УДК 004.415.2

К ВОПРОСУ ОЦЕНКИ ДОСТОВЕРНОСТИ ИНФОРМАЦИИ ДЛЯ ПРЕДОТВРАЩЕНИЯ MITM-АТАКИ ПРИ ПЕРЕДАЧЕ ЗАКРЫТОЙ ИНФОРМАЦИИ ПО ОТКРЫТЫМ КАНАЛАМ СВЯЗИ

Атрощенко В.А.[1], Руденко М.В.[1], Дьяченко Р.А.[1], Багдасарян Р.Х.[1]

[1]ФГБОУ ВПО «Кубанский государственный технологический университет», Краснодар, Россия (350072, г. Краснодар, ул. Московская, 2), e-mail: adm@kgtu.kuban.ru

В статье представлен метод проверки достоверности данных при передаче закрытой информации по открытым каналам связи для обнаружения факта компрометации канала передачи данных. Данный метод основан на построении мультиграфа, содержащего множество значений информационных элементов и связей между ними. На основе построенного мультиграфа производится анализ целостности путей доступа мультиграфа для выявления и удаления избыточных взаимосвязей между информационными элементами. Разработан метод проверки достоверности данных при передаче закрытой информации по открытым каналам связи. Проведен анализ передачи данных пользователями информационных требований. Построены мультиграфы, содержащие множество значений информационных элементов и связей между ними. Проведен анализ путей доступа мультиграфа. Произведен расчет показателей достоверности информации.

Ключевые слова: информационная система, мобильное приложение, ios, android, передача данных, сетевой протокол, канал связи, http, https, tcp/ip.

THE QUESTION OF THE ACCURACY OF THE INFORMATION TO PREVENT MITM-ATTAKS IN TRASFER PUBLIC INFORMATION THROUGH OPEN COMMUNICATION

Atroshchenko V.A.[1], Rudenko M.V.[1], Dyachenko R.A. [1], Bagdasaryan R.K. [1]

[1]Kuban State Technology University, Krasnodar, Russia (350072, Krasnodar, street Moskovskaya, 2), e-mail: adm@kgtu.kuban.ru

The article presents a method for validating the transfer secret information through open communication channels for detection of the fact compromise of the data link. This method is based on the construction of a multigraph, comprising a plurality of values of information elements and the connections between them. Based on the constructed multigraph, an analysis of integrity paths multigraph to identify and eliminate redundant links between information items. Developed a method for validating the transfer of classified information through open channels of communication.The analysis of the data by users of the information requirements. Built multigraphs having a plurality of values of information elements and relationships between them. The analysis of access routes multigraph. The calculation of indicators of reliability of information.

Key words: information system, mobile application, ios, android, transfer data, network protocol, link, http, https, tcp/ip.

Введение

В современном мире особенно актуальной проблемой становится обеспечение защиты данных. Предложенный ранее метод передачи закрытых данных по открытым сетям [2], как и многие другие методы передачи информации [7], подвержен MITM-аттаке. MITM-атака — метод компрометации канала связи, при котором взломщик, подключившись к каналу между контрагентами, осуществляет активное вмешательство в протокол передачи, удаляя, искажая или навязывая ложную [6] информацию. По этой причине при передаче закрытых данных по открытым сетям проверка достоверности информации является актуальной проблемой [3]. Под достоверностью информации понимается соответствие принятого сообщения переданному. Анализ метода взлома MITM-атаки показывает, что достоверность

информации является интегральной характеристикой, зависящей от качества проектирования всех уровней передачи данных: физического, логического, ошибок при отправлении, передаче и получении информации.

Цели и задачи исследования

Целью данной работы является разработка метода проверки достоверности данных при передаче закрытой информации по открытым каналам связи для обнаружения факта компрометации канала передачи данных.

Задачи исследования:

1) построение мультиграфов, содержащих множество значений информационных элементов и связей между ними;
2) анализ целостности путей доступа мультиграфа для выявления и удаления избыточных взаимосвязей между информационными элементами;
3) расчет показателей достоверности информации.

Теоретическое положение

Пусть множество данных (передаваемых информационных сообщений), получаемых от пользователя s из общего количества пользователей n:

$$m_n = \left\{ m_s^n \right\}, \text{ где} \quad (1)$$

s — текущий пользователь;

n — количество пользователей.

Множество данных (информационных сообщений), передаваемые всеми n пользователями:

$$m = \bigcup_n m_n, \text{ где} \quad (2)$$

m_n — множество данных (сообщений), получаемых от n-пользователей;

n — количество пользователей.

Построение мультиграфа информационных требований

При анализе передачи данных пользователями информационные требования формируются мультиграфом, каждой вершине которого соответствует определенное множество значений информационных элементов:

$$d_i^{ns} \square d_s^n, \text{ где} \quad (3)$$

d_i^{ns}— множество значений получаемых информационных элементов (сообщений);

d_s^n — множество вершин информационных элементов от пользователя s из общего количества пользователей n;□

i — текущий информационный элемент (сообщение).

Ориентированные дуги мультиграфа, указывающие на последовательность обращений к клиенту (серверу) при передаче данных:

$$f_v^{ns} \square f_s^n, \text{ где} \tag{4}$$

f_v^{ns} — множество ориентированных дуг мультиграфа, показывающие передачу данных пользователя s из общего количества пользователей n;

f_s^n— множество ориентированных дуг мультиграфа;

$\square v$ — текущая ориентированная дуга мультиграфа.

Следовательно, можем получить множества всех информационных элементов и связей между ними:

$$d_z = \bigcup_n \bigcup_s d_s^n, \text{ где} \tag{5}$$

$$f_z = \bigcup_n \bigcup_s f_s^n, \text{ где} \tag{6}$$

Связи между информационными элементами имеют вид $\overleftrightarrow{/1:1/}, \overleftrightarrow{/1:M/}, \overleftrightarrow{/M:M/}$.

В нашем случае между двумя информационными элементами имеется связь типа $\overleftrightarrow{/1:1/}$, тогда вводится связь типа $\overleftrightarrow{/1:M/}$ в прямом направлении и связь типа $\overleftrightarrow{/1:M/}$ в обратном направлении. Семантическое значение каждой из полученных связей определяется семантическим значением исходной связи.

Составим мультиграф G_s^n, которому будут соответствовать информационные требования $M_s^n : G_s^n =< d_s^n, f_s^n, \varphi_s^n >$, где $d_s^n = \left\{ d_{is}^n \right\}$ — множество вершин (информационных элементов); $f_s^n = \left\{ f_v^{ns} \right\}, f_v^{ns} = (d_i^{ns}, d_j^{ns})$ — множество связей (отражают связи между информационными элементами); $\varphi_s^n : f_s^n \to d_s^n \square d_s^n$ — функция, ставящая в соответствие каждой дуге f_s^n упорядоченную пару (d_i^{ns}, d_j^{ns}) вершин из множества d_s^n.

Мультиграф G_s^n обладает следующими свойствами. Каждая вершина помечена. Метки вершин являются уникальными идентификаторами информационных элементов и определяют их семантическое значение.

Каждая дуга f_{ijv}^{ns} помечена метками двух типов:

1. $T_{f_{ijv}^{ns}} = (d_i^{ns}, d_j^{ns})_v = \left\{\overrightarrow{/1:1/}; \overrightarrow{/1:M/}; \overleftarrow{/1:M/}\right\}$ — определяет тип и направление связи между вершинами в мультиграфе G_s^n.

2. $C_{f_{ijv}^{ns}}$ — определяет семантическое значение связи между информационными элементами d_i^{ns} и d_j^{ns}, отображаемой дуги f_{ijv}^{ns}.

Любые две вершины мультиграфа G_s^n могут иметь несколько взаимосвязей. В этом случае дуги, соединяющие эти вершины, должны отличаться, по крайней мере, меткой второго типа.

Функция φ_s^n, определяющая наличие дуг между вершинами мультиграфа G_s^n, задана матрицей инциденций $W_s^n = \omega_{iv}^{ns}$, где

$$\omega_{iv}^{ns} = \begin{cases} +1, & \exists f_{ijv}^{ns}(T_{f_{ijv}^{ns}}) = \{\overrightarrow{/1:1/}; \overrightarrow{/1:M/}; \overrightarrow{M:1/}\}, \\ -1, & \exists f_{ijv}^{ns}(T_{f_{ijv}^{ns}}) = \{\overleftarrow{/1:1/}; \overleftarrow{/1:M/}; \overleftarrow{/M:1/}\}, \\ 0 & \end{cases} \quad (7)$$

Проверка достоверности данных

Анализ путей доступа мультиграфа G_s^n позволяет выявить и удалить избыточные взаимосвязи между информационными элементами. При анализе достоверность информации может быть нарушена при удалении избыточных информационных элементов и связей.

Для проверки достоверности информации используется данное выражение:

$$P_{zc} = \frac{\sum_{d_i \in D_{zc}} \chi_i + \sum_{L_{ij\mu} \in L_{zc}} N_{L_{ij\mu}}}{\sum_{d_i \in D_z} \chi_i + \sum_{L_{ijv} \in L_z} N_{L_{ijv}}}, \text{ где} \quad (8)$$

χ_i — количество экземпляров i-го информационного элемента;

$L_{ijv}(L_{ij\mu})$ — количество экземпляров связей между информационными элементами, просматриваемых при прохождении $L_{ijv}(L_{ij\mu})$-го пути доступа с учетом интенсивности его прохождения.

Множество всех информационных элементов и связей между ними:

$$D_z = \bigcup_n \bigcup_s d_s^n \quad (9)$$

Пересечение множества всех информационных элементов и связей между ними и

множества ключевых вершин:

$$D_{zc} = D_z \bigcap D_c \tag{10}$$

Множество всех путей доступа из входных вершин $d\frac{n}{s}(in)$:

$$L_z = \bigcup_n \bigcup_s L_s^n \tag{11}$$

Пересечение множества всех путей доступа из входных вершин $d\frac{n}{s}(in)$и множества путей доступа:

$$L_{zc} = L_z \bigcap L_c \tag{12}$$

Рассчитанные показатели достоверности информации сравниваются с заданными. При их несоответствии определяются причины возникновения ошибок, производится их локализация и вносятся исправления в структуру данных.

Заключение

Разработан метод проверки достоверности данных при передаче закрытой информации по открытым каналам связи. Проведен анализ передачи данных пользователями информационных требований. Построены мультиграфы, содержащие множество значений информационных элементов и связей между ними. Проведен анализ путей доступа мультиграфа. Произведен расчет показателей достоверности информации.

Список литературы

1. Атрощенко В.А., Руденко М.В., Дьяченко Р.А., Чигликова Н.В. К вопросу исследования предметной области информационной системы расчетов с предприятиями ЖКХ // Современные проблемы науки и образования. – 2012. – № 3. - URL: www.science-education.ru/103-6137 (дата обращения: 18.06.2013).

2. Атрощенко В.А., Дьяченко Р.А., Руденко М.В., Багдасарян Р.Х. К вопросу разработки алгоритма передачи закрытых данных по открытым сетям между мобильным устройством и распределенными серверами // Научные чтения имени профессора Н.Е. Жуковского. Сборник научных статей III Международной научно-практической конференции / Филиал Военного учебно-научного центра Военно-воздушных сил «Военно-воздушная академия им. проф. Н.Е. Жуковского и Ю.А. Гагарина». — Краснодар : Филиал Военного учебно-научного центра Военно-воздушных сил «Военно-воздушная академия им. проф. Н.Е. Жуковского и Ю.А. Гагарина», 2013. — С. 216–220.

3. Все приложения мобильного банкинга в России уязвимы [Электронный ресурс]. — URL: http://banks.cnews.ru/top/2013/03/07/vse_prilozheniya_mobilnogo_bankinga _v_rossii_uyazvim y_ 521778 / (дата обращения: 01.05.13).
4. Кульба В.В., Ковалевский С.С., Косяченко С.А., Сиротюк В.О. Теоретические основы проектирования оптимальных структур распределённых баз данных. Серия «Информатизация России на пороге XXI века». - М. : СИНТЕГ, 1999. - 660 с.
5. Половко А.М., Гуров С.В. Основы теории надежности БХВ. – СПб., 2006. - 702 с.
6. Список последних MITM-атак [Электронный ресурс]. — URL: http://www.securrity.ru/tags/MitM-атака/ (дата обращения: 01.05.13).
7. MITM-атака [Электронный ресурс]. — URL: http://ru.wikipedia.org/wiki/MITM (дата обращения: 01.05.13).

Рецензенты:

Ключко Владимир Игнатьевич, доктор технических наук, профессор, заведующий кафедрой ВТиАСУ, ФГБОУ «Кубанский государственный технологический университет» (Министерство образования и науки РФ), г. Краснодар.

Пиотровский Дмитрий Леонидович, доктор технических наук, профессор, заведующий кафедрой АПП, ФГБОУ «Кубанский государственный технологический университет» (Министерство образования и науки РФ), г. Краснодар.