УДК 004.056.53

Применение методов машинного обучения для защиты IoT устройств от несанкционированного доступа по выявленным каналам.

Матюха Д.В. (Университет ИТМО)
Научный руководитель – к.т.н., доцент ПИиКТ Оголюк А.А.
(Университет ИТМО)

Рассмотрены актуальные каналы несанкционированного доступа для устройств интернета вещей. Проведен обзор актуальных методов машинного обучения применительно к задаче защиты устройств интернета вещей от несанкционированного доступа по выявленным каналам. Проведен ряд экспериментов с инструментарием на базе нейронной сети типа Автокодировщик.

Введение. По данным исследований компании Gartner, на 2015 год в городах функционировали 1,1 млрд IoT-устройств. По мнению компании IDC, в 2020 г. рынок IoT достигнет 1,7 трлн. долларов. Многие компании-поставщики в наши дни создают IoT-платформы, инвестируют в программное обеспечение, выделяют больше денег на научно-исследовательские разработки и финансирование частных бизнес-моделей. Рост популярности IoT устройств за последние годы приводит к увеличению числа атак на эти системы. Проблемы безопасности для IoT устройств обусловлены значительной зависимостью защищенности устройства от производителя устройства. Производитель сам может выступать в роли злоумышленника и внедрять в свою продукцию программно-аппаратные закладки.

Основная часть. В ходе анализа ряда IoT устройств различного назначения (wi-fi радио, роутеры, IP камеры и т.д) был выделен класс устройств, функционирующих по общему принципу, а также выявлены основные каналы несанкционированного доступа к такого рода устройствам:

- Небезопасные сетевые протоколы
- Ошибки реализации встроенного программного обеспечения
- Технические каналы утечки информации
- Программно-аппаратные закладки

В ходе анализа уязвимостей, реализуемых по данным каналам НСД, были сформулированы несколько ограничений:

1) Существует два базовых режима работы устройства: легитимный и нелегитимный; предполагается, что изначально устройство работает в легитимном режиме продолжительное время (например, закладка присутствует, но не влияет на систему).
2) Сетевой трафик, генерируемый устройством в этих двух режимах отличается.

В таком случае задачу защиты устройств от НСД можно переформулировать как задачу детектирования аномалий сетевого трафика трафика, что сводится к задаче классификации. Для выбора метода решения этой задачи требуется также учитывать основные требования, предъявляемые к методам защиты:

1) Универсальность (для исследуемого класса устройств с учетом ограничений).
2) Независимость от производителя (в том числе, от используемых протоколов).

Иными словами, задача классификации должна решаться вне зависимости от используемых протоколов передачи данных, наличия или отсутствия шифрования трафика.

В задаче детектирования аномалий сетевого трафика можно выделить ряд параметров, однако, в зависимости от конкретного устройства, важность каждого параметра

может изменяться, то есть заранее определить, какие параметры трафика в какой степени влияют на свойство нелегитимности невозможно. Исходя из этого необходимо выбрать подходящие методы машинного обучения.

Был проведен обзор актуальных методов машинного обучения. В результате, в качестве приоритетного метода классификации для решения задачи детектирования аномалий в трафике при разработке инструментария для защиты от несанкционированного доступа для IoT устройств был выбран классификатор на основе искусственных нейронных сетей исходя из следующих тезисов:

1. Широкий выбор архитектур в зависимости от конкретных условий задачи.
2. Возможность комбинировать архитектуры, создавая ансамбль нейронных сетей - аналог группы экспертов.
3. Возможность работать с объектами, параметры которых нельзя заранее охарактеризовать.
4. Возможность внесения знаний в задачу извне - за счет обучения части сети на другой, более простой задаче (transfer learning).
5. Возможность выявлять зависимости во времени, используя новые не известные на входе параметры для классификации.
6. Возможность решать задачу в режиме реального времени.
7. Минимизация участия эксперта в решении задачи.

На данный момент был проведен ряд экспериментов с инструментарием на базе нейронной сети типа Автокодировщик, которые позволили сделать вывод о возможности применения предлагаемого подхода для решения задачи защиты устройств от НСД по выявленным каналам. Также, был выявлен ряд недостатков предложенного метода.

Выводы. Предложенные методы защиты могут применяться в реальных системах с целью тестирования IoT устройств и выявления в них программно-аппаратных закладок, а также в качестве средства защиты от несанкционированного доступа для IoT устройств. Применение реализованных способов позволяет улучшить защищенность IoT устройств от несанкционированного доступа по исследованным каналам.

Дальнейшие пути исследования:

- Провести более полный анализ существующих техник машинного обучения с целью выбора наиболее подходящих для решения поставленных задач.
- Создать актуальную модель исследуемого класса устройств для оценки эффективности соответствующего метода машинного обучения.
- Провести ряд экспериментов с применением выбранных методов машинного обучения.
- Оценить возможность применения выделенных методов машинного обучения в зависимости от конкретных условий.