Управление защищенной сетью

Эффекты шифрования

Сказка о счастье

Сказка

С зерном реальности.

Ощущение безопасности

- Всеобщчий мониторинг – это проблема.
- Попробуем ответить на всеобщчий мониторинг всеобщчим шифрованием.
- И проблема решена.

- Но по какой цене?

Шифрование в сети

- Шифрование присудствует в течение длительного времени. На разных уровнях. Реализовано по разному.
- Проверка подлинности (authentication) и шифрование (encryption).
- Оппортунистическое шифрование (Opportunistic encryption).
- Доступность шифрования.

Относительность важности

- Проблемы конфиденциальности не должны превращать сеть в неуправляемую.
- Сеть должна работать.
- Отсутствие обслуживания, ухудшенное обслуживание, и обычное обслуживание.
- Никакой конфиденциальности, частичная конфиденциальность, и полная конфиденциальность.

Все-ли сломано?

- Доступ к открытому трафику и удостоверениям пользователей, безусловно, помогает. Но это не обязательно.
- Времена выполнения ’debug all ' на работающем сетевом узле в основном прошло.
- Отсутствие доступа к открытому трафику и сигнализации может привести к появлению дефектных/небезопасных/ разрушительных практик и расширений протоколов.

Общие тенденции

- Атаки не ухудшаються. Атаки будут только улучшаться.
- Интерфейс между апликацией и сетью.
- Количество типов трафика сокращается. HTTP поверх TLS в качестве универсального транспортного протокола.
- Общий уровень шифрования в использовании не собирается снижаться.

Контекст

- От мониторинга на домашней беспроводной сети до мониторинга выхода всеи страны.
- End to end пользовальское шифрование, шифрование сессий, шифрование транспорта.
- Транзитные провайдеры, провайдеры апликаций, хостинг провайдеры.
- Центр обработки данных как новое ядро сети.
- Расшифровка и терминирование входных сессий и открытый трафик внутри DC. Масштаб расшифровки.

Взаимодействие с транспортом

- Само шифрование не сильно меняет обьем передачи данных
- Специальные меры сокрытия (регулировка размера и времени) могут менять обьем.
- Мультиплексирование (HTTP2, QUIC) может сильно изменить битрейт.
- Требования к пропускной способности – 100Gbps, конечно, есть везде, но есть и мобильные сети.
- Шифрование нижних транспортных слоев - оптический транспорт.

Политика безопасности

- Несанкционированное туннелирование трафика – HTTP в качестве универсального протокола туннелирования.
- Соблюдение политики безопасности в среде отсутствия видимости. Вирусы, черви, трояны, утечка данных, защита от вредоносных программ
- Механизмы предотвращения кражы данных работают на незашифрованных потоках. Хэширование объектов не является достаточно надежным.
- Центральный контроль против управления в конечных точках.

Видео с кошками

- Мое видео не работает. Ваше шифрование её сломало.
- Глубина видимости DPI. Оптимизации для CDN.
- HTTP-redirects. Usage-based billing.
- Сигнализация для мультимедии реального времени должна быть видна промежуточным элементам сети.

Управление ключами

- Управление ключами в масштабе.
- Местоположение проблемы – транспорт, применение ключей, или управление ключами?
- Нападения на управление ключами, как правило, являются более продуктивными.

Отказ в обслуживании

- Наличие DoS трафика, не связанного с трафиком приложения.
- DoS fingerprinting, защита от DoS-атак, видимость в трафик атаки.
- Умные DoS атаки и кража информации против brute force DoS атак.

Балансировщики и оптимизаторы

- Интегрированные и автономные балансировщики нагрузки. Видимость в заголовки пакетов.
- Перехват TLS в средах балансировки нагрузки.
- Повышение производительности прокси-серверов, оптимизация транспорта на большие расстояния.
- Локальный контент, контекстная реклама – нужен специальный механизм для этого.
- ALGs и middleboxes останутся в сети на долго.

Законный перехват

- Законный перехват (lawful intercept) должен работать.
- Это не тема для шуток.
- Тонкая грань между законным и незаконным перехватом.

OAM

- Маркировка пакетов для целей OAM.
- Пассивный мониторинг, service level OAM, проверка SLA.
- Синтетические сервисные зонды.

Кэширование и хранение

- Шифрование данных в состоянии покоя.
- Дедупликация.
- Слепое кэширование.
- Сжатие содержимого.
- Блокировка содержимого.
- Шифрование снижает эффективность кэширования.

Управление сетью

- Расшифровка для устранения неполадок выполняется автономным дешифрованием с использованием приватных ключей, доступных out of band.
- Это обычная практика.
- Важно иметь подходящие инструменты.

Сетевая инфраструктура

- Эволюция RPF и control plane snooping. Производительность приложений и мониторинг, диагностика сети и устранение неполадок.
- 2-tuple, 5-tuple анализ в различных местах в сети.
- Фильтрация на основе URL-адресов и DNS разрешения
- Шифрованный DNS.

Качество обслуживания (QoS)

- Кондиционирование трафика и маркировка на зашифрованной полезной нагрузке.
- Все это http над TLS, веб-страницы и на основе вебсокетов общение в реальном времени-это только http над TLS.
- Управление перегрузками в соответствии с трафиком приложений.

Нужно ли меньше шифровать?

- Нет. Вместо этого мы должны найти лучшие способы работы в зашифрованной среде.
- И мы должны понимать, что будут попытки заблокировать шифрование.
- Мы не должны делать зла в сети тоже. Это кажется немного труднее достичь, хотя.

Путь вперед

- IETF работает над набором рекомендаций для внедрения всеобщего шифрования.
- Нам интересна ваша обратная связь о вашем опыте с шифрованием.
- Некоторые вещи могут быть сломанные/неоптимальные или приняты неправильные предположения. Ето нужно рассмотреть и исправить.

Дискуссия

Все сказки когда-то заканчиваются.