Monitoring connections security with zERT - Part 1

Matteo Bottazzi

Fabio Massimo Ottaviani

Enzo Rossi

EPV Technologies

September 2022

1 Introduction

Security is one of the most important strengths of the z/OS system. This is the reason why IBM continues to enhance data security with initiatives such as pervasive encryption.

Even if not all companies require pervasive encryption, most companies need to encrypt network traffic between the mainframe and the outside world.

With z/OS 2.3 IBM introduced the z/OS Encryption Readiness Technology (zERT). It is a new capability of the Communications Server which allows the collection of information from the TCP/IP stack about cryptographic security attributes of IPv4 and IPv6 application traffic, protected using the TLS, SSL, SSH and IPSec cryptographic network security protocols. Information about Enterprise Extender connections are also collected.

This information can be written to new subtypes of SMF 119 records and analyzed to improve connections security.

In this paper we will explain how to customize TCP/IP to collect zERT information and which are the most relevant measurements collected. We will also show some examples of reports which can be used to analyze and improve the security of your connections.