Octrooiraad

(12) A **Terinzagelegging** (11) **9000968**

Nederland (19) **NL**

(54) **Beveiligingssysteem voor een hoofdcomputer.**

(51) Int.Cl.[5]: G06F 1/00.

(71) Aanvrager: Paul Broertjes te Valburg.

(74) Gem.: Ir. R. Hoijtink c.s.
Octrooibureau Arnold & Siedsma
Sweelinckplein 1
2517 GK 's-Gravenhage.

(21) Aanvrage Nr. 9000968.

(22) Ingediend 23 april 1990.

(32) - -

(33) - -

(31) - -

(62) - -

(43) Ter inzage gelegd 18 november 1991.

De aan dit blad gehechte stukken zijn een afdruk van de oorspronkelijk ingediende beschrijving met conclusie(s) en eventuele tekening(en).

Beveiligingssysteem voor een hoofdcomputer

Meer en meer worden gevallen bekend, waarbij op ongewenste wijze toegang tot een computersysteem is verkregen, bijvoorbeeld door middel van het breken van een eenvoudige beveiligingscode en dergelijke. Bekende systemen zijn beschreven in de Europese octrooiaanvrage EP-A_3-0131421 alsmede in de in deze publicatie aangehaalde literatuur.

Bij een dergelijk bekend systeem wordt een aparte communicatielijn gebruikt voor het uitzenden van een willekeurig getal vanaf de hoofdcomputer naar een perifeer opgestelde codeerorgaan waarin een beperking plaatsvindt, waarna via een inverse bewerking in de hoofdcomputer wordt gecontroleerd of de juiste bewerking is uitgevoerd. Voor dit bekende systeem zijn twee extra communicatielijnen benodigd, terwijl de overige communicatielijnen door een "hacker" kunnen worden afgetapt, waarbij geheime informatie door die "hacker" verkregen kan worden. Bovendien is uit het gegeven dat van de bewerking in het perifere codeerorgaan ook een inverse bewerking bestaat, het wellicht mogelijk de code, dat wil zeggen de functionele bewerking, te breken.

De onderhavige uitvinding verschaft een beveiligingssysteem volgens conclusie 1.

Het beveiligingssysteem volgens de onderhavige uitvinding kan op eenvoudige wijze worden opgenomen in een bestaand computersysteem, dan wel voorzien van een vaste communicatielijn tussen een hoofdcomputer en een perifere computer (conclusie 3) dan wel in een veelvuldig voorkomende configuratie waarbij de hoofdcomputer op een openbaar netwerk is aangesloten (conclusie 4).

Verdere voordelen, kenmerken en details zullen duidelijk worden aan de hand van een beschrijving van de voorkeursuitvoeringsvorm van de onderhavige uitvinding, met referentie aan de bijgevoegde tekeningen waarin tonen:

fig. 1 een schema van een eerste uitvoeringsvorm volgens de onderhavige uitvinding;

fig. 2 een schema van een tweede voorkeursuitvoeringsvorm volgens de onderhavige uitvinding; en

fig. 3 een schema van detail III uit fig. 1.

Het systeem volgens de onderhavige uitvinding kan worden toegepast bij een hoofdcomputer voorzien van randapparaten (terminals) maar bij voorkeur een systeem volgens conclusie 2.

Een hoofdcomputer 1 (fig. 1), voorzien van autorisatiemiddelen 2 is via een modulator-demodulator (modem) 3 op een vaste communicatie- of huurlijn 4 aangesloten. Een perifeer opgestelde computer 5 is via een modem 6 op deze huurlijn 4 aangesloten. Tussen de modem 6 en de perifere computer 5 is een autorisatieorgaan 7 opgenomen.

Vanzelfsprekend kunnen op de hoofdcomputer 1 verscheidene perifere computers zijn aangesloten.

Indien een perifere computer 5 toegang vraagt tot de hoofdcomputer 1 wordt door de autorisatiemiddelen 2, die in het onderhavige uitvoeringsvoorbeeld bij voorkeur in programmatuur zijn uitgevoerd, een willekeurig getal naar de perifere computer 5 gestuurd, voorafgegaan door een door het autorisatieorgaan 7 te herkennen signaal, bijvoorbeeld het "BREAK"-signaal, dat wil zeggen een reeks van minimaal acht digitale 'enen'.

Het autorisatieorgaan 7, (fig. 3) omvat bij voorkeur een microprocessor (μ P) en in EPROM opgeslagen programmacode. Bij voorkeur is het EPROM-geheugen zodanig uitgevoerd dat de programmacode niet uitleesbaar is, bijvoorbeeld door het met behulp van elektronisch signaal of anderszins onherstelbaar verbreken van de "READ"-ingang van het EPROM-geheugen.

Het autorisatieorgaan 7 herkent het BREAK-signaal en voert vervolgens een functionele bewerking uit op het na de acht enen door de hoofdcomputer uitgestuurde getal. Bij voorkeur is de (relatief simpele) functionele bewerking voor verschillende randapparaten hetzelfde, maar maken deze telkens gebruik van een ander grondgetal in die bewerking.

De uitkomst van deze bewerking wordt via de communicatielijn 4 teruggestuurd naar de autorisatiemiddelen 2 die de uitkomst vergelijken met de voor dat randapparaat verwachte uitkomst van de bewerking. Hierna vindt op gebruikelijke

wijze communicatie plaats tussen de moedercomputer 1 en de perifere computer 5. Bij voorkeur wordt dit dataverkeer op enige tijdstippen onderbroken, teneinde te verifiëren of de hoofdcomputer nog steeds is aangesloten op een perifeersysteem voorzien van het juiste autorisatieorgaan.

De autorisatiemiddelen in de hoofdcomputer 1 kunnen ook voorzien zijn van een aparte microprocessor opdat geen processortijd van de hoofdcomputer wordt gebruikt voor de autorisatieroutines.

Zowel voor de gebruiker van de hoofdcomputer als de gebruiker van de perifeer opgestelde computer is het beveiligingssysteem volledig transparant, dat wil zeggen dat beiden niets merken van het uitvoeren van de autorisatieroutines. Bij normaal dataverkeer geeft het autoriseerorgaan de data gewoon door aan een perifeer randapparaat en vice versa, bijvoorbeeld via de bekende seriële RS 232-uitgang.

Bij voorkeur wordt dit bereikt doordat het autorisatieorgaan in een zogeheten polling modus de data bemonstert en doorgeeft, behalve indien de code voorafgaand aan het autorisatiegetal wordt aangeleverd, bijvoorbeeld de genoemde acht opvolgende enen, waarna de microprocessor in het autorisatieorgaan voor korte tijd de communicatie met de hoofdcomputer overneemt en het datatransport naar de perifeer opgestelde computer wordt onderbroken.

Noch de gebruiker van de perifere computer, noch de gebruiker van de moedercomputer behoeven enige kennis te hebben van de grondgetallen van de autorisatieroutines. Zelfs kan na installatie dienaangaande, informatie ook door de installateur vernietigd worden, opdat fraudegevoeligheid van een beveiligingssysteem tot een minimum wordt gereduceerd.

Indien een moedercomputer 11 (fig. 2) via een modem 13 is aangesloten op een openbaar netwerk zoals telefoonlijnen waarvan er één met 14 is aangeduid, zijn ter autorisatie voor de perifeer opgestelde computer 15 - via een modem 16 en een autorisatieorgaan 17, eveneens op de telefoonlijn 14 aangesloten - zijn de autorisatiemiddelen 12 voorzien van schakelmiddelen 21 en een besturingsorgaan 22. Een autorisatiedeel 23 is bij voorkeur op voornoemde wijze uitgevoerd met een se-

parate microprocessor, terwijl het autorisatieorgaan 17 overeenkomstig aan autorisatieorgaan 7 is uitgevoerd.

Het besturingsdeel 22 van het autorisatieorgaan 12 is bij voorkeur voorzien van een emulatiekaart voor een harde schijf, waarbij de BIOS-routine van de hoofdcomputer wordt afgeleid om de werking van de in hardware uitgevoerde hardeschijfemulator te initiëren. Hierdoor worden mechanische storingen vermeden, kunnen geen zogeheten virussen geïntroduceerd worden, wordt voorkomen dat software van het autoriseerorgaan wordt gecopieerd en kan snel toegang verkregen worden tot het besturingsdeel.

De onderhavige uitvoering verschaft een beveiligingssysteem dat elegant is in te passen in bestaande communicatiesystemen, zonder dat extra communicatie-lijnen beschikbaar behoeven te zijn.

C O N C L U S I E S

1. Systeem voor beveiliging van de toegang tot een hoofdcomputer, omvattende:

- een hoofdcomputer die met een of meer communicatielijnen te koppelen is, en die is voorzien van autorisatiemiddelen,
- een perifeer opgesteld randapparaat dat via een communicatielijn met de hoofdcomputer te koppelen is, en
- een, op de communicatielijn en het randapparaat aangesloten autorisatieorgaan, waarbij door het autorisatieorgaan een bewerking op een door de autorisatiemiddelen geleverd signaal wordt uitgevoerd en waarbij het resultaat van de bewerking door de autorisatiemiddelen wordt gecontroleerd ter autorisatie van toegang tot de hoofdcomputer.

2. systeem volgens conclusie 1, waarbij het randapparaat een perifeer opgestelde computer is en waarbij de hoofdcomputer en de perifere computers via modem (modulator-demodulator) met de communicatielijn zijn gekoppeld.

3. Systeem volgens conclusie 1 en 2, waarbij de communicatielijn hoofdzakelijk vast tussen de hoofdcomputer en de perifere computer is opgenomen en waarbij de autorisatiemiddelen als programmatuur in de hoofdcomputer zijn uitgevoerd.

4. Systeem volgens conclusie 1 en 2, waarbij de hoofdcomputer via een modem is aangesloten op een openbaar netwerk, en waarbij de autorisatiemiddelen zijn voorzien van schakelmiddelen voor het met het openbaar netwerk koppelen van verschillende uitgangslijnen van de hoofdcomputer, na autorisatie door de autorisatiemiddelen.

5. Systeem volgens conclusie 1-4 waarbij het autorisatie-orgaan een microprocessor en een niet-uitleesbaar geheugen omvat.

6. Systeem volgens één van de conclusies 1-5, waarbij het autorisatie-orgaan in een 'polling' modus werkzaam is.

FIG.1

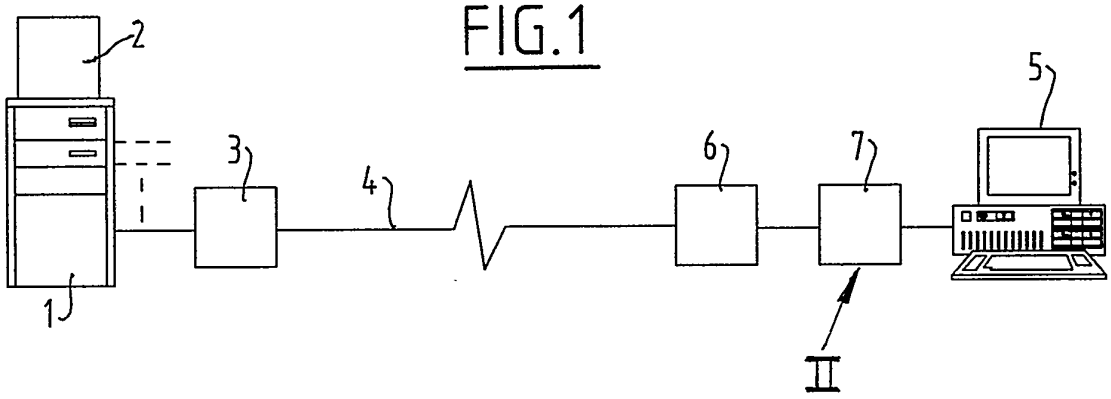
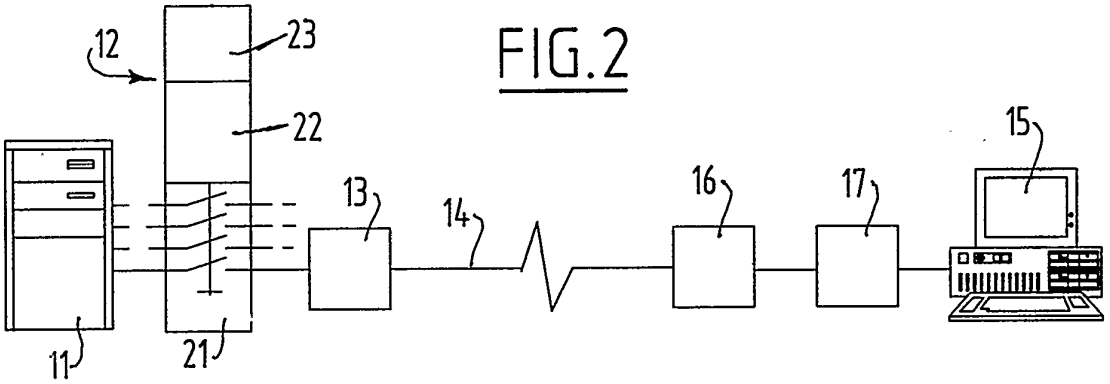


FIG.2



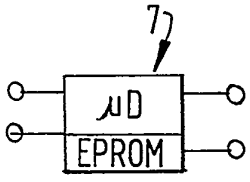


FIG.3

9000968

14181-1