(19) Deutsches Patent- und Markenamt

(10) **DE 10 2020 114 199 A1** 2021.12.02

(12) # Offenlegungsschrift

(21) Aktenzeichen: **10 2020 114 199.8**
(22) Anmeldetag: **27.05.2020**
(43) Offenlegungstag: **02.12.2021**

(51) Int Cl.: ***G06F 21/55*** (2013.01)

(71) Anmelder:
Basler Aktiengesellschaft, 22926 Ahrensburg, DE

(74) Vertreter:
Maiwald Patentanwalts- und Rechtsanwaltsgesellschaft mbH, 40212 Düsseldorf, DE

(72) Erfinder:
Adank, Sebastian, 22926 Ahrensburg, DE;
Mehden, Timm von der, 22926 Ahrensburg, DE;
Dekarz, Jens, 23843 Bad Oldesloe, DE

(56) Ermittelter Stand der Technik:

US	**2005 / 0 283 614**	**A1**
EP	**3 144 842**	**A1**
EP	**3 726 408**	**A1**
WO	**2016/ 139 079**	**A1**

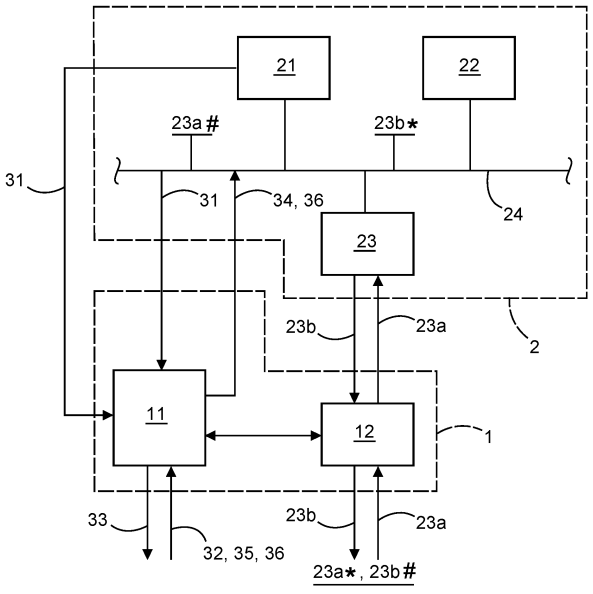
Prüfungsantrag gemäß § 44 PatG ist gestellt.

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen.

(54) Bezeichnung: **Absicherung von Computersystemen gegen Manipulationen und Funktionsanomalien**

(57) Zusammenfassung: System (1) zur Absicherung eines Computersystems und/oder Steuerungssystems (2) gegen Manipulationen und Funktionsanomalien, umfassend ein Überwachungsmodul (11), welches mindestens eine erste Schnittstelle (11a), eine zweite Schnittstelle (11b) sowie mindestens einen Speicher (11c) aufweist und dazu ausgebildet ist,

• Informationen (31), die den Systemzustand des Computersystems und/oder Steuerungssystems (2) charakterisieren, über die erste Schnittstelle (11a) zu empfangen;
• eine verschlüsselte Anfrage (32) nach dem Systemzustand über die zweite Schnittstelle (11b) zu empfangen und mit einem in dem Speicher (11c) abgelegten Anfragen-Schlüssel (41) zu entschlüsseln;
• aus mindestens einem Teil der über die erste Schnittstelle empfangenen Informationen (31) eine Antwort (33) auf die Anfrage (32) zu generieren;
• die Antwort (33) mit einem unter Heranziehung der Anfrage (32) ermittelten Antwort-Schlüssel (42) zu verschlüsseln und über die zweite Schnittstelle (11b) auszugeben;
• einen neuen Anfragen-Schlüssel (41*) zu ermitteln, der ein gemeinsames Geheimnis ist, das auch dem Absender der Anfrage (32) zugänglich ist; und
• diesen neuen Anfragen-Schlüssel (41*) in dem Speicher (11c) abzulegen.



Beschreibung

[0001] Die Erfindung betrifft die Absicherung von Computersystemen, insbesondere in IoTgeräten, gegen Manipulationen sowie allgemein gegen Funktionsanomalien unabhängig von deren Ursache.

Stand der Technik

[0002] Der Nutzwert von Geräten für das Internet of Things (IoT) wird zu einem großen Teil durch deren Vernetzung über eine oder mehrere Schnittstellen bestimmt. Diese Vernetzung schafft jedoch Angriffsflächen. Sobald über Schnittstellen empfangene Daten von Software auf dem Gerät verarbeitet werden, besteht ein Risiko, dass ein Angreifer mit speziell präparierten, bewusst nicht der Spezifikation für den Datenaustausch entsprechenden Daten der Software auf dem Gerät seinen Willen aufzwingt und so die Kontrolle über das Gerät übernimmt.

[0003] Wenn die Software auf dem Gerät beispielsweise erwartet, dass gemäß Spezifikation eine bestimmte Menge Daten geliefert wird, und für diese Menge Daten Platz im Arbeitsspeicher reserviert, dann kann ein Angreifer einfach mehr Daten als vorgesehen schicken. Wird dies in der Software nicht explizit abgefangen, werden die Daten über die Grenze des eigentlich reservierten Bereichs hinaus geschrieben (Pufferüberlauf). Der Angreifer kann auf diesem Wege möglicherweise für den Kontrollfluss der Software relevante Speicheradressen überschreiben und auch gleich Code mitliefern, der statt der ursprünglich geplanten Aktivität der Software als Nächstes ausgeführt werden soll.

[0004] Daneben gibt es noch eine Fülle weiterer Möglichkeiten, durch manipulierte Daten Situationen zu erzeugen, die beim Entwurf des Kontrollflusses der Software nicht vorgesehen waren. Jede dieser Situationen hat das Potential, so zu eskalieren, dass schließlich vom Angreifer mitgelieferter Code ausgeführt wird oder die Software zumindest abstürzt und die Arbeit einstellt. Auch wenn sich der Programmierer der Software spezielle Mühe gibt, solche Manipulationen vorherzusehen, ist es nur eine Frage der Zeit, bis ein Angreifer eine völlig neue und im Entwurf des Kontrollflusses noch nicht abgehandelte Situation kreiert.

Aufgabe und Lösung

[0005] Es ist daher die Aufgabe der Erfindung, Manipulationen und Funktionsanomalien in Computersystemen und/oder Steuerungssystemen auch in dem Fall, dass deren Software vollständig unter der Kontrolle eines Angreifers ist, zumindest zu erkennen, so dass entsprechende Gegenmaßnahmen eingeleitet werden können.

[0006] Diese Aufgabe wird erfindungsgemäß gelöst durch ein System gemäß Hauptanspruch. Weitere vorteilhafte Ausgestaltungen ergeben sich aus den darauf rückbezogenen Unteransprüchen.

Offenbarung der Erfindung

[0007] Im Rahmen der Erfindung wurde ein System zur Absicherung eines Computersystems und/oder Steuerungssystems gegen Manipulationen und Funktionsanomalien entwickelt.

[0008] Hierbei ist unter Manipulation insbesondere jeder bewusst herbeigeführte Eingriff in das Computersystem und/oder Steuerungssystem zu verstehen, der zum Ziel hat, einen Systemzustand, und/oder eine bestimmungsgemäße Funktionalität, des Computersystems und/oder Steuerungssystems zu stören oder zu verändern. Eine solche Manipulation kann insbesondere beispielsweise einen Eingriff in den Kontrollfluss der Software des Computersystems und/oder Steuerungssystems beinhalten, so dass diese Software hinterher etwas Anderes tut als ursprünglich vorgesehen. Beispielsweise kann das Computersystem und/oder Steuerungssystem zum für den Angreifer kostenlosen Schürfen von Kryptowährungen, zum Versenden unerwünschter E-Mails („Spam“) oder zum Versenden unnützer Datenpakete im Rahmen eines „Distributed Denial of Service“ (DDoS)-Angriffs umfunktioniert werden. Der Angriff kann aber auch etwa bewirken, dass das Computersystem und/oder Steuerungssystem sensible Daten (etwa Zugangsdaten zu anderen Systemen) preisgibt oder seine primäre Funktion dem Willen des Angreifers anpasst. Beispielsweise kann eine Überwachungskamera zu bestimmten Zeiten kommentarlos das Aktualisieren des Bildes einstellen, damit der Angreifer unerkannt Zugang erhält.

[0009] Der Begriff der Funktionsanomalie ist hingegen nicht auf solche Anomalien beschränkt, die bewusst von Menschen herbeigeführt wurden. Vielmehr umfasst dieser Begriff auch beispielsweise Situationen, in denen die Hardware des Computersystems und/oder Steuerungssystems, und/oder eine daran angeschlossene Peripherie (etwa ein Sensor), defekt oder aus anderen Gründen (wie etwa Verschleiß oder Verschmutzung) funktionsunfähig ist.

[0010] Das System umfasst ein Überwachungsmodul mit mindestens eine ersten Schnittstelle, einer zweiten Schnittstelle und mindestens einem Speicher, wobei dieser Speicher bevorzugt unabhängig vom Speicher des Computersystems und/oder Steuerungssystems ist. Die erste Schnittstelle ist bevorzugt eine physische Schnittstelle, die in Hardware direkt auf den Speicher des Computersystems und/oder Steuerungssystems zugreifen kann. Das Überwachungsmodul empfängt Informationen, die den Systemzustand des Computersystems und/

oder Steuerungssystems charakterisieren, über die erste Schnittstelle und beantwortet auf der Basis dieser Informationen eine über die zweite Schnittstelle empfangene Anfrage nach dem Systemzustand. Diese Kommunikation über die zweite Schnittstelle läuft verschlüsselt ab. Diese Verschlüsselung verhindert zum einen ein unbefugtes Mitlesen der Informationen während der Übertragung über die zweite Schnittstelle und über ein Netzwerk, mit dem diese zweite Schnittstelle möglicherweise verbunden ist. Zum anderen wird durch das Schlüsselmanagement dieser Verschlüsselung sichergestellt, dass

- nur ein befugter Kommunikationspartner sich nach dem Systemzustand des Computersystems und/oder Steuerungssystems, der möglicherweise sensitive Informationen umfasst, erkundigen kann und
- eine möglicherweise kompromittierte Software des Computersystems und/oder Steuerungssystems die Antwort des Überwachungsmoduls auch dann nicht fälschen kann, wenn diese Software Daten in das gleiche Netzwerk zu senden vermag, mit dem auch die zweite Schnittstelle des Überwachungsmoduls verbunden ist.

[0011] Zu diesem Zweck entschlüsselt das Überwachungsmodul eine verschlüsselte Anfrage, die es über die zweite Schnittstelle empfangen hat, mit einem in dem Speicher abgelegten Anfragen-Schlüssel. Dies liefert nur dann ein sinnvolles Ergebnis, wenn der Absender der Anfrage den korrekten Anfragen-Schlüssel benutzt hat, also als befugter Kommunikationspartner im Besitz dieses Anfragen-Schlüssels ist.

[0012] Das Überwachungsmodul generiert aus mindestens einem Teil der über die erste Schnittstelle empfangenen Informationen eine Antwort auf die Anfrage. Diese Informationen und insbesondere beispielsweise ihr Detaillierungsgrad können beispielsweise durch den Inhalt der Anfrage gesteuert werden. Beispielsweise kann mit einer ersten Anfrage eine summarische Information angefordert werden, ob das Computersystem und/oder Steuerungssystem im Ganzen, und/oder in bestimmten Teilaspekten, ordnungsgemäß funktioniert. Wenn sich hierbei abzeichnet, dass nicht alles in Ordnung ist, können mit weiteren Anfragen mehr Details angefordert werden, wie beispielsweise Protokolldateien bestimmter auf dem Computersystem und/oder Steuerungssystem laufender Dienste oder auch Speicherabbilder bestimmter laufender Prozesse.

[0013] Die Beschränkung von Anfragen auf Absender, die im Besitz des gültigen Anfragen-Schlüssels sind, ist insbesondere im Hinblick auf die letztgenannten detaillierten Anfragen wichtig. So kann beispielsweise ein Speicherabbild eines zum Internet hin offenen Serverprozesses, der TLS-Verschlüsselung unterstützt, den privaten Schlüssel enthalten, mit dem dieser Serverprozess sich beim Verbindungsaufbau ausweist. Wer diesen privaten Schlüssel erbeutet, kann eine Fälschung des Serverprozesses aufsetzen, ohne dass anfragende Clients einen Zertifikatfehler melden.

[0014] Die Antwort wird mit einem unter Heranziehung der Anfrage ermittelten Antwort-Schlüssel verschlüsselt und über die zweite Schnittstelle ausgegeben. Es wird ein neuer Anfragen-Schlüssel ermittelt, der ein gemeinsames Geheimnis ist, das auch dem Absender der Anfrage (32) zugänglich ist. Dieser neue Anfragen-Schlüssel wird in dem Speicher abgelegt.

[0015] Darunter, dass der neue Anfragen-Schlüssel ein auch dem Absender der Anfrage zugängliches „gemeinsames Geheimnis“ ist, wird insbesondere verstanden, dass der neue Anfragen-Schlüssel aus Informationen gebildet wird, die sowohl dem Überwachungsmodul als auch dem Absender der Anfrage sowie optional auch weiteren autorisierten Absendern von Anfragen zugänglich sind, jedoch keinem unbefugten Dritten.

[0016] Beispielsweise kann der neue Anfragen-Schlüssel unter Heranziehung einer auf eine vorherige Anfrage gelieferten Antwort ermittelt werden. Da diese Antwort vom Systemzustand des Computersystems und/oder Steuerungssystems abhängt, der sich im normalen Betrieb nicht ändern sollte, kann in die Bildung des Anfragen-Schlüssels noch eine nicht vorhersagbare Zusatzinformation eingebracht werden. Dies kann beispielsweise ein Wert aus einem Zufallsgenerator sein. Der Wert kann sich beispielsweise auch aus veränderlichen Systemzuständen ergeben, wie etwa aus einem Hash über den Stack, IO-Informationen oder Informationen über Schnittstellen des Computersystems und/oder Steuerungssystems.

[0017] Besonders vorteilhaft ist die nicht vorhersagbare Zusatzinformation eine Information, die auch der Absender der Anfrage von sich aus beschaffen kann, die aber gleichwohl keinem unbefugten Dritten zugänglich ist. Dann muss weder diese Zusatzinformation noch der neue Anfragen-Schlüssel vom Überwachungsmodul an den Absender der Anfrage übermittelt werden. Dies erleichtert die Verwaltung der Anfragen-Schlüssel insbesondere in einer Konstellation, in der Anfragen von mehreren Absendern im Wechsel beantwortet werden sollen. Neue Anfragen-Schlüssel müssen dann nicht ständig aktiv an alle potentiell Anfragenden verteilt werden.

[0018] Ist hingegen die nicht vorhersagbare Zusatzinformation beim Absender der Anfrage (bzw. beim weiteren autorisierten potentiellen Absender künftiger Anfragen) nicht verfügbar, kann der neue An-

fragen-Schlüssel beispielsweise mit dem Antwort-Schlüssel verschlüsselt und gemeinsam mit der Antwort übermittelt werden, also beispielsweise in diese Antwort eingepackt werden.

[0019] Alternativ oder auch in Kombination hierzu kann der neue Anfragen-Schlüssel beispielsweise unter Heranziehung der Anfrage ermittelt werden. Dann übernimmt der Absender der Anfrage den aktiveren Part bei der Verwaltung der Anfragen-Schlüssel.

[0020] Beispielsweise kann der Absender der Anfrage auf seiner Seite in beliebiger Weise (etwa mit einem Zufallsgenerator) einen Antwort-Schlüssel erzeugen und im Rahmen der Anfrage verschlüsselt an das Überwachungsmodul schicken. Der Absender kann jedoch auch beispielsweise beliebige andere Informationen an das Überwachungsmodul schicken, die es dem Überwachungsmodul ermöglichen, einen auch auf der Seite des Absenders vorhandenen Antwort-Schlüssel zu errechnen. Unabhängig davon, welcher Weg im Einzelnen gewählt wird, verfügen nach dem erfolgreichen Entschlüsseln der Anfrage durch das Überwachungsmodul sowohl dieses Überwachungsmodul als auch der Absender der Anfrage über den Antwort-Schlüssel als gemeinsames Geheimnis.

[0021] In völlig analoger Weise wird auch der neue Anfragen-Schlüssel ein gemeinsames Geheimnis, das nur der Absender der Anfrage und das Überwachungsmodul kennen.

[0022] Die außerhalb des Überwachungsmoduls auf dem Computersystem und/oder Steuerungssystem laufende Software hat keinen Zugriff auf den Anfragen-Schlüssel oder auf den Antwort-Schlüssel. Sie kann daher keine gefälschten Antworten des Überwachungsmoduls erzeugen, die vom Absender der Anfrage als gültig gewertet werden. Das Wechseln des Antwort-Schlüssels bewirkt darüber hinaus, dass alte, echte Antworten des Überwachungsmoduls, die bei der Übertragung über die zweite Schnittstelle bzw. über ein daran angeschlossenes Netzwerk mitgeschnitten wurden, nicht später wiederverwendet werden können. Eine korrumpierte Software des Computersystems und/oder Steuerungssystems kann also nicht den wahren Systemzustand verschleiern, indem sie gezielt die Übertragung der echten Antwort des Überwachungsmoduls über das Netzwerk unterdrückt und dem Absender der Anfrage stattdessen die zuvor mitgeschnittene alte Antwort schickt.

[0023] Die Verschlüsselung der Kommunikation zwischen dem Absender der Anfrage und dem Überwachungsmodul kann insbesondere beispielsweise eine symmetrische Verschlüsselung sein. Die Verschlüsselung kommt dann mit wesentlich geringeren Hardwareressourcen aus als eine asymmetrische Verschlüsselung benötigen würde. Das Überwachungsmodul ist idealerweise als separates Hardwaremodul ausgebildet mit einem eigenen Prozessor und einem Speicher, auf den die auf dem Computersystem und/oder Steuerungssystem ansonsten laufende Software keinen Zugriff hat. Rechenkapazität in einem solchen Hardwaremodul ist erheblich teurer als „normale“ Rechenkapazität in dem Computersystem und/oder Steuerungssystem.

[0024] In einer besonders vorteilhaften Ausgestaltung ist das Überwachungsmodul zusätzlich dazu ausgebildet, unter Heranziehung des Antwort-Schlüssels einen neuen Anfragen-Schlüssel zu bilden und in dem Speicher abzulegen. Insbesondere kann beispielsweise der Antwort-Schlüssel als Anfragen-Schlüssel für die nächste Anfrage genutzt werden. Ein und derselbe Schlüssel ist dann immer noch genau einmal gültig für die Verschlüsselung einer Anfrage an das Überwachungsmodul und genau einmal gültig für die Verschlüsselung einer Antwort vom Überwachungsmodul. Es ist also in beiden Richtungen der Kommunikation nicht möglich, alte Nachrichten wiederzuverwenden (Replay).

[0025] In einer weiteren besonders vorteilhaften Ausgestaltung wird ein in der Anfrage enthaltener Schlüssel zusätzlich authentifiziert, bevor er für die Bildung des Antwort-Schlüssels herangezogen wird. Hierzu wird ein Komprimat eines in der Anfrage enthaltenen Schlüssels mit einem Vergleichs-Komprimat verglichen, das zuvor im Speicher des Überwachungsmoduls abgelegt wurde.

[0026] Unter einem Komprimat wird jede verdichtete Form von Daten verstanden, die keinen Rückschluss auf die ursprünglichen Daten zulässt. Das Komprimat kann insbesondere dahingehend kryptographisch sicher sein, dass es nicht mit vertretbarem Aufwand möglich ist, zu einem vorgegebenen Komprimat Daten zu finden, die auf genau dieses Komprimat abgebildet werden. Ein Beispiel für ein solches kryptographisch sicheres Komprimat ist ein Hashwert.

[0027] Das Vergleichs-Komprimat kann insbesondere mit der vorherigen Anfrage des Absenders geliefert worden sein. Das heißt, mit jeder Anfrage kann der Absender der Anfrage im Voraus ankündigen, welchen Antwort-Schlüssel er mit der nächsten Anfrage schicken wird, ohne dass dieser Antwort-Schlüssel bis zu dem Zeitpunkt, zu dem diese nächste Anfrage tatsächlich kommt, bereits in dem Überwachungsmodul hinterlegt sein muss. Das „Einklinken“ eines neuen, unautorisierten Anfragenden in die Kommunikation mit dem Überwachungsmodul wird dadurch zusätzlich erschwert.

[0028] Wenn das mit der aktuellen Anfrage gelieferte Komprimat mit dem aktuell im Speicher des Über-

wachungsmoduls hinterlegten Vergleichs-Komprimat übereinstimmt, hat der Absender der Anfrage „Wort gehalten“ und genau denjenigen Schlüssel übermittelt, den er zuvor angekündigt hat. Dieser Schlüssel wird dann für die Bildung des Antwort-Schlüssels herangezogen, beispielsweise, indem er unmittelbar als Antwort-Schlüssel verwendet wird. Weiterhin wird ein in der Anfrage enthaltenes neues Komprimat, mit dem der bei der nächsten Anfrage übermittelte Schlüssel angekündigt wird, als neues Vergleichs-Komprimat im Speicher des Überwachungsmoduls abgelegt.

[0029] Weiterhin kann das Überwachungsmodul zusätzlich unter Heranziehung des neuen Komprimats einen neuen Anfragen-Schlüssel für die nächste Anfrage ermitteln und in dem Speicher ablegen. Insbesondere kann beispielsweise das neue Komprimat selbst als neuer Anfragen-Schlüssel genutzt werden und muss dann nur einmal im Speicher des Überwachungsmoduls hinterlegt sein. Der Absender von Anfragen muss also pro Abfrage nur einen einzigen neuen Schlüssel generieren, den er als Antwort-Schlüssel für die nächste Anfrage ankündigt, und das Komprimat dieses neuen Schlüssels sichert dann auch gleich die Übertragung der nächsten Anfrage ab. Dies bringt einen Geschwindigkeitsvorteil, denn die Erzeugung neuer, nicht vorhersehbarer Schlüssel ist je nach Qualität eines für die Erzeugung von Zufallszahlen verwendeten Pseudozufallszahlengenerators und je nach Komplexität des nachgeschalteten Algorithmus für die Weiterverarbeitung dieser Zufallszahlen zu einem Schlüssel zeitaufwändig. Dies gilt insbesondere, wenn von einer zentralen Stelle aus eine Vielzahl von Computersystemen und/oder Steuerungssystemen überwacht wird und für jede Anfrage in jeder dieser Kommunikationsbeziehungen immer wieder neue Schlüssel erzeugt werden müssen.

[0030] Die Informationen, die den Zustand des Computersystems und/oder Steuerungssystem charakterisieren und auf deren Basis das Überwachungsmodul die Antwort auf die Anfrage generiert, können insbesondere beispielsweise solche Informationen beinhalten, die sich im normalen Betrieb des Computersystems und/oder Steuerungssystems nicht oder nur in vorhersehbarer Weise ändern. Aus Änderungen dieser Informationen, die sich nicht mehr im Rahmen des Erwarteten bewegen, kann dann geschlossen werden, dass sich das Computersystem und/oder Steuerungssystem in einem anormalen oder gar manipulierten Zustand befindet.

[0031] Ein Beispiel hierfür ist von mindestens einem Prozessor des Computersystems und/oder Steuerungssystems ausführbarer Programmcode. Die Software des Computersystems und/oder Steuerungssystems sollte sich im normalen Betrieb nicht ändern, es sei denn, es wird gerade ein Update oder ein Patch eingespielt. Veränderungen der Software, die sich hierdurch nicht erklären lassen, sind mit hoher Wahrscheinlichkeit böswillig eingebracht worden. Die Software kann auf dem Massenspeicher (etwa Festplatte, SSD, Flash-Speicher oder SD-Karte) untersucht werden, von dem das Computersystem und/oder Steuerungssystem sie beim Booten lädt. Die Software kann aber auch beispielsweise im Arbeitsspeicher (RAM) des Computersystems und/oder Steuerungssystems untersucht werden. Letzteres ermöglicht es insbesondere, Manipulationen zu erkennen, bei denen Schadcode in den Arbeitsspeicher eingeschleust und der Kontrollfluss der Software auf diesen Schadcode umgebogen wurde.

[0032] Die letztgenannten Manipulationen lassen sich alternativ oder in Kombination hierzu auch aufspüren, indem die Größe und/oder der Inhalt nominell ungenutzter Speicherbereiche des Steuerungssystems und/oder Computersystems untersucht werden. Vielfach wird Schadcode gerade in solche Bereiche geladen (etwa durch „Heap spraying“) und dann versucht, einen oder mehrere Zeiger im Kontrollfluss der Software (etwa Rücksprungadressen auf einem Stack) so zu ändern, dass sie in den mit dem Schadcode belegten Speicherbereich zeigen. Weiterhin können durch die Untersuchung nominell ungenutzter Speicherbereiche insbesondere auch Versuche erkannt werden, „Use after free“-Lücken auszunutzen, bei denen die Software einen Speicherbereich zwar freimeldet, aber danach immer noch fälschlicherweise darauf zugreift.

[0033] Gerade IoT-Geräte und andere Systeme werden häufig lange in einem stationären Zustand betrieben, in dem eine gleichbleibende Konstellation von Anwendungen läuft und sich der Inhalt zumindest großer Teile des Arbeitsspeichers nicht ändern sollte. Im Extremfall sollte sich am Inhalt des Arbeitsspeichers gar nichts ändern mit Ausnahme derjenigen Bereiche, in denen die aktuell laufenden Anwendungen ihre aktuellen Eingaben und Verarbeitungsergebnisse dieser Eingaben abspeichern. Bei allen nicht durch den laufenden Betrieb erklärbaren Veränderungen des Speicherinhalts liegt der Verdacht nahe, dass ein Angreifer eine der Anwendungen für seine Zwecke umfunktioniert hat.

[0034] Die Überwachung des Arbeitsspeichers ist insbesondere vorteilhaft im Zusammenhang mit einem Überwachungsmodul, dessen erste Schnittstelle hardwaremäßig direkt auf diesen Arbeitsspeicher zugreifen kann. Der Arbeitsspeicher kann dann an der auf dem Computersystem und/oder Steuerungssystem laufenden Software vorbei ausgelesen werden. Diese Software bekommt von der Überwachung also nichts mit. Somit kann eine bösartige Software keine Gegenmaßnahmen ergreifen, um ihre Entdeckung zu erschweren, wie etwa das Vorgaukeln des Originalzustandes immer an der Stelle, an der der Speicherinhalt gerade geprüft wird. Weiterhin erschwert

es eine solche minimale Schnittstelle, das Überwachungsmodul und die auf ihm implementierte Software anzugreifen. Das Überwachungsmodul muss den Speicherinhalt nur mit einem Originalzustand vergleichen, was beispielsweise durch Abgleich eines Hashwerts über diesen Speicherinhalt mit einer Referenz geschehen kann. Eine tiefergehende Interpretation dieser Daten, die einen Angriff durch das gezielte Vorlegen ungültig formatierter oder in sonstiger Weise unerwarteter Daten begünstigt, entfällt.

[0035] Die Software des Computersystems und/oder Steuerungssystems kann beispielsweise auch Konfigurationsdaten für mindestens ein feldprogrammierbares Gatterarray, FPGAs, oder mindestens einen anderen programmierbaren Logikbaustein des Computersystems und/oder Steuerungssystems, beinhalten. Beispielsweise kann im Rahmen der Initialisierung der Software vorgesehen sein, dass diese Konfigurationsdaten auf den entsprechenden Logikbaustein geladen werden und der Logikbaustein dann dazu veranlasst wird, entsprechend dieser Konfigurationsdaten zu arbeiten.

[0036] Ein weiteres Beispiel bilden fest hinterlegte und/oder nur von extern änderbare Parameter, die die Arbeit des Computersystems und/oder Steuerungssystems beeinflussen. Diese Parameter sollten sich im normalen Betrieb ebenfalls nicht ändern. Eine Änderung von extern kann beispielsweise über das Überwachungsmodul angestoßen werden, etwa mit der einer Anfrage, mit der auch der Systemzustand abgefragt wird. Das Überwachungsmodul kann die Änderungen an das Computersystem und/oder Steuerungssystem weitergeben und anschließend den solchermaßen autorisiert veränderten Systemzustand zurückgeben. Diesen Systemzustand kann der Absender der Anfrage dann für die weitere Überwachung als Referenz speichern. An dieser Referenz können spätere Veränderungen gemessen werden. Alternativ können die Parameter auch über eine beliebige Schnittstelle des Computersystems und/oder Steuerungssystems geändert werden, und der auf die nächste Anfrage hin gelieferte, wiederum autorisiert veränderte Systemzustand kann dann für die weitere Überwachung als Referenz gespeichert werden.

[0037] In einer weiteren vorteilhaften Ausgestaltung ist das Überwachungsmodul zusätzlich dazu ausgebildet, nach einer vorgegebenen Metrik ein Maß für eine Veränderung von zur Bildung der Antwort herangezogenen Informationen innerhalb eines vorgegebenen Zeitraums zu ermitteln. Dann kann das Überwachungsmodul die an den Absender der Anfrage gelieferten Informationen bereits dahingehend aufbereiten, dass Veränderungen, für die es eine plausible Erklärung gibt, nicht als verdächtig gewertet werden. So ist es beispielsweise bei Computersystemen, die Anfragen aus dem Internet entgegennehmen, üblich, dass die Last an Anfragen tageszeitlich schwankt. Diese Schwankungen sind kein Anzeichen für einen Angriff. Ein plötzlicher Sprung auf eine dann anhaltende Vollauslastung der CPU kann hingegen darauf hindeuten, dass die CPU für das Schürfen von Kryptowährung eingesetzt wird. Ein plötzlicher Sprung der Eingabe-Ausgabe-Auslastung auf anhaltende Vollauslastung kann beispielsweise darauf hindeuten, dass versucht wird, die Datenbestände zu verschlüsseln. Dementsprechend kann das Überwachungsmodul auch dazu ausgebildet sein, in Antwort darauf, dass die festgestellte Veränderung ein vorgegebenes Kriterium erfüllt, mindestens eine Gegenmaßnahme gegen einen Angriff auf das Computersystem und/oder Steuerungssystem, und/oder gegen eine Fehlfunktion des Computersystems und/oder Steuerungssystems, zu veranlassen.

[0038] Für die Entscheidung über Gegenmaßnahmen ist das Überwachungsmodul aber nicht auf sich selbst gestellt. In einer weiteren vorteilhaften Ausgestaltung ist das Überwachungsmodul zusätzlich dazu ausgebildet, in Antwort darauf, dass es über die zweite Schnittstelle einen mit dem in dem Speicher abgelegten Anfragen-Schlüssel verschlüsselten Steuerbefehl empfangen hat, mindestens eine Gegenmaßnahme gegen einen Angriff auf das Computersystem und/oder Steuerungssystem, und/oder gegen eine Fehlfunktion des Computersystems und/oder Steuerungssystem, zu veranlassen. Das Überwachungsmodul hat dann den direkten Durchgriff auf das Computersystem und/oder Steuerungssystem, um die Maßnahme durchzuführen. Hingegen trifft der Absender der Anfrage, also der Kommunikationspartner des Überwachungsmoduls, die Entscheidung über die Einleitung von Maßnahmen. Der Absender kann beispielsweise die Information über den Systemzustand, die er mit der Antwort vom Überwachungsmodul geliefert bekommen hat, mit beliebigen anderen Informationsquellen abgleichen, um zu prüfen, ob die Information auf einen Angriff hindeutet.

[0039] Sollte das Überwachungsmodul gar nicht mehr auf Anfragen antworten, kann dies beispielsweise darauf hindeuten, dass es von einem Angreifer gekapert oder aber funktionsunfähig gemacht wurde. Es ist dann davon auszugehen, dass der Angreifer die bisher verwendeten Anfragen-Schlüssel und Antwort-Schlüssel kennt. Auch dies kann den Anlass bilden, eine oder mehrere Gegenmaßnahmen zu veranlassen, bis hin zur Trennung des Computersystems und/oder Steuerungssystems vom Netzwerk oder von der Stromversorgung, um zu verhindern, dass weiterer Schaden angerichtet wird. Es können auch beispielsweise Systeme, die mit dem betroffenen System zusammenarbeiten, benachrichtigt werden, damit sie diese Zusammenarbeit einstellen. Dadurch kann beispielsweise ein schrittweises Unterwandern eines ganzen Netzwerks oder gar eine wur-

martige Ausbreitung von Schadcode von einem System zum anderen erschwert werden.

[0040] Als Gegenmaßnahme kann beispielsweise ein Alarm ausgegeben werden, der einen Techniker dazu veranlasst, der Ursache des beobachteten abweichenden Zustands bzw. Verhaltens auf den Grund zu gehen. Sofern das Überwachungsmodul noch erreichbar und nicht gekapert ist, kann das Computersystem bzw. Steuerungssystem dazu veranlasst werden, Betriebsdaten, Protokolldaten und/oder Diagnoseinformationen auszugeben. Es kann auch ein Selbsttest des Computersystems bzw. Steuerungssystems veranlasst werden.

[0041] Das Computersystem bzw. Steuerungssystem kann abgeschaltet, neugestartet oder auf Werkseinstellungen zurückgesetzt werden. Es kann ein Software-Update und/oder ein Patch auf das Computersystem bzw. Steuerungssystem eingespielt werden. Hierbei kann ein Software-Update beispielsweise eine aktualisierte Version der Software umfassen, die unter anderem bestimmte bekannte Fehler behebt, während ein Patch der Software keine neue Funktionalität hinzufügen, sondern ausschließlich Fehler beheben soll.

[0042] Es kann auch die Wertigkeit des Computersystems und/oder Steuerungssystems in einem dezentralen Peer-to-Peer-Netzwerk reduziert werden. Auf diese Weise kann zumindest eine Basisfunktionalität des Computersystems und/oder Steuerungssystems weiter genutzt werden, während schädliche Auswirkungen innerhalb des Peer-to-Peer-Netzwerks minimiert werden können. Das Computersystem bzw. Steuerungssystem kann auch in einen Notbetrieb versetzt werden.

[0043] Zur Schadensbegrenzung kann das Computersystem bzw. Steuerungssystem auch veranlasst werden, wichtige Daten durch Versenden über eine Kommunikationsschnittstelle vor dem Verlust zu schützen und/oder vertrauliche Daten durch Löschen vor der Preisgabe zu schützen.

[0044] Es kann auch eine logistische Maßnahme veranlasst werden, wie etwa ein Service-Einsatz und/oder ein Geräteaustausch am Ort des Computersystems und/oder Steuerungssystems.

[0045] Das Überwachungsmodul kann weiterhin dazu ausgebildet sein, in Antwort darauf, dass es über die zweite Schnittstelle ein mit dem in dem Speicher abgelegten Anfragen-Schlüssel verschlüsseltes Update empfangen hat, das Einspielen des Updates auf das Computersystem bzw. Steuerungssystem zu veranlassen. Auf diese Weise kann sichergestellt werden, dass Updates nur aus einer vertrauenswürdigen Quelle bezogen werden, die sich durch den Besitz des aktuellen Anfragen-Schlüssels ausgewiesen hat.

[0046] Wenn das Überwachungsmodul den Systemzustand an den Absender der Anfrage berichtet, kann dies in beliebiger Form erfolgen. Wie zuvor erwähnt, können die Informationen, die den Systemzustand charakterisieren, in verschiedenen Detaillierungsgraden bis hin zu Speicherabbildern geliefert werden. Für die summarische Überwachung, ob sich überhaupt etwas geändert hat, genügen Informationen mit einem deutlich geringeren Volumen. Gerade IoT-Geräte sind häufig über Mobilfunk oder über Funkfrequenzen mit begrenztem Sendezeitanteil (Duty Cycle) angebunden, so dass innerhalb einer bestimmten Zeiteinheit nur ein begrenztes Datenvolumen übertragen werden kann. Wenn die Routine-Überwachung auf ein kleines Datenvolumen reduziert werden kann, kann mehr Datenvolumen auf die detaillierte Untersuchung verdächtiger Zustände oder Aktivitäten verwendet werden.

[0047] Daher beinhaltet in einer weiteren vorteilhaften Ausgestaltung die vom Überwachungsmodul generierte Antwort

- einen Hashwert von zur Bildung der Antwort herangezogenen Informationen, und/oder
- ein nach einer vorgegebenen Metrik ermitteltes Maß für eine Veränderung dieser Informationen innerhalb eines vorgegebenen Zeitraums.

[0048] In einer weiteren besonders vorteilhaften Ausgestaltung umfasst das System weiterhin mindestens ein Sicherheitsmodul, über das die Kommunikation von und zu mindestens einer Schnittstelle des Computersystems und/oder Steuerungssystems geführt ist. Dieses Sicherheitsmodul ist dazu ausgebildet, die Weiterleitung von Daten von und zu dieser Schnittstelle vom Ergebnis einer Überprüfung

- des Absenders der Daten, und/oder
- des Empfängers der Daten, und/oder
- der Form und/oder des Inhalts der Daten,

abhängig zu machen.

[0049] Auf diese Weise lässt sich die Sicherheitsentwicklung des Computersystems und/oder Steuerungssystems besonders gut von der Anwendungsentwicklung entkoppeln.

[0050] Wie zuvor erläutert, werden die meisten Angriffe mit speziell präparierten ungültigen Eingaben über Schnittstellen geführt, mit denen der Angreifer der Software seinen Willen aufzwingen möchte, sobald die Software diese Eingaben verarbeitet. Wenn die Software gegen Angriffe dieser Art gehärtet werden soll, ist viel zusätzlicher Code für die Prüfung erforderlich, ob die Eingaben den Spezifikationen ent-

sprechen. Wenn das verwendete Datenformat beispielsweise eine Angabe der Größe zu übermittelnder Bilddaten in Bytes gefolgt von den Bilddaten selbst beinhaltet, muss geprüft werden, ob auf die Größenangabe wirklich nur die angekündigte Menge an Bytes folgt oder ob mehr Bytes folgen mit dem Ziel, einen Pufferüberlauf zu provozieren. Wenn Eingaben in Textform verarbeitet werden, muss geprüft werden, ob darin Sonderzeichen enthalten sind, mit denen die weitere Verarbeitung in eine ganz andere als die ursprünglich vorgesehene Richtung gelenkt werden kann (wie etwa bei SQL-Injection). Die Software ist also ein Gemisch aus Code, der die eigentliche Funktionalität des Computersystems und/oder Steuerungssystems beinhaltet, und Code für die Überprüfung der Eingaben auf mögliche Angriffe. Dies erschwert die Entwicklung der Software und erhöht das Risiko, dass die letztendlich ausgelieferte Version der Software doch noch Sicherheitslücken aufweist. Wird beispielsweise eine ordnungsgemäß gegen ungültige Eingaben gesicherte Routine aus der Software entfernt, um sie durch eine neue Version zu ersetzen, kann schnell vergessen werden, alle zuvor vorhandenen Prüfungen auf ungültige Eingaben auch in der neuen Version umzusetzen.

[0051] Das Sicherheitsmodul ermöglicht es, einen großen Teil derartiger Überprüfungen vorgelagert durchzuführen, bevor die eigentliche Software des Computersystems und/oder Steuerungssystems die Eingaben zu Gesicht bekommt. Die Entwicklung dieser Software kann dann im Wesentlichen darauf fokussiert sein, dass das Computersystem bzw. Steuerungssystem das tut, was es bei gültigen Eingaben soll. Es drängt sich nicht mehr die Frage in den Vordergrund, ob die Software in böswilliger Absicht dazu überredet werden kann, etwas zu tun, was sie nicht tun soll.

[0052] Zugleich ermöglicht es das Überwachungsmodul, nicht nur die Funktionalität der Software zu überwachen, sondern auch auf sicherem Wege Updates hierfür einzuspielen.

[0053] In einer besonders vorteilhaften Ausgestaltung ist das Sicherheitsmodul dazu ausgebildet, die Weiterleitung von Daten davon abhängig zu machen, dass in Ansehung eines vorgegebenen Satzes von Regeln

- eine Beziehung zwischen dem Sender der Daten und dem Empfänger der Daten plausibel ist, und/oder
- die Daten für ihren Empfänger voraussichtlich verarbeitbar sind.

[0054] So sind beispielsweise Kameras und andere Sensoren Quellen für physikalische Messdaten, während ein für die Auswertung dieser Daten vorgesehenes Computersystem eine Senke für diese physikalischen Messdaten ist. Es ist dann plausibel, dass die Sensoren große Mengen an Messdaten an das Computersystem für die Auswertung weitergeben. Hingegen ist es nicht plausibel, dass in größerem Umfang Daten in umgekehrter Richtung von dem Computersystem für die Auswertung an die Sensoren oder von einem Sensor zum anderen fließen sollen. Stattdessen kann beispielsweise Datenverkehr von einem Sensor zum anderen auf einen Versuch zurückgehen, ausgehend von dem einen Sensor einen Schadcode wurmartig zu anderen Sensoren zu verbreiten. Datenverkehr zwischen dem Internet und einem Sensor kann darauf hindeuten, dass ein Angreifer die Kontrolle über den Sensor übernommen hat und der Sensor jetzt gar nicht mehr seine ursprüngliche Aufgabe erfüllt, sondern etwas völlig anderes tut.

[0055] Die Prüfung, ob die Daten für den Empfänger voraussichtlich verarbeitbar sind, kann beispielsweise anhand eines von dem Empfänger erwarteten Datenformats, und/oder anhand eines vom Empfänger erwarteten Wertebereichs der Daten, erfolgen. Auf diese Weise kann beispielsweise ein Versuch erkannt werden, durch einen gezielten Verstoß gegen die Vorgaben eines Dateiformats oder einer anderen Vorgabe (etwa die bereits erwähnte Ankündigung einer ersten Anzahl Bytes und Lieferung einer größeren Menge Bytes, Uhrzeiten mit Stundenzahlen jenseits der 24 und Minutenzahlen jenseits der 60, negative Werte für eine Lichtintensität) den Kontrollfluss der Software des Empfängers in eine nie von ihrem Entwickler beabsichtigte Richtung zu lenken.

[0056] In einer weiteren besonders vorteilhaften Ausgestaltung ist das Sicherheitsmodul dazu ausgebildet, die Weiterleitung von Daten davon abhängig zu machen, dass der Absender die Daten mit einem vorgegebenen Schlüssel verschlüsselt und/oder signiert hat. Auf diese Weise können beispielsweise Versuche unterbunden werden, sich in einem Netzwerk, über das der Absender und der Empfänger der Daten miteinander kommunizieren, als der Absender auszugeben. Wenn die Daten nicht oder nicht mit dem richtigen Schlüssel verschlüsselt wurden, schlägt die Entschlüsselung fehl, und das Sicherheitsmodul kann die Daten gar nicht weiter analysieren.

[0057] Unautorisierte Daten bereits in diesem Stadium abzufangen ist deutlich einfacher und daher sicherer als eine Konformität mit einem Datenformat zu prüfen. Die Prüfung von Formaten ist eine vergleichsweise breite, fehlerträchtige Schnittstelle, die ihrerseits mit großer Sorgfalt zu implementieren ist, damit sie nicht durch bewusst ungültig formatierte Daten ihrerseits unterwandert werden kann.

[0058] Das Sicherheitsmodul kann insbesondere dazu ausgebildet sein, zur Weiterleitung an die Schnittstelle des Computersystems und/oder Steue-

rungssystems eingehende verschlüsselte Daten zu entschlüsseln sowie von dieser Schnittstelle eingehende unverschlüsselte Daten zu verschlüsseln.

[0059] In einer weiteren vorteilhaften Ausgestaltung ist das Sicherheitsmodul dazu ausgebildet, einen Schlüssel für die Verschlüsselung, und/oder für die Entschlüsselung, unter Heranziehung mindestens eines vom Überwachungsmodul bezogenen Schlüssels und/oder Hashwerts zu ermitteln. Beispielsweise kann ein Schlüssel, der aktuell für die Verschlüsselung einer Anfrage nach dem Systemzustand gültig ist, auch für den Versand von für die Schnittstelle des Computersystems und/oder Steuerungssystems bestimmten Daten gültig sein. Es ist dann wie bei den Anfragen nach dem Systemzustand für einen ständigen Wechsel der Schlüssel gesorgt, die eine Wiederverwendung alter Daten (Replay) verhindert.

[0060] In einer weiteren besonders vorteilhaften Ausgestaltung ist das Sicherheitsmodul zusätzlich dazu ausgebildet, unter Heranziehung gültiger Eingangsdaten, die es für die Weiterleitung zu der Schnittstelle des Computersystems und/oder Steuerungssystems empfangen hat, mindestens einen Eingangsdaten-Hashwert zu ermitteln und diesen Eingangsdaten-Hashwert zur Bildung mindestens eines Schlüssels heranzuziehen. Dann können beispielsweise die Eingangsdaten selbst genutzt werden, um Schlüssel für die über das Sicherheitsmodul vermittelte Kommunikation mit Schnittstellen des Computersystems und/oder Steuerungssystems, und/oder Schlüssel für die Kommunikation mit dem Überwachungsmodul, zu wechseln. Auf diesem Wege sind neue Schlüssel schneller erhältlich als durch Verwendung eines Pseudozufallszahlengenerators. Sofern die Eingangsdaten nicht vorhersehbar sind, sind sie ein gemeinsames Geheimnis zwischen ihrem Absender und dem Sicherheitsmodul.

[0061] In einer weiteren besonders vorteilhaften Ausgestaltung beinhaltet die vom Überwachungsmodul generierte Antwort auch den Eingangsdaten-Hashwert. Auf diese Weise lässt sich zusätzlich kontrollieren, ob Eingangsdaten ordnungsgemäß beim Sicherheitsmodul ankommen und vom Sicherheitsmodul als gültig erkannt werden. Damit lassen sich Versuche erkennen, das Computersystem und/oder Steuerungssystem in seiner Funktion zu beeinflussen, indem gültige Eingangsdaten beispielsweise bei der Übertragung über ein Netzwerk verfälscht oder unterdrückt werden.

[0062] Das Sicherheitsmodul kann weiterhin dazu ausgebildet sein, bei einer Aktualisierung des Eingangsdaten-Hashwerts neben aktuellen Eingangsdaten auch den bisherigen Eingangsdaten-Hashwert für das Ermitteln des neuen Eingangsdaten-Hashwerts heranzuziehen. Dies schafft im Hinblick auf die kryptographische Sicherheit von aus Eingangsdaten erzeugten Schlüsseln einen Ausgleich dafür, dass die Eingangsdaten nur bedingt zufällig sind. So lassen sich beispielsweise Bilddaten, die eine Kamera liefert, in gewissen Grenzen auf Grund eigener Beobachtungen der gleichen Szenerie vorhersagen. Indem nun auch der bisherige Eingangsdaten-Hashwert verwendet wird, ist die komplette Historie der Eingangsdaten für die generierten Schlüssel relevant.

[0063] In einer weiteren besonders vorteilhaften Ausgestaltung ist das Überwachungsmodul, bzw. das Sicherheitsmodul, dazu ausgebildet, in Antwort darauf, dass es für eine vorbestimmte Zeitdauer keine mit einem aktuell gültigen Schlüssel authentifizierten Anfragen, Befehle bzw. Daten erhalten hat, auch mit früher gültigen Schlüsseln authentifizierte Anfragen, Befehle bzw. Daten zu akzeptieren. Der beschriebene Wechsel von Schlüsseln macht es erforderlich, dass das Überwachungsmodul, bzw. das Sicherheitsmodul, und der jeweilige Kommunikationspartner sich ständig gegenseitig auf dem neuesten Stand halten, was den jeweils nächsten gültigen Schlüssel angeht. Es kann Situationen geben, in denen eine derartige Information nicht beim Empfänger ankommt. Beispielsweise kann die Information bei der Übertragung über ein Netzwerk verlorengehen, oder der Kommunikationspartner kann den Schlüssel verlieren, etwa bei komplett entladenem Akku. In diesem Fall kann durch den Rückgriff auf früher gültige Schlüssel die Kommunikation ohne manuellen Eingriff wieder hergestellt werden.

[0064] Die Erfindung bezieht sich auch auf ein Datenverarbeitungsmodul, Datenspeichermodul, Kameramodul, Sensormodul und/oder Aktormodul. Dieses Modul weist das zuvor beschriebene System auf, und/oder es weist einen FPGA-Baustein auf, der schaltungstechnisch so in das Modul integriert ist, dass er sich durch Programmierung zu dem zuvor beschriebenen System, und/oder zu einem Überwachungsmodul und/oder Sicherheitsmodul dieses Systems, herrichten lässt. Wie zuvor erläutert, kann dann die Sicherheitsentwicklung des Datenverarbeitungsmoduls, Datenspeichermoduls, Kameramoduls, Sensormoduls und/oder Aktormoduls von der jeweiligen Anwendungsentwicklung entkoppelt werden. Dementsprechend werden Entwicklungszyklen verkürzt. Insbesondere können die Sicherheitsfunktionen, nachdem sie einmal in Form eines Überwachungsmoduls bzw. Sicherheitsmoduls implementiert wurden, für verschiedene Anwendungen ohne oder mit nur geringen spezifischen Anpassungen wiederverwendet werden.

[0065] Die Funktionalität des Überwachungsmoduls, und/oder des Sicherheitsmoduls, kann ganz oder teilweise in Software realisiert sein. Daher bezieht sich die Erfindung auch auf ein Computerprogramm mit maschinenlesbaren Anweisungen, die, wenn sie auf

einer Hardwareplattform ausgeführt werden und/oder als Konfiguration in diese Hardwareplattform eingebracht werden, die Hardwareplattform zu dem zuvor beschriebenen System, und/oder zu einem Überwachungsmodul und/oder Sicherheitsmodul dieses Systems, herrichten.

[0066] Ebenso bezieht sich die Erfindung auch auf einen maschinenlesbaren Datenträger, und/oder ein Downloadprodukt, mit dem Computerprogramm.

Figurenliste

[0067] Nachfolgend wird der Gegenstand der Erfindung anhand von Figuren erläutert, ohne dass der Gegenstand der Erfindung hierdurch beschränkt wird. Es ist gezeigt:

Fig. 1: Zusammenwirken des Systems **1** mit einem beispielhaften Computersystem und/oder Steuerungssystem **2**;

Fig. 2: Beispielhafter Ablauf innerhalb des Überwachungsmoduls **11** des Systems **1**;

Fig. 3: Beispielhafter Ablauf innerhalb des Sicherheitsmoduls **12** des Systems **1**.

[0068] **Fig. 1** zeigt beispielhaft das Zusammenwirken eines Ausführungsbeispiels des Systems **1** mit einem beispielhaften Computersystem und/oder Steuerungssystem **2**. Das stark vereinfacht dargestellte Computersystem und/oder Steuerungssystem **2** umfasst einen Speicher **21**, eine CPU **22** sowie eine Schnittstelle **23** zur Kommunikation mit der Außenwelt. Der Speicher **21**, die CPU **22** und die Schnittstelle **23** sind untereinander über ein Bussystem **24** verbunden.

[0069] Das System **1** zur Absicherung des Computersystems und/oder Steuerungssystems **2** umfasst in dem in **Fig. 1** gezeigten Beispiel ein Überwachungsmodul **11** und ein Sicherheitsmodul **12**. Das Überwachungsmodul **11** liest Informationen **31** über den Systemzustand des Computersystems und/oder Steuerungssystems **2** aus. In **Fig. 1** sind beispielhaft ein Abgriff aus dem Bussystem **24** und ein Abgriff aus dem Speicher **21** als Datenquellen eingezeichnet. Es sind jedoch alternativ oder auch in Kombination hierzu beliebige weitere Datenquellen verwendbar, wie beispielsweise Sensoren beliebiger Art. So kann etwa die Systemauslastung über die Temperatur oder die Lüfterdrehzahl der CPU **22** ermittelt werden.

[0070] Das Überwachungsmodul **11** ermittelt auf eine Anfrage **32** hin aus den Informationen **31** eine Antwort **33** und beantwortet damit die Anfrage **32**. Mit dieser Antwort **33** kann eine in **Fig. 1** nicht eingezeichnete externe Entität, wie beispielsweise ein Operator, prüfen, ob in Bezug auf das Computersystem und/oder Steuerungssystem **2** Handlungsbedarf besteht. Wenn Handlungsbedarf besteht, kann diese externe Entität einen Befehl **35** an das Überwachungsmodul **11** schicken, der das Überwachungsmodul **11** dazu veranlasst, eine Gegenmaßnahme **34** auf das Computersystem und/oder Steuerungssystem **2** auszuüben. Ein beispielhafter Ablauf innerhalb des Überwachungsmoduls **11** ist in **Fig. 2** näher erläutert.

[0071] Auf dem gleichen Weg kann auch ein Update oder Patch **36** zum Einspielen auf das Computersystem und/oder Steuerungssystem **2** zugeführt werden.

[0072] Das Sicherheitsmodul **12** prüft eingehende Daten **23a**, die für die Schnittstelle **23** bestimmt sind, sowie von der Schnittstelle **23** ausgehende Daten **23b** vor der Weiterleitung an die Schnittstelle **23**, bzw. an die Außenwelt. Geprüft werden können neben den Daten **23a**, **23b** selbst auch der Absender **23a***, **23b***, und/oder der Empfänger **23a#**, **23b#**, der Daten **23a**, **23b**. Ein beispielhafter Ablauf innerhalb des Sicherheitsmoduls **12** ist in **Fig. 3** näher erläutert.

[0073] **Fig. 2** zeigt einen beispielhaften Ablauf innerhalb eines Ausführungsbeispiels des Überwachungsmoduls **11**. Das Überwachungsmodul **11** hat eine erste Schnittstelle **11a**, die mit dem Computersystem und/oder Steuerungssystem **2** verbindbar ist, eine zweite Schnittstelle **11b** für die Kommunikation mit der Außenwelt sowie einen Speicher **11c**.

[0074] Das Überwachungsmodul **11** nimmt über die zweite Schnittstelle **1** 1b eine Anfrage nach dem Systemzustand des Computersystems und/oder Steuerungssystems **2** entgegen. Diese Anfrage wird mit einem aus dem Speicher **11c** bezogenen Anfragen-Schlüssel **41** entschlüsselt. Dabei kommt neben der eigentlichen Anfrage **32** auch ein Antwort-Schlüssel **42** zum Vorschein. Das Überwachungsmodul **11** ruft über seine erste Schnittstelle **11a** Informationen **31** zum Systemzustand aus dem Computersystem und/oder Steuerungssystem **2** ab und generiert hieraus eine Antwort **33** auf die Anfrage **32**, die mit dem Antwort-Schlüssel **42** verschlüsselt über die zweite Schnittstelle **11b** ausgegeben wird. Aus der Anfrage **32**, hier aus dem Antwort-Schlüssel **42**, wird weiterhin ein neuer Anfragen-Schlüssel **41*** ermittelt und in dem Speicher **11c** abgelegt. Auf diese Weise ist ein stetiger Wechsel der verwendeten Schlüssel gewährleistet, und eine Wiederverwendung alter Nachrichten (Replay) wird verhindert.

[0075] Wie bereits im Zusammenhang mit **Fig. 1** erläutert, kann mit einem über die zweite Schnittstelle **11b** eingehenden Befehl **35** die Ausübung einer Gegenmaßnahme **34** gegen einen abnormalen Zustand, und/oder eine abnormale Aktivität, des Computersystems und/oder Steuerungssystems **2** ausgeübt werden. Ebenso kann auf diesem Wege ein Update oder Patch **36** auf das Computersystem und/oder Steuerungssystem **2** aufgespielt werden.

[0076] Fig. 3 zeigt einen beispielhaften Ablauf innerhalb eines Ausführungsbeispiels des Sicherheitsmoduls **12**. Ob Daten **23a**, **23b** von ihrem jeweiligen Absender **23a***, **23b*** an ihren jeweiligen Empfänger **23a#**, **23b#** weitergeleitet werden, hängt von Regeln **12a** ab. Bevor diese Regeln geprüft werden, kann insbesondere beispielsweise anhand einer Signatur **S** der Daten **23a**, **23b** der jeweilige Absender **23a***, **23b*** authentifiziert werden. Auf diese Weise können Versuche unterbunden werden, durch Vorspiegeln eines falschen Absenders (Spoofing) den falschen Anschein zu erwecken, dass Daten den Regeln **12a** entsprechen.

[0077] Ein erster Anteil **12a1** dieser Regeln **12a** knüpft die Weiterleitung der Daten **23a**, **23b** an Bedingungen hinsichtlich der Beziehungen zwischen den jeweiligen Absendern **23a***, **23b*** und Empfängern **23a#**, **23b#** der Daten **23a**, **23b**. Auf diese Weise kann etwa die wurmartige Ausbreitung eines Schadcodes in einem Netzwerk von IoT-Geräten, die eigentlich nur mit einem zentralen Server und nicht unmittelbar untereinander kommunizieren sollen, unterbunden werden.

[0078] Ein zweiter Anteil **12a2** der Regeln **12a** knüpft die Weiterleitung der Daten **23a**, **23b** an die Bedingung, dass die Daten **23a**, **23b** voraussichtlich für ihren jeweiligen Empfänger **23a#**, **23b#** verarbeitbar sind. Hiermit können beispielsweise Angriffe mit ungültigen Daten **23a**, **23b**, die den Kontrollfluss der Software des jeweiligen Empfängers **23a#**, **23b#** in eine unvorhergesehene neue Richtung lenken sollen, unterbunden werden.

Bezugszeichenliste

1	System zur Absicherung
11	Überwachungsmodul des Systems 1
11a, 11b	Schnittstellen des Überwachungsmoduls 11
11c	Speicher des Überwachungsmoduls 11
12	Sicherheitsmodul des Systems 1
12a	Regeln für Datenverkehr in Sicherheitsmodul 12
12a1	Regeln zu Absender-Empfänger-Beziehungen für Daten **23a**, 23b
12a2	Regeln zu Verarbeitbarkeit der Daten **23a**, 23b
2	Computersystem und/oder Steuerungssystem
21	Speicher des Computersystems und/oder Steuerungssystems 2
22	Prozessor (CPU) des Computersystems und/oder Steuerungssystems 2
23	Schnittstelle des Computersystems und/oder Steuerungssystems 2
23a	für Schnittstelle **23** bestimmte eingehende Daten
23a*	Absender der Daten **23a**
23a#	Empfänger der Daten 23a
23b	aus Schnittstelle **23** ausgehende Daten
23b*	Absender der Daten 23b
23b#	Empfänger der Daten 23b
24	Bussystem des Computersystems und/oder Steuerungssystems 2
31	Zustand des Computersystems und/oder Steuerungssystems 2
32	Anfrage nach Zustand 31
33	Antwort auf Anfrage 32
34	Gegenmaßnahme gegen abnormalen Zustand/abnormale Aktivität
35	Befehl für Gegenmaßnahme 34
36	Update oder Patch für Computersystem und/oder Steuerungssystem 2
41	Anfragen-Schlüssel
41*	neuer Anfragen-Schlüssel
42	Antwort-Schlüssel
S	Signatur

Patentansprüche

1. System (1) zur Absicherung eines Computersystems und/oder Steuerungssystems (2) gegen Manipulationen und Funktionsanomalien, umfassend ein Überwachungsmodul (11), welches mindestens eine erste Schnittstelle (11a), eine zweite Schnittstelle (11b) sowie mindestens einen Speicher (11c) aufweist und dazu ausgebildet ist,
• Informationen (31), die den Systemzustand des Computersystems und/oder Steuerungssystems (2) charakterisieren, über die erste Schnittstelle (11a) zu empfangen;
• eine verschlüsselte Anfrage (32) nach dem Systemzustand über die zweite Schnittstelle (11b) zu empfangen und mit einem in dem Speicher (11c) abgelegten Anfragen-Schlüssel (41) zu entschlüsseln;
• aus mindestens einem Teil der über die erste Schnittstelle empfangenen Informationen (31) eine Antwort (33) auf die Anfrage (32) zu generieren;

• die Antwort (33) mit einem unter Heranziehung der Anfrage (32) ermittelten Antwort-Schlüssel (42) zu verschlüsseln und über die zweite Schnittstelle (11b) auszugeben;
• einen neuen Anfragen-Schlüssel (41*) zu ermitteln, der ein gemeinsames Geheimnis ist, das auch dem Absender der Anfrage (32) zugänglich ist; und
• diesen neuen Anfragen-Schlüssel (41*) in dem Speicher (11c) abzulegen.

2. System (1) nach Anspruch 1, wobei das Überwachungsmodul (11) zusätzlich dazu ausgebildet ist, den neuen Anfragen-Schlüssel (41*) mit dem Antwort-Schlüssel zu verschlüsseln und gemeinsam mit der Antwort (33) über die zweite Schnittstelle (11b) auszugeben.

3. System (1) nach einem der Ansprüche 1 bis 2, wobei das Überwachungsmodul (11) zusätzlich dazu ausgebildet ist, den neuen Anfragen-Schlüssel (41*) unter Heranziehung der Anfrage (32) zu ermitteln.

4. System (1) nach einem der Ansprüche 1 bis 3, wobei das Überwachungsmodul (11) zusätzlich dazu ausgebildet ist, unter Heranziehung des Antwort-Schlüssels (42) einen neuen Anfragen-Schlüssel (41*) zu bilden und in dem Speicher (11c) abzulegen.

5. System (1) nach einem der Ansprüche 1 bis 4, wobei das Überwachungsmodul (11) zusätzlich dazu ausgebildet ist,
• ein Komprimat eines in der Anfrage enthaltenen Schlüssels mit einem in dem Speicher abgelegten Vergleichs-Komprimat zu vergleichen, und in Antwort darauf, dass das Komprimat mit dem Vergleichs-Komprimat übereinstimmt,
• ein in der Anfrage enthaltenes neues Komprimat als neues Vergleichs-Komprimat in dem Speicher abzulegen und
• den in der Anfrage enthaltenen Schlüssel für die Bildung des Antwort-Schlüssels (42) heranzuziehen.

6. System (1) nach Anspruch 5, wobei das Überwachungsmodul (11) zusätzlich dazu ausgebildet ist, unter Heranziehung des neuen Komprimats einen neuen Anfragen-Schlüssel (41*) zu ermitteln und in dem Speicher (11c) abzulegen.

7. System (1) nach einem der Ansprüche 1 bis 6, wobei die Informationen (31), die den Zustand des Computersystems und/oder Steuerungssystems (2) charakterisieren, eine oder mehrere der folgenden Informationen umfassen:
• von mindestens einem Prozessor des Computersystems und/oder Steuerungssystems (2) ausführbaren Programmcode, und/oder
· fest hinterlegte und/oder nur von extern änderbare Parameter, die die Arbeit des Computersystems und/oder Steuerungssystems (2) beeinflussen, und/oder
• Konfigurationsdaten für mindestens ein feldprogrammierbares Gatterarray, FPGAs, oder mindestens einen anderen programmierbaren Logikbaustein des Computersystems und/oder Steuerungssystems (2), und/oder
• Größe und/oder Inhalt nominell ungenutzter Speicherbereiche des Steuerungssystems und/oder Computersystems (2).

8. System (1) nach einem der Ansprüche 1 bis 7, wobei das Überwachungsmodul (11) zusätzlich dazu ausgebildet ist, nach einer vorgegebenen Metrik ein Maß für eine Veränderung von zur Bildung der Antwort (33) herangezogenen Informationen (31) innerhalb eines vorgegebenen Zeitraums zu ermitteln.

9. System (1) nach Anspruch 8, wobei das Überwachungsmodul (11) zusätzlich dazu ausgebildet ist, in Antwort darauf, dass die festgestellte Veränderung ein vorgegebenes Kriterium erfüllt, mindestens eine Gegenmaßnahme (34) gegen einen Angriff auf das Computersystem und/oder Steuerungssystem (2), und/oder gegen eine Fehlfunktion des Computersystems und/oder Steuerungssystems (2), zu veranlassen.

10. System (1) nach einem der Ansprüche 1 bis 9, wobei das Überwachungsmodul (11) zusätzlich dazu ausgebildet ist, in Antwort darauf, dass es über die zweite Schnittstelle (11b) einen mit dem in dem Speicher (11c) abgelegten Anfragen-Schlüssel (41) verschlüsselten Steuerbefehl (35) empfangen hat, mindestens eine Gegenmaßnahme (34) gegen einen Angriff auf das Computersystem und/oder Steuerungssystem (2), und/oder gegen eine Fehlfunktion des Computersystems und/oder Steuerungssystems (2), zu veranlassen.

11. System (1) nach einem der Ansprüche 9 bis 10, wobei die Gegenmaßnahme (34) eine oder mehrere der folgenden beinhaltet:
• es wird ein Alarm ausgegeben;
• das Computersystem bzw. Steuerungssystem (2) wird abgeschaltet, neugestartet oder auf Werkseinstellungen zurückgesetzt;
• es wird ein Software-Update und/oder ein Patch auf das Computersystem bzw. Steuerungssystem (2) eingespielt;
• die Wertigkeit des Computersystems und/oder Steuerungssystems (2) in einem dezentralen Peer-to-Peer-Netzwerk wird reduziert;
• das Computersystem bzw. Steuerungssystem (2) wird dazu veranlasst, Betriebsdaten, Protokolldaten und/oder Diagnoseinformationen auszugeben;
• das Computersystem bzw. Steuerungssystem (2) wird dazu veranlasst, wichtige Daten durch Versenden über eine Kommunikationsschnittstelle vor dem Verlust zu schützen;

• das Computersystem bzw. Steuerungssystem (2) wird dazu veranlasst, vertrauliche Daten durch Löschen vor der Preisgabe zu schützen;
• das Computersystem bzw. Steuerungssystem (2) wird in einen Notbetrieb versetzt;
• es wird eine logistische Maßnahme, wie einen Service-Einsatz und/oder einen Geräteaustausch am Ort des Computersystems und/oder Steuerungssystems (2), veranlasst; und/oder
• ein Selbsttest des Computersystems bzw. Steuerungssystems (2) wird veranlasst.

12. System (1) nach einem der Ansprüche 1 bis 11, das Überwachungsmodul (11) zusätzlich dazu ausgebildet ist, in Antwort darauf, dass es über die zweite Schnittstelle (11b) ein mit dem in dem Speicher (11c) abgelegten Anfragen-Schlüssel (41) verschlüsseltes Update (36) empfangen hat, das Einspielen des Updates (36) auf das Computersystem bzw. Steuerungssystem (2) veranlasst.

13. System (1) nach einem der Ansprüche 1 bis 12, wobei die vom Überwachungsmodul (11) generierte Antwort (33)
• einen Hashwert von zur Bildung der Antwort (33) herangezogenen Informationen (31), und/oder
• ein nach einer vorgegebenen Metrik ermitteltes Maß für eine Veränderung dieser Informationen (31) innerhalb eines vorgegebenen Zeitraums, beinhaltet.

14. System (1) nach einem der Ansprüche 1 bis 13, weiterhin umfassend mindestens ein Sicherheitsmodul (12), über das die Kommunikation von und zu mindestens einer Schnittstelle (23) des Computersystems und/oder Steuerungssystems (2) geführt ist, wobei das Sicherheitsmodul (12) dazu ausgebildet ist, die Weiterleitung von Daten (23a, 23b) von und zu dieser Schnittstelle (23) vom Ergebnis einer Überprüfung
• des Absenders (23a*, 23b*) der Daten (23a, 23b), und/oder
• des Empfängers (23a#, 23b#) der Daten (23a, 23b), und/oder
• der Form und/oder des Inhalts der Daten (23a, 23b), abhängig zu machen.

15. System (1) nach Anspruch 14, wobei das Sicherheitsmodul (12) dazu ausgebildet ist, die Weiterleitung von Daten (23a, 23b) davon abhängig zu machen, dass in Ansehung eines vorgegebenen Satzes von Regeln (12a)
• eine Beziehung zwischen dem Absender (23a*, 23b*) der Daten (23a, 23b) und dem Empfänger (23a#, 23b#) der Daten (23a, 23b) plausibel ist (12a1), und/oder
• die Daten für ihren Empfänger (23a#, 23b#) voraussichtlich verarbeitbar sind (12a2).

16. System (1) nach Anspruch 15, wobei mindestens eine Regel sich auf ein von dem Empfänger erwartetes Datenformat, und/oder auf einen von dem Empfänger erwarteten Wertebereich der Daten (23a, 23b), bezieht.

17. System (1) nach einem der Ansprüche 14 bis 16, wobei das Sicherheitsmodul (12) dazu ausgebildet ist, die Weiterleitung von Daten (23a, 23b) davon abhängig zu machen, dass der Absender die Daten mit einem vorgegebenen Schlüssel verschlüsselt und/oder signiert hat.

18. System (1) nach Anspruch 17, wobei das Sicherheitsmodul (12) dazu ausgebildet ist, zur Weiterleitung an die Schnittstelle (23) des Computersystems und/oder Steuerungssystems eingehende verschlüsselte Daten (23a) zu entschlüsseln sowie von dieser Schnittstelle (23) eingehende unverschlüsselte Daten (23b) zu verschlüsseln.

19. System (1) nach einem der Ansprüche 17 bis 18, wobei das Sicherheitsmodul (12) dazu ausgebildet ist, einen Schlüssel für die Verschlüsselung, und/oder für die Entschlüsselung, unter Heranziehung mindestens eines vom Überwachungsmodul (11) bezogenen Schlüssels und/oder Hashwerts zu ermitteln.

20. System (1) nach einem der Ansprüche 17 bis 19, wobei das Sicherheitsmodul (12) zusätzlich dazu ausgebildet ist, unter Heranziehung gültiger Eingangsdaten (23a), die es für die Weiterleitung zu der Schnittstelle (23) des Computersystems und/oder Steuerungssystems (2) empfangen hat, mindestens einen Eingangsdaten-Hashwert zu ermitteln und diesen Eingangsdaten-Hashwert zur Bildung mindestens eines Schlüssels heranzuziehen.

21. System (1) nach Anspruch 20, wobei die vom Überwachungsmodul (11) generierte Antwort auch den Eingangsdaten-Hashwert beinhaltet.

22. System (1) nach einem der Ansprüche 20 bis 21, wobei das Sicherheitsmodul (12) weiterhin dazu ausgebildet ist, bei einer Aktualisierung des Eingangsdaten-Hashwerts neben aktuellen Eingangsdaten (23a) auch den bisherigen Eingangsdaten-Hashwert für das Ermitteln des neuen Eingangsdaten-Hashwerts heranzuziehen.

23. System (1) nach einem der Ansprüche 1 bis 22, wobei das Überwachungsmodul (11), bzw. das Sicherheitsmodul (12), dazu ausgebildet ist, in Antwort darauf, dass es für eine vorbestimmte Zeitdauer keine mit einem aktuell gültigen Schlüssel authentifizierten Anfragen, Befehle bzw. Daten erhalten hat, auch mit früher gültigen Schlüsseln authentifizierte Anfragen, Befehle bzw. Daten zu akzeptieren.

24. Datenverarbeitungsmodul, Datenspeichermodul, Kameramodul, Sensormodul und/oder Aktormo-

dul mit einem System (1) nach einem der Ansprüche 1 bis 23, und/oder mit einem FPGA-Baustein, der schaltungstechnisch so in das Datenverarbeitungsmodul, Datenspeichermodul, Kameramodul, Sensormodul und/oder Aktormodul integriert ist, dass er sich durch Programmierung zu dem System (1) nach einem der Ansprüchen 1 bis 21, und/oder zu einem Überwachungsmodul (11) und/oder Sicherheitsmodul (12) dieses Systems, herrichten lässt.

25. Computerprogramm, enthaltend maschinenlesbare Anweisungen, die, wenn sie auf einer Hardwareplattform ausgeführt werden und/oder als Konfiguration in diese Hardwareplattform eingebracht werden, die Hardwareplattform zu einem System nach einem der Ansprüche 1 bis 23, und/oder zu einem Überwachungsmodul und/oder Sicherheitsmodul dieses Systems, herrichten.

Es folgen 2 Seiten Zeichnungen

Anhängende Zeichnungen

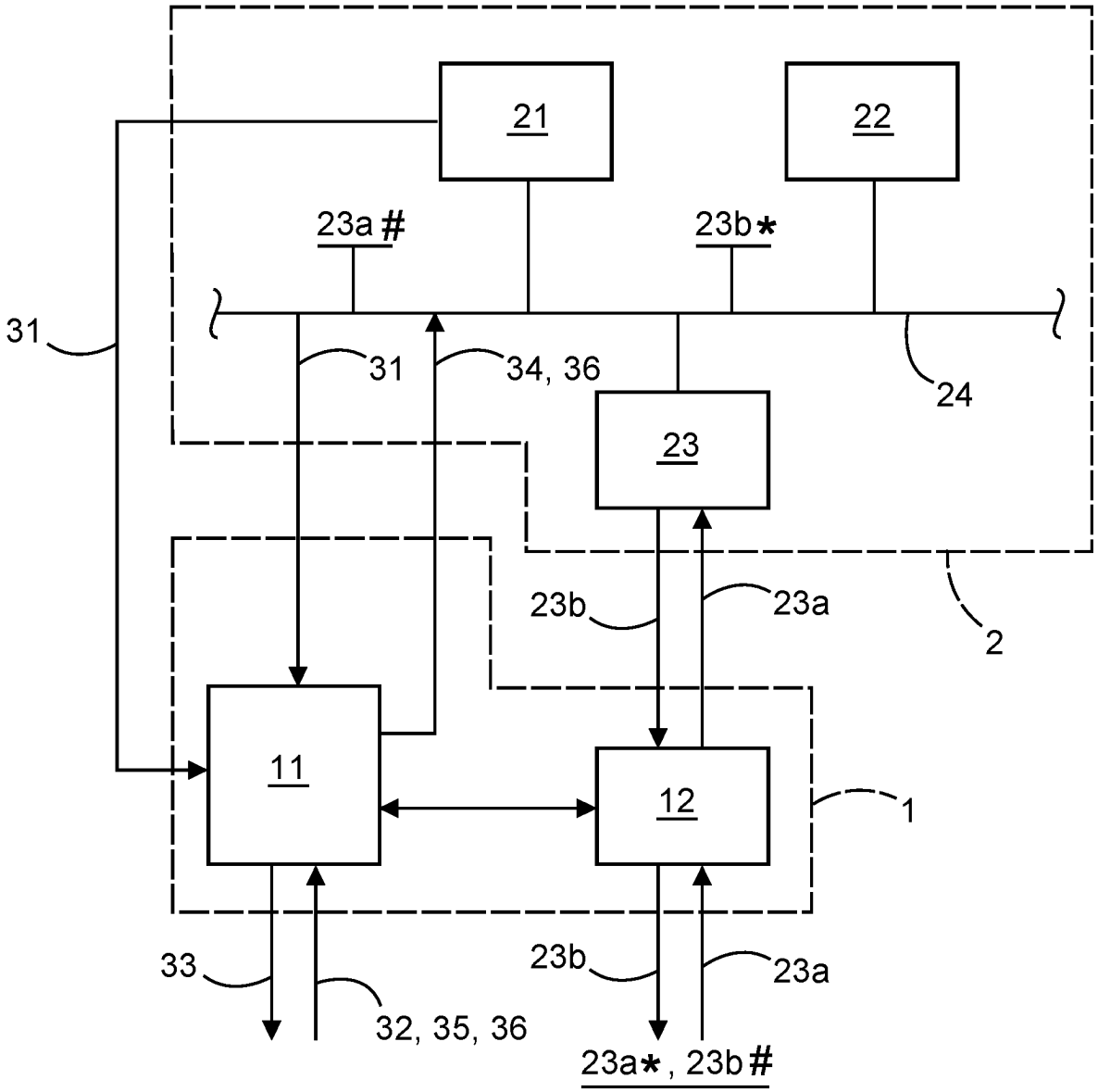


Fig. 1

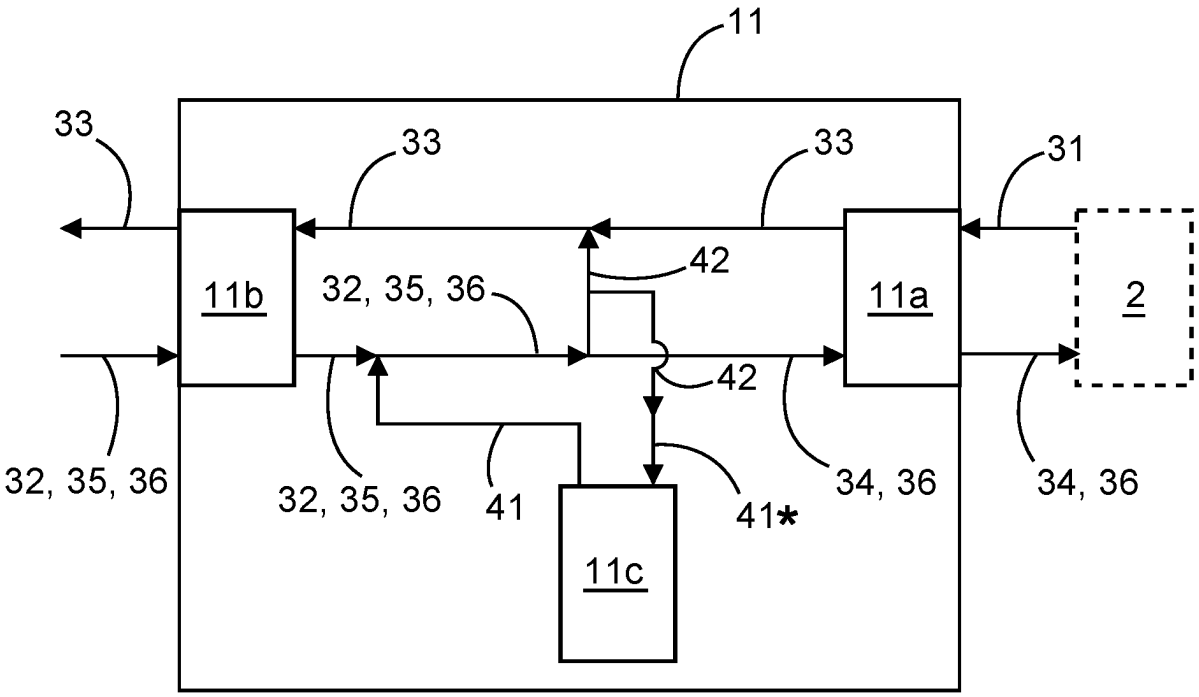


Fig. 2

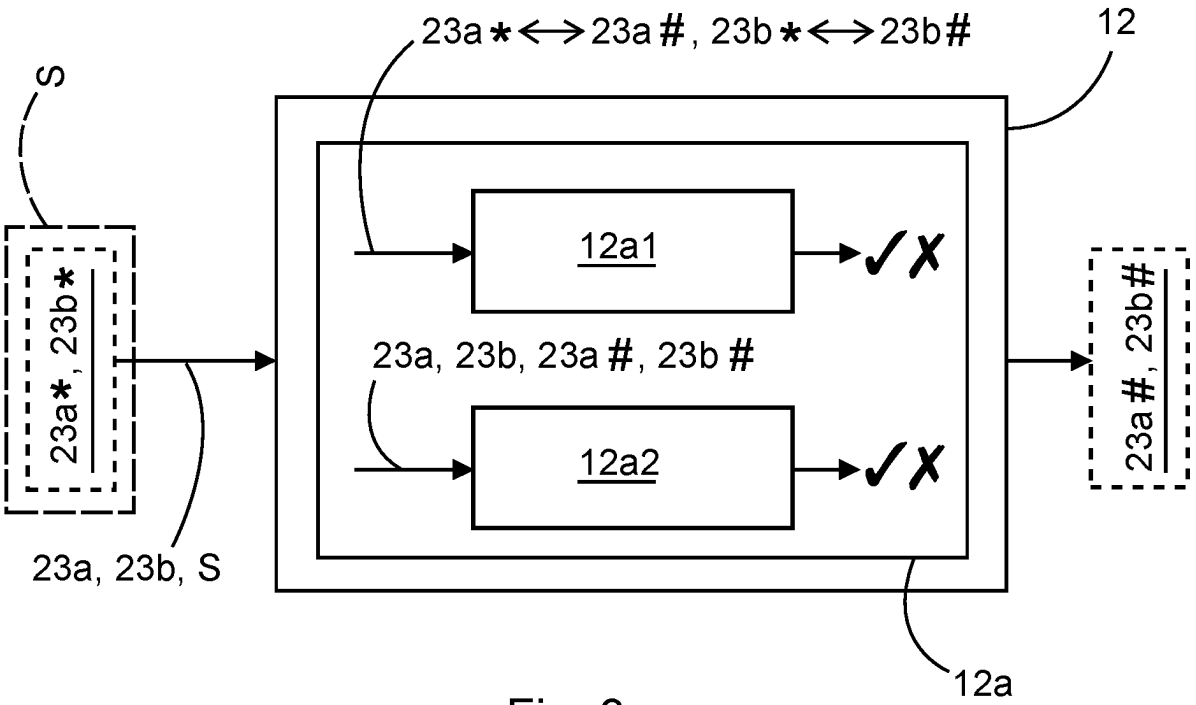


Fig. 3

