(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) **EP 4 080 822 A8**

(12) **CORRECTED EUROPEAN PATENT APPLICATION**

(15) Correction information:
Corrected version no 1 (W1 A1)
Corrections, see
Bibliography INID code(s) 30

(48) Corrigendum issued on:
23.11.2022 Bulletin 2022/47

(43) Date of publication:
26.10.2022 Bulletin 2022/43

(21) Application number: **22169106.6**

(22) Date of filing: **20.04.2022**

(51) International Patent Classification (IPC):
H04L 9/40 *(2022.01)* ***G06F 21/55*** *(2013.01)*

(52) Cooperative Patent Classification (CPC):
H04L 63/1416; G06F 21/554; H04L 63/0236; H04L 63/1408

(84) Designated Contracting States:
AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR
Designated Extension States:
BA ME
Designated Validation States:
KH MA MD TN

(30) Priority: **20.04.2021 US 202117235544**
22.10.2021 US 202117508596
22.10.2021 US 202117508614
15.03.2022 US 202217695047
05.04.2022 US 202217713827

(71) Applicant: **Centripetal Networks, Inc.**
Portsmouth, NH 03801 (US)

(72) Inventors:
- **MOORE, Sean**
  Portsmouth (US)
- **ROGERS, Jonathan R.**
  Portsmouth (US)
- **MUTOLO, Vincent**
  Portsmouth (US)
- **GEREMIA, Peter**
  Portsmouth (US)

(74) Representative: **MFG Patentanwälte**
Meyer-Wildhagen Meggle-Freund
Gerhard PartG mbB
Amalienstraße 62
80799 München (DE)

(54) **METHODS AND SYSTEMS FOR EFFICIENT THREAT CONTEXT-AWARE PACKET FILTERING FOR NETWORK PROTECTION**

(57) A threat intelligence gateway (TIG) may protect TCP/IP networks from network (e.g., Internet) threats by enforcing certain policies on in-transit packets that are crossing network boundaries. The policies may be composed of packet filtering rules with packet-matching criteria derived from cyber threat intelligence (CTI) associated with Internet threats. These CTI-derived packet-filtering rules may be created offline by policy creation and management servers, which may distribute the policies to subscribing TIGs that subsequently enforce the policies on in-transit packets. Each packet filtering rule may specify a disposition that may be applied to a matching in-transit packet, such as deny/block/drop the in-transit packet or pass/allow/forward the in-transit packet, and also may specify directives that may be applied to a matching in-transit packet, such as log, capture, spoof-tcp-rst, etc. Often, however, the selection of a rule's disposition and directives that best protect the associated network may not be optimally determined before a matching in-transit packet is observed by the associated TIG. In such cases, threat context information that may only be available (e.g., computable) at in-transit packet observation and/or filtering time, such as current time-of-day, current TIG/network location, current TIG/network administrator, the in-transit packet being determined to be part of an active attack on the network, etc., may be helpful to determine the disposition and directives that may best protect the network from the threat associated with the in-transit packet. The present disclosure describes examples of methods, systems, and apparatuses that may be used for efficiently determining (e.g., accessing and/or computing), in response to the in-transit packet, threat context information associated with an in-transit packet. The threat context information

EP 4 080 822 A8

may be used to efficiently determine the disposition and/or one or more directives to apply to the in-transit packet. This may result in dispositions and/or directives being applied to in-transit packets that better protect the network as compared with solely using dispositions and directives that were predetermined prior to receiving the in-transit packet.

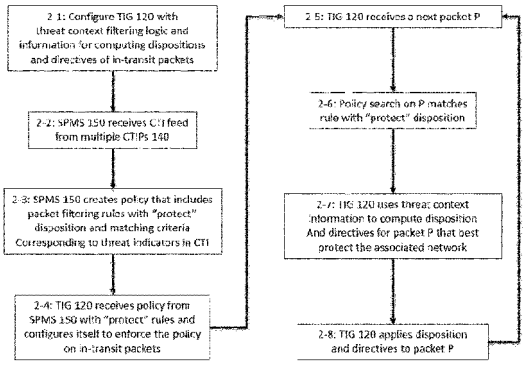

FIG. 2