ОБНАРУЖЕНИЕ УГРОЗЫ ДЛЯ БЕСПРОВОДНОЙ СЕТИ WI-FI СИГНАТУРНЫМ МЕТОДОМ

Гусельников Дмитрий Сергеевич

магистрант, Федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет ИТМО», РФ, г. Санкт-Петербург

DETECTING A THREAT TO A WI-FI WIRELESS NETWORK USING A SIGNATURE METHOD

Dmitry Guselnikov

Graduate student, Federal State Autonomous Educational Institution of Higher Education "ITMO National Research University", Russia, St. Petersburg

Аннотация. На фоне стремительного развития беспроводных сетей, зачастую их безопасность не соответствует необходимому уровню. Беспроводные инфраструктуры уязвимы и могут подвергаться различным сетевым атакам. Одним из наиболее важных средств защиты от атак на беспроводные сети – это система обнаружения атак. Одним из подходов к обнаружению угроз для беспроводной сети Wi-Fi является сигнатурный метод.

Abstract. Against the background of the rapid development of wireless networks, their security often does not meet the required level. Wireless infrastructures are vulnerable and may be subject to various network attacks. One of the most important means of protection against attacks on wireless networks is an attack detection system. One of the approaches to detecting threats to a Wi-Fi wireless network is the signature method.

Ключевые слова: сигнатура, образ, анализ, признак, беспроводная сеть, Wi-Fi, сетевая атака, угроза.

Keywords: signature, image, analysis, feature, wireless network, Wi-Fi, network attack, threat.

Беспроводные сети имеют неоспоримые преимущества перед традиционными кабельными сетями: простота развертывания, мобильность пользователей в зоне действия сети, простое подключение новых пользователей. С другой стороны, невысокий уровень безопасности таких сетей зачастую ограничивает их применение. В последние годы атаки на локальные беспроводные сети стали обычным явлением [3, с. 95].

Вопрос уязвимости сетей Wi-Fi и протокола IEEE 802.11 изучается в течение долгого времени. Несмотря на это, проблема безопасности не стала менее важной, так как появляются новые стандарты и технологии для передачи данных [2, с. 939].

Одним из подходов к обнаружению угроз для беспроводной сети Wi-Fi является описание в виде сигнатуры (signature) и поиск этого паттерна в зоне мониторинга (например, сетевой

трафик или журналы регистрации). Это похоже на необучаемое сканирование вирусов (антивирусные сканеры являются ярким примером данной системы обнаружения атак).

Этот механизм обнаружения выявляет потенциальные атаки, когда поведение пользователя соответствует установленным правилам. Наличие полной базы данных таких правил имеет первостепенное значение для экспертных систем обнаружения атак.

Экспертные системы — это системы, которые в контексте обнаружения атак определяют принадлежность события к классу атак на основе имеющихся шаблонов. Эти шаблоны основаны на практике специалистов и находятся в специализированном хранилище, называемом базой знаний. В большинстве случаев шаблоны экспертных систем основаны на так называемых сигнатурах.

Сигнатуры – это шаблоны, сопоставленные известным атакам или злоупотреблениям в системах. Они могут быть простыми (строка знаков, соответствующая поиску отдельного условия или команды) или сложными (измене состояния защиты, выраженное как формальное математическое выражение, последовательность действий или совокупность строк журнала регистрации) [4, с. 143].

Преимущества сигнатурного метода: эффективное определение атак; отсутствие большого числа ложных срабатываний; надежное определение использования конкретного инструментального средства или метода атаки; возможность наиболее точно задать параметры сигнатуры. Недостатки сигнатурного метода: необходимость обновлять базы сигнатур для обнаружения новых атак; невозможность выявления атак, не описанных в экспертной системе; невозможность выявить атаки, отличающиеся от сигнатурного описания, либо без описания [1, с. 49].

В современных информационных системах широко используются методы определения принадлежности исследуемого объекта к одному (или нескольким) заданным классам, сформированным на основе схожих свойств, атрибутов или закономерностей.

Изображение в теории распознавания - объект, принадлежащий или не принадлежащий к одному классу изображений на основании наличия похожих признаков. Признак — это свойство или измеряемая величина, которая характерна для данного изображения. Установление, а также применение свойств предметов обширно используется в системах распознавания образов. Свойства считаются ключевыми аспектами с целью установления принадлежности исследуемого предмета к конкретному классу. Атаки имеют все шансы являться найдены вместе с поддержкой распространенных приборов, а также способов распознавания образов. Атаки владеют некоторыми чертами, какие присущи только лишь им. Способ, подобранный с целью распознавания образов во взаимоотношении свойств атак, состоит в поочередном сопоставлении отображений изучения с абсолютно всеми сигнатурами любого эталона. С целью формулировки проблемы распознавания образов атак на базе сетевого трафика при построении математической модели применяются относительные символы, приведенные в таблице 1.

Таблица 1.

Относительные символы

Относительные символы	**Пояснение**
$Q = \{Q_1, Q_2, \dots, Q_n\}$	Множество образов (атак), где n - количество образов
$P_{Q_y} = \{P_{Q_{y.1}}, P_{Q_{y.2}} \dots P_{Q_{y.m}}\}$	Сигнатура признаков (свойств атак), где y – номер о количество признаков
	Образ, который необходимо распозна

q_x	
p_{xj}	Признак исследуемого образа
L_{xj}	Коэффициент ассоциативности (мера бли

Для опознавания предоставляется часть сетевого трафика q_x за определенный период времени. Комплект образов предполагает собою комплекс атак, которые характеризуются группой характерных свойств. В случае если все без исключения свойства атак содержатся в изучаемом образе, то он считается деструктивным. Правило разделения (ПР) используется для оценки соответствия между исследуемым образом и известным эталонным образом. Решение о соответствии образа одному из эталонных образов принимается на основе результатов функции разделения (RF). Математическая модель обнаружения атак WI-FI является следующей:

$$\mathrm{RF}_{q_x Q_y} = \sum_{j=1}^{m} L_{xj}, \qquad L_{xj} = \begin{cases} 1, \text{если } p_{xj} = P_{Q_y.j} \\ 0, \text{ если } p_{xj} \neq P_{Q_y.j} \end{cases},$$

RP: $q_x \in \mathrm{Q}_y \Leftrightarrow \mathrm{RF}_{q_x Q_y} \equiv m$;

Анализ и изучение моделей сетевого трафика систем связи WI-FI выявил группу знаков, которые характеризуют рассматриваемые атаки. По итогу была сформирована таблица модификаций атак, а также атрибутов (табл. 2).

Таблица 2.

Признаки основных типов атак WI-FI

Признаки / **Образы**		**P_1**	**P_2**	**P_3**	**P_4**
		Битовое значения поля Type	**Битовое значения поля Subtype**	**Количество кадров/с.**	**MAC отправител**
Q_1	Деаутентификация клиента (со стороны точки доступа Wi-Fi)	00	1010/ 1100	>10	AP_mac
Q_2	Деаутентификация клиента (со стороны клиента)	00	1010/ 1100	>10	STA_mac
	Флуд маяками	00	1000	>15	Other_mac

Q_3						
Q_4	Флуд зондирующими запросами	00	0100	>10	Other_mac	
Q_5	Попытка нелегитимного подключения	00	1011	>1	Other_mac	
Q_6	DoS аутентификации	00	1011	>5	Other_mac	

Other_mac – любой неизвестный mac-адрес чужого устройства;

AP_mac - mac-адрес Wi-Fi точки;

STA_mac - mac-адрес клиента Wi-Fi;

Broadcast – передается всем устройствам, находящимся поблизости.

Таким образом, как бы часто ни обновлялись базы данных сигнатур атак и уязвимостей, всегда существует временная задержка между сообщением о новой атаке (уязвимости) и появлением сигнатуры. Сокращение этой временной задержки является одной из основных задач для систем обнаружения атак. После проведения моделирования математического представления реальности целевых областей, информационных систем и их подсистем, сетевого трафика и выявления атак возможно переключаться напрямую к исследованию представленных способов.

Список литературы:

1. Ананьин Е.В., Кожевникова И.С., Лысенко А.В., Никишова А.В. Методы обнаружения аномалий и вторжений // Проблемы Науки. 2016. №34 (76). URL: https://cyberleninka.ru/article/n/metody-obnaruzheniya-anomaliy-i-vtorzheniy (дата обращения: 02.05.2023).

2. Баранова Е.А., Зарешин С.В. Анализ защищенности беспроводных клиентов // Современные информационные технологии и ИТ-образование. 2018. №4. URL: https://cyberleninka.ru/article/n/analiz-zaschischennosti-besprovodnyh-klientov (дата обращения: 02.05.2023).

3. Васильев В.И., Шарабыров И.В. Интеллектуальная система обнаружения атак в локальных беспроводных сетях // Вестник УГАТУ = Vestnik UGATU. 2015. №4 (70). URL: https:// cyberleninka.ru/article/n/ intellektualnaya-sistema-obnaruzheniya-atak-v-lokalnyh-besprovodnyh-setyah (дата обращения: 02.05.2023).

4. Лукацкий А.В. Обнаружение атак. 2.СПб.: Мастер систем, 2003. – 563 с.