СИСТЕМА АНАЛИЗА СЕТЕВОГО ТРАФИКА
PROTOSPHERE

Protosphere — система глубокого анализа сетевого трафика (DPI). Может встраиваться как компонент в системы мониторинга, классификации, защиты от вторжений и утечек информации. Регистрирует несоответствия между реализацией протокола и фактическим трафиком. Позволяет быстро добавлять поддержку новых (в том числе закрытых) протоколов благодаря универсальности внутреннего представления.

ИСП РАН

ОСОБЕННОСТИ И ПРЕИМУЩЕСТВА

Protosphere — инновационная система, основанная на научных исследованиях технологий анализа сетевого трафика. Объединяет ключевые особенности иностранных аналогов (Wireshark, Microsoft Message Analyzer) с универсальным внутренним представлением, позволяющим быстро расширять возможности анализа.

PROTOSPHERE — ЭТО:

- Оптимальные возможности ядра системы:
  - универсальная модель представления данных при разборе сетевого трафика;
  - обработка данных, содержащих искажения, потери, перестановки и дублирование пакетов, а также асимметричный трафик;
  - поддержка анализа сжатых и зашифрованных данных;
  - поддержка туннелей произвольной конфигурации;
  - поддержка связанных потоков.
- Поддержка всех этапов анализа сетевой трассы — каждый этап с отдельным компонентом визуализации, все компоненты синхронизированы:
  - локализация одного или нескольких исследуемых сетевых соединений на графе сетевых взаимодействий и в дереве сетевых потоков;
  - детализация выделенных соединений на временной диаграмме;
  - наглядное представление выделенных в сетевых пакетах полей в дереве разбора сетевого потока;
  - выявление несоответствий между реализацией протокола и фактическим трафиком в журнале диагностики;
  - извлечение и анализ данных произвольного уровня (L7+).
- Быстрое расширение списка поддерживаемых протоколов:
  - API доступ к результатам разбора;
  - локализация ошибок разбора;
  - возможность отладки разрабатываемого модуля на потоке, позволяющая существенно ускорить поддержку новых протоколов.
- Поддержка двух режимов работы: на потоке и в отложенном режиме.
- Продвинутый графический интерфейс, позволяющий выбирать наиболее удобный вариант представления результатов проводимого анализа.
- Ускоренная кастомизация благодаря универсальности внутреннего представления:
  - поддержка новых протоколов;
  - извлечение новых типов данных;
  - настройка формата выдачи результатов анализа;
- Адаптация под сетевой канал и доступные вычислительные ресурсы: гибкая система конфигурирования позволяет находить баланс между детализацией/точностью анализа и потребляемыми ресурсами.

ДЛЯ КОГО ПРЕДНАЗНАЧЕНА PROTOSPHERE?

— Компании, занимающиеся тестированием реализаций сетевых протоколов (в том числе во встраиваемых ОС и сетевой аппаратуре).
— Компании-разработчики средств сетевой безопасности (межсетевых экранов, а также систем обнаружения и предотвращения вторжений).
— Компании по производству техники, нуждающейся в повышенном уровне безопасности из-за обязательной сертификации.
— Компании, которым требуется контроль и мониторинг сетевых каналов в режиме реального времени.

ПОДДЕРЖИВАЕМЫЕ ПЛАТФОРМЫ И АРХИТЕКТУРЫ

Архитектуры: Intel x86-64.
Платформы: ОС Windows, ОС на базе ядра Linux.

СХЕМА РАБОТЫ