Орлов В.Л., Курако Е.А.

Сервис-браузер и атаки типа Man in the middle

Аннотация: Рассматривается устойчивость информационной системы использующей технологию сервис-браузера к атакам Man in the middle. Сервис-браузерная технология сравнивается с веб-браузерной технологией для данного типа атак. Анализируются предпринимаемые меры безопасности.

Ключевые слова: сервис-браузер, атаки, безопасность, информационная система, сеть

В современном мире к информационным системам предъявляются все более строгие требования по устойчивости и безопасности работы. Исследованиям различных угроз в данной области посвящено множество работ. Одной из наиболее значимой угроз, являются атаки типа «человек посредине» (Man in the middle – MITM), которую также называют атакой посредника [1].

Атаки данного типа осуществляются при передаче данных от одного узла другому и, как правило, не зависят от самих узлов. Следует отметить, что эти угрозы можно разделить на активные и пассивные. Активные – это такие атаки, при которых злоумышленник вмешивается в передачу пакетов данных, удаляя или подменяя их. При пассивных атаках ведется только прослушивание каналов связи. Заметим, что в основном, предварительно происходит прослушивание сетевого трафика, а уже после анализа злоумышленник переходит к активным действиям.

Главная опасность заключается в том, что на стадии пассивных очень трудно обнаружить. Трудности обуславливаются тем, что все вредоносная активность происходит вне наблюдаемых узлов. Необходимо проводить постоянный анализ сетевой активности. Существуют и другие методы определения, например, по временным задержкам [2]. Но все равно существующие методы не позволяют достоверно выявлять производимые атаки.

Технология сервис-браузера [3] по сути является распределенной, то есть обеспечивает функционирование на разных узлах, объединенных в сеть. В силу этого она может подвергаться

рассматриваемому типу атак. Условно схему работы данного браузера можно представить, так, как это изображено на рисунке 1. При этом сервис-браузер через публичную сеть взаимодействует с сервером приложений, который, в свою очередь, общается с сервером баз данных.

Таким образом, сеть разделена на два фрагмента. Первый фрагмент предназначен для общения клиентских рабочих мест и сервера приложений посредством сервис-браузера. Он является общедоступным, например, может работать через глобальную сеть Интернет. Второй фрагмент – это внутренняя закрытая сеть информационной системы, где сервера взаимодействуют между собой. Она является частной, и никто, кроме серверов, не имеют в нее доступ.

Таким образом, при рассмотрении атак типа MITM следует рассмотреть два направления защиты.

Рисунок 1 – Схема работы сервис-браузера

Для участка публичной сети обеспечить безопасность необходимо криптографическими средствами. Наиболее прост и распространен способ замены открытого протокола HTTP на зашифрованный протокол HTTPS. К сожалению, простое использование функций шифрования канала, не гарантирует полноценной защиты [4]. В работе рекомендуется использовать пользовательские браузеры, обеспечивающих возможность своего списка доверенных сертификатов. Сервис-браузер, в отличие от стандартного веб-браузера, создавался для ограниченного круга

пользователей, обязательно проходящих аутентификацию и авторизацию. При реализации сервис-браузерной технологии была заложена возможность заранее определять список доверенных сертификатов или список доверенных корневых центров. В результате сервис-браузер прикрывает достаточно слабое место протокола HTTPS – взаимную аутентификацию.

При этом важно понимать, что использование пользователем беспроводных сетей, подключение к общественной сети в непроверенных местах может значительно облегчить злоумышленнику пассивный сбор информации.

Для фрагмента, образующего внутреннюю сеть, часть реализуемой защиты можно обеспечить административными мерами. То есть обеспечить функционирование серверов в закрытом периметре, чтобы доступ к ним имел ограниченный круг пользователей. При этом также, как и в случае публичной сети, необходимо обеспечить шифрование трафика между узлами.

Литература:

1. *Арзуманян Э.А., Чумаков А.А.* МИТМ-атака. Угроза информационной безопасности в РФ // Znanstvena Misel. – 2019. – № 8-1(33). – С. 37-40.

2. *B. Aziz; G. Hamilton* Detecting Man-in-the-Middle Attacks by Precise Timing / Third International Conference on Emerging Security Information, Systems and Technologies (18-23 June 2009 Athens, Greece). – Athens, 2009. – P. 81-86 – URL: https://ieeexplore.ieee.org/abstract/document/5211025 (дата обращения 06.10.2021).

3. *Курако Е.А., Орлов В.Л.* Сервис-браузеры для информационных систем // Программная инженерия. – 2017. – Т. 8. №9. – С. 413-421.

4. *Акулов А.А.* Подмена SSL-сертификатов как средство перехвата зашифрованного трафика // Символ науки: международный научный журнал. – 2018. – № 1-2. – С. 19-21.