WHITE PAPER

Encrypted packet metadata vs. flow/IPFIX metadata

Plixer

Introduction

There is some debate among security professionals as to the relative value of flow metadata as compared to packet metadata for detecting threats using network traffic. Consistently, all parties agree that the network layer is perhaps the most effective layer for threat detection. It is often said that the ultimate source of truth is the packet. While this is still true today, encryption makes getting to the source difficult. In today's world where over 90% of internet traffic and 80% of enterprise traffic is encrypted, the most meaningful packet evidence is obscured from the security teams unless they can decrypt the packet to examine the payload before re-encryption occurs. However, decryption is not without its challenges as well as implications on security posture, privacy, and compliance.

Cost of decryption

Decrypting packets comes with a heavy cost. When considering packet decryption operations, enterprises will need to think about the following:

- How to capture and retain packets for a long enough period of time
- Implementing dedicated decryption systems
- Managing keys to decrypt packets to continue to protect privacy

Dwell times for threats continue to be greater than 200 days, which makes retaining packets from the network for that length of time a prohibitively expensive undertaking. Not to mention the complexity added to the network to capture the packets by deploying a "shadow" IT infrastructure of TAPs, SPANs, packet brokers, packet probes, etc. If somehow you can accomplish this feat, dedicated decryption devices must also be deployed adding to the cost, complexity, and administrative burden. Then there is the topic of data privacy management, which traffic should/can be decrypted. Even if you overcome all of these obstacles, there is still the reality that you will never have all the keys to decrypt all the packets, and attackers won't share their keys with you when they encrypt their communications.

Reports show that attackers are using encryption in over 60% of their attacks. Why? Because attackers know that if you don't have their encryption keys, you can't see inside the packet. Also, if

attackers can obfuscate their activity to look like normal encrypted traffic they can evade your defenses. Enterprises should have all the keys to decrypt their traffic, so not being able to decrypt some traffic can be a sign of an attack against your organization. On the other hand, it is typical to have encrypted traffic on the network that will not be able to be decrypted but is normal. SecOps teams need detection systems to alert them when there is unusual traffic on the network regardless of if that traffic is encrypted or not.

Encrypted packet vs. flow/IPFIX

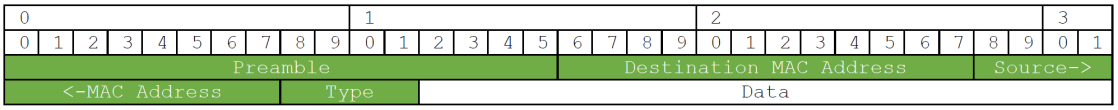
Since many organizations have limited or no encryption capabilities, let's try to understand what is visible in an encrypted packet. First, let's look at the OSI model to understand where parts of the packet exist.

OSI model

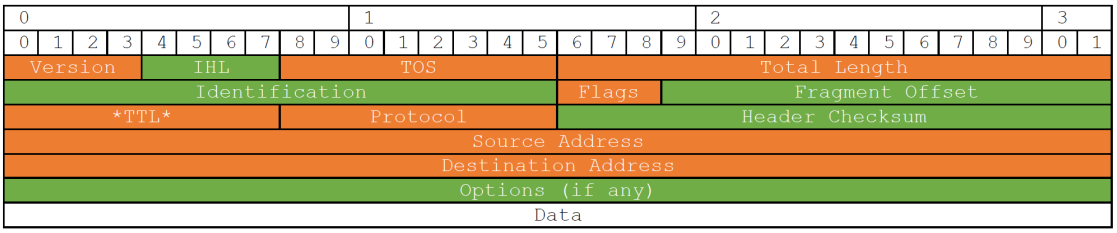
Layer		Protocol Data Unit	Function
7	Application	Data	High-level protocols - **HTTP, and many others**
6	Presentation		Translation of data between a networking service and an application - **TLS**
5	Session		Managing communication sessions - **TLS**
4	Transport	Segment, Datalink	Reliable transmission of data segments between points on a network - **TCP, UDP, IPsec, TLS**
3	Network	Packet	Structuring and managing a multi-node network - **IPv4/IPv6**
2	Data Link	Frame	Transmission of data frames between two nodes connected by a physical layer - **Ethernet**
1	Physical	Wired, Wireless	Transmission and reception of raw bit streams over a physical medium - **CAT5, Radio waves**

It is important to understand that TLS encryption "fits" into the OSI model starting at layer 4 as it contains characteristics of the transport, session, and presentation layers and is individually established on a session-by-session basis. It is also important to understand that Flow/IPFIX only exports information from Layers 3 & 4 and does not export IPsec or TLS information while Deep Packet Inspection (the packet) will contain Layer 2-7 information. Below are the various frame/packet header formats for ethernet, IPv4, and TCP. While there are others (IPv6, UDP, ICMP, etc.) these are the most common formats in enterprise networks and/or involved with TLS encryption.

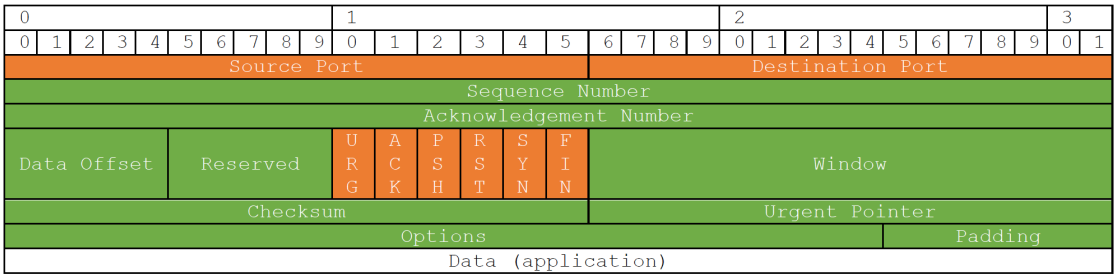
Ethernet II frame format



IPv4 packet format



TCP datagram format



Blue = Flow/IPFIX
Green = Encrypted packet
Orange = Both

Important Notes: When consuming packets, the entire frame length is available. With Flow/IPFIX any length will be based on the IP packet length and will be an average packet length of the flow. TTL for Flow/IPFIX will be reported as either Min/Max or Average TTL if sampling is being used.

There are several fields available in an encrypted packet that are not available to Flow/IPFIX. Fields like Window and TTL that are not exported in Flow/IPFIX can be used to derive security value for the SecOps team, but the real value is in the Data Field of the TCP datagram, which is not available when encryption is in use. Below is a table comparing the availability of fields in an encrypted packet and Flow/IPFIX.

Fields of the packet

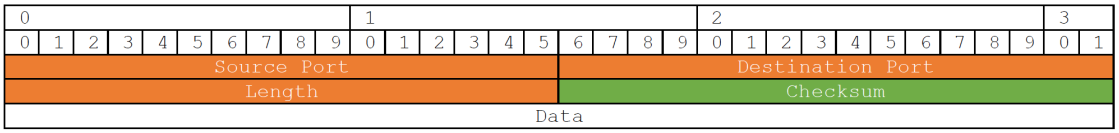
Where Found	Field	Encrypted Packet	Flow/ IPFIX	Security Value
Ethernet	Preamble	Yes	No	None
	Dest. MAC	Yes	No	Id's physical address of hosts
	Src. MAC	Yes	No	Id's physical address of hosts
	Type	Yes	No	None
IP	Version	Yes	Yes	
	IHL	Yes	No	None
	TOS	Yes	Yes	
	Total Length	Yes	Yes*	
	Identification	Yes	No	None
	Flags	Yes	Yes	
	Fragment Offset	Yes	No	None
	TTL	Yes	Yes*	
	Protocol	Yes	Yes	
	Header Checksum	Yes	No	None
	Src. Address	Yes	Yes	
	Dest. Address	Yes	Yes	
	Options	Yes	No	None
TCP	Src. Port	Yes	Yes	
	Dest. Port	Yes	Yes	
	Seq. Number	Yes	No	None
	Ack. Number	Yes	No	None
	Data Offset	Yes	No	None
	Reserved	Yes	No	None
	TCP Flags	Yes	Yes	
	Window	Yes	No	Possible
	Checksum	Yes	No	None
	Urgent Pointer	Yes	No	None
	Options	Yes	No	None
	Padding	Yes	No	None

While it appears that there are many fields available in an encrypted packet versus flow, the reality is that those fields don't lend any security value. Encryption is a great equalizer of the debate, are packets better than flow, in the end, both are all using the same set of metadata.

Other Types of Packets

So where does all this hype around the security value of the packet come from? From the packet perspective, it is all about the payload and inspecting the application and the type of information being exchanged between the hosts on the network. There are other common protocols used that haven't been discussed, those are the UDP and ICMP protocols. There is no encryption for ICMP; however, ICMP information is reported via Flow/IPFIX so there are virtually no differences. UDP is a simple format.

UDP datagram format



Because UDP is a connectionless protocol, only certain types of applications will use UDP. These fall into 2 types of applications, video/multimedia, and simple request/reply applications. Several are listed below:

- VoIP (Uses TLS)
- IPTV (Uses TLS)
- DHCP
- DNS (Uses TLS)
- SNMP (Uses AES128 encryption)
- NTP (Uses TLS)
- SYSLOG (Uses TLS)

Since this paper talks about the encrypted packet, once again if the UDP data is encrypted, then the packet metadata is the same as Flow/IPFIX metadata.

TLS

TLS has been mentioned several times in this paper. The following is a brief primer on TLS that may be helpful. TLS (Transport Layer Security) is an IETF standard that provides authentication, privacy, and data integrity between two hosts communicating via an application/service. TLS is the most widely deployed security protocol in use today. TLS provides an end-to-end encrypted session between two hosts at and within the application layer. For example, the HTTP session between your browser and https://www.cisco.com is secured and separate from the HTTP session between that same browser and https://www.plixer.com. For the purposes of this paper, since Flow/IPFIX doesn't report on TLS information, this topic is out of scope.

KPIs and 3rd party data

These types of data are out of scope for this paper, but other security software vendors will attempt to add them in as part of their "packet" solution. Key Performance Indicators (KPIs, most often associated with Application Performance Management solutions) are metrics derived from observing host-to-host communications. KPIs are not directly related to security, however, with additional analysis, some KPIs can be leading indicators of a security event.

Other data like user identity, operating system, vulnerability scan results, network location, etc. are all very valuable and enrich the metadata collected by both packet and Flow/IPFIX solutions.

Conclusion

While there are more fields available in an encrypted packet than Flow/IPFIX, many do not serve any purpose when it comes to detecting security events. It is not the intention of this paper to advocate for an investment in either a packet or a Flow/IPFIX security solution. Encryption is an equalizing factor in the metadata available from the packet with respect to Flow/IPFIX metadata. Due to the difficulties in storing packets for long periods of time and decrypting network-wide, a combination of packet and flow-based solutions should be deployed. Plixer employs this approach by allowing operators of the Plixer NDR platform to consume flow metadata from the entire network infrastructure. The platform can capture packets (Plixer FlowPro probe converts packets to IPFIX) anywhere that is deemed critical. For more information on the Plixer NDR platform visit https://plixer.com/products/ndr.