

[SS 1] ..fi epodoc

 Database: EPODOC

[EPODOC: SS 1] Wine and counterfeiting

Results in EPODOC 713

[SS 2] ss1 and tracing and system

Results in EPODOC 2

[SS 3] ..li



1/2 © EPODOC / EPO

PN - [US2010205670](#) A1 20100812

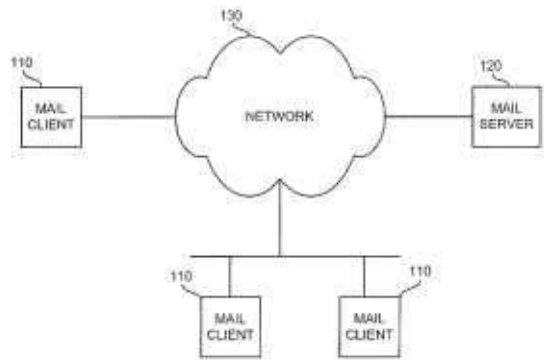
PR - US20100762366
20100418; US20080249804
20081010; US20030654771
20030904; US20020251403
20020920; US20010881145
20010614; US20010881074
20010614; US20020407975P
20020905; US20010341462P
20011214; US20000212425P
20000619

AP - US20100762366 20100418

DT - **

CT - || R141 (A1)
[US6678270](#) B1 20040113 [
] (GARFINKEL SIMSON L [US]);
[US6215763](#) B1 20010410 [
] (DOSHI BHARAT TARACHAND
[US], et al);
[US5905859](#) A 19990518 [
] (HOLLOWAY MALCOLM H [US],
et al);
[US6609205](#) B1 20030819 [
] (BERNHARD THOMAS E [US], et
al);
[US6119236](#) A 20000912 [
] (SHIPLEY PETER M [US]);
[US6981158](#) B1 20051227 [
] (SANCHEZ LUIS [US], et al)

100



CCI - [H04L51/12](#) ; [G06F21/562](#) ;
[H04L63/145](#)

PA - AZURE NETWORKS LLC [US]

TI - METHOD AND APPARATUS
FOR **TRACING** PACKETS

AB - A **system** and method for performing source path isolation in a network. The **system** comprises an intrusion detection **system** (IDS), a source path isolation server (**SS1**) and at least one router configured to operate as a source path isolation router (SR1) operating within an autonomous **system**. When IDS detects a malicious packet, a message is sent to **SS1**. **SS1** in turn generates a query message (QM) containing at least a portion of the malicious packet. Then, QM is sent to participating routers located one hop away. SR1 uses the query message to determine if it has observed the malicious packet by comparing it with locally stored information about packets having passed through SR1. SR1 sends a reply to **SS1**, and **SS1** uses the reply to identify the ingress point into the network of the malicious packet.

2/2 © EPODOC / EPO

PN - [US2009313339](#) A1 20091217

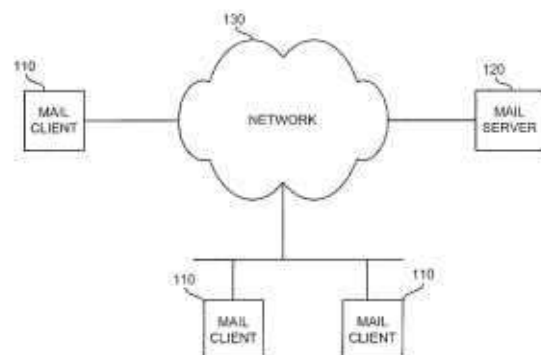
PR - US20080249804
20081010; US20030654771
20030904; US20020251403
20020920; US20010881145
20010614; US20010881074
20010614; US20020407975P
20020905; US20010341462P
20011214; US20000212425P
20000619

AP - US20080249804 20081010

DT - **

CT - || R141 (A1)

100



[US6678270](#) B1 20040113 [] (GARFINKEL SIMSON L [US]);
[US6529498](#) B1 20030304 [] (CHENG DEAN [US]);
[US6215763](#) B1 20010410 [] (DOSHI BHARAT TARACHAND [US], et al);
[US5521910](#) A 19960528 [] (MATTHEWS WALLACE [US]);
[US5905859](#) A 19990518 [] (HOLLOWAY MALCOLM H [US], et al);
[US6609205](#) B1 20030819 [] (BERNHARD THOMAS E [US], et al);
[US6119236](#) A 20000912 [] (SHIPLEY PETER M [US]);
[US6981158](#) B1 20051227 [] (SANCHEZ LUIS [US], et al)

CCI - [H04L51/12](#) ; [G06F21/562](#) ; [H04L63/145](#)

TI - METHOD AND APPARATUS FOR **TRACING** PACKETS

AB - A **system** and method for performing source path isolation in a network. The **system** comprises an intrusion detection **system** (IDS), a source path isolation server (**SS1**) and at least one router configured to operate as a source path isolation router (SR1) operating within an autonomous **system**. When IDS detects a malicious packet, a message is sent to **SS1**. **SS1** in turn generates a query message (QM) containing at least a portion of the malicious packet. Then, QM is sent to participating routers located one hop away. SR1 uses the query message to determine if it has observed the malicious packet by comparing it with locally stored information about packets having passed through SR1. SR1 sends a reply to **SS1**, and **SS1** uses the reply to identify

the ingress point into the
network of the malicious packet.

[SS 3]