Embracing the Looming Challenge of 100% Encryption

How ExtraHop Reveal(x) real-time decryption technology provides security insights and forensic evidence without compromising sensitive or regulated data.

Abstract

Research shows that global usage of encryption is skyrocketing inside corporate networks (the East-West corridor), on the public internet, and in the North-South channel between them. Studies also indicate that attackers are intentionally using encrypted traffic to hide their malicious acts more than ever before.

In this paper, you'll learn how ExtraHop Reveal(x) Network Traffic Analytics enables SecOps to see and fight these threats that are hiding in the encrypted dark space.

Table of Contents

Dark Space: Why Decryption Is Necessary for SecOps Success

Encryption is on the rise, and it's a good thing for privacy. But it's also a boon to hackers. Encryption, both inside corporate networks and on the public internet, creates dark space and blind spots that attackers use to hide their activities from security teams.

Today, the majority of web traffic is encrypted, a trend driven by major web technology providers. The Google Transparency Report says that 91% of web traffic to Google in the United States is encrypted, with similarly high percentages of encrypted requests from many other countries worldwide. And data center traffic is increasingly encrypted as organizations respond to regulatory and customer requirements, and more and more technology vendors turn encryption on by default. A 2018 Ponemon study found that the number of businesses applying encryption across their enterprise networks has increased steadily since 2005 across all industry sectors, from 15% in 2005 to 43% in 2018.

Hackers have taken the cue and are increasingly hiding their malicious payloads and communications inside encrypted traffic. The 2018 Annual Cybersecurity Report from Cisco showed that 70% of the malware binaries they sampled took advantage of encrypted network traffic in some manner. The

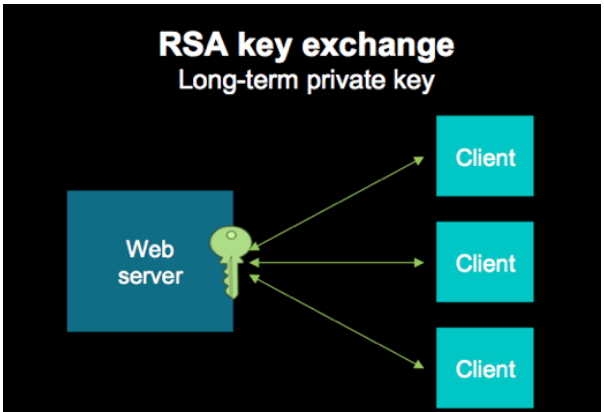
Symantec 2017 Internet Security Threat Report found a 60% increase in malware that specifically used SSL to encrypt its own communications.

Visibility into encrypted communications is essential for detecting malicious access patterns to databases, storage, and APIs, as well as getting visibility into encrypted internal authentication activity associated with lateral movement, data staging, and privilege escalation. Analyzing the actual contents of transactions across the network allows for faster identification and remediation of threats *before* a headline-making data breach happens. On the other hand, decrypting traffic indiscriminately can introduce the risk of having sensitive data in cleartext, easier for hackers to steal, and may violate regulations for businesses that handle PCI or HIPAA regulated data, or businesses subject to GDPR.

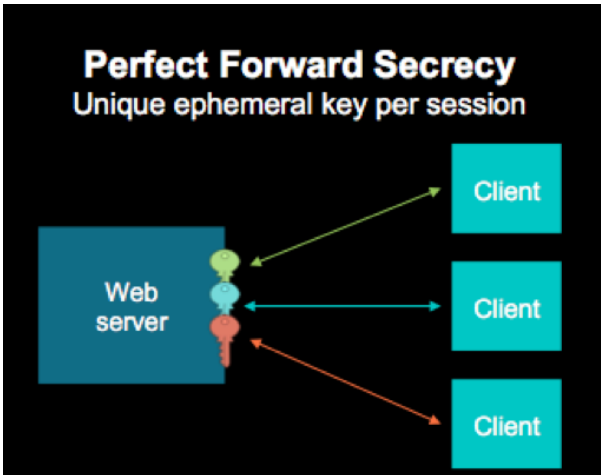
The Evolution of Ciphers and Standards: TLS 1.3 and Default PFS

Not only is encryption growing more prevalent, but the strength of the encryption being used is also increasing. In March of 2018, IETF ratified TLS 1.3 as the new standard encryption protocol for network communications. This brought many changes to how encrypted communications will work for businesses that adopt TLS 1.3. The most impactful aspect of this update is the inclusion of Perfect Forward Secrecy (PFS) as a default setting. Previous versions of TLS allowed the use of the now deprecated RSA ciphers for key exchange, and allowed servers and clients to use long-term private keys from which individual session keys could be derived. This meant that if the private key for a server or client was compromised at any point, all of that device's communications over the period of time the key was in use would be vulnerable to malicious actors.

PFS, using Elliptic Curve Diffie-Hellman Encryption, creates an ephemeral session key, or "secret," for each conversation. The



RSA key exchange, now deprecated, used a long term private key that meant if the key was compromised, many communications over a long period of time could be decrypted.



With PFS, standard in TLS 1.3, every session is encrypted with a new ephemeral session secret, so that any compromised key can only decrypt a single session.

ephemeral secret is only used for that conversation, and cannot be derived from the private key of either the server or the client. Even if an attacker compromised a session secret, it would only decrypt that session. Other sessions with the same server would still be secure.
For hackers trying to steal large databases of intellectual property or millions of credit card numbers, this presents a significant challenge.

Unfortunately, the same challenge is presented to SecOps teams who need visibility into their traffic in order to detect and investigate threats.

How To Decrypt Traffic: A Tale Of Two Methods

There are two models for accessing and decrypting data for security analytics:

1. Interception/Man-in-the-Middle
2. Out-of-band monitoring and decryption

The interception, or man-in-the-middle (MitM), model requires placing a device in-line on the network so that all messages passing across the network are captured by the MitM device, decrypted, analyzed, then re-encrypted and sent along to their final destination. Though this model is widely used, recent research has shown that it introduces more security risks than it solves. Because MitM devices decrypt data in-line, they have to at least temporarily store cleartext data, making them a juicy target for hackers. Research also shows that up to 60% of MitM solutions increase risk by re-encrypting messages using a weaker cipher suite than the original message had used. Additionally, MitM solutions inherently introduce network latency, and none are architected to perform well at the scale and throughput needs of modern enterprise networks.

Therefore, the out-of-band monitoring and decryption method is preferable for SecOps teams monitoring internal (East-West) traffic for hidden threats. Out-of-band solutions acquire a copy of network traffic from a network tap or port mirror. Since they're not preventing the original communications from going through, they do not introduce any network latency, nor do they need to re-encrypt the communications, which eliminates the risk of using lower-quality encryption algorithms.

How ExtraHop Reveal(x) Out-of-Band Decryption Works

ExtraHop Reveal(x) is an out-of-band solution that conducts all decryption and analytics "on box." This means it never needs to send any cleartext data across the network nor re-encrypt any messages. This approach means that Reveal(x) introduces no risk, and may even reduce the attack surface of the enterprise.

Data Acquisition

For hardware-based out-of-band solutions, acquiring data via a network tap or port mirror is a fairly straightforward process. Reveal(x) appliances can ingest, decrypt, and analyze up to 100 Gbps of traffic in real time.

In the cloud or virtualized environments, Reveal(x) uses a lightweight forwarder to acquire the packets.

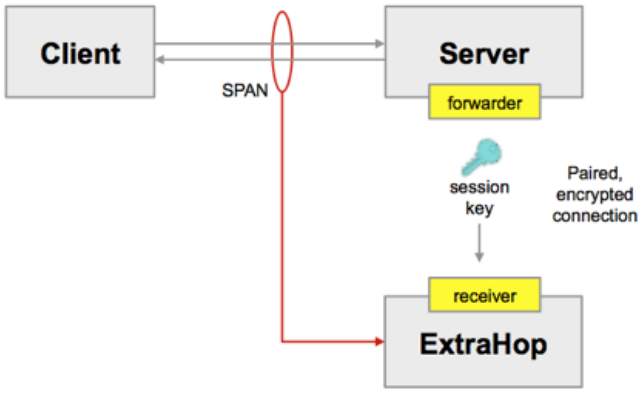
Taking Advantage of Decryption While Still Protecting Sensitive Data

Reveal(x) is designed to provide users with deep, meaningful network traffic analysis while protecting the privacy of sensitive data, personal identifiers, or data regulated by various industry standards such as HIPAA, PCI, SOX, GDPR, and others. Customers choose exactly which traffic to send to Reveal(x) for analytics so they can avoid analysing sensitive or regulated data. However, it is not necessary to completely ignore sensitive traffic this way because Reveal(x), by default, does not expose data that is in scope for the above-listed regulations. The platform provides customizable controls for data access using Application Inspection Triggers and Role Based Access Controls (RBAC), so SecOps teams can get the visibility they need while staying fully compliant.

Using and Protecting Your Private Keys in TLS 1.3

Reveal(x) accesses the ephemeral session secrets for each conversation with a lightweight secret-sharing agent installed on each server whose communications need to be decrypted.

The agent securely transmits session secrets from each server across a PFS encrypted channel to the Reveal(x) appliance, where they are securely stored and only accessible to users with the highest level of administrative privilege.



How ExtraHop maintains security while getting and using session secrets on the out of band appliance.

An Important Note on RSA Key Exchange
It should be noted that as of TLS 1.3, RSA key exchange is deprecated. Reveal(x) still allows users to upload RSA keys, because many customer systems still use earlier versions of SSL/TLS. This is considered an insecure practice, and we recommend eliminating use of RSA and adopting TLS 1.3.

Accessing Critical Data with Need-To-Know Decryption

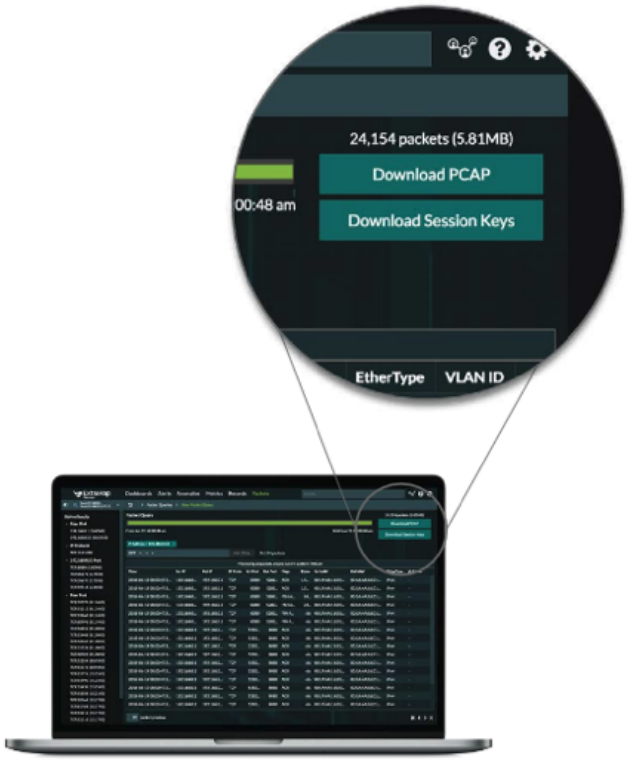
Normally, you can get all the information you need for incident investigation and response from the metrics provided by Reveal(x) without needing any person to lay eyes on unencrypted data. However, sometimes seeing the packets themselves is the only way to prove exactly what happened. Whether you're proving to a third-party vendor that their action constituted an SLA violation or providing evidence of regulatory compliance, sometimes you need access to cleartext packets.

Reveal(x) is able to provide highly granular, role-based access to the decryption keys for specific sessions. We've covered how the data and PFS session keys are acquired in earlier sections. Here's what the experience is like for individual users:

Reveal(x) users may be assigned one of three levels
of access:

1. No Access
2. Access to Packets Only
3. Access to Packets and Secrets

Users with access to packets and secrets will see a new "Download Session Keys" button when looking at packets in Reveal(x). This will enable those users to download the asymmetric key to decrypt the packets transmitted between the specific clients, during the specific time window of their search. The nature of asymmetric key encryption means that the keys accessible by highly-privileged Reveal(x) users can only decrypt the exact packets the user selects. Even if the asymmetric key was compromised, it could not be used on anything beyond that narrow range of packets.



Reveal(x) makes it simple to download precise packet captures and TLS 1.3 session keys for immediate forensic investigation of encrypted data.

Diving Deep with WireShark

While Reveal(x) uses its decryption capabilities to provide the richest data for real-time analysis and metrics, and to provide data for machine learning behavioral detection, the product does not provide the capability, on-appliance, to manually examine individual packets that have been decrypted using PFS session keys. To decrypt and examine downloaded packets, users with the highest level of privilege need to download the session keys and the relevant PCAP files and use Wireshark to open and examine them.

How Hackers Hide Their Tracks With Encryption

The visibility challenges for security operations teams will only grow more pressing as hackers get better at using encrypted channels inside target networks to conceal their reconnaissance and lateral movement activities. For example, attackers have recently been observed using SSL/TLS to hide malware callback activity for command and control purposes. By decrypting all TLS traffic on the network, SecOps teams can more easily distinguish between normal, benign TLS communications, and that being used by bad actors to conceal recon, lateral movement, unauthorized database access and authentication transactions, and more.

Attackers often take advantage of the encryption already in place inside the target network. For example, if an attacker has compromised an internal client, and is using that machine to attempt to log into a sensitive database, those communications are likely already encrypted. An analytics tool *without* decryption capabilities would see that some communication had happened between the compromised machine and the database, but not much else. An analytics tool with L7 visibility and TLS 1.3 decryption would be able to see that the compromised machine was repeatedly trying and failing to log in to the sensitive database—or worse, that they successfully logged in, retrieved sensitive data, and then dropped the audit table to erase their tracks. The added context and detail offered by both L7 visibility and decryption can make a material difference in the SecOps team's ability to understand the level of risk and react appropriately.

A third, less common scenario occurs when attackers actively encrypt their own communications using different methods or protocols than those present on the target network. If these communications are observed by an analytics tool without decryption capability, they may appear as benign network traffic. However, if the SecOps team is decrypting all of their *other* network traffic, and they encounter a conversation that can't be decrypted, that provides a strong, immediate signal that the traffic is malicious and should be investigated.

Is Decryption Necessary for Detection and Investigation?

Many vendors of monitoring and analytics products make claims that it is unnecessary to decrypt traffic because they believe SecOps can get enough information out of limited data such as NetFlow and log analytics. For the reasons listed above, they are wrong. Decrypting and analyzing packets all the way down to the application payload at Layer 7 frequently provides a level of definitive insight that allows SecOps to prioritize their actions and respond confidently before damage is done, in a way that encrypted data limited to L4 flow communications cannot.

ExtraHop Reveal(x) is the only network traffic analytics product capable of decrypting PFS traffic at line rate at sustained 100 Gbps of throughput to provide unprecedented visibility, definitive insights, and immediate answers about the things that matter most to the SOC.

Learn More About The Looming Challenge of Encryption

Blog Series: Unpacking The Looming Challenge of Encryption for SecOps, Parts 1 & 2
Blog Post: What is Perfect Forward Secrecy?
Video: How Does ExtraHop Perfect Forward Secrecy Decryption Work?

Already A Customer and Want To Get Started?

Here are some handy links to ExtraHop documentation about how to get started with decryption in ExtraHop Reveal(x) Network Traffic Analytics:

Admin UI Guide to SSL Decryption
Perfect Forward Secrecy Installation
Installing PFS Forwarder on F5