Università degli Studi di Perugia
Facoltà di Scienze Matematiche, Fisiche e Naturali

Corso di Laurea Magistrale in

Informatica

Seminario di Sicurezza Informatica

Safer Internet

Studenti:
Luca Caprini
Fabiana Zollo

Professore:
Prof. Stefano Bistarelli

Anno Accademico 2010-2011

Sommario

L'obiettivo di questa relazione consiste nel fornire una panoramica generale sulle attività di protezione, filtro e monitoraggio riguardanti l'utilizzo di Internet da parte di bambini e adolescenti.

Indice

Elenco delle figure

Introduzione

L'avvento delle tecnologie digitali ha facilitato enormemente la libertà di espressione e di comunicazione in tutto il mondo. L'accesso ad Internet e l'utilizzo di smartphone di ultima generazione diventa sempre più diffuso in Europa e nel resto del mondo e bambini e ragazzi rappresentano una buona parte degli usufruitori di queste tecnologie.

Tuttavia, sebbene Internet rappresenti una risorsa inestimabile, la rete è spesso piena di insidie e pericoli, e la protezione dei minori non deve essere trascurata. Al di là dei vantaggi e delle opportunità offerti, Internet comporta anche una serie di rischi per i bambini e gli adolescenti: dall'accesso a contenuti inappropriati (pornografia, violenza, autolesionismo, istigazione ad atti illegali), all'esposizione a predatori online e ad ambiti pericolosi in cui potrebbero essere coinvolti (pedofilia, cyber-bullying*, sexting†).

Per occuparsi attivamente del problema, la Commissione Europea ha creato un programma apposito per la protezione dei bambini e dei ragazzi che utilizzano Internet ed altre tecnologie di comunicazione, il *Safer Internet Work Programme (cap. 1)*.

In ogni modo, il mercato fornisce ai genitori numerosi strumenti per proteggere i minori da questo tipo di minacce. Si tratta dei cosiddetti *Parental Control Tool*. In questa relazione cercheremo, quindi, di offire una panoramica generale sui modi in cui è possibile utilizzare questo tipo di strumenti, focalizzandoci soprattutto sulla loro efficacia e sulla loro sicurezza e analizzandone le funzionalità *(cap. 2)*.

Va ricordato che, riguardo ad ogni possibile classificazione dei *Parental Control Tool*, è importante considerare, in primo luogo, che tipo di periferica viene utilizzata dal minore per accedere ad Internet. Infatti, oltre ai PC, che rappresentano sicuramente il mezzo più comune per accedere alla rete, anche gli smartphone e le console di gioco permettono, nella stragrande maggioranza dei casi, di servirsi di Internet e di altre applicazioni online.

*Utilizzo dei mezzi di informazione e comunicazione in modo da sostenere deliberatamente e ripetutamente comportamenti ostili da parte di individui o gruppi, intesi a danneggiare altri.

†Il termine (crasi delle parole inglesi sex (sesso) e texting (pubblicare testo) è un neologismo utilizzato per indicare l'invio di immagini sessualmente esplicite o di testi inerenti al sesso attraverso i mezzi informatici.

Capitolo 1

Safer Internet Work Programme

Il *Safer Internet Work Programme*[1] descrive ogni anno le attività che la Commissione Europea intende intraprendere riguardo alla sicurezza della rete, gli obiettivi da raggiungere, i criteri di ricerca, i risultati attesi, il budget disponibile per ogni tipo di soluzione proposta e fornisce, infine, informazioni sugli eventi previsti. Lo scopo generale del Programma è promuovere un utilizzo più sicuro di Internet e delle altre tecnologie, educare gli utenti - in modo particolare i bambini, i genitori e gli educatori - e combattere contro contenuti illegali o condotte violente assunte online. La forma principale di contenuto illegale coperta dal Programma è il materiale riguardante abusi sull'infanzia, razzismo e xenofobia. Per quanto riguarda , invece, le condotte violente, particolare importanza assumono i fenomeni del grooming* e del cyber-bullying.

Possiamo definire contenuto nocivo tutto ciò che genitori, insegnanti, assistenti sociali ed altri adulti responsabili dei bambini considerano dannoso. Il concetto di cosa sia nocivo, ovviamente, varia a seconda dei Paesi e delle culture. Esistono, comunque, diversi mezzi per combattere contenuti di questo tipo, ognuno dei quali ha bisogno di essere usato in combinazione con gli altri per incrementare la propria efficacia: strumenti tecnici, educazione e sensibilizzazione, rafforzamento delle disposizioni legali (qualora esistano).

Il centri Safer Internet promuovono campagne di sensibilizzazione pubblica trasmettendo un messaggio positivo sulle opportunità di un utilizzo più ampio ed intenso delle tecnologie di informazione e comunicazione, fornendo contemporaneamente adeguate informazioni sui rischi e i modi in cui evitarli.

*Per grooming si intendono tutte quelle azioni deliberatamente intraprese allo scopo di stabilire una connessione emotiva con un bambino, in modo da ridurne le inibizioni preparandolo ad attività sessuali o allo sfruttamento.

Capitolo 2

Parental Control Tool

Come già anticipato nell'introduzione, i *Parental Control Tool* sono strumenti in grado di proteggere bambini e adolescenti dalle insidie della rete. E' possibile identificare almeno tre modi in cui è possibile servirsene: installazione client su un PC; sottoscrizione ad un servizio di filtro online, che non ha bisogno di essere installato sul PC; una combinazione di entrambe le soluzioni. I Parental Control Tool consentono principalmente di eseguire tre tipi attività per proteggere i minori:

- ◇ **Personalizzazione dei filtri da applicare al contenuto Web:** lasciare che i minori possano unicamente accedere a contenuti appartenenti a criteri definiti durante la fase di configurazione del tool; è possibile bloccare o meno contenuti riguardanti un determinato argomento, una lista di URL o specifiche parole chiave.
- ◇ **Blocco dell'utilizzo:** bloccare l'utilizzo di un protocollo o di un'applicazione a prescindere dal contenuto.
- ◇ **Monitoraggio delle applicazioni e del contenuto Web a cui si ha accesso:** visualizzare un resoconto di *se*, *quando* e *quanto* il bambino ha avuto accesso ad un determinato sito web.

I tre principali problemi a cui un tool deve essere in grado di far fronte sono la visualizzazione di contenuti inappropriati, il divenire vittime di comunicazioni dannose e il trascorrere troppo tempo su Internet o utilizzando una certa applicazione.

I parametri di classificazione di un tool sono essenzialmente quattro:

Funzionalità Le funzionalità che il tool è in grado di fornire con successo.

Sicurezza La resistenza del tool a tentativi di by-pass tramite azioni specifiche.

Efficacia Quanto il tool è in grado di bloccare contenuti nocivi e di permettere contenuti non dannosi.

Usabilità Quanto il tool risulta facile da installare, configurare ed usare per l'utente medio.

In questa relazione ci serviremo dei risultati rilasciati il 13 gennaio 2011 dal *SIP-Bench II*, progetto finanziato dall'Unione Europea [2].

I criteri che determinano la scelta del tool più appropriato dipendono, naturalmente, dal tipo di attività che si intende esguire; non esiste un tool perfetto: i genitori dovrebbero cercare, quindi, quello che più degli altri fa fronte alle proprie necessità, trovando un giusto equilibrio tra funzionalità offerte, efficacia, sicurezza e usabilità.

Per quanto concerne le funzionalità del tool, se si è già in possesso della periferica di comunicazione, la prima caratteristica da valutare è sicuramente la compatibilità; bisogna controllare, infatti, che il tool sia compatibile col sistema operativo (ad esempio Windows, Linux, Mac OS X) e la relativa versione (ad esempio XP, Vista, 7). Inoltre, se l'accesso alla periferica è aperto a più di un bambino con differenti necessità di filtro, è necessario creare e gestire più di un utente con caratteristiche specifiche e personalizzate. Le funzionalità messe a disposizione da questo tipo di strumenti sono diverse e dipendono dallo specifico tool preso in considerazione. In generale, è possibile creare una lista di parole chiave in modo da evitare tutte le pagine web che le contengano, o impostare delle restrizioni di tempo sull'utilizzo della periferica da parte del minore. Alcuni tool consentono anche di bloccare determinati protocolli o applicazioni e di monitorare completamente l'attività del bambino sia dal punto di vista delle applicazioni utilizzate, che dai contenuti visualizzati sul web. E' possibile, ad esempio, bloccare totalmente la navigazione web, o applicazioni che consentono la visualizzazione di immagini e video in streaming, o ancora la condivisione di contenuti tramite operazioni di upload e download (FTP/P2P). Ad ogni modo, una delle preoccupazioni maggiori da parte dei genitori è costituita dalle possibilità di comunicazione con il mondo esterno che la rete offre. Infatti, gli strumenti di comunicazione rappresentano un'importante opportunità per bambini e ragazzi per condividere opinioni e creare nuove amicizie; ciò nonostante, essi sono al tempo stesso pericolosi, poichè i minori potrebbero facilmente entrare in contatto con persone potenzialmente pericolose che approfittano dell'anonimato garantito dallo username. In questi casi è possibile bloccare applicazioni che permettono di chattare e inviare messaggi o email a specifici contatti (ad esempio Skype, Msn Messenger, IRC, email client, webmail provider).

Per quanto riguarda, invece, la sicurezza del tool da utilizzare, è importante sottolineare che, soprattutto gli adolescenti, potrebbero essere in grado di bypassarlo o disinstallarlo. Sarebbe bene, quindi, selezionare at-

tentamente il tool tenendo conto della sua resistenza a differenti tipi di violazioni, quali:

- ◇ **Bypassare il tool accedendo alle pagine proibite:** usando gli indirizzi IP, servizi di traduzione online, la cache di Google, un browser alternativo;
- ◇ **Bypassare il tool modificando le impostazioni relative ai limiti di tempo**;
- ◇ **Disabilitare il tool:** chiudendolo attraverso il Task Manager, disinstallandolo senza la richiesta di una password, usando un Live CD in sostituzione del sistema operativo di default, formattando l'hard disk.

Nelle prossime sezioni analizzeremo con maggior dettaglio le caratteristiche dei Parental Control Tool disponibili, rispettivamente, per PC, smartphone e console.

2.1 Parental Control Tool per PC

I PC sono sicuramente il mezzo più comune per navigare in Internet e consentono agli utenti di accedere alle pagine web, condividere esperienze e contenuti tramite i social network, comunicare con altre persone.

Nell'analisi dei tool disponibili prenderemo in considerazione i fattori a cui abbiamo precedentemente accennato, ossia le funzionalità, la sicurezza, l'efficacia e l'usabilità.

2.1.1 Funzionalità e Sicurezza

Nessuno dei tool presi in esame raggiunge il massimo grado di funzionalità (in una scala da 0 a 4). I prodotti con i tre punteggi più elevati sono risultati **Vise [3.5], CyberSieve [3.4]** e **Windows Vista [3.2]**. Vediamo nel dettaglio quali caratteristiche sono state considerate nella valutazione dei tool esaminati servendoci delle tabelle 2.1 e 2.2 che illustrano i risultati ottenuti dai test svolti nell'ambito del progetto. Le tabelle mostrano le capacità di ogni singolo tool [Yes/No] nel soddisfare le necessità più comuni. Se il prodotto esaminato ha superato il test, nella cella corrispondente della tabella viene assegnata la lettera Y; in caso contrario, la lettera N. Le ultime due colonne della tabella 2.2 indicano, rispettivamente, il tasso di funzionalità [F] e quello di sicurezza [S] in una scala da 0 a 4.

Y:	Yes
N:	No
Y:	Web-based only (web-based streaming or email)
B:	Block
M:	Monitor
Cf:	Contact Filter
B/W list:	Black/White list
W, M, L (OS):	Windows, Mac, Linux

Area of need	Compatibility	Users	Filtering customization			Keywords	Time	Usage restriction						
Functionality	OS	Mgmnt	Content filtering			keywords	Time	Web access		Streaming		P2P		FTP
Specific issue	W/M/L	Mgmt of users	Topics	Urls White	Urls Black list	B/W list	Time limit	B	M	B	M	B	M	B
Vise	W	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	Y
CyberSieve	W	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	Y
Windows Vista	W	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	Y	N	Y
PureSight	W	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	N
Intego	M	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	Y
Kaspersky ISS	W	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	N
Safe Eyes	W, M	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	Y
Profil	W	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	Y	N	N
TFK	W	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	Y	N	N
Mac OS X	M	Y	N	Y	Y	N	Y	Y	Y	Y	Y	Y	N	N
Optenet	W	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	Y	N	Y
CA Security S.	W	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	Y	N	N
Cyber Patrol	W	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	Y	N	N
CYBERsitter	W	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	Y	N	N
Net Nanny	W	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	Y	N	Y
eScan	W	N	Y	Y	Y	Y	Y	Y	Y	Y	N	N	N	N
Trend Micro	W	Y	Y	Y	Y	N	Y	Y	Y	Y	N	N	N	N
Brightfilter	W	Y	Y	Y	Y	N	Y	Y	N	Y	N	N	N	N
Norton ISS	W	Y	Y	Y	Y	N	Y	N	Y	Y	N	N	N	N
F-Secure	W	N	Y	Y	Y	N	Y	Y	Y	Y	N	N	N	N
OpenDNS Basic	W, M, L	Y	Y	Y	Y	N	N	Y	N	Y	N	Y	N	N
McAfee IS	W	Y	Y	Y	Y	N	Y	Y	N	Y	N	N	N	N
Norman	W	Y	Y	Y	Y	N	Y	Y	Y	Y	N	N	N	N
FilterPak	W	Y	Y	N	N	N	N	N	Y	N	N	N	N	N
Alice	W	N	Y	N	N	N	N	N	N	Y	N	N	N	N
Zone Alarm	W	N	Y	N	N	N	N	N	N	Y	N	N	N	N

Figura 2.1: Tabella delle funzionalità per PC (a)

Area of need	Usage restriction related to communication activities										F	S
Functionality	IRC			Skype			MSN			email		
Specific issue	B	M	Cf	B	M	Cf	B	M	Cf	B	Score	Score
Vise	Y	Y	Y	Y	Y	N	Y	Y	N	Y	3,5	1
CyberSieve	Y	Y	N	Y	Y	N	Y	Y	N	Y	3,4	1
Windows Vista	Y	Y	N	Y	Y	N	Y	Y	N	Y	3,2	1
PureSight	Y	Y	Y	N	N	N	Y	Y	Y	Y	3,0	4
Intego	N	N	N	Y	Y	N	Y	Y	N	Y	3,0	2
Kaspersky ISS	N	N	N	Y	Y	N	Y	Y	Y	Y	3,0	1
Safe Eyes	N	N	N	Y	Y	N	Y	Y	N	Y	3,0	1
Profil	N	N	N	Y	Y	N	Y	Y	Y	Y	2,9	4
TFK	N	N	N	Y	Y	N	Y	Y	N	Y	2,7	1
Mac OS X	N	N	N	Y	Y	N	Y	Y	N	Y	2,6	4
Optenet	Y	N	N	Y	N	N	Y	N	N	Y	2,6	1
CA Security S.	Y	N	N	N	N	N	Y	Y	Y	Y	2,4	4
Cyber Patrol	N	N	N	Y	N	N	Y	N	N	Y	2,4	2
CYBERsitter	N	N	N	Y	N	N	Y	N	N	Y	2,4	1
Net Nanny	N	N	N	N	N	N	Y	Y	N	Y	2,2	4
eScan	N	N	N	N	N	N	N	N	N	Y	1,4	4
Trend Micro	N	N	N	N	N	N	N	N	N	Y	1,4	1
Brightfilter	N	N	N	N	N	N	Y	N	N	Y	1,4	0
Norton ISS	N	N	N	N	N	N	N	N	N	Y	1,3	4
F-Secure	N	N	N	N	N	N	N	N	N	Y	1,3	1
OpenDNS Basic	N	N	N	N	N	N	N	N	N	Y	1,3	0
McAfee IS	N	N	N	N	N	N	N	N	N	Y	1,3	0
Norman	N	N	N	N	N	N	N	N	N	N	1,3	0
FilterPak	N	N	N	N	N	N	N	N	N	Y	0,6	1
Alice	N	N	N	N	N	N	N	N	N	Y	0,5	4
Zone Alarm	N	N	N	N	N	N	N	N	N	Y	0,5	4

Figura 2.2: Tabella delle funzionalità per PC (b)

2.1.2 Efficacia

L'efficacia di un tool viene calcolata sulla base delle sue performance nel bloccare i contenuti dannosi per i minori e nel consentire quelli sicuri. Quando ciò non avviene alla perfezione, ci si può imbattere in due fenomeni opposti: l'*underblocking* e l'*overblocking*. Il primo si verifica quando un tool permette di accedere a del contenuto nocivo, il secondo quando viene bloccato del

contenuto sicuro. Pertanto, il tasso di underblocking indica quanto il contenuto dannoso non è filtrato; il tasso di overblocking quanto il contenuto sicuro viene bloccato. Un tool ottimale sarà caratterizzato, quindi, da bassi valori di underblocking e overblocking. La tabella 2.3 mostra l'efficacia dei tool (in %) nel bloccare il contenuto a seconda dell'argomento.

Topic	Adult content		Violent		Racist		Drugs		Crime		Selfdamage		Gambling	
	Overblocking	Underblocking	Overblocking	Underblocking	Overblocking	Underblocking	Overblocking	Underblocking	Overblocking	Underblocking	Overblocking	Underblocking	Overblocking	Underblocking
Alice	2	76	1	93	6	67	3	56	7	68	14	93	23	46
Brightfilter	16	20	13	48	16	40	17	26	54	45	16	40	38	24
CA Security S.	30	23	11	57	12	47	21	26	45	47	19	49	41	31
CyberPatrol	12	18	14	77	22	67	23	49	23	49	48	57	37	13
CyberSieve	16	54	12	90	32	73	37	52	32	63	19	83	41	19
CYBERsitter	9	29	8	90	11	82	9	85	20	67	12	85	15	63
eScan	56	41	5	71	16	80	50	51	36	85	13	65	90	50
FilterPak	10	89	15	94	15	87	13	86	15	69	14	95	13	84
F-Secure	0	32	0	87	0	92	0	77	2	96	0	97	0	68
Intego	7	57	1	95	1	96	1	78	15	95	2	97	0	95
Kaspersky ISS	28	19	5	73	10	85	29	40	56	55	2	95	52	36
Mac OS X	16	17	11	78	20	85	0	91	0	94	0	96	0	85
McAfee IS	8	20	1	67	0	55	5	32	22	60	0	80	23	23
Net Nanny	18	44	4	87	16	53	41	31	23	59	6	86	55	32
Norman	12	86	14	93	16	87	11	86	14	69	12	96	7	84
Norton ISS	6	33	12	88	17	69	16	88	3	55	4	79	2	61
OpenDNS Basic	2	71	0	88	0	82	1	81	2	64	0	92	12	75
Optenet	19	22	4	62	10	46	9	23	45	50	3	79	27	23
Profil	13	45	2	77	3	53	2	63	2	63	8	89	5	61
PureSight	14	39	5	75	6	57	10	42	19	59	8	81	18	60
Safe Eyes	20	16	14	49	2	50	17	29	18	63	11	58	25	29
TFK	0	45	5	89	0	71	5	58	4	66	2	70	0	71
Trend Micro	7	79	1	84	3	66	2	53	26	59	3	75	19	56
Vise	50	36	51	34	73	34	62	37	100	32	64	35	34	40
Windows Vista	30	14	26	56	48	54	46	24	65	45	42	53	50	63
Zone Alarm	2	76	1	93	6	67	3	56	7	68	14	93	23	46

Figura 2.3: Efficacia in relazione all'argomento

2.1.3 Usabilità

Abbiamo già definito precedentemente l'usabilità di un tool come quanto questo risulti, per l'utente medio, facile da installare, configurare ed usare. I tre migliori prodotti testati sono risultati **CyberPatrol [3.32], Kaspersky [3.14]** e **OpenDNS [3.11]**. Alcuni dei tool presentano procedure di installazione e configurazione decisamente semplici per evitare errori da parte dell'utente, ma le possibilità di personalizzazione sono di conseguenza molto povere. Al contrario, altri tool sono caratterizzati da opzioni di configurazione molto estese, ma il rischio di eventuali errori in questo modo aumenta. La tabella 2.4 illustra i risultati ottenuti dai test.

[I = Installation , C = Configuration, U = Usage]

Usability Tests	Alice *	Brightfilter	CA Security Suite	CyberPatrol	CyberSieve	CyberSitter	eScan	FilterPak	F-Secure	Intego	Kaspersky ISS	Mac OS X	McAfee IS	Net Nanny	Norman	Norton ISS	OpenDNS Basic	Optenet	Profil	PureSight	Safe Eyes	TFK	Trend Micro	Vise	Windows Vista	Zone Alarm
I	/	2,4	2,92	2,4	2,54	2,4	2,4	2,5	3,19	2,8	2,9	/	2,8	2,5	3,3	3,07	2,9	2,2	2,68	2,75	2,3	2,1	2,5	2,3	/	2,6
C	/	3,5	2,78	3,8	2,82	3,01	2,2	2,2	2,36	2,5	3,3	2,6	2,7	2,6	2,6	2,73	3,4	2,3	2,59	2,94	2,62	2,5	3	2,1	3,2	2,4
U	/	2,1	1,96	3,2	2,22	1,6	2,7	1,9	2,33	3,2	3,2	2,8	2,5	2,4	1,6	2,05	2,8	1,7	3,23	2,45	2,5	1,9	2,8	2,4	2,4	1,9
Overall score	/	2,9	2,6	3,3	2,6	2,5	2,4	2,2	2,5	2,8	3,1	2,7	2,6	2,5	2,4	2,6	3,1	2,1	2,8	2,8	2,5	2,2	3	2	3	2,3

Figura 2.4: Risultati relativi all'usabilità

2.2 Parental Control Tool per Smartphone

Gli smartphone sono una delle periferiche maggiormente di moda tra i più giovani per accedere ad Internet, guardare video in streaming e comunicare con altre persone usando applicazioni specifiche come quelle di messaggistica instantanea. Tuttavia, ci sono pochi strumenti che consentono di filtrare il contenuto delle pagine web su smartphone e il loro utilizzo è limitato a determinati Paesi (ad esempio, *RubyStar* per *Symbian OS* in Europa è disponibile unicamente per il Regno Unito e l'Irlanda). Il progetto a cui facciamo riferimento in questa relazione ha basato i propri test su due differenti dispositivi/sistemi operativi: **iPhone 3GS** e **Nokia E75 - Symbian 3.1**. L'iPhone fornisce un proprio parental control tool che consente di limitare l'utilizzo di alcuni protocolli/applicazioni come l'accesso ad Internet, YouTube, email; permette anche di filtrare il contenuto sulla base di valutazioni nazionali. Ciò nonostante, è comunque necessario utilizzare un tool esterno per filtrare il contenuto delle pagine web in base all'argomento. Le tabelle in figura 2.5 illustrano, rispettivamente, le principali funzionalità dei tool interni agli smartphone testati e di quelli esterni.

Y: Yes

Y*: Yes for YouTube only

Y:** Yes for Podcasted music, video

N: No

B: Block

M: Monitor

Cf: Contact filter

B/W list: Black and or White list

Embedded Parental control tool

Area of need	Usage restriction												Usage restriction related to communication										
Functionality/Specific issue	Web access	Application running		Application download		Application Purchase		Video streaming		Video playing			Skype			MSN			email				
	B	B	F	B	F	B	F	B	F	B	F		B	M	Cf	B	M	Cf	B				
iPhone 3GS	Y	Y	Y	Y	Y	Y	Y	Y*	Y**	Y	Y		N	N	N	N	N	N	Y				
Nokia E75 - Symbian 3.1	N	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A		N/A	N/A	N/A	N/A	N/A	N/A	N/A				

External Parental control tool

Area of need	Compatibility	Filtering customization				Keywords	Time	Usage restriction				Usage restriction related to communication									
Functionality/Specific issue	OS	Content filtering				Keywords	Time	Web access		Streaming		Skype			MSN			email			
		Web filtering	Topics	Urls White list	Urls Black list	B/W list	Restriction	B	M	B	M	B	M	F	B	M	F	B	Score	Score
SafeEyes Mobile (iPhone 3GS)	iPhone 3.0 or later	Y	Y	Y	Y	N	N	N	N	Y	N	N	N	N	N	N	N	Y	1,4	0
Security Shield 8.8.13 (Symbian 3.1)	BlackBerry, Symbian, Windows Mobile, or Android	N	N	N	N	Y[email]	N	N	N	N	N	N	N	N	N	N	N	Y	0,2	0

Figura 2.5: Tabella delle funzionalità per smartphone

2.3 Parental Control Tool per Console

Lo scopo delle console è prima di tutto il gioco, piuttosto che fornire accesso ad Internet. Ad ogni modo, esse vengono anche utilizzate per giocare online, chattare con altri giocatori ed effettuare operazioni di download. Tutte le console testate (**Wii, PS3, Xbox 360**) hanno il proprio parental control tool interno, ma nessuno di questi è capace di filtrare le pagine web a seconda dei contenuti. Le due console che abilitano l'utente alla navigazione web (Wii e PS3) possono servirsi di un tool esterno (rispettivamente *Astaro* e *Trend Micro Kids Safety*) per consentire di filtrare le pagine in base agli argomenti trattati. Per quanto riguarda l'Xbox, il problema non si pone in quanto quest'ultima non permette all'utente di navigare in rete.

Y: Yes

N: No

N/A: Not Available

B: Block

M: Monitor

Cf: Contact filter

F: Filter

B/W list: Black and or White list

External parental control tool

Area of need	Web content filtering	Users' profile	Filtering Customization			Keywords	Time restrictions	F	S
Functionality /Specific issue	Filtering of web-pages	Management	Topic filtering	Black list	White list	Keywords	Time limit settings	Score	Score
Astaro (Wii)	Y	N	N	N	N	N	N	0,6	4
Trend Micro Kids Safety (PS3)	Y	N	N	N	N	N	N	0,6	2
N/A (Xbox 360)	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A

Embedded parental control tool

Area of need	Web Access	Content Purchasing	Online communication		Online Gameplay	
Functionality /Specific issue	Blocking access to the Internet	Content purchase blocking	Chat		Gameplay	
			B	F	B	F
Wii	Y	Y	Y	N	Y	N
PS3	Y	Y	Y	N	Y	Y
Xbox 360	Y	Y	Y	Y	Y	Y

Figura 2.6: Tabella delle funzionalità per console

Capitolo 3

Esempi

In questa sezione cercheremo di vedere come funzionano nella pratica i parental control tool di cui abbiamo ampiamente discusso nel capitolo precedente. Abbiamo deciso di prendere in considerazione i tool interni offerti da due dei sistemi operativi più diffusi, Mac OS X e Windows 7.

3.1 Mac OS X Parental Control Tool

Il filtro per contenuti Internet è integrato all'interno del sistema operativo e consente di limitare l'accesso a Internet indipendentemente dal browser web utilizzato. l filtro può operare in tre diverse modalità:

1. **Illimitato:** la navigazione non viene limitata, ma i siti web visitati dall'account vengono memorizzati in un registro e sono possono essere consultati dall'amministratore.

2. **Automatico:** il filtro tenta di bloccare i siti web che presentano contenuti inadatti. Per farlo, viene utilizzata la stessa tecnologia usata dall'applicazione Mail per identificare i messaggi indesiderati. Il filtro è in grado di identificare con un alto livello di precisione se una pagina Web è sicura o meno basandosi sull'esame di diverse caratteristiche del sito, compresi il testo e la struttura. Inoltre, vengono bloccati tutti i siti Web che si identificano come siti per adulti con i sistemi di classificazione RTA[3] o SafeSurf[4] e forza ricerche sicure in alcuni motori di ricerca. In questo modo il filtro per contenuti Internet registra tutti i siti Web visitati e bloccati e li contrassegna come tali in un registro specifico.

3. **White list:** il filtro blocca tutti i siti web che non si trovano nell'elenco. Tuttavia, nel caso di molti siti Web, il filtro tiene conto del nome del dominio, non del percorso. Ad esempio, se `http://www.example.com`

viene aggiunto all'elenco, `http://pictures.example.com` verrà autorizzato, come anche `http://www.example.com/movies`. Anche in questo caso i siti web visitati e bloccati vengono registrati e possono essere aggiunti o rimossi dalla lista successivamente.

E' importante notare che, in alcuni casi, il filtro automatico potrebbe bloccare per errore un sito web sicuro o consentire l'accesso ad un sito per adulti. Ciò potrebbe verificarsi, ad esempio, se il sito utilizza un linguaggio non comune, oppure se nella pagina non sono quasi presenti elementi di testo. Tuttavia, l'utente può consentire l'accesso ai siti web bloccati per errore e viceversa autenticandosi come amministratore.

Inoltre, il filtro non è in grado di analizzare i contenuti crittografati tramite crittografia SSL (l'url solitamente inizia con https). Per questo motivo, i siti web crittografati che non si trovano nella White list verranno bloccati dal filtro automatico.

3.2 Windows 7 Parental Control Tool

Windows 7 fornisce degli strumenti integrati nel sistema operativo attraverso i quali è possibile impostare dei limiti temporali in modo da controllare quanto tempo il bambino trascorre davanti al pc e decidere quali giochi e/o applicazioni possono essere utilizzate e quando. Per quanto riguarda la sicurezza online, invece, è necessario utilizzare *Windows Live Family Safety*. L'applicazione consente di gestire in remoto i siti web a cui il minore può avere accesso, di eseguire ricerche sicure tramite Bing, Google, Yahoo! e altri popolari motori di ricerca, di limitare l'accesso ai contatti approvati di *Windows Live Hotmail* e *Windows Live Messenger* e di monitorare le attività online.

Conclusioni

In questa relazione ci siamo occupati del problema del Safer Internet, cercando di analizzare da diversi punti di vista le soluzioni proposte dai diversi tool esistenti per ovviare ai rischi a cui la rete espone i suoi utilizzatori più giovani.
Le soluzioni gratuite più valide sono rappresentate sicuramente dai tool interni ai sistemi operativi Windows e Mac OS X, che, come abbiamo visto, offrono buone funzionalità e discreti livelli di efficienza e sicurezza e consentono, senza alcuna spesa aggiuntiva, di gestire e monitorare l'attività del bambino/adolescente su Internet.

Dai risultati ottenuti possiamo affermare che, sebbene un prodotto perfetto non esista, esistono tool validi che possono adattarsi alle più svariate situazioni e vengono incontro alle esigenze dei genitori. Ciò nonostante, è necessario ricordare che, attualmente, la maggiorparte dei tool funziona in modo ottimale unicamente per la lingua inglese e non esistono ancora prodotti eccellenti per le altre lingue.

Bibliografia

[1] Commission of the European Union. Safer Internet Work Programme 2011. http://ec.europa.eu/information_society/activities/sip/index_en.htm, March 2011.

[2] Cybion Srl and Stiftung Digitale Chancen coordinated by Innova Europe. Benchmarking of parental control tools for the online protection of children - SIP-Bench II. http://ec.europa.eu/information_society/activities/sip/projects/filter_label/sip_bench2/index_en.htm, January 2011.

[3] http://www.rtalabel.org/.

[4] http://www.safesurf.com/ssplan.htm.

[5] http://en.wikipedia.org/wiki/Cyber-bullying.

[6] http://it.wikipedia.org/wiki/Sexting.

[7] Mac OS X v10.5, 10.6: About the Parental Controls Internet content filter. http://support.apple.com/kb/ht2900.

[8] Windows 7 - Parental Control Tool Features. http://windows.microsoft.com/en-US/windows7/products/features/parental-controls.