FLOWMON WEBINAR 24. 3. 2020

**Encrypted Traffic Analysis for Security & Compliance**

FM OS 10.03.02
Table of contents

1. Executive Summary 3
2. Encrypted Traffic Analysis (ETA) Dashboard 3
3. FMC Profiles 4
   3.1. TLS Server version reporting Use Case 4
   3.2. Detection of Malware by JA3 fingerprints Use Case 6
4. ETA Analyses 8
   4.1. Public key length and algorithm analysis Use Case 8
   4.2. Server Name Indication (SNI) Analysis Use Case 9
5. Certificate checkup notification Use Case 10
6. FMC Chapters 11
7. Conclusions 12
1. EXECUTIVE SUMMARY

Encrypted Traffic Analysis (ETA) is a method of malware detection and cryptographic assessment of secured network sessions, which does not rely on decryption.

New research from Flowmon and IDG Connect shows 99% of IT managers recognize encrypted network traffic as a source of security risks, but two-thirds of businesses fail to protect their assets from both internal and external threats misusing SSL/TLS.

TLS (a successor to SSL) handshake is a non-encrypted session through which client and server negotiate the encryption rules. Only after a secure channel is established, the traffic becomes encrypted. By reading the handshake and its specific parameters we can identify unusual behaviour. Download the Whitepaper here.

2. ENCRYPTED TRAFFIC ANALYSIS (ETA) DASHBOARD

Flowmon Dashboard provide us single pane of glass for Network and Security Operation (NetOps and SecOps) with customizable or preconfigured templates widgets (applied from Configuration Center -> Configuration Templates). It is possible to create multiple Dashboards which present different view on the network information (e.g. one dashboard for network operation, other for security or encrypted traffic analyses and many more). Responsive design allows to view dashboard on mobile phones and tablets.

---

1. EXECUTIVE SUMMARY

Encrypted Traffic Analysis (ETA) is a method of malware detection and cryptographic assessment of secured network sessions, which does not rely on decryption.

New research from Flowmon and IDG Connect shows 99% of IT managers recognize encrypted network traffic as a source of security risks, but two-thirds of businesses fail to protect their assets from both internal and external threats misusing SSL/TLS.

TLS (a successor to SSL) handshake is a non-encrypted session through which client and server negotiate the encryption rules. Only after a secure channel is established, the traffic becomes encrypted. By reading the handshake and its specific parameters we can identify unusual behaviour. Download the Whitepaper here.

2. ENCRYPTED TRAFFIC ANALYSIS (ETA) DASHBOARD

Flowmon Dashboard provide us single pane of glass for Network and Security Operation (NetOps and SecOps) with customizable or preconfigured templates widgets (applied from Configuration Center -> Configuration Templates). It is possible to create multiple Dashboards which present different view on the network information (e.g. one dashboard for network operation, other for security or encrypted traffic analyses and many more). Responsive design allows to view dashboard on mobile phones and tablets.
3. FMC PROFILES

3.1 TLS SERVER VERSION REPORTING USE CASE

TLS Server Version Report provide information about used TLS Protocol versions in whole monitored traffic (recommended parent FMC Profile is All Sources) with visibility into potential unsecure and vulnerable cryptography mechanism. It allows to show us lower TLS Protocol version than recommended TLS Protocol version for advanced security (e.g. TLS 1.0, TLS 1.1, TLS 1.2 or SSL versions).

New Widget setup

1. Selection of a suitable pre-prepared chapter from Flowmon Monitoring Center (FMC -> Reports -> Chapters)
2. Type of Chart (Pie or Linear/Logarithmic)
3. Selection of time interval for data conversion
4. Number of TOP Time series in the chart and their values
5. Possibility of linear or logarithmic condition and colour of table
1. Profile name
2. Parent profile of source data for new profile
3. Group definition like “ETA”
4. Start date can be recalculated with history data
5. Expiration for data collection
6. “Real” type is with real data stored on disc and “Shadow” is about only data for graphing
7. Granularity for interval of collected data samples
8. Specification of unlimited count of channels

1. Position above or under X-axis
2. Every one channel is defined by filter
3. User can choose parent’s profile channels with concrete source data
3.2 DETECTION OF MALWARE BY JA3 FINGERPRINTS USE CASE

JA3 is a much more effective way to detect malicious activity over SSL than IP or domain-based IOCs. Since JA3 detects the client application, it does not matter if malware uses DGA (Domain Generation Algorithms), or different IPs for each C2 host, or even if the malware uses Twitter for C2, as JA3 can detect the malware itself based on how it communicates, rather than what it communicates to. This is a straightforward way how to use Flowmon to find possible threats in connection with detecting specific JA3 fingerprints. In this Use case we have been used JA3 database: https://sslbl.abuse.ch/ja3-fingerprints/

What is JA3 Fingerprint?

• Method describing encrypted communication between client and server
• Calculated during TLS handshake

How it works:

1. consists of headers from Client Hello message from TLS / SSL handshake
3. finally, MD5 hash is applied, which corresponds to the JA3 fingerprint de350869b8c85de67a350c8d186f1e6

IMPORTANT NOTE

Bypassing proxy by camouflage of encrypted traffic:

• camouflage can be recognized by negotiated encryption, usually ciphers are proposed, which are generally recognized as compromised or already compromised
• communication to the Internet directed to compromised IP addresses, compromised HTTP hostname, SNI (name servers in the certificate), etc. Communication is detected by the BLACKLIST method in the ADS module.
IMPORTANT NOTE

In case of profile filter definition with JA3 fingerprints monitoring is not important how many fingerprints are used for the specific malware, it need to be used “OR” as separator between every tls-ja3 parameter.

IMPORTANT NOTE

For relevant encrypted communication outputs where the TLS Handshake parameters are located, it is advisable to add one of the encrypted communication parameters, in our case “tls-sver”, without a value, to the filter.
4. ETA ANALYSES

4.1 PUBLIC KEY LENGTH AND ALGORITHM ANALYSIS USE CASE

Weak short keys and outdated algorithms are a serious security risk. Insufficient key length makes it easier for an attacker to perform brute force decryption. Outdated algorithms suffer from vulnerabilities malicious actors can exploit to break in (think Heartbleed). We should always check the key length and algorithm as one because different algorithms require different key lengths, for example, elliptic curve cryptography algorithms (ECC) have shorter keys while having equivalent key strength as RSA (RFC 4492):

![Figure 9: Time Interval Selection](image)

Also thanks to the visibility of the key length parameter or its algorithm, we are able to identify possible risks in the network, associated with this and resulting greater vulnerability due to simpler encryption. Based on the parameter used, it is also possible to create a chapter for the calculated data in the widget in the Flowmon dashboard.

![Figure 10: TLS Public Key Length Analysis](image)
4.2 SERVER NAME INDICATION (SNI) ANALYSIS USE CASE

Similarly to ALPN, SNI is a TLS extension. It allows TLS-capable servers to host multiple services on the same IPs. Clients add this extension with the hostname of the website they want to connect to.

IMPORTANT NOTE

In case of data volume analysis in this way, the TOP10 results of the largest data volumes transmitted in communication with individual TLS server name (SNI) results. Based on the parameter used it is also possible to create a chapter for the calculated data in the widget in Flowmon dashboard.
5. CERTIFICATE CHECKUP
NOTIFICATION USE CASE

While checking for expired certificates is an obvious step, we might also want to check for soon-to-be-expired certificates to prepare in advance. Furthermore, monitoring certificates and their usage in development, testing and production environments is a way to protect against and identify leaking private keys and other sensitive information.

Flowmon allow us to setup notification that the SSL certificate has expired and needs to be renew. For the purposes of notification, it is possible to use several combined actions, such as notification on an e-mail, run a user script or send a syslog to SIEM System.

1. Name of Alert
2. Parent profile like source of data
3. Additional filter as condition
4. Used channels from parent profile
5. Condition based on total flow summary
6. How many times is alert triggered
7. Actions may be combined
6. FMC CHAPTERS

In the REPORTS tab in the left panel of the FMC module, it is possible to click through to the CHAPTERS section, where chapters are defined as a source of pre-calculated data, not only for reports, but also for the widgets in Flowmon Dashboard itself. These chapters can be fully utilized also for the purpose of monitoring encrypted traffic.

1. Name and Description of Chapter
2. Source Profile of traffic data
3. Channels selection in profile
4. Type of Chapter (Pie or Linear/Logarithmic)
5. No. Of TOP values
6. Parameter statistics
7. Sort by value
8. Chapter columns description
9. Filter specification
10. Recomputing of data in time
7. CONCLUSIONS

99% of IT professionals see encrypted traffic as a possible source of security threats. Don't let the encrypted traffic turn into security risk. Gain a scalable visibility of threats in encrypted traffic when preserving privacy and with no impediment to latency for both, Network and Cloud Operation (NetOps) and Security Operation (SecOps) with Flowmon Probes, Flowmon Collectors and Flowmon ADS.

www.flowmon.com