MINISTERO DELLO SVILUPPO ECONOMICO
DIREZIONE GENERALE PER LA LOTTA ALLA CONTRAFFAZIONE
UFFICIO ITALIANO BREVETTI E MARCHI

DOMANDA DI INVENZIONE NUMERO	**102009901722621**
Data Deposito	**10/04/2009**
Data Pubblicazione	**10/10/2010**

Classifiche IPC

Titolo

SISTEMA DI PROTEZIONE UNIVERSALE PER DISPOSITIVI DI TELEFONIA MOBILE (INCLUSI SMARTPHONE, PDA, NETBOOK E MODEM) CONTRO VIRUS INFORMATICI E ATTACCHI ESTERNI BASATO SU HARDWARE CON FUNZIONI DI FILTRO E ISPEZIONE DEI COMANDI E DELLE INFORMAZIONI CHE VENGONO SCAMBIATI TRA TERMINALE MOBILE, RETE TELEFONICA E SIM.

Descrizione dell'invenzione industriale dal titolo:

Sistema di protezione universale per dispositivi di telefonia mobile (inclusi Smartphone,PDA, Netbook e modem) contro virus informatici e attacchi esterni basato su hardware con funzioni di filtro e ispezione dei comandi e delle informazioni che vengono scambiati tra terminale mobile, rete telefonica e SIM.

a nome di: Ivanov Michail

di nazionalità Italiana domiciliato in Torino

Via Valeggio n 36 - 10129

Codice fiscale: VNVMHL70E01Z105H

Residente A.I.R.E. Mnichovickà 717/8 Praha 4 - Haje Repubblica Ceca

inventore designato: Ivanov Michail

TO 2009 A 000283

depositata il 10 APR 2009 n_____

CLASSIFICAZIONE WIPO

H 04 M 1/68

DESCRIZIONE

La diffusione di massa dei terminali di telefonia mobile ha ormai raggiunto livelli tali da essere costantemente presenti nella vita quotidiana della maggior parte della popolazione mondiale.

L' evoluzione dei terminali da semplice "telefonino" a "Smartphone" , "PDA" o "Netbook" ha permesso agli utenti di usufruire oltre a capacità di connettività Internet sempre più efficienti anche capacità di acquisizione ed elaborazione di informazioni paragonabili sempre più ai Computer da ufficio. Di conseguenza i nuovi dispositivi seguono ovunque l'utente e custodiscono moli di dati sempre più importanti per volume e per sensibilità.

Negli ultimi anni la diffusione dei terminali mobili ha anche introdotto un nuovo modo di comunicazione tramite SMS con grandi vantaggi economici, temporali e di riservatezza. Per agevolare l'utilizzo di tale servizio i telefoni sono ormai predisposti con sistemi che supportano la scrittura con tastiere o software che interpretano e velocizzano le funzionalità più comuni. Con l'evoluzione applicativa di tali sistemi si è introdotto il rischio di un possibile attacco da parte di virus o agenti esteri al telefono che vogliono impossessarsi di informazioni, o che vogliono compromettere la funzionalità, o utilizzo illecito di risorse. L'aumento delle prestazioni e delle funzionalità dei più recenti

dispositivi non è andato di pari passo con l'aumento della sicurezza degli stessi poiché pensati per essere usati su reti multistandard e dotati di connettività sempre più sofisticata.

Di recente il furto di dati, i tentativi di frode o le violazioni della privacy si sono moltiplicate tanto da diventare un fenomeno tanto preoccupante da aver persino destato l'interesse del COPASIR, il Comitato per la sicurezza della Repubblica, su alcune pratiche di controllo dei terminali tramite un particolare software acquistabile via Internet a basso costo.

Questi attacchi sono basati su programmi spia che possono essere installati da remoto sul dispositivo e che ne permettono un costante monitoraggio riuscendo a raccogliere tantissime informazioni, come la rubrica, l'elenco delle chiamate, gli sms e altri contenuti. Inoltre questo tipo di programma permette di avere a disposizione una vera e propria cimice che registra le telefonate e che fornisce informazioni sulla posizione precisa del cellulare interessato agendo come un cellulare spia.

Le reti mobili permettono di inviare tramite il canale SMS dati generici in formato binario. Quello che l'utente conosce nella vita quotidiana è l'SMS testuale che è fatto per trasportare unicamente testo e rappresenta uno standard per poter essere compatibile con qualunque telefono. Qualche anno fa

si diffusero gli EMS che sono dei messaggi "potenziati" che permettono di trasportare altre informazioni come disegni, suoni, ecc. La messaggistica EMS non si è diffusa molto poichè ogni produttore ha creato un suo protocollo proprietario e l'operatore non ha promosso questa tecnologia non avendone un ritorno economico significativo. L'avvento dell'MMS, nuovo standard, permette il trasferimento di informazioni di vario tipo video, audio, applicazioni e l'operatore tariffa questo servizio con un valore superiore al SMS dato il maggior numero di informazioni che si possono trasportare con tale mezzo.

Da qualche anno si comincia a sentire della diffusione di virus per cellulari e principalmente i produttori di antivirus si sono dedicati alla realizzazione di software sviluppati appositamente per i cellulari più diffusi. Maggior parte delle soluzioni si basano sulla protezione dai virus che possono essere trasmessi dalle mail o tramite file trasportati sui telefoni o tramite bluetooth o wifi o attraverso la navigazione Internet. Gli antivirus che devono essere fatti specificamente in accordo con i produttori dei cellulari, e quindi per i vari sistemi operativi, tali soluzioni agiscono in modo efficace quando un virus comincia a diffondersi ed i produttori degli antivirus ne vengono a conoscenza studiando una soluzione e rilasciando un aggiornamento dei propri software in modo che gli utenti possano usufruirne.

Per semplificare l'utilizzo dei telefoni e l'installazione di software aggiuntivi la maggior parte dei telefoni permette di installare automaticamente software o di essere reindirizzati automaticamente ad una pagina Internet con la sola pressione di un tasto del telefono. Molte delle operazioni che vengono fatte sul telefono si eseguono con poca attenzione e questo ci rende facile preda di virus e attacchi informatici. Infatti molti dei virus di cui si sente parlare ultimamente sui media, sono trasmessi tramite SMS che trasportano nel testo un link che se premuto fa scaricare ed installare un software virus che (nel caso più grave) permette di trasformare il telefono in spia per intercettazioni illegali.

La presente invenzione, partendo dalla nozione di tali inconvenienti, intende porvi rimedio.

Pertanto, uno scopo della presente invenzione è quello di provvedere un sistema e relativo metodo per un filtro hardware che si inserisce tra telefono e SIM, che monitora, filtra e ispeziona qualunque dato che arrivi dalla rete mobile alla SIM e dalla SIM al telefono. In pratica nella configurazione "sicura" il sistema di sicurezza di seguito chiamato "SIM Defender" non permetterà il transito di alcuna informazione che non sia testo e che non abbia all'interno di questo alcun link che venga interpretato dal telefono per una connessione Internet. Con un filtro hardware separato dal terminale telefonico e dalla SIM è

possibile avere un ambiente sicuro a prova di manomissione e che non può essere aggirato o disattivato se non con un intervento fisico. E' anche scopo dell'invenzione di provvedere un sistema e relativo metodo per permettere non solo di risolvere l'attuale problema dei virus che vengono scaricati tramite link, ma anche da tutti i futuri attacchi che sfrutteranno i sistemi per gli aggiornamenti e configurazioni da remoto OTA (over the air). E' anche scopo dell'invenzione di provvedere un sistema e relativo metodo che, interagendo con la SIM, sarà compatibile con tutti i telefoni attuali e futuri e non avrà bisogno di software che si installa sul terminale. E' anche scopo dell'invenzione di provvedere un sistema e relativo metodo per proteggere anche la SIM dagli attacchi che possono venire dal telefono o per mezzo delle periferiche ad esso connesse. Ad esempio molti telefoni permettono di accedere alla SIM a periferiche esterne tramite bluetooth e di utilizzarne i servizi o le informazioni salvate su esso. In caso di compromissione del telefono sarà possibile per un attaccante accedere ai contatti della SIM tramite bluetooth. Anche in questo caso si potranno filtrare le richieste fatte alla SIM e richiedere un intervento e l'autorizzazione dell'utente segnalando un comportamento anomalo.

Pur esistendo dispositivi hardware che si interpongono tra SIM e telefono con diverse funzionalità, non esistono sistemi concepiti per proteggere e filtrare le

comunicazioni che vengono scambiate tra telefono rete e SIM. Infatti i sistemi esistenti interagiscono sulle comunicazioni tra telefono e sim per eludere i meccanismi di protezione del telefono i cosidetti "SIM unlocker" (ad esempio telefoni venduti da alcuni operatori che funzionano esclusivamente con la SIM venduta in abbinamento). Altri sistemi sono stati concepiti per invio di sms cifrati , comandi di localizzazione o allarme (collegato a periferiche supplementari). Il sistema SIM Defender viene concepito per offrire il miglior sistema di protezione dagli attacchi che possono essere effettuati sfruttando le capacità della sim e del telefono. Il SIM Defender potrà essere basato sull'utilizzo di hardware già esistenti (come i suddetti SIM Unlocker) implementando un propria logica oppure realizzando un dispositivo hardware specifico. La realizzazione di tale hardware ha come unico vincolo l'adattabilità ai contatti elettrici presenti sul telefono/smartphone/modem e sulla SIM/USIM.

La forma e l'architettura del SIM Defender potrà variare molto a seconda dell'esigenza di adattarsi ad uno specifico modello di telefono piuttosto che alla adattabilità a tutti i modelli di telefoni. La forma potrà variare anche in relazione ai componenti e funzionalità che potranno essere implementate.

In vista di tali scopi, l'invenzione provvede un sistema per la protezione universale per dispositivi di telefonia mobile contro virus informatici e attacchi

esterni basato su funzioni di filtro e ispezione dei comandi e delle informazioni che vengono scambiati tra terminale mobile, rete telefonica e SIM come specificato nel preambolo della descrizione, la cui caratteristica essenziale forma oggetto della rivendicazione 1.

L'invenzione provvede inoltre un metodo per il controllo delle informazioni che vengono inviate e scambiate con la SIM interponendosi fisicamente tra telefono e SIM stessa potendo così filtrare, eliminare o rifiutare tutte le informazioni o i comandi non strettamente necessari alle comunicazioni mobili o che non sono espressamente voluti dall'utente come specificato nel preambolo della descrizione, la cui caratteristica essenziale forma oggetto della rivendicazione2. Le rivendicazioni suddette si intendono qui riportate. L'idea di soluzione, quale rivendicata nelle rivendicazioni allegate, permette di conseguire efficacemente gli scopi sopra elencati. Essa consiste essenzialmente nel provvedere un sistema per evitare qualunque tipo di virus o attacco informatico che possa essere effettuato sfruttando il canale delle comunicazioni dati ed sms che transitano dalla rete verso la sim e il telefono e viceversa, interponendosi fisicamente tra sim e telefono e monitorando tutto il traffico informativo.

Il metodo secondo l'invenzione comprende i seguenti passi:

a) inserimento di un elemento molto sottile (SIM Guardian) tra i contatti

elettrici del telefono e quelli della sim in modo da far passare corrente come se l'elemento non esistesse ma in modo da poter filtrare, ed eliminare tutte le informazioni che possono compromettere il normale uso del telefono

b) l'elemento che si interpone tra SIM e telefono è dotato microprocessore che ospita una logica programmabile che permette di monitorare le informazioni ed elaborarle in tempo reale

c) il microprocessore può essere altresì collocato in prossimità dell'elemento che si interpone tra sim e telefono, in modo da adattarsi a vari tipi di telefono che in alcuni casi non permetterebbero alcun elemento estraneo

d) il microprocessore può essere dotato di periferiche di comunicazione wireless autonome in modo da poter fornire ulteriori funzionalità ed usi futuri

e) il microprocessore può essere di tipo "sicuro" in modo da poter implementare funzionalità crittografiche, di autenticazione e custodia sicura di informazioni.

f) L'elemento sottile di cui alla lettera a) può essere realizzato con un materiale isolante (in materiale plastico, in carta, con una sottile pellicola) su cui è applicato il circuito stampato, i contatti elettrici ed il microchip. Inoltre l'elemento può essere la SIM stessa a cui sono state apportare opportune modifiche hardware o in cui è stata inserita parte della logica che dialoga

tramite collegamenti cablati o wireless con altri oggetti quali microchip, dispositivi di memoria o periferiche esterne.

g)SIM Defender controlla tutte le comunicazioni entranti e uscenti tra telefono, sim e rete. In particolar modo analizza i messaggi SMS ricevuti attraverso la rete telefonica prima che il messaggio venga trasferito al telefono. Se nel messaggio sono presenti indirizzi Internet o link che possono essere interpretati dal telefono, questi vengono rimossi o modificati in modo da renderli innocui.

h) SIM Defender analizza i messaggi SMS ricevuti attraverso la rete telefonica e nella configurazione più sicura elimina tutti i messaggi in formato binario che non possono essere interpretati come testo e che possono essere potenzialmente dannosi per il telefono. La configurazione di sicurezza può essere impostata a discrezione del utente

i)Lo standard di comunicazione delle SIM/USIM con i terminali prevede molte operazioni e funzioni che possono essere eseguite da remoto come la richiesta di localizzazione o di spedizione messaggi o la possibilità di effettuare una chiamata su richiesta. Queste funzioni sono state studiate per fornire servizi all'operatore o per coadiuvare operazioni di soccorso o di indagine per le forze pubbliche. Purtroppo queste funzioni non sono visibili all'utente e il più delle

volte non sono utilizzate o implementate. Dato che queste funzioni impattano molto sulla privacy dell'utente che può essere violata senza che questo ne venga avvertito, la soluzione SIM Defender si propone di escludere a richiesta le suddette funzioni della SIM, e di fornire la possibilità di utilizzo delle funzioni esclusivamente all'utente. Quindi sim defender può bloccare le richieste di localizzazione o spedizione di informazioni inviate alla SIM, ma può allo stesso tempo fornire le stesse funzioni all utente che avrà il totale controllo dello strumento di comunicazione (terminale mobile + SIM Defender + SIM).

j) Con la notevole diffusione dei telefoni mobili, molte persone sono vittime di spam ovvero di messaggi non desiderati . Lo spam può riguardare sia l'invio di SMS ed MMS non richiesti, sia telefonate da parte di numeri indesiderati. Potendo inserire un applicazione di antispam nel sim defender, si fornisce una funzione non legata al telefono, e che si può trasferire con le sue configurazioni in ogni nuovo telefono che l'utente decide di adottare. IL SIM Defender con la funzione antispam elimina i messaggi contenenti testi definiti dall'utente e rifiuta automaticamente le telefonate da numeri definiti come spam

k) SIM Defender può fornire un valido strumento di protezione della privacy potendo limitare le chiamate entranti e uscenti verso numeri definiti dal utente e filtrando e custodendo SMS provenienti da contatti definiti dall'utente in

modo che gli SMS non siano normalmente visibili sul telefono se non accedendo al Sim Defender con una password.

l) SIM Defender può essere programmato sia dal telefono autenticandosi come amministratore del dispositivo che da remoto con invio di messaggi cifrati contenenti le configurazioni sia tramite server con interfaccia web per una gestione facilitata delle configurazioni. Questa funzionalità può essere un valido strumento per il controllo e la protezione dei minori.

SIM Defender può inoltre proteggere la SIM da tentativi di accesso non autorizzato attuati attraverso attacchi che sfruttano la connessione Bluetooth o wifi.

La presente invenzione risulterà maggiormente dalla descrizione dettagliata che segue, con riferimento ai disegni allegati, forniti a solo titolo di esempio, in cui:

- la fig. 1 è uno schema illustrante la configurazione generale del sistema per controllo e filtro informazioni che vengono scambiate tra sim rete e telefono

Ciascun dispositivo di controllo per sim viene programmato o preconfigurato con almeno una delle seguenti funzioni:

- Filtro informazioni scambiate tra telefono sim e rete mobile

- Elaborazione informazioni scambiate tra sim telefono e rete mobile
- Applicazioni che operino attivamente e che possano fare eseguire operazioni a sim o al telefono
- Interfaccia di gestione che comunica tramite lo standard del STK (sim tool kit) o USAT (USIM application tool) presente in tutti i telefoni che permette una facile configurazione delle applicazioni o impostazioni di filtro
- Logging e visualizzazione delle operazioni ed informazioni scambiate tra terminale mobile, sim e rete. Questa funzione può essere regolata in modo da aumentare o diminuire i dettagli delle iterazioni.
- Localizzazione, invio sms o chiamate vocali su richiesta dell'utente.

Naturalmente, numerose varianti potranno, in pratica essere apportate rispetto a quanto descritto ed illustrato a solo titolo di esempio, senza per questo uscire dall'ambito dell'invenzione e quindi dal dominio della presente privativa industriale.

RIVENDICAZIONI TO 2009 A 000283

1) Sistema per la protezione universale per dispositivi di telefonia mobile contro virus informatici e attacchi esterni basato su funzioni di filtro e ispezione dei comandi e delle informazioni che vengono scambiati tra terminale mobile, rete telefonica e SIM collegati con rispettivi apparecchi di telecomunicazione connessi in una rete telefonica comune, ad esempio GSM / UMTS / CDMA / satellitare, caratterizzato dal fatto che comprende, un dispositivo elettronico ed il quale è fisicamente separato e collegato, tramite mezzi di connessione locale alla SIM sfruttandone i contatti standard e ad un rispettivo apparecchio di telecomunicazione, a sua volta connesso in detta rete telefonica , di modo che detto primo dispositivo di comunicazione possa interagire con la SIM in modo trasparente e che le informazioni passino sempre tramite il dispositivo filtrante che può quindi monitorare, filtrare ed elaborare in tempo reale le informazioni passanti. Il suddetto sistema è raffigurato nella figura 1 composto dalla rete telefonica(1) che si collega via radio al telefono mobile (2) oppure allo smartphone (3) o al modem(4) i quali dialogano con la SIM/USIM(6) tramite il SIM Defender(5)

2) Sistema secondo la rivendicazione 1 in cui il microprocessore può essere

dotato di periferiche di comunicazione wireless autonome in modo da poter fornire ulteriori funzionalità ed usi futuri

3) Sistema secondo la rivendicazione 1 in cui il microprocessore può essere di tipo "sicuro" in modo da poter implementare funzionalità crittografiche, di autenticazione e custodia sicura di informazioni.

4) Sistema secondo la rivendicazione 1 in cui l'elemento sottile può essere realizzato con un materiale isolante (in materiale plastico, in carta, con una sottile pellicola) su cui è applicato il circuito stampato, i contatti elettrici ed il microchip. Inoltre l'elemento può essere la SIM stessa a cui sono state apportare opportune modifiche hardware o in cui è stata inserita parte della logica che dialoga tramite collegamenti cablati o wireless con altri oggetti quali microchip, dispositivi di memoria o periferiche esterne.

5) Metodo per protezione universale per dispositivi di telefonia mobile (inclusi Smartphone, PDA, netbook, modem) contro virus informatici e attacchi esterni basato su funzioni di filtro e ispezione dei comandi e delle informazioni che vengono scambiate tra terminale mobile, rete telefonica e SIM/USIM, caratterizzato dal fatto che per proteggere detti terminali si interpone un elemento molto sottile (SIM Guardian) tra i contatti elettrici del telefono e

quelli della sim in modo da far passare corrente come se l'elemento non esistesse ma in modo da poter filtrare, ed eliminare tutte le informazioni che possono compromettere il normale uso del telefono, detto elemento che si interpone tra SIM e telefono è dotato di microprocessore che ospita una logica programmabile, detto microprocessore può essere altresì collocato in prossimità dell'elemento che si interpone tra sim e telefono, in modo da adattarsi a vari tipi di telefono che in alcuni casi non permetterebbero alcun elemento estraneo, e permettere di monitorare le informazioni ed elaborarle in tempo reale.

6) Metodo secondo la rivendicazione 5 caratterizzato dal fatto che comprende almeno una delle funzioni consistenti nella:

a) attuazione del controllo di tutte le comunicazioni entranti e uscenti tra telefono, sim e rete, analizzando i messaggi SMS ricevuti attraverso la rete telefonica e segnalando eventuali anomalie e/o pericoli all'utente prima che il messaggio venga trasferito al telefono.

b) bonifica del contenuto dei messaggi, qualora nel messaggio fossero presenti indirizzi Internet o link che possono essere interpretati dal telefono, questi vengono rimossi o modificati in modo da renderli innoqui.

c) (solo nella configurazione più sicura) eliminazione di tutti i messaggi in

formato binario che non possono essere interpretati come testo e che possono essere potenzialmente dannosi per il telefono, La configurazione di sicurezza può essere impostata a discrezione del utente

d) a richiesta del utente, esclusione delle funzioni di richiesta di localizzazione e/o di spedizione messaggi e/o composizione di una chiamata su richiesta della SIM e/o attivazione del microfono e/o lettura della rubrica dei contatti) e fornitura all'utente , in maniera esclusiva, della possibilità di utilizzo delle funzioni di richiesta di localizzazione e/o di spedizione messaggi e/o composizione di una chiamata su rischiesta della SIM e/o attivazione del microfono e/o lettura della rubrica dei contatti per un totale controllo dello strumento di comunicazione (terminale mobile + SIM Defender + SIM).

f) funzione di antispam indipendentemente dal telefono eliminando i messaggi contenti testi definiti dall'utente e rifiutando automaticamente le telefonate da numeri definiti come spam

g) limitazione delle chiamate entranti e uscenti verso numeri definiti dal utente e filtrando e custodendo SMS provenienti da contatti definiti dall'utente in modo che gli SMS non siano normalmente visibili sul telefono se non accedendo al Sim Defender con una password.

h) protezione della SIM da tentativi di accesso non autorizzato attuati

attraverso attacchi che sfruttano la connessione Bluetooth o wifi.

i) eliminazione di tutti i messaggi EMS, notifiche MMS , messaggi broadcast, che possono essere potenzialmente dannosi per il telefono, La configurazione di sicurezza può essere impostata a discrezione del utente

7) Metodo secondo la rivendicazione 5 caratterizzato dal fatto SIM Defender può essere programmato sia dal telefono autenticandosi come amministratore del dispositivo che da remoto con invio di messaggi cifrati contenenti le configurazioni sia tramite server con interfaccia web per una gestione facilitata delle configurazioni. Questa funzionalità può essere un valido strumento per il controllo e la protezione dei minori.

RIVENDICAZIONI TO 2009 A 000283

1) Sistema per la protezione universale per dispositivi di telefonia mobile contro virus informatici e attacchi esterni basato su funzioni di filtro e ispezione dei comandi e delle informazioni che vengono scambiati tra terminale mobile, rete telefonica e SIM collegati con rispettivi apparecchi di telecomunicazione connessi in una rete telefonica comune, ad esempio GSM / UMTS / CDMA / satellitare, caratterizzato dal fatto che comprende, un dispositivo elettronico ed il quale è fisicamente separato e collegato, tramite mezzi di connessione locale alla SIM sfruttandone i contatti standard e ad un rispettivo apparecchio di telecomunicazione, a sua volta connesso in detta rete telefonica , di modo che detto primo dispositivo di comunicazione possa interagire con la SIM in modo trasparente e che le informazioni passino sempre tramite il dispositivo filtrante che può quindi monitorare, filtrare ed elaborare in tempo reale le informazioni passanti. Il suddetto sistema è raffigurato nella figura 1 composto dalla rete telefonica(1) che si collega via radio al telefono mobile (2) oppure allo smartphone (3) o al modem(4) i quali dialogano con la SIM/USIM(6) tramite il SIM Defender(5)

2) Sistema secondo la rivendicazione 1 in cui il microprocessore può essere

dotato di periferiche di comunicazione wireless autonome in modo da poter fornire ulteriori funzionalità ed usi futuri

3) Sistema secondo la rivendicazione 1 in cui il microprocessore può essere di tipo "sicuro" in modo da poter implementare funzionalità crittografiche, di autenticazione e custodia sicura di informazioni.

4) Sistema secondo la rivendicazione 1 in cui l'elemento sottile può essere realizzato con un materiale isolante (in materiale plastico, in carta, con una sottile pellicola) su cui è applicato il circuito stampato, i contatti elettrici ed il microchip. Inoltre l'elemento può essere la SIM stessa a cui sono state apportare opportune modifiche hardware o in cui è stata inserita parte della logica che dialoga tramite collegamenti cablati o wireless con altri oggetti quali microchip, dispositivi di memoria o periferiche esterne.

5) Metodo per protezione universale per dispositivi di telefonia mobile (inclusi Smartphone, PDA, netbook, modem) contro virus informatici e attacchi esterni basato su funzioni di filtro e ispezione dei comandi e delle informazioni che vengono scambiate tra terminale mobile, rete telefonica e SIM/USIM, caratterizzato dal fatto che per proteggere detti terminali si interpone un elemento molto sottile (SIM Guardian) tra i contatti elettrici del telefono e

quelli della sim in modo da far passare corrente come se l'elemento non esistesse ma in modo da poter filtrare, ed eliminare tutte le informazioni che possono compromettere il normale uso del telefono, detto elemento che si interpone tra SIM e telefono è dotato di microprocessore che ospita una logica programmabile, detto microprocessore può essere altresì collocato in prossimità dell'elemento che si interpone tra sim e telefono, in modo da adattarsi a vari tipi di telefono che in alcuni casi non permetterebbero alcun elemento estraneo, e permettere di monitorare le informazioni ed elaborarle in tempo reale.

6) Metodo secondo la rivendicazione 5 caratterizzato dal fatto che comprende almeno una delle funzioni consistenti nella:

a) attuazione del controllo di tutte le comunicazioni entranti e uscenti tra telefono, sim e rete, analizzando i messaggi SMS ricevuti attraverso la rete telefonica e segnalando eventuali anomalie e/o pericoli all'utente prima che il messaggio venga trasferito al telefono.

b) bonifica del contenuto dei messaggi, qualora nel messaggio fossero presenti indirizzi Internet o link che possono essere interpretati dal telefono, questi vengono rimossi o modificati in modo da renderli innoqui.

c) (solo nella configurazione più sicura) eliminazione di tutti i messaggi in

formato binario che non possono essere interpretati come testo e che possono essere potenzialmente dannosi per il telefono, La configurazione di sicurezza può essere impostata a discrezione del utente

d) a richiesta del utente, esclusione delle funzioni di richiesta di localizzazione e/o di spedizione messaggi e/o composizione di una chiamata su richiesta della SIM e/o attivazione del microfono e/o lettura della rubrica dei contatti) e fornitura all'utente , in maniera esclusiva, della possibilità di utilizzo delle funzioni di richiesta di localizzazione e/o di spedizione messaggi e/o composizione di una chiamata su rischiesta della SIM e/o attivazione del microfono e/o lettura della rubrica dei contatti per un totale controllo dello strumento di comunicazione (terminale mobile + SIM Defender + SIM).

f) funzione di antispam indipendentemente dal telefono eliminando i messaggi contenti testi definiti dall'utente e rifiutando automaticamente le telefonate da numeri definiti come spam

g) limitazione delle chiamate entranti e uscenti verso numeri definiti dal utente e filtrando e custodendo SMS provenienti da contatti definiti dall'utente in modo che gli SMS non siano normalmente visibili sul telefono se non accedendo al Sim Defender con una password.

h) protezione della SIM da tentativi di accesso non autorizzato attuati

attraverso attacchi che sfruttano la connessione Bluetooth o wifi.

i) eliminazione di tutti i messaggi EMS, notifiche MMS , messaggi broadcast, che possono essere potenzialmente dannosi per il telefono, La configurazione di sicurezza può essere impostata a discrezione del utente

7) Metodo secondo la rivendicazione 5 caratterizzato dal fatto SIM Defender può essere programmato sia dal telefono autenticandosi come amministratore del dispositivo che da remoto con invio di messaggi cifrati contenenti le configurazioni sia tramite server con interfaccia web per una gestione facilitata delle configurazioni. Questa funzionalità può essere un valido strumento per il controllo e la protezione dei minori.

TO 2008 A 000283