3, 125993, Russia

e-mail: nevolin.ao@yandex.ru

Abstract

Data encryption is not always possible today. In some situations attacker does not actually need to decode information – he just can organize DDOS-attack and turn attacked system off for a some (maybe long) time. If information system uses encryption protocols, it's always a good hint for security analyst – if data is encrypted, that means than there is something important.

There are some ways to protect data and whole system – by alternative methods of secure data processing, digital steganography for example. A new method is protocol masking. In this way we encode some protocol so it looks like another. So attacker does not actually know what kind of information is transferred through channel that he is listening.

While encoding one protocol as another we must remember to keep it's basic characteristic similar to referenced protocol. If we don't, attacker can easily not only detect fact of masking, but also find out which protocol we used originally. So we need some metrics to describe measure of information "protectiveness". These metrics can be, for example, statistical characteristics of protocol. If we keep them the same, the fact of protocol change will not be discovered by security analyst.

This article describes offered model of whole system. Also it proposes a models of attacker and legal user. Some strong mathematical measures of encoding efficiency are then introduced. They are based on statistical characteristics (commands or their parameters probability and other). Finally, some methods of XML-based protocols obfuscation are described and analyzed at the point of view of proposed characteristics.

Keywords: information security, encryption, steganography, man in the middle, hidden dataflow.

References

1. Gurevich O.S., Kessel'man M.G., Trofimov A.S., Chernyshov V.I. *Trudy MAI*, 2017, no. 94. URL: http://trudymai.ru/eng/published.php?ID=81143

2. Titov A.G., Neretin E.S., Dudkin S.O., Brusnikin P.M. *Trudy MAI*, 2019, no. 105. URL: http://trudymai.ru/eng/published.php?ID=104257

3. Romanov A.M., Gringoli F., Sikora A. *Trudy MAI*, 2019, no. 108. URL: http://trudymai.ru/eng/published.php?ID=109522. DOI: 10.34759/trd-2019-108-13

4. Shikhin S.M. *Trudy MAI*, 2019, no. 109. URL: http://trudymai.ru/eng/published.php?ID=111442. DOI: 10.34759/trd-2019-109-28

5. Khummanee S., Khumseela A., Puangpronpitag S. Towards a new design of firewall: Anomaly elimination and fast verifying of firewall rules, *2013 10th International Joint Conference on Computer Science and Software Engineering (JCSSE)*, 29 - 31 May 2013, Thailand. DOI:10.1109/JCSSE.2013.6567326

6. Sheng H., Wei L., Zhang C., Zhang X. Privacy-Preserving Cloud-Based Firewall for IaaS-based Enterprise, *2016 International Conference on Networking and Network Applications (NaNA)*, 23 - 25 July 2016, Hakodate, Japan. DOI: 10.1109/NaNA.2016.37

7. Wei L., Hongyu L., Xiaoliang Z. A network data security analysis method based on DPI technology, *2016 7th IEEE International Conference on Software Engineering and Service Science (ICSESS)*, 26 - 28 August 2016, Beijing, China, DOI: 10.1109/ICSESS.2016.7883228

8. Nagpal B., Sharma P., Chauhan N., Panesar A. DDoS tools: Classification, analysis and comparison, *2015 2nd International Conference on Computing for Sustainable Global Development (INDIACom)*, 11 - 13 March 2015, New Delhi, India.

9. Wu Z., Wang C., Zeng H. Research on the comparison of Flood DDoS and Low-rate DDoS, *2011 International Conference on Multimedia Technology*, 26 - 28 July 2011, Hangzhou, China. DOI: 10.1109/ICMT.2011.6002141

10. Zelenskii M.D. *IV Vserossiiskaya nauchno-tekhnicheskaya konferentsiya «Studencheskaya nauka dlya razvitiya informatsionnogo obshchestva»: sbornik materialov*, Stavropol', Severo-Kavkazskii federal'nyi universitet, 2016, pp. 241 - 243.

11. Davis S., Burnett I. Collaborative Editing using an XML Protocol. TENCON 2005, *2005 IEEE Region 10 Conference*, pp. 1-5. DOI: 10.1109/TENCON.2005.300936.

12. Abramov M.V., Shek V.M. *Gornyi informatsionno-analiticheskii byulleten'*, 2004, no. 4, pp. 134 - 137.

13. Brazhuk A.I. *II Vserossiiskaya nauchnaya konferentsiya s mezhdunarodnym uchastiem «Informatsionnye tekhnologii v modelirovanii i upravlenii: podkhody, metody, resheniya: sbornik trudov*, Tol'yatti, Izdatel' Kachalin Aleksandr Vasil'evich, 2019, pp. 435 - 442.

14. Peng Y., Chen Y., Shen B. An Adaptive Approach to Recommending Obfuscation Rules for Java Bytecode Obfuscators, *2019 IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC)*, 15 - 19 Jul 2019, Milwaukee, USA. DOI: 10.1109/COMPSAC.2019.00023

15. Sipakov D.S., Gubenko N.E. *Vseukrainskaya nauchno-tekhnicheskaya konferentsiya aspirantov i molodykh uchenykh «Informatsionno-upravlyayushchie sistemy i tekhnologii»*, Donetsk, DonNTU, 2014, pp. 37 - 42.

16. Ivanov P.S. *Obfuskatsiya i zashchita programmnykh produktov*. URL: http://citforum.ru/security/articles/obfus

17. Nevolin A.O. *Elektrosvyaz'*, 2019, no. 8, pp. 49 - 52.

18. Venttsel' E.S., Ovcharov L.A. *Teoriya veroyatnostei i ee inzhenernye prilozheniya* (Theory of Probabilities and its Engineering applications), Moscow, Nauka, 1988, 480 p.

19. Kibzun A.I., Goryainova E.R., Naumov A.V., Sirotin A.N. *Teoriya veroyatnostei i matematicheskaya statistika: bazovyi kurs s primerami i zadachami* (Probability theory and mathematical statistics. Basic course with examples and tasks), Moscow, Fizmatlit, 2002, 224 p.

20. Nevolin A.O. *VIII Mezhdunarodnaya nauchno-tekhnicheskaya konferentsiya «Grazhdanskaya aviatsiya na sovremennom etape razvitiya nauki, tekhniki i obshchestva: tezisy dokladov*, Moscow, Izd-vo MGTU GA, 2008, pp. 70 – 71.