(19) SCHWEIZERISCHE EIDGENOSSENSCHAFT
EIDGENÖSSISCHES INSTITUT FÜR GEISTIGES EIGENTUM

(11) CH 700 308 A2

(51) Int. Cl.: G06F 21/00 (2006.01)
H04L 29/06 (2006.01)

Patentanmeldung für die Schweiz und Liechtenstein
Schweizerisch-liechtensteinischer Patentschutzvertrag vom 22. Dezember 1978

(12) PATENTANMELDUNG

(21) Anmeldenummer: 00102/09

(22) Anmeldedatum: 22.01.2009

(43) Anmeldung veröffentlicht: 30.07.2010

(71) Anmelder:
Martin Blapp, Rüttelistrasse 13
4416 Bubendorf (CH)

(72) Erfinder:
Martin Blapp, 4416 Bubendorf (CH)

(54) Ein technisches System in der Hardware oder im Kernel eines E-Mail Gateways, um die Betriebs-Infrastruktur oder das Betriebs-System gegen DDos-Angriffe aus dem Internet zu schützen.

(57) Beschrieben wird folgend ein technisches System in der Hardware oder im Kernel von E-Mail Gateways, um diese gegen Überlastung und Ausfall-Situationen zu schützen, vor allem gegen DDoS-Angriffe aus dem Internet. Das System funktioniert ohne Umleitung der Verbindungen auf ein anderes System, ohne irgendwelche Markierungen der IP-Header, ohne Modifikationen und dem Blockieren von SMTP-Verbindungen im Zusammenspiel mit einer Kernel-IP-Whitelist. Das System betrifft nur das SMTP-Protokoll und generell Protokolle, die auf Letzterem basieren, wie SMTPS. Massive Überlastungs-Situationen, die von solchen DDoS-Angriffen hervorgerufen werden, oder auch viele gleichzeitige Verbindungen von verschiedenen IP-Adressen, die die Software oder Hardware zur gleichen Zeit beanspruchen, können zum Stillstand von Software oder Hardware oder zu extrem langsamen Antwort-Zeiten vom betroffenen Betriebssystem und der ausgeführten Software führen.

Beschreibung

[0001] Das zur Patentierung angemeldete System wird direkt im Kernel oder der Firmware [1] eines Mail-Gateways [2] eingesetzt, und verlangsamt bestimmte [3] SMTP-Verbindungen oder Verbindungs-Versuche [4] während eines DDoS-Angriffs [5], während dem normaler SMTP-Verkehr normal zirkulieren kann, falls sich der Verbindende Rechner auf einer Ausnahmen-Liste des Kernels [6] befindet. Diese guten Verbindungen werden ohne Verzögerung der betroffenen Applikation zugewiesen, die diese wie gewohnt verarbeiten kann. Das System betrifft ausschliesslich das SMTP-Protokoll und Protokolle die auf letzterem basieren, wie SMTPS.

[0002] Verzögerte Verbindungen können alle Socket-Verbindungen neben der Whiteliste betreffen, oder Verbindungen mit spezifischen Merkmalen wie Protokoll-Buffer, TCP-Optionen [7]. Das System macht an den Verbindungen keine Modifikation [8], keine Markierungen [9], keine Weiterleitungen [10], noch blockiert direkt keine Verbindungen [11]. Es besteht nur aus einer oder mehreren Warteschlangen [12], die eine bestimmte Anzahl Verbindungen bedienen können, und über einen Überfluss-Mechanismus verfügen, der nach der FILO Methode [13] funktioniert. Traditionelle E-Mail Gateways hingegen funktionieren nach der FIFO [14] Methode. Natürlich ist es neben dem System immer noch möglich, mit einer Kernel Whitelist die Verbindungen zu markieren, weiterzuleiten, zu blockieren oder QoS [15] Methoden anzuwenden. Die einzige verwendete Methode die das zur Patentierung angemeldete System verwendet ist das Verlangsamen der verdächtigen [16] SMTP-Verbindungen. Die Verbindungen können dabei bis 300 Sekunden pausiert werden und der verbindende Rechner wird dabei in diesem Zeitrahmen gezwungen, auf die Antwort des Kernels, das sogenannte Begrüssungs-Banner [17] zu warten. Das Konzept des Accept Filters wurde bereits bei anderen Protokollen eingesetzt, allerdings ist der Mechanismus dort anders implementiert [18].

[0003] Ein mit einer solchen SMTP-Verzögerung eingesetztes E-Mail Gateway kann viel mehr SMTP-Verkehr als ein normaler Gateway handhaben und ist sozusagen immun gegen direkte Angriffe von grossen Bot-Netzen [19]. Weil der Speicherverbrauch im Kernel viel kleiner ist als unter dem Betriebssystem, dauert es verständlicherweise einiges länger, bis der Server an seine Grenzen stösst [21]. Und das System kann so den Prozessor entlasten, in dem Kontext-Wechsel des Kernels vermieden werden,, da die Verbindungen noch nicht an die Applikation im Betriebssystem durchgestellt worden sind. Die Vorteile dieses Vorgehens sind also geringerer Speicherverbrauch, verbesserte System-Stabilität und dadurch die Möglichkeit mehrere Server zu einer Instanz zusammenzufassen.

Neuer Erfindungswert:

[0004] Herkömmliche DOoS-Schutz Systeme funktionieren ausschliesslich mit Blacklists oder Daten-Filterung, oder sie leiten verdächtige Datenströme an weitere Geräte weiter.

[0005] Beachten Sie folgende Patente: WO0 233 870A2, CN1 968 147A, EP1 691 529A1, WO2004 068 285A2, WO03 017 613A1.

[0006] Das vorgestellte System benötigt diese Methoden nicht. Es funktioniert ausschliesslich mit dem Verzögern der betroffenen Verbindungen für eine vordefinierte Wartezeit mit einer zugehörigen Warteschlange mit einer eingeschränkten Anzahl Verbindungen. Das System erlaubt sogar schlechten Verbindungen das Zielsystem zu erreichen, falls die Wartezeit korrekt abgewartet wird. Systeme die eine solche Wartezeit implementieren existieren zwar schon, aber sie wurden bisher noch nie im Kernel implementiert. Sie wurden bisher immer nur Programmen oder als Teil des Betriebssystems eingesetzt, wo sie massive Prozessor-Belastung und Ausfall-Situationen nicht verhindern konnten.

Technisches Vokabular, Erklärungen

[0007] [1] Der Kernel ist der Teil eines Betriebssystems, der direkt mit der Hardware kommuniziert. Ein Kernel kann in die Hardware integriert sein, oder auf der Hardware zusammen mit einem Betriebssystem laufen. Das erfundene System funktioniert nur im Kernel.

[0008] [2] E-Mail Gateways sind Server die E-Mail empfangen und zu weiter entfernten Servern weiterleiten, oder E-Mails an lokale E-Mail Briefkästen zustellen. Ein E-Mail Gateway kann internen oder externen E-Mail Verkehr bearbeiten. Das vorgestellte und zur Patentierung angemeldete System funktioniert nur mit E-Mail Gateways die über Zugang zum Internet verfügen.

[0009] [3] SMTP steht für «Simple Mail Transfer Protocol», auf Deutsch: «einfaches Mail Übermittlungs-Protokoll» und ist eines der ältesten Protokolle, das auf TCP-IP aufsetzt.

[0010] [4] Ein Angreifer kann eine oder mehrere SMTP-Verbindungen öffnen, ohne irgendwelche Daten zu senden. Das erfundene Systeme hält diese Verbindungen offen, ohne dafür die Verbindungen an die verantwortliche E-Mail-Server Applikation überstellen zu müssen.

[0011] [5] DDoS, distributed denial of Service attacks heisst auf Deutsch übersetzt soviel wie, Verteilte Angriffe auf eine Dienstleistung. Dies ist bei E-Mail der Aufbau von Verbindungen von vielen unterschiedlichen IP-Adressen aus, mit dem Ziel den angegriffenen SMTP-Server anzuhalten, oder das vom Angriff ebenfalls betroffene Betriebssystem ausser Betrieb zu setzen.

[0012] [6] Die im Kernel enthaltene Ausnahmen-Liste kann IP-Adressen, IP-Netze enthalten oder auch leer bleiben.

[0013] [7] Die beschriebenen Methoden sind bekannt als passive Betriebssystem-Erkennung (OSPF).

[0014] [8] Verbindungen zu modifizieren meint den Inhalt, die Daten der Verbindungen zu ändern und die Sockets zu markieren.

[0015] [9] Verbindungen zu markieren meint diese zu markieren, ohne den Inhalt der Verbindungen zu modifizieren.

[0016] [10] Verbindungen weiterzuleiten meint diese an ein fremdes System umzuleiten, das die Verbindungen dann anders behandeln kann.

[0017] [11] Mit Blockieren ist das direkte Beenden der Verbindungen im Kernel oder das Verbindungsverhalten gemeint. Das zur Patentierung angemeldete System kann Verbindungen ebenfalls zurückweisen, aber nur wenn die Warteschlange überfüllt ist. Dann ist das Verhalten ähnlich wie bei System-weiten Verbindungs-Limiten.

[0018] [12] Eine Listen-Warteschlange ist ein Konzept das von UNIX-Systemen her bekannt ist. Damit gemeint ist eine Warteschlange mit Sockets, bei denen zwar die Verbindung zwischen beiden Systemen hergestellt worden ist, aber die einzelnen Verbindungen noch nicht an die Applikationen überwiesen worden sind.

[0019] [13] FILO steht für: als erster hinein, als letzter heraus

[0020] [14] FIFO steht für: als erster hinein, als erster heraus

[0021] [15] QoS, Quality of Service ist ein System um die Qualität eines Dienstes gewährleisten zu können.

[0022] [16] Verdächtige Verbindungen können alle IP-Adressen betreffen, die nicht in der Whitelist sind, oder zur Unterscheidung kann auch die passive Erkennung mit der Betriebssystem-Erkennung (OSPF) eingesetzt werden.

[0023] [17] Das SMTP Protokoll nötigt den Sender-Rechner einer E-Mail auf die Begrüssungs-Zeile des Empfangs-Servers zu warten. Die Wartezeit beträgt dabei maximal 300 Sekunden.

[0024] [18] Das Accept-Filter System wurde ursprünglich von David Filo bei Yahoo! erfunden und wurde zu einem ladbaren Kernel-Modul von Alfred Perlstein erweitert. Das Accept-Filter Konzept wurde am 25. Juni 2000 ins FreeBSD UNIX-Betriebssystem integriert.

[0025] [19] Botnets sind eine grosse Anzahl von gehackten Systemen, die zentral von einem oder mehreren Programmen kontrolliert werden (bots). Der Hauptsächliche Verwendungszweck von diesen Botnets ist es SPAM zu senden, oder andere Computer Systeme anzugreifen.

[0026] [20] Userland meint alle Applikationen die in einem Betriebssystem laufen, mit Ausnahme des Kernel, und allen Teilen des Betriebssystems wie Kernel-Module, die im Kernel Kontext arbeiten.

[0027] [21] Es existieren systemweite Verbindungs-Limiten, oder Limiten die pro verantwortliches Protokoll die Verbindungen pro Programm limitieren. Verbindungs-Limiten können auch die Anzahl Verbindungen nach ihrer IP-Herkunft limitieren.

[0028] [22] Ist der Prozess den Status eines Hauptprozessors zu speichern und wiederherzustellen (den Kontext), so dass verschiedene Programme oder Threads einen Hauptprozessor miteinander nutzen können. Context Switches sind ein essentieller Bestandteil moderner Multitasking Betriebssysteme. Sie sind allerdings recht aufwendig, und daher hängt die Geschwindigkeit eines Betriebssystems und derer Applikationen massiv von der Implementation und Optimierung von Context Switches ab. Ja nach Implementation braucht ein Context-Switch mehr oder weniger Resourcen.

Bild Beschreibungen:

[0029] Bild 1 FIFO Warteschlange (als erster hinein, als erstes heraus) ohne Accept-Filter. Dieses Bild zeigt ein unmodifiziertes Betriebssystem unter massiver Last. Das System weist alle Verbindungen zurück und kann zwischen den Verbindungen eines Angreifers und normalen Verbindungen nicht unterscheiden.

[0030] Bild 2 FILO Warteschlange (als erster hinein, als letzter heraus) mit aktivem Accept-Filter. Die Verbindungen dieser Warteschlange schlafen für eine vordefinierte Zeit im Kernel bevor sie weiterverarbeitet werden.

[0031] Bild 3 Ansicht eines unakzeptierten Sockets.

[0032] Bild 4 Fast die gleiche Ansicht wie Bild 3, zeigt den Inhalt eines unakzeptierten Sockets. Das temporäre Empfangs-Speicher des Sockets enthält noch keine Daten.

[0033] Bild 5 Fast die gleiche Ansicht wie Bild 6, zeigt aber den Inhalt eines akzeptieren Sockets. Der temporäre Empfangsspeicher enthält bereits Daten und das Socket wurde eventuell schon zur Applikation durchgestellt.

[0034] Bild 6 Ansicht eines akzeptierten Sockets.

[0035] Bild 7 Zeigt das UNIX Socket Modell und wo der SMTP Accept-Filter genau platziert ist.

[0036] Bild 8 Die Funktionsweise/Arbeitsablauf mit der Kernel Whitelist und der zusätzlichen Betriebssystem-Erkennung. Es sind mehrere E-Mail Warteschlangen (queues) mit unterschiedlichen Wartezeiten möglich. Unterschieden werden in der Grafik 'Gute Verbindungen' von Unix-Systemen her, 'Unbekannte Verbindungen' von nicht bekannten Betriebssystemen und Bot-Net-Verbindungen von mehrheitlich auf Windows-basierenden Systemen.

[0037] Bild 9 Die Funktionsweise/Arbeitsablauf mit nur der Kernel Whitelist und einem aktiven Accept-Filter mit einer definierten Schlaf-Zeit.

Patentansprüche

1. Die Methode SMTP-Verbindungen im Kernel offen zu halten (accf_smtp), ohne CPU-Zeit zu gebrauchen.
2. Die Verbindung des smtp accept Filters in Anspruch [1] mit einer Hardware oder Kernel basierten internen Whitelist oder Ausnahmen-Liste.
3. Die Kombination der passiven Betriebssystem-Erkennung (OSPF) Methode im Zusammenspiel mit den Ansprüchen [1] und [2], um Angriffe von Spammern von normalen Verbindungen zu trennen und letztere ungehindert durchzulassen.
4. Das Gebrauchsmuster der Ansprüche [1], [2] und [3] mit Verwendungszweck der Spam-Filterung oder Spam-Reduktion.
5. Das beschriebene System in [1] kann eine oder mehrere unterschiedliche Wartezeiten für den SMTP-Verkehr benutzen, falls die Verbindung als verdächtige SMTP-Verbindungen oder DDoS-Verkehr eingestuft worden sind.
6. Das Verteidigungs-System [1] kann einmal oder mehrmals auf dem gleichen Betriebssystem ausgeführt werden (mehrere Instanzen des Mailservers und von accf_smtp). Das System profitiert dabei von verschiedenen Wartezeiten.

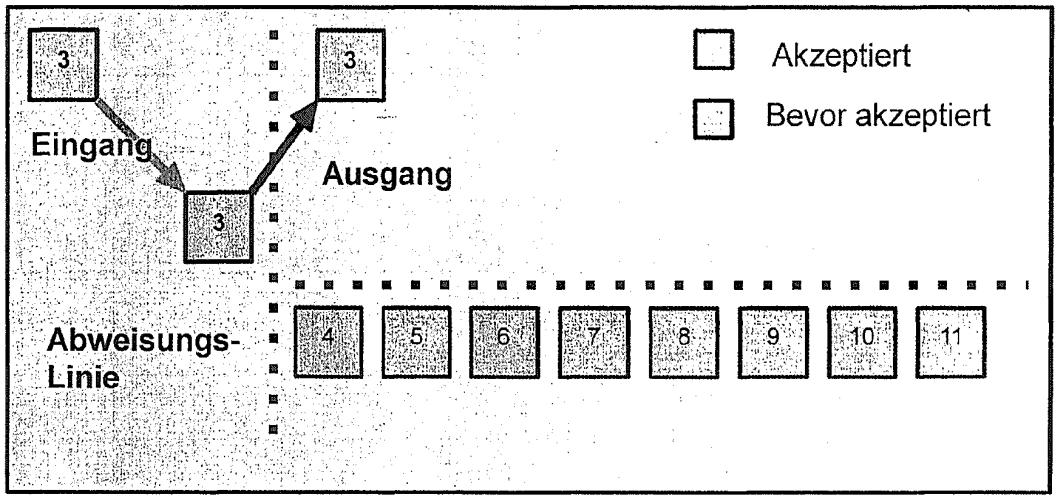
3
3
Eingang
Ausgang
3
Akzeptiert
Bevor akzeptiert
Abweisungs-
Linie
4
5
6
7
8
9
10
11

Bild 1

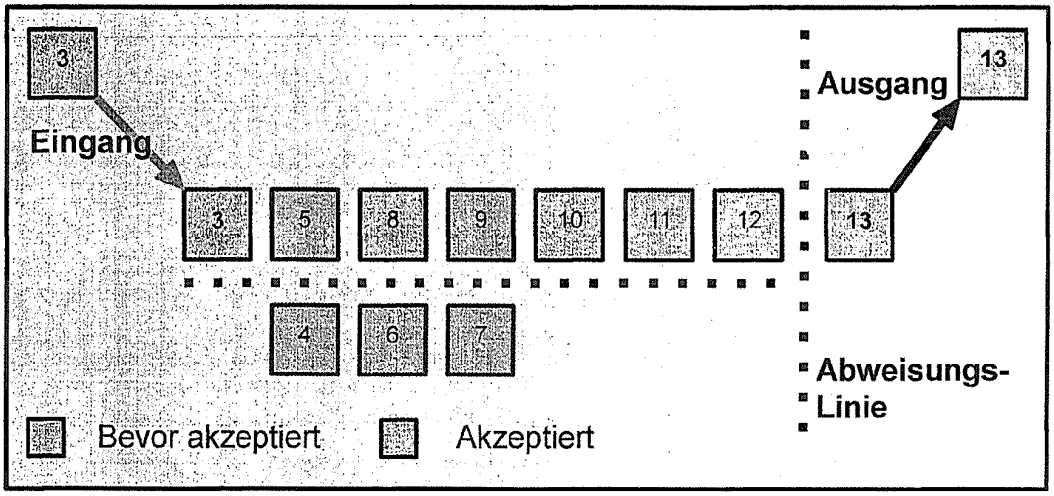
3
Eingang
3
5
8
9
10
11
12
4
6
7
Ausgang
13
13
Abweisungs-
Linie
Bevor akzeptiert
Akzeptiert

Bild 2

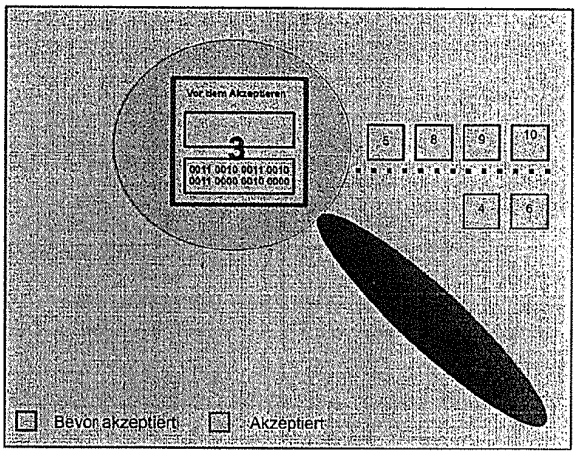

Bild 3

Bild 4

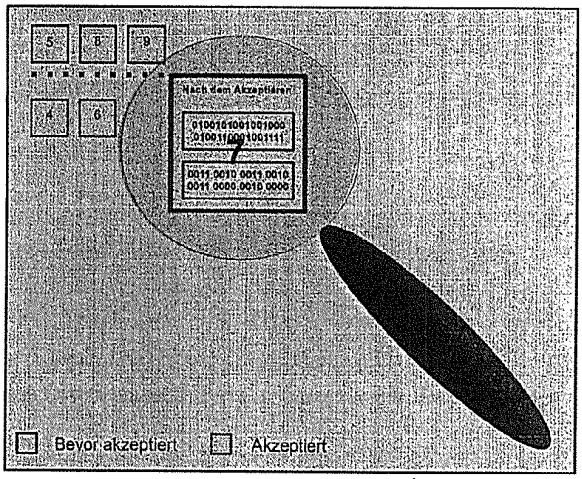

Bild 6

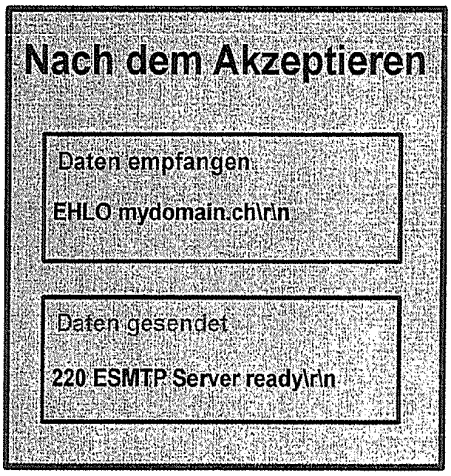

Bild 5

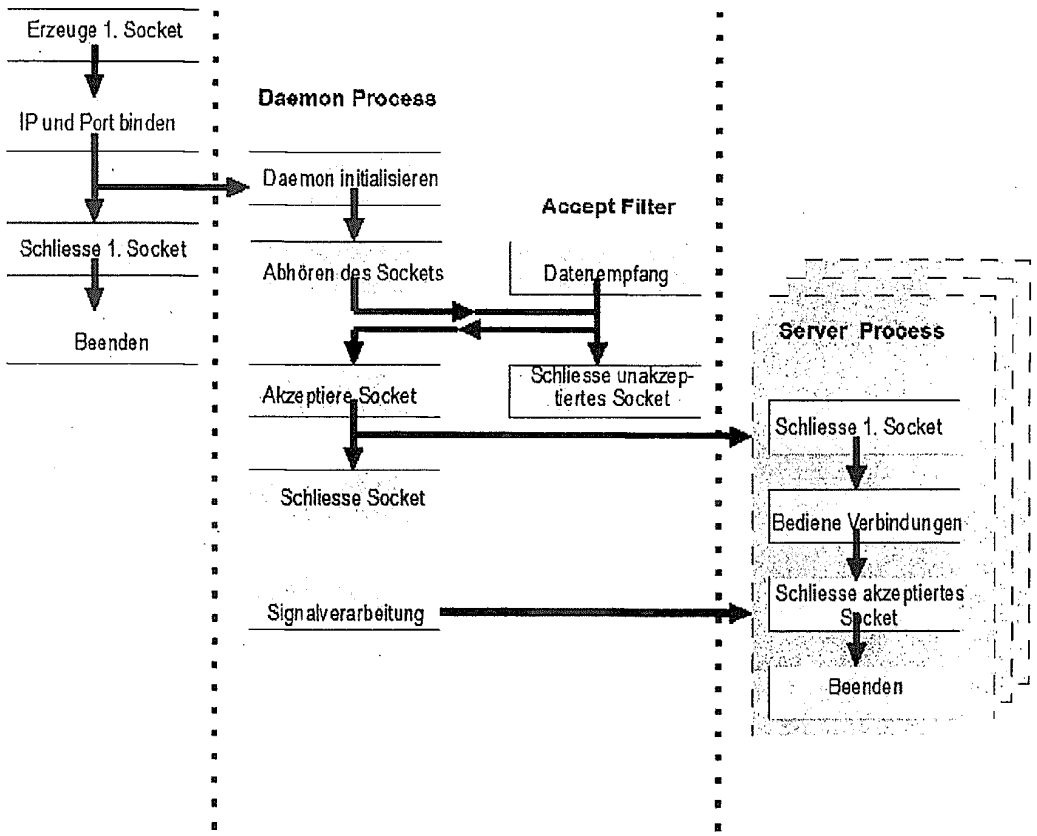
Erzeuge 1. Socket
IP und Port binden
Schliesse 1. Socket
Beenden
Daemon Process
Daemon initialisieren
Abhören des Sockets
Akzeptiere Socket
Schliesse Socket
Signalverarbeitung
Accept Filter
Datenempfang
Schliesse unakzeptiertes Socket
Server Process
Schliesse 1. Socket
Bediene Verbindungen
Schliesse akzeptiertes Socket
Beenden

Bild 7

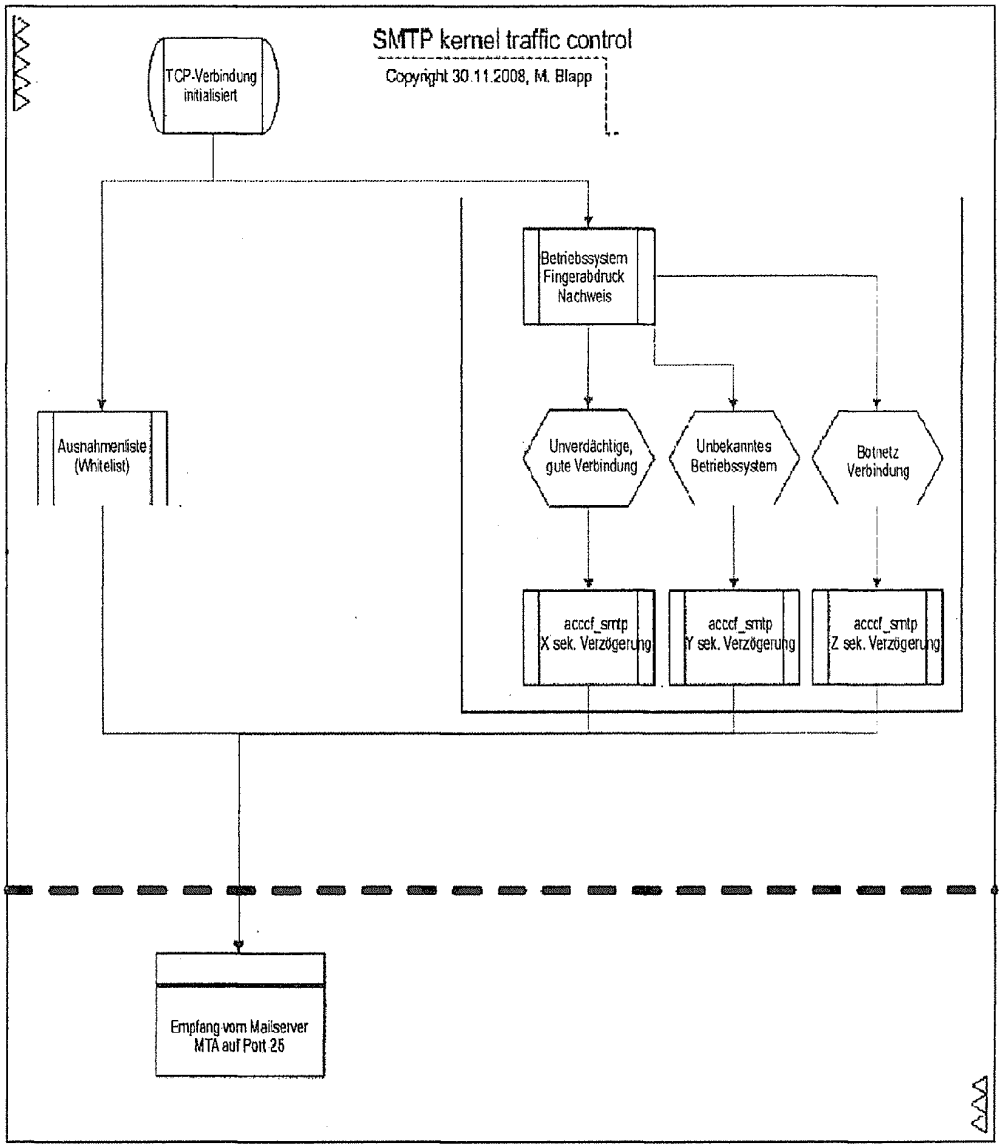
SMTP kernel traffic control
Copyright 30.11.2008, M. Blapp
TCP-Verbindung initialisiert
Betriebssystem Fingerabdruck Nachweis
Ausnahmenliste (Whitelist)
Unverdächtige, gute Verbindung
Unbekanntes Betriebssystem
Botnetz Verbindung
acccf_smtp X sek. Verzögerung
acccf_smtp Y sek. Verzögerung
acccf_smtp Z sek. Verzögerung
Empfang vom Mailserver MTA auf Port 25

Bild 8

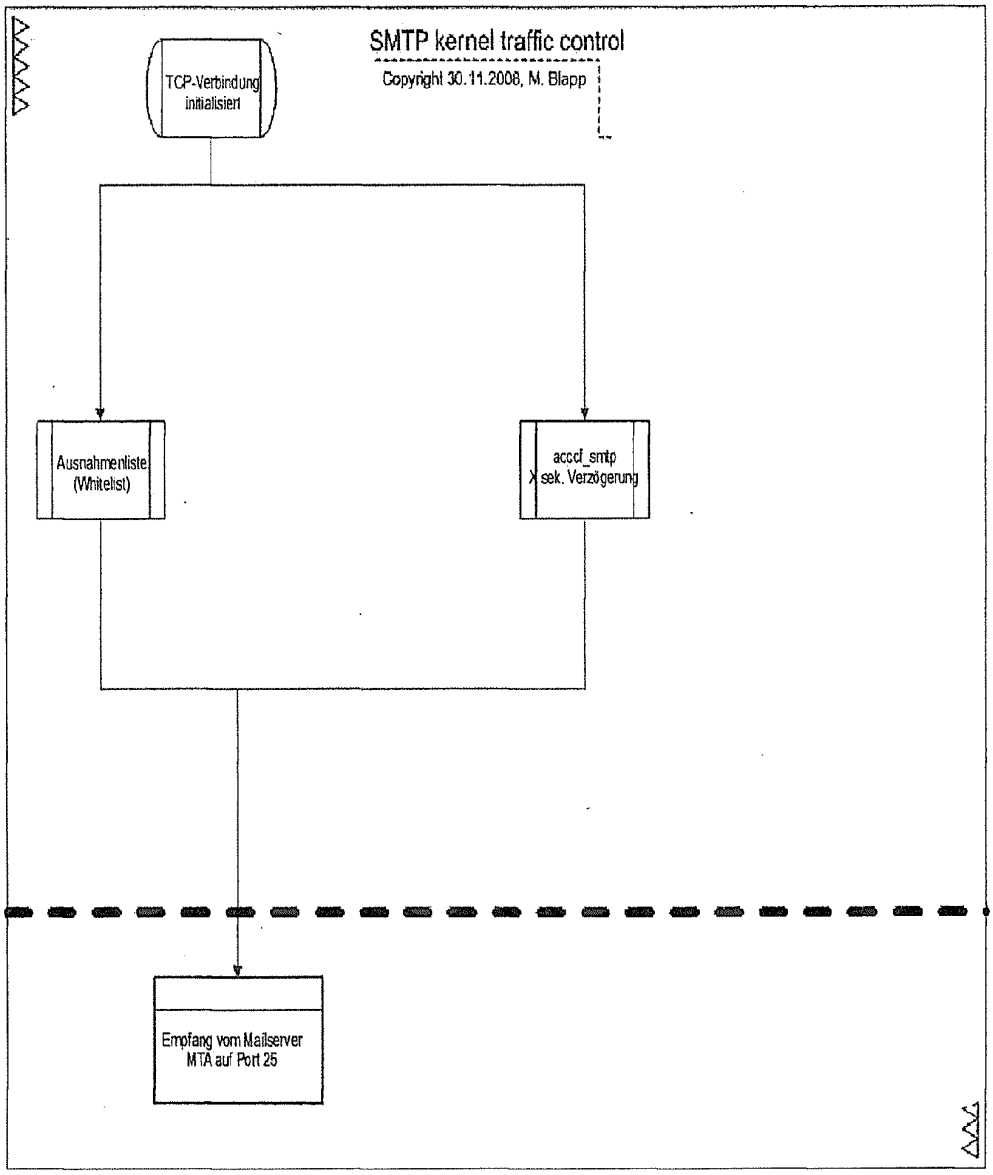
SMTP kernel traffic control
Copyright 30.11.2008, M. Blapp
TCP-Verbindung initialisiert
Ausnahmenliste (Whitelist)
accd_smtp
sek. Verzögerung
Empfang vom Mailserver MTA auf Port 25

Bild 9