Программный комплекс обработки и классификации пакетного трафика «TRACE TA»

ПК «TRACE TA» представляет собой набор программных компонентов (SDK), встраиваемый в пользовательские приложения для добавления в них функциональности анализа и распознавания сетевого пакетного трафика.

Область применения — сетевые решения и решения для кибербезопасности (PCEF, FW, SD-WAN, IPS/IDS/DLP и др.).

Основные возможности

☑ Распознавание более 50 протоколов и 600 сервисов, с которыми ассоциируется поток (суммарно более 700 наименований). Многие протоколы/сервисы могут быть распознаны по первому пакету (FPC/FPI).

☑ Глубокий анализ пакетов (DPI) до уровня L7 включительно сетевой модели OSI, обработка шифрованного и обфусцированного трафика (анонимайзеры, туннели), извлечение и обновление метаданных в режиме реального времени.

☑ Возможность классификации шифрованного трафика, не распознанного до конечного сервиса, по обобщённым категориям (веб-сёрфинг, стриминг и др.).

☑ Поддержка многопроцессорности и многопоточности: до 1024 потоков обработки (один поток на ядро процессора) на один экземпляр программы. Скорость обработки до 8 Гбит/с на ядро.

☑ Постоянная актуализация признаков и правил классификации с возможностью их предоставления Заказчику (плановый выпуск обновлений 2 раза в месяц). Загрузка признаков производится без прерывания работы пользовательского приложения.

☑ Возможность добавления функций под фактические нужды Заказчика: регистрация собственных классов трафика (протоколов, сервисов), добавление признаков в имеющиеся классы, разработка алгоритмов классификации по запросу.

Идентификация сетевых протоколов и сервисов

Основной функцией ПК «TRACE TA» является идентификация сетевых потоков (flow, сессий). Результат идентификации потока — полный стек обнаруженных в нём протоколов и сервисов (L3-L7), например, «IPv4, TCP, HTTP, Google».

Данная функция позволяет обеспечивать полную «прозрачность» трафика IP-сетей до уровня конечных абонентских приложений в режиме реального времени.

Получение метаданных

ПК «TRACE TA» в процессе обработки сетевого потока позволяет определять специфичные для конкретных протоколов/сервисов метаданные:

☑ извлекаемые (из пакетов) — например, URI для HTTP, SNI для TLS/SSL/QUIC;

☑ вычисляемые — например, тип услуги для распространённых мессенджеров (текстовый чат, аудио- или видеозвонок, передача файлов и др.).

Архитектура

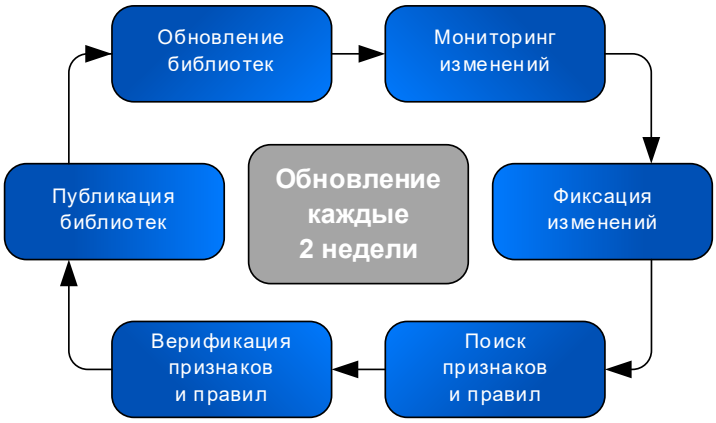
ПК «TRACE TA» поставляется в виде комплекта библиотек C/C++ для Linux, функции которых вызываются из пользовательского приложения согласно API, предоставляемому в виде документированных заголовочных файлов.

Данная архитектура обеспечивает гибкость и простоту интеграции в имеющиеся решения Заказчика, не требует создания собственных приложений анализа и распознавания трафика, что облегчает разработку продукта Заказчика и уменьшает сроки его вывода на рынок.

Актуальность признаков и правил классификации

ПК «TRACE TA» обеспечивает стабильно высокий уровень качества классификации сетевого трафика за счёт постоянного обновления признаков и правил классификации, поставляемых внутри библиотек trace-bundle и trace-asset, которые могут быть «бесшовно» обновлены во время работы без необходимости перезапуска или прерывания выполнения пользовательского приложения.

Состав распознаваемых протоколов/сервисов пополняется на регулярной основе. Достигнутые темпы добавления новых протоколов/сервисов позволяют сокращать отставание от зарубежных лидеров отрасли. Уже сейчас за счёт оптимизации очереди добавления имеется возможность распознавать около 95 % интернет-трафика абонентов операторов связи РФ как по количеству потоков, так и по объёму данных.



Справочная система

В состав ПК «TRACE TA» входит справочник распознаваемых протоколов и сервисов, для каждого из которых описано, что именно распознаётся, приведены перечни получаемых метаданных, применимых настроек обработки.

Для сервисов детализирована структура их трафика (какие вообще протоколы/сервисы распознаются в трафике данного сервиса с учётом сценариев его применения), на основании которой Заказчик может строить высокоуровневые правила обработки трафика (тарификация, фильтрация, блокировка и др.).

Ключевые преимущества

- Разработка программного ядра, мониторинг актуальности и обновление признаков и правил классификации выполняются своими силами на территории РФ и в соответствии с требованиями российского законодательства. Доступность продукта не зависит от санкций. Стоимость не зависит от колебаний курса валют.
- Поддерживаются все основные существующие группы методов классификации трафика: сигнатурные, эвристические, связывание (корреляция) потоков, статистический анализ (включая машинное обучение).
- Постоянное развитие продукта осуществляется собственным центром компетенций по анализу трафика. Коллектив состоит из исследователей, разработчиков и инженеров, имеющих более чем 20-летний опыт изучения трафика, создания вычислительных комплексов.
- Обеспечивается комплексное сопровождение продукта с оперативной обратной связью: регулярное и внеочередное обновление признаков, устранение ошибок, доработка комплекса на заказ (адаптация под нужды Заказчика).
- Продукт в значительной степени ориентирован на рынок РФ и стран СНГ. Особое внимание уделяется распознаванию российских сервисов (онлайн-кинотеатры, социальные сети, СМИ, банки и др.).

ООО «ТехАргос»

127015, г. Москва, ул. Новодмитровская, 2Б, ДЦ «Дмитровский»

Телефон: +7(495) 411-90-37

Web: https://t-argos.ru/

E-mail: mail@t-argos.ru

Оформить заявку на презентацию и демонстрацию возможностей продукта