Operating a Secure Network

Effects of Encryption

A Fairy Tale of Happiness

A Fairy Tale

With a grain of reality though.

A Feeling of Security

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

- Just at what cost?

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

Lawful Intercept

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

OAM

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

Caching and Storage

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

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.

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.

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.

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.

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.

Discussion

All fairy tales eventually come to an end.