Operating a Secure Network

Effects of Encryption

A Fairy Tale of Happiness

Управление защищенной сетью

Эффекты шифрования

Сказка о счастье

A Fairy Tale

With a grain of reality though.

Сказка

С зерном реальности.

A Feeling of Security

- Pervasive Monitoring is a problem.
- Let’s Address Pervasive Monitoring with Pervasive Encryption.
- Problem solved.

- Just at what cost?

Ощущение безопасности

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

- Но по какой цене?

Encryption in the network

- Has been around for long. At different layers. Done in different ways.
- Authentication and encryption.
- Opportunistic encryption, strong end to end encryption.
- Accessibility of encryption.

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.

Relativity of Importance

- Privacy concerns should not make the network to become unmanageable.
- The network has to work.
- No service vs degraded service vs full service.
- No privacy vs compromised privacy vs full privacy.

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.

Is Everything Broken?

- Access to cleartext traffic and user identities certainly helps. It is not mandatory though.
- The times of running ‘debug all’ on a production node have mostly passed.
- Lack of access to cleartext payload and signalling may result in development of inherently flawed/insecure/damaging operational practices and protocol extensions.

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.

General Trends

- Attacks will not get worse. Attacks will only get better.
- Application to network interface.
- Traffic type distribution is narrowing. HTTP over TLS as the universal transport protocol.
- The level of encryption in use is not going to decrease.

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.

The Context

- The scope of monitoring – from a sniffer on a home wireless link to monitoring country egress links.
- Use to user (application to application) vs session level encryption vs transport level encryption.
- Transit providers, application providers, hosting providers.
- Eyeballs vs service/content generation
- Datacenter as the new core of the network.
- Decryption/termination of ingress sessions and keeping intra-DC traffic clear. Scale of decryption.

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.

Transport interaction

- Encryption itself does not change the bit rate much.
- Special concealment measures as padding and size adjustment may do.
- Multiplexing (HTTP2, QUIC) may change bit rate a lot.
- Overlays and insecure underlay.
- Bandwidth requirements – 100G is certainly there, but mobile links are also present.
- Encryption of lower transport layers – optical.

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.

Security Policy

- Unauthorized traffic tunnelling over specific application ports – HTTP as the universal tunnelling protocol.
- Security policy compliance due to lack of visibility.
- Data Loss Prevention mechanisms work on unencrypted streams. Object hashing is not reliable enough.
- Enterprise policy enforcement – viruses, worms, tojans, data leaks, malware protection.
- Central control vs control at the end points.

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.

Cat Videos

- My video is broken. Your encryption broke it.
- DPI visibility. CDN optimization.
- HTTP redirect for usage based billing.
- Content size and partial transfers. Zero rating content reachability.
- Real-time media signalling needs to be visible to intermediate network elements.

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.

Key Management

- Key management at scale.
- The location of the problem – transport, application, or key management?
- Attacks on key management tend to be more productive.

Управление ключами

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

DoS

- Presence of DoS attack traffic not related to the application use.
- Fingerprinting, DoS protection, visibility into attack traffic.
- Intelligent DoS attacks/information theft vs brute force traffic based DoS.

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.

Load Balancers and Optimizers

- Integrated and standalone load balancers. Anycasting on custom header fields. Visibility into headers.
- TLS interception on load balancing environments.
- Performance enhancing proxies, long distance transport optimizations.
- Content, advertisement injection – need a better dedicated mechanism for that.
- ALGs and middleboxes are here to stay.

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.

Lawful Intercept

- Lawful Intercept has to work.
- This is not a topic for joking.
- A thin line between lawful and unlawful intercept.

Законный перехват

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

OAM

- Packet marking for OAM purposes.
- Passive monitoring, service level OAM, SLA validation.
- Synthetic service probes.

OAM

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

Caching and Storage

- Data at rest encryption.
- Deduplication.
- Blind caching.
- Content compression.
- Content blocking.
- Encryption decreases effectiveness of caching.

Кэширование и хранение

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

Network Management and Operations

- Decryption for troubleshooting purposes is done by offline encryption by using private keys available out of band.
- This is a common practice.
- Tooling is important.

Управление сетью

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

Network Infrastructure

- Evolution of RPF and control plane snooping.
- Application performance and monitoring, network diagnostics and troubleshooting.
- 2-tuple, 5-tuple analysis for various places in network and encryption technologies.
- Filtering based on URL lookup and DNS resolution
- Encrypted DNS.

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.

QoS

- Traffic conditioning and marking on encrypted payload.
- Everything is HTTP over TLS, web page and websocket based realtime communication is just HTTP over TLS.
- Congestion management according to application traffic.

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.

Do we need to encrypt less?

- No. We need to find better ways to operate in encrypted environment instead.
- And we need to realize that there will be attempts to block encryption.
- We should do no evil on the network too. This one seems a bit harder to achieve though.

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.

Way Forward

- IETF is working on a set of recommendations for widespread encryption deployment.
- Please provide feedback on your experiences with encryption.
- There may be broken/suboptimal things and incorrect assumptions. That needs to be addressed and fixed.

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.

Discussion

All fairy tales eventually come to an end.

Дискуссия

Все сказки когда-то заканчиваются.