TECHNISCHER LÖSUNGSVORSCHLAG **Aktenzeichen: B2014-023**

Titel: Sicherheitskritisches System mit zusätzlichem Sicherheitsmechanismus

Autor/en: **Dr. Florian Gagel, Dr. Winfried Rappold**

Unternehmenseinheit: **Diehl BGT Defence GmbH & Co. KG**

Einleitung

Die vorliegende Erfindung betrifft ein sicherheitskritisches System, welches zumindest zwei physikalisch getrennte, miteinander in Verbindung stehende Einheiten umfasst, mit zumindest einem zusätzlichen Sicherheitsmechanismus zum Schutz vor unrechtmäßigen Zugriffen und vor Manipulation durch unberechtigte Dritte.

Problem

Die Zugänglichkeit und Netzverfügbarkeit von angreifbaren Zielen, wie sicherheitskritischen Waffensystemen steigt. Gleichzeitig sind in letzter Zeit vermehrt Sicherheitslücken bei eingeführten Waffensystemen entdeckt worden. Solche Lücken sind nachträglich meist nur schwer und mit sehr hohem – insbesondere zeitlichem und finanziellem - Aufwand zu beheben. Angriffe auf zunehmend digitalisierte sicherheitskritische Systeme mit oder ohne funkgebundenen Netzwerken sind demnach nicht auszuschließen, so dass eine elektronische Penetration in IT-basierte Infrastruktursysteme und einzelne operative Systeme eine durchaus realistische Bedrohung darstellt. Hauptaugenmerk muss daher auf der sicheren Kommunikation zwischen den einzelnen physikalisch voneinander getrennten Einheiten eines Systems liegen. Durch Manipulation oder unautorisierte Zugriffe von Dritten kann hier besonders hoher Schaden angerichtet werden. Ein grundsätzlicher Bedarf an Sicherheitsvorkehrungen für sicherheitskritische, speziell militärische Systeme ist somit selbsterklärend. Der Sicherheitsmechanismus gemäß vorliegender Erfindung soll den Aufwand zur Behebung von bestehenden Sicherheitslücken reduzieren und gleichzeitig die Gesamtsicherheit des Systems erhöhen. Im Vordergrund steht dabei ein sicherer Datenaustausch zwischen den einzelnen physikalisch voneinander getrennten Einheiten des sicherheitskritischen Systems.

Bisherige Lösungsansätze

Eine Möglichkeit für den Schutz gegen Cyberangriffe ist die Verwendung von hardwarebasierten Verschlüsselungsgeräten. Organisatorische Sicherheit, insbesondere der physikalische Zugang zu Schnittstellen und Bedienelementen eines sicherheitskritischen Systems oder im Fall eines Waffensystems zu einer taktischen Operationszentrale, kann durch physikalische Zutrittskontrollen bewerkstelligt werden. Beide Maßnahmen (IT-Sicherheit, organisatorisch) stellen bereits heute einen gewissen Schutz dar.

Eine weitere zeit- und kostenintensive Lösung zur Steigerung der Sicherheit eines sicherheitskritischen Systems besteht darin, Software in einer oder mehrerer der physikalisch getrennten Einheiten des sicherheitskritischen Systems zu ändern und dort neue Schnittstellen und/oder Sicherheitsmechanismen zu integrieren.

Lösung/Umsetzung

Die technische Lösung der Erfindung sieht vor, zumindest einen konfigurierbaren Hardware-Proxy an einer Schnittstelle einer der physikalisch getrennten Einheiten des sicherheitskritischen Systems vorzuschalten. Geschickterweise wird jeder Schnittstelle einer physikalisch getrennten Einheit ein solcher Proxy vorgeschaltet. Hierdurch kann auf eine Änderung der Software der physikalisch getrennten Einheiten verzichtet werden. Stattdessen übernimmt der Proxy, welcher in zusätzlicher Hardware integriert ist, die Implementierung der Gegenstelle mit dem zusätzlichen bzw. neuen Sicherheitsmechanismus sowie die Umsetzung auf die bestehende Schnittstelle der einen physikalisch getrennten Einheit hin.

Physikalisch befindet sich der zumindest eine Proxy auf einer der physikalisch getrennten Einheiten. Der Proxy trennt somit den neuen/zusätzlichen Sicherheitsmechanismus vom bestehenden sicherheitskritischen System. Die unabhängige Hardware-Komponente „Proxy“ erlaubt es, zeitnah zusätzliche Sicherheitsmechanismen auf eigener Hardware und / oder neue Schnittstellen zu implementieren, ohne hierbei jedoch in Hard- und Software des bestehenden sicherheitskritischen Systems eingreifen zu müssen.

Der Proxy kann als SoC (System on a Chip) mit vorzugsweise ARM-Prozessoren sowie ggf. zusätzlicher FPGA-Hardware ausgeführt sein. Eine solche Ausgestaltung eines Proxys zeichnet sich durch einen geringen Energiebedarf bei gleichzeitig hoher Performance aus und erlaubt vorteilhafterweise ein Booten von einer SD-Karte oder einem USB-Stick aus. Für den Austausch von Software bzw. Implementierung eines neuen oder zusätzlichen Sicherheitsmechanismus genügt es somit, die SD-Karte oder den USB-Stick auszutauschen, welche bzw. welcher neben dem Betriebssystem des SoC auch gleich die Proxy-Software umfassen kann.

Für eine einfache Bridge-Konfiguration eines als SoC ausgeführten Proxys sollten zwei Ethernet-Schnittstellen vorhanden sein. Die Bridge verbindet dabei gemäß OSI-Definition Subnetze protokollmäßig auf der Schicht 2 (LLC, IEEE 802.2) oder 2a (MAC-Layer) des OSI-Referenzmodells. Durch diese Konfiguration hat der SoC bzw. der Proxy keine eigene IP-Adresse und kann daher prinzipiell nicht über Ethernet angegriffen werden. Insbesondere durch eine Konfiguration als transparente Bridge wird eine Angreifbarkeit des Proxys über die bestehende Infrastruktur des sicherheitskritischen Systems vermieden. Denn eine transparente Bridge lernt sowohl, welche MAC-Adressen sich in welchem Teilnetz befinden als auch mögliche Empfänger, indem die Absender von Paketen in den einzelnen Teilnetzen in eine interne Weiterleitungstabelle eingetragen werden. Anhand dieser Informationen kann die Bridge den Weg zum Empfänger bestimmen. Die Absenderadressen werden laufend aktualisiert, um Änderungen sofort zu erkennen. Der Vorteil der transparenten Bridge liegt unter anderem darin, dass die Anwesenheit des als Bridge fungierenden Proxy von außen nicht funktional festgestellt werden kann, da dort keine Funktionsänderung des „Gesamt“-Systems sichtbar ist – wie zuvor erwähnt – hat der Proxy zudem keine eigene IP-Adresse und bietet somit auch keine Angriffsfläche, da er deshalb selber nicht angesprochen werden kann. Zwar besteht die theoretische Möglichkeit, die Anwesenheit eines Proxys über

sekundäre Effekte außerhalb des Funktionalitätsraums des „Gesamt“-Systems festzustellen, da die Anwesenheit eines Proxys zu einer geringfügigen Laufzeitverzögerung der IP-Pakete führt. Es verhält sich jedoch so, dass dies weder eine Beeinträchtigung der Funktionalität des „Gesamt“-Systems zur Folge hat, da das IP-Protokoll keine festen Laufzeiten definiert bzw. voraussetzt, noch sind durch anderweitige Effekte bedingte etwaige Laufzeitverzögerungen von „Proxy“-bedingten Laufzeitverzögerungen eindeutig unterscheidbar. Weiterhin erhöht ein Proxy in transparenter Bridge-Konfiguration den sogenannten Hop-Count der IP-Pakete nicht, wodurch sich eine Bridge sonst verraten würde.

Funktionsweise

Interessant für den Einsatz eines solchen Proxys sind allgemein sicherheitskritische Systeme, insbesondere aber militärische Systeme, welche aus mindestens zwei physikalisch getrennten Einheiten bestehen, die miteinander in Verbindung stehen. Diese beiden Einheiten können zum Beispiel ein Wirk- oder Aufklärungssystem und eine Kontroll- oder Bodenstation sein, welche uni- oder bidirektional miteinander verbunden sind. Übertragungswege dabei sind vorzugsweise Ethernet oder Datenlink wie TCP/IP (Transmission Control Protocol/Internet Protocol) oder UDP (User Datagram Protocol). Die Identifizierung der am Netzwerk teilnehmenden physikalisch getrennten Einheiten bzw. Rechner geschieht über IP-Adressen. Ein Rechner oder allgemein ein Gerät mit IP-Adresse wird im TCP/IP-Jargon als Host bezeichnet. Die Funktionsweise des Erfindungsgegenstands soll im Folgenden schematisch erklärt werden.

Legende

A	=	Wirk- oder Aufklärungssystem (z.B. Launcher, Drohne)
B	=	Verbindung (Ethernet oder Datenlink, z.B. TCP/IP/UDP), uni- oder bidirektional
C	=	Kontroll- oder Bodenstation
D	=	in Hardware implementierter und als Bridge angeschlossener Proxy
´	=	Änderung

Stand der Technik

Beim vorbekannten Stand der Technik sind A und C über B miteinander verbunden. Der Zugriff auf A oder C ist in diesem Fall nicht eingeschränkt.

Sollten nun nachträglich zusätzliche Sicherheitsmechanismen, wie bspw. Verschlüsselung oder Authentifizierung, eingeführt werden, um den Zugriff aus A einzuschränken oder zu sichern, so wurden bisher Änderungen an A vorgenommen.

Fall a) Einsatz eines Proxys

Der Vorschlag besteht jetzt darin, A nicht zu ändern, sondern folgendermaßen zu verfahren:

Die Komponente A bleibt unverändert. Der Proxy D1 wird in die Verbindung B eingesetzt und befindet sich bei A. Der Proxy D1 implementiert zur Seite C hin die neue Schnittstelle bzw. den neuen Sicherheitsmechanismus und setzt diesen zur Seite A hin auf die bestehende

Schnittstelle um. Zusätzlich zum Proxy D1 wird die neue Schnittstelle auch in C integriert, welches daher als C´ bezeichnet wird.

Fall b) Einsatz eines zweiten Proxys

In diesem Fall bleibt auch C unverändert, denn ein zweiter Proxy D2 übernimmt die neue Schnittstelle. Dieser Fall ist dann sinnvoll, wenn nur der Strecke B misstraut wird.

In allen Fällen ist D als Bridge ausgeführt, besitzt somit keine eigene IP-Adresse und ist prinzipiell nicht über B angreifbar. D kann aber bevorzugt eine zusätzliche, nicht über B erreichbare Schnittstelle besitzen. Sinnvoll ist z.B. eine SD-Karte oder ein USB-Stick, über welchen er dynamisch konfiguriert werden kann (Software-Änderungen, Schlüssel für Authentifizierung).

Anwendungsbeispiele

Beispiel 1

Im ersten Beispiel ist ein bestehendes GBAD-System (Ground Based Air Defence), bestehend aus einem Wirksystem, wie zum Beispiel LKW mit Launcher und Waffenrechner, mit der abgesetzten Kontrollstation über Ethernet verbunden. Die Kontrollstation ist ein Standard-PC und kann auch mit weiteren Systemen, wie FüWES (Führungs- und Waffeneinsatzsystem) bzw. Aufklärungssystemen/ Radar vernetzt sein. Die Software des Wirksystems mit seiner definierten Kommandierungsschnittstelle ist bereits eingeführt und abgenommen. Es ist aber nicht ausgeschlossen, dass die Kommandierungsschnittstelle auch Dritten im Detail bekannt ist. Da die Software der bestehenden Kontrollstation z. B. als potentiell unsicher erkannt wurde, soll die Kommandierungsschnittstelle zum Wirksystem um zusätzliche Authentifizierungsmechanismen erweitert werden (z. B. spezieller Abschuss-Code). Es ist hierfür nicht mehr wie zuvor notwendig das Wirksystem hinsichtlich Software und/oder Schnittstelle zu ändern, denn die Änderung und Umsetzung der Kommandierungsschnittstelle kann jetzt über den Hardware-Proxy stattfinden. Es genügt der Austausch einer SD-Karte oder eines USB-Sticks. Diese Datenträger können zudem aktuelle Sicherheitsschlüssel enthalten. Der Hardware-Proxy befindet sich physikalisch nahe beim Launcher beziehungsweise in der Nähe des Waffenrechners und wird einfach als Bridge in die bestehende Ethernet-Verbindung zwischengeschaltet.

Beispiel 2

Im zweiten Beispiel wird eine Drohne über einen Datenlink von einer abgesetzten Bodenstation kommandiert. Dieser Link wird um eine zusätzliche oder geänderte Verschlüsselung erweitert oder aber einer Formatänderung unterzogen. In diesem Fall wird die Drohne einfach mit dem Proxy ausgerüstet, was aufgrund dessen geringen Strombedarfs und Gewichts keine große Einschränkung darstellt. Die neue Verschlüsselungsumsetzung wird durch den Proxy übernommen, welcher zur Seite der Drohne hin auf die bestehende Schnittstelle umsetzt.