P 0400498

75.198/BT
PCT/EP01/01055

KIVONAT

Eljárás hardver és szoftver hitelesítésére hálózatos rendszerben

A találmány tárgya eljárás, amely hardver egységeket és szoftver egységeket tartalmazó, a rendszer buszon (SB) keresztül kapcsolódó rendszer alkotóelemekből (SK1...SKn) álló hálózati rendszer (S) védelmére vonatkozik.

A találmánynak megfelelően minden rendszer alkotóelem (SK1...SKn) tartalmaz a hardver egységekhez egy eredetiség azonosítót (K1...Kn) és/vagy a szoftver egységekhez egy további eredetiség vagy integritás biztosító azonosítót (S1...Sn). Továbbá a rendszer buszhoz (SB) kapcsolódó központi ellenőrző egységet (PM) biztosítunk, amellyel az eredetiség azonosítót (K1...Kn) és/vagy integritás biztosító azonosítót (S1...Sn) ellenőrizzük.

Jellemző ábra: 1. ábra

P 04 00 498

S. B. G. & K.
Szabadalmi Ügyvivői Iroda
H-1062 Budapest, Andrássy út 113.
Telefon: 461-1000, Fax: 461-1099

75.198/BT
PCT/EP01/01055

Eljárás hardver és szoftver hitelesítésére hálózatos rendszerben

Infineon Technologies AG, Münich, DE

A jelen találmány tárgya eljárás, amely hardver egységeket és szoftver egységeket tartalmazó és az SB rendszer buszon keresztül kapcsolódó SK1...SKn rendszer alkotóelemekből álló S hálózati rendszer védelmére vonatkozik.

Egy ilyen rendszert például a következő esetekben alakíthatunk ki:

- rendszer elektromos fogyasztásmérő állások távolsági lekérdezésére az elektromos hálózaton vagy az elektromos táphálózaton keresztül
- adatbázis szerver klienseken keresztül történő hozzáféréssel
- belső adatcserét tartalmazó kliens/szerver konfiguráció
- berendezések távolsági beállítása
- számlaegyenlegek távolsági lekérdezése
- processzorok/mikrokontrollerek hálózatával rendelkező járművek rendszerei, különösen a motor vezérlés, a riasztó rendszer vagy a központi zár biztonsági rendszere
- stb.

A szimmetrikus és az aszimmetrikus titkosító eljárások általánosan ismertek, ahol a kommunikációs csoportok között biztonságos üzenet csatorna alakul ki. Olyan további

szimmetrikus és az aszimmetrikus eljárásokat, mint például a digitális aláírás vagy az üzenet azonosító kód (MAC Message Authentication Code) általában akkor alkalmazunk, amikor az üzenet, egy csoport vagy egy kódkulcs eredetisége és/vagy integritása ellenőrizhető a fogadó egységnél. Az általános alapokat például W. Fumy és H. P. Rieß „Kriptographie" („Entwurf und Analyse symmetrischer Kryptosysteme" R. Oldenburg Verlag München, Wien, 1988) könyvében teszi közzé.

A jelen találmány célja a fent említett szoftver és hardver rendszerek védelme az illetéktelen beavatkozások ellen.

A találmánynak megfelelően ezt a célt az 1. igénypontban felállított sajátságokkal érjük el.

A kifejlesztett eljárás, különösen a hatékony működés alatt, megóvja egy rendszer szoftvereit és hardvereit az illetéktelen változtatásoktól és/vagy felismeri a beavatkozást.

A kifejlesztett eljárás egy kiviteli alakjában a rendszer berendezéseihez a külső hozzáférés ellenőrzés alatt áll. Ezek közé tartozik többek között a rendszer alkotóelemek és/vagy ezek hardver és szoftver alkotóelem részeinek cseréje vagy helyreállítása.

A további előnyös kiviteli alakokat a kapcsolódó igénypontok teszik közzé.

Az 1. ábrán bemutatott S rendszer az SB rendszer buszon keresztül kapcsolódó SK1 - - SKn rendszer alkotóelemekből áll. Az SK1 - SKn rendszer alkotóelemek hardver és szoftver egységeket tartalmaznak, amelyeket részletesen nem ismertetünk és az egyes SK1 - SKn rendszer alkotóelemek saját speciális feladatának megfelelően alakítunk ki. Az SK1 - SKn rendszer alkotóelemek például megvalósíthatók személyi számítógépekkel, printerekkel, szerverekkel, de ugyanakkor létrehozhatók, mint egy motor vezérlésén belüli eszközök, amelyek például processzorok és memóriák.

A találmánynak megfelelően az S rendszerben az SB rendszer buszhoz kapcsolódó PM központi ellenőrző egység áll rendelkezésre. Továbbá az SK1 - SKn rendszer alkotóelemek hardver egységei K1 - Kn eredetiség azonosítóval vannak ellátva.

Hasonlóan az SK1 - SKn rendszer alkotóelemek szoftver egységei S1 - Sn további eredetiség, vagy integritás biztosító azonosítót tartalmaznak.

Az S1 - Sn integritás biztosító azonosító tárolása az S rendszer kiviteli alakjának megfelelően szabadon választható.

A K1 - Kn eredetiség azonosítót és/vagy az S1 - Sn integritás biztosító azonosítót előnyösen a megfelelő egységek fejlesztési eljárásának végén a szállítás előtt hozzuk létre. A K1 - Kn eredetiség azonosító lehet például a hardver áramkör sorozatszáma, de például kiegészítőleg el lehet látni a dátummal is. Az S1 - Sn integritás biztosító azonosítók előnyösen közismert kódkulcs eljárást alkalmazó digitális aláírások vagy szimmetrikus eredetiség és/vagy integritás kódok (MAC Message Authentication Code), amelyeket egy megbízható entitás hoz létre.

Az adott S rendszer hardver/szoftver eszközeit a hatékony működésük közben ellenőrizzük. Az ellenőrzést megvalósíthatjuk úgynevezett csapda alkalmazásával, azaz az egyik SK1 - SKn rendszer alkotóelem kérelmére. Az ellenőrzést ugyanakkor kivitelezhetjük úgynevezett lekérdezés alkalmazásával, azaz a PM ellenőrző egység kérelmére. A K1 - Kn eredetiség azonosító vagy az S1 - Sn integritás biztosító azonosítók ellenőrzését minden esetben központilag a PM ellenőrző egységen belül hajtjuk végre. Az ellenőrzést például végrehajthatjuk az S rendszer kikapcsolásával és/vagy teljesítményének csökkentésével, de például ugyancsak megvalósíthatjuk a működés alatt meghatározott időintervallumonként.

Amikor ellentmondásba ütközünk az S rendszert például kikapcsolhatjuk. Továbbá egy jobban vagy kevésbé részletezett üzenetet küldhetünk az IM információs egységhez. Következésképp az IM információs egység például közvetlen kapcsolódhat PM ellenőrző egységhez.

A találmány egy kiviteli alakjában a PM ellenőrző egység EAS bemeneti/kimeneti illesztőegységet tartalmaz. Ez az EAS bemeneti/kimeneti illesztőegység szolgálja az egyetlen hozzáférési lehetőséget az S rendszerhez. Azaz ezen az EAS bemeneti/kimeneti illesztőegységen keresztül teljesítjük a belépést kívülről az S rendszer adataihoz és funkcióihoz. Ekkor a belépő személynek és/vagy entitásnak mind az azonosítását és a hozzáférési jogosultságainak ellenőrzését végrehajtjuk.

A hozzáférés egy másik formája például az SK1 - SKn rendszer alkotóelemein belül a megfelelő egységek szoftverének frissítése. Ekkor a belépő személynek és/vagy entitásnak mind az azonosításának ellenőrzését és a jogosultságainak meghatározását újra végrehajtjuk, a megfelelő frissítés kivitelezése érdekében. Továbbá elsőként a szoftver adott azonosítójának és/vagy a megfelelő S1 - Sn integritás biztosító azonosítójának ellenőrzését hajtjuk végre. Ugyanezt tesszük az SK1 - SKn rendszer alkotóelemek hardver egységeinek cseréjekor.

Az alábbiakban a találmány további kiviteli alakjait mutatjuk be.

Az adott SK1 - SKn rendszer alkotóelemek és a PM ellenőrző egység közötti adatcsere védelem alatt állhat a K1 - Kn eredetiség azonosítók és az S1 - Sn további eredetiség és/vagy integritás biztosító azonosítók ellenőrzésekor. A védelem kialakítható belső digitális aláírással vagy MAC-vel. Továbbá az információcserét titkosíthatjuk. Ehhez a rejtjelezéshez a rendszerben használt titkosító függvények függetlenek azoktól a titkosító mechanizmusoktól, amelyeket a K1 - Kn eredetiség azonosítók vagy az S1 - Sn integritás biztosító azonosítók létrehozásához használtunk. Főként ezeket a mechanizmusokat nem feltétlenül kell az SK1 - SKn rendszer alkotóelemeken belül kialakítani, hanem egy közbenső, további önálló kódkulcs menedzsmentet alkalmazhatunk. A PM ellenőrző egység megfelelően úgy alakítható ki, mint amely kód elosztó központként működik.

A találmány egy további kiviteli alakjában a hardver egység K1 - Kn eredetiség azonosítói kialakításkor ugyancsak titkosító függvényeknek vethetők alá a rendszeren belül. Ekkor a K1 - Kn eredetiség azonosítókat például az adott S rendszer maga hozza létre

a kezdeti állapotot beállító lépés alkalmával. Ez ugyancsak végrehajtható központilag a PM ellenőrző egységben.

Az adott biztonsági követelményeknek megfelelően mind a szimmetrikus és az aszimmetrikus titkosító eljárások alkalmazhatók egyaránt külső és belső használatra.

Szabadalmi igénypontok

1. Eljárás hardver egységeket és szoftver egységeket tartalmazó és a rendszer buszon (SB) keresztül kapcsolódó rendszer alkotóelemekből (SK1...SKn) álló hálózati rendszer (S) védelmére, *azzal jellemezve, hogy*:
minden rendszer alkotóelem (SK1...SKn) tartalmaz a hardver egységekhez eredetiség azonosítót (K1...Kn) és/vagy a szoftver egységekhez további eredetiség vagy integritás biztosító azonosítót (S1...Sn), illetve
a rendszer buszhoz (SB) kapcsolódó központi ellenőrző egységet (PM) biztosítunk, amellyel az eredetiség azonosítót (K1...Kn) és/vagy az integritás biztosító azonosítót (S1...Sn) ellenőrizzük.

2. Az 1. igénypont szerinti eljárás, *azzal jellemezve, hogy* az ellenőrző egységhez (PM) kapcsolódó információs egység (IM) bocsátja ki az ellenőrző egység üzeneteit.

3. Az 1. vagy a 2. igénypont szerinti eljárás, *azzal jellemezve, hogy* az ellenőrző egység (PM) bemeneti/kimeneti illesztőegysége (EAS) szolgálja az egyetlen külső belépési lehetőséget a rendszerbe (S), ahol az ellenőrző egység (PM) a külső belépéssel kapcsolatosan végrehajtja az azonosítást és a belépési jogosultságok ellenőrzését.

4. A megelőző igénypontok bármelyike szerinti eljárás, *azzal jellemezve, hogy* a az eredetiség azonosító (K1...Kn) és/vagy a további eredetiség vagy integritás biztosító azonosító (S1...Sn) megvizsgálására az ellenőrző egység (PM) és az egyik rendszer alkotóelem (SK1...SKn) közötti adatcserét minden esetben megvédjük digitális aláírások, MAC-k (Message Authentication Codes) és/vagy titkosítás alkalmazásával.

5. A megelőző igénypontok bármelyike szerinti eljárás, *azzal jellemezve, hogy* a rendszerbe (S) az ellenőrző egység (PM) bemeneti/kimeneti illesztőegységén (EAS) keresztül betöltött szoftverhez kapcsolódó integritás biztosító azonosítót (S1...Sn) az ellenőrző egységben (PM) vizsgáljuk, és a szoftvert digitális aláírással látjuk el, vagy MAC védelem alá helyezzük és/vagy titkosítjuk, majd az egyik rendszer alkotóelemhez (SK1...SKn) továbbítjuk.

6. A 4. vagy az 5. igénypont szerinti eljárás, *azzal jellemezve, hogy* a belső digitális aláírást a MAC védelmet és/vagy a titkosítást a rendszeren (S) belül hajtjuk végre önállóan.

7. A megelőző igénypontok bármelyike szerinti eljárás, *azzal jellemezve, hogy* a kezdeti állapot beállító lépésben a rendszer alkotóelemek (SK1...SKn) hardver egységeinek eredetiség azonosítóit (K1...Kn) a rendszeren (S) belül hozzuk létre.

A meghatalmazott

Dr. Bokor Tamás
szabadalmi ügyvivő
az S.B.G. & K. Szabadalmi Ügyvivői Iroda
tagja
H-1062 Budapest, Andrássy út 113.
Telefon: 461-1000 Fax: 461-1099

75.198/BT
PCT/EP01/01055

Az alkalmazott hivatkozási jelek jegyzéke

EAS	bemeneti/kimeneti illesztőegység
PM	központi ellenőrző egység
IM	információs egység
K1...Kn	eredetiség azonosító
SK1...SKn	rendszer alkotóelem
S1...Sn	további eredetiség vagy integritás biztosító azonosító
S	hálózati rendszer

P 0400498

Blatt 1/1

FIG 1