ГАРДА TrACE (Traffic Analysis and Classification Engine)

Программный комплекс обработки и классификации пакетного трафика

Ключевые возможности

- **C/C++ SDK, предназначенный для встраивания в пользовательские приложения**
- **декапсуляция / дефрагментация / изменение порядка следования: реализация всех этапов подготовки пакета/потока перед началом классификации**
- **поддержка возможности обработки одностороннего трафика (повышение скорости обнаружения в случае наблюдения трафика только в одном направлении)**
- **широкий набор методов классификации: сигнатурные, поведенческий анализ, корреляция потоков, статистический / эвристический анализ и др.**
- **поддержка технологии first packet classification: идентификация потоков IP-трафика по первому пакету на основе DNS и методов кэширования служб**
- **обновляемая и расширяемая база протоколов / сервисов / приложений, собственная исследовательская лаборатория с более чем 20-летним опытом работы**
- **поддержка запуска нескольких экземпляров**
- **динамическое обновление: возможность интеграции периодических выпусков обновлений программного обеспечения ГАРДА TrACE Classify Bundle без прерывания выполнения приложений**
- **кастомизация: возможность подключения собственных идентификаторов трафика и создания индивидуальных событий, разработка моделей, способов и алгоритмов классификации «на заказ»**

ГАРДА TrACE предоставляет усовершенствованный механизм классификации сетевых протоколов, сервисов и приложений, основанный на технологии deep packet inspection (DPI) и позволяющий обеспечить полную «прозрачность» трафика IP-сетей до уровня конечных пользовательских приложений в режиме реального времени.

Идентификация сетевых сервисов и приложений

Результатом процесса идентификации сетевого потока (flow) является стек протоколов, определяемый на основании расширенных, в сравнении с традиционными решениями, знаниями о трафике. Стек протоколов содержит все обнаруженные уровни протоколов для обработанных потоков.

Извлечение и обогащение метаданных

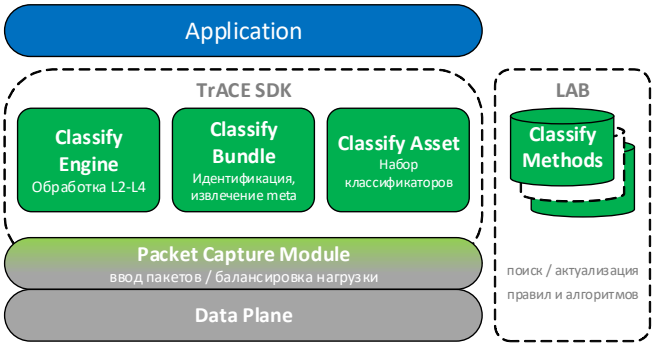
ГАРДА TrACE в процессе обработки пакета / сетевого потока позволяет определять специфичные для конкретных протоколов метаданные двух видов:

- извлекаемые непосредственно из тела пакета (HTTP URL, и др.);
- вычисляемые (результаты классификации типов трафика (чат, голос/видео и др.).

Архитектура

ГАРДА TrACE – это комплект встраиваемых библиотек, модулей и инструментов (SDK) для разработки программного обеспечения, интегрируемый в сетевые программные комплексы или решения в области кибербезопасности.

Архитектура ***ГАРДА TrACE*** разработана с учетом возможности интеграции в решения сторонних производителей, не требует создания собственных приложений для распознавания протоколов, упрощает разработку продукта и уменьшает сроки вывода продукта на рынок.



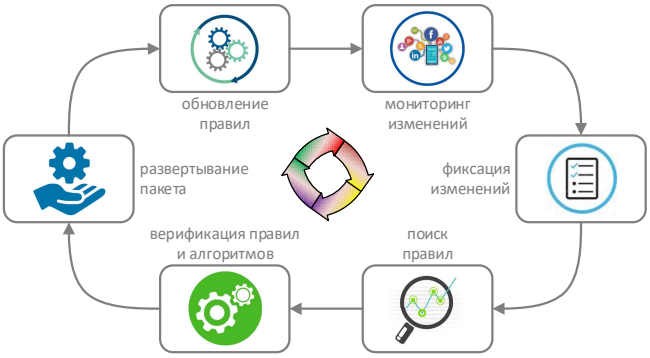
ГАРДА TrACE – платформа отечественной разработки:

- разработана с использованием C/C++, не привязана к конкретной реализации или конкретному производителю, а специфичные и задокументированные методы API позволяют подключать собственные сигнатуры и правила классификации;
- масштабируемое решение: возможность запуска нескольких экземпляров для достижения требуемой производительности и максимальной гибкости;
- поддерживает платформы x86, функционирует в Unix-подобных операционных системах (Linux, FreeBSD и т.д.).

Актуальность правил классификации

ГАРДА TrACE обеспечивает стабильно высокий уровень качества классификации сетевого трафика. Это достигается путем регулярного обновления сигнатур, способов и алгоритмов классификации, поставляемых в виде наборов классификаторов протоколов ***Classify Bundle и Classify Asset***, которые могут быть «бесшовно» интегрированы в библиотеку во время работы без необходимости перезапуска прерывания пользовательских приложений.

За поддержание правил классификации сетевого трафика в актуальном состоянии отвечает собственная исследовательская лаборатория с более чем 20-летним опытом работы.



Преимущества ГАРДА *TrACE* в сравнении с зарубежными аналогами

Разработка и поддержка собственного ClassifyEngine ***ГАРДА TrACE*** ведется коллективом высококвалифицированных программистов.

Сформирована собственная научная школа из ученых, исследователей и инженеров, специализирующихся на проблемах обработки информации, имеющих обширный опыт создания элементов и вычислительных комплексов.

Основные преимущества ГАРДА TrACE в сравнении с зарубежными аналогами:

- стоимость комплекса не зависит от колебаний курса валют;
- создан для работы в соответствии с законодательством РФ и особенностями российского трафика (поддерживает выделение URL по спискам Роскомнадзора, способен классифицировать иной запрещенный трафик);
- обеспечен оперативной технической поддержкой;
- устанавливается на любые серверные платформы, удовлетворяющие минимальным требованиям;
- стабильный режим выпуска обновлений;
- ***ГАРДА TrACE*** интегрирован с другими продуктами сетевой безопасности ГК «Гарда» (DPI/PCEF, Anti-DDoS, WAF, NGFW и др.), что гарантирует его надежность и высокое качество реализации.