KidSafe parental control software white paper
Authors: Mike Collins, Stjohn Goldfinger
Revision: 4.4, Date of issue: 2009-09-16

This document will outline the problems parents face when their children regularly use a computer that may also be connected to the internet. We will describe our development strategy to combat these potential problems and our parental control software features. Hopefully after reading this document the danger areas each feature solves will then be fully understood by the parent or involved adult. Finally we offer a comparison between our KidSafe Total Control software and secure USB key against other parental control software products available today.

We have broken the document down into the following sections:

- **Problem Areas** – analysis of the actual problems faced by parents.

- **Behavioural Patterns** - the patterns of behaviour that result in children's safety being compromised.

- **Microsoft Windows inbuilt parental control features** – description and analysis of the drawbacks and limited approach of the parental control systems and functionality within the Windows Operating system.

- **KidSafe Total Control and secure USB key Product Suite** – the KidSafe product development concept and how it addresses the above problem areas.

- **Comparative View –** a look at how the KidSafe Total Control compares against other existing parental control products, and why it is largely inaccurate to attempt this comparison.

Problem Areas

Instead of making simple functional comparisons between one product and another, it is more accurate first to look at the problems faced by parents, their families, the patterns of behaviour and the actions undertaken by their children that can often lead them into trouble or areas where they really need help and guidance.

There are two fundamental problem or danger areas involving computer internet usage that we should examine:

1. The first is children looking at inappropriate content for example pornography or drugs related pages and other material deemed objectionable by the child's parents or guardians.

2. The second is the danger of children communicating with online predators and paedophiles.

These two problems are very different in the way they manifest themselves and need addressing in an equally different manner. It could be argued that the second problem area is the most concerning and because of this, we have looked very carefully at how kids end up "*talking*" to strangers on the internet. You should take into consideration that statistically speaking presently 97% of child abuse occurs in cases where the abuser knows the family or child personally so let us not take these concerning issues out of proportion to the likely hood of

occurrence. Unfortunately however trends and effects are constantly shifting so knowledge and guidance is the key to the safety and wellbeing of your family.

We have conducted a real-life study of based on my daughter and her friend's use of the Internet. From this detailed and personal family analysis, it was possible to practically look at how we could address these danger areas. More specifically we created the KidSafe Total Control software and secure USB key. These problems are growing exponentially and are far more complex than simply:

- filtering and logging internet traffic
- monitoring messaging clients and chat sessions for phrases like 'SEX' or 'WHAT IS YOUR AGE'
- blocking bad websites

Although we do think that some difficult situations can call for difficult decisions to be made we believe that privacy should be invaded only where absolutely necessary.

Equally important areas of concern and consideration relate not only to internet usage but to computer usage in general. It would appear kids are spending more and more time in front of the monitor screen and keyboard as opposed to the television set. The computer is the new and grossly more powerful silicon ray tube. Consider:

3. Emotional, intellectual and psychological development of young minds and nascent personalities.

4. Health wellbeing and fitness of young bodies.

Spending large amounts of time online or sitting gaming for hours on end can't be good for the health, wellbeing of fitness or young bodies. Increasingly this type of prolonged activity is being linked to the early onset of weight problems and the retardation of psychological and intellectual development.

The following section details the patterns of behaviour (computer and internet usage) as shown by children and teenagers. It also shows how this can result in contact with unknown parties.
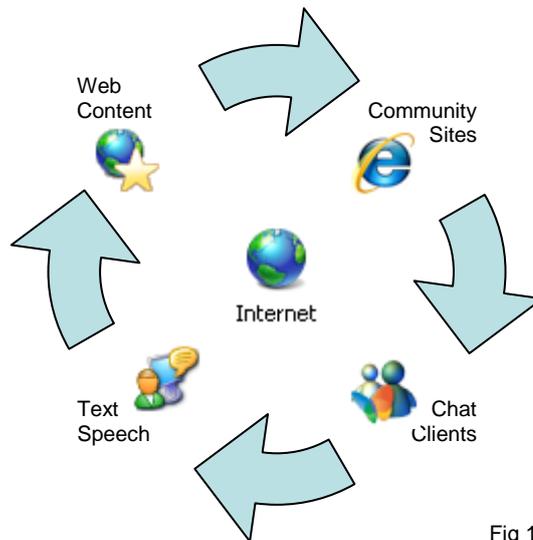
Behavioural Patterns:

Fig 1 – show cycle of behaviour

1. **Community Sites** – the current web trend throughout the UK, Europe and US is for kids to use community websites. The most common and well established of these are www.myspace.com, www.facebook.com, www.youtube.com and www.bebo.com.

   These websites allow users (especially kids) to create there own profile and mini-domains. The personal profiles can include musical preferences, self written blogs, video and picture archives. Most sites have a minimum age policy (14+) but there is usually no verification of this policy at all. Lots of kids and teenagers love these sites because they allow them a degree of freedom and individuality that they may not normally enjoy at home or be ready for.   It also gives them a community medium to express opinions and thoughts that are often given more credence because the true age and identity of the writer can easily be hidden. There are countless news articles about kids using and writing blogs that appear to be from adults.

   In addition to the blogs, these sites provide facilities to publish pictures and allow other users the option to comment on these and leave private messages. Combine this with the current trend for mobile phones to have cameras and video clip features then it is a simple process for kids to upload their pictures and videos to their online profile for the world to see.

   The sites allow and encourage sharing of this personal information by making it easy for users to add friends and friends of friends to their online profile. Friend's pictures are displayed on each profile, this creates a popularity contest. The more friends you have, or appear to have (no one really has 300 friends) the more popular and *'cool'* you are or appear to be.

   This is a potential cause for concern. It is a simple matter for a child abuser, predator or paedophile to set up a fictitious MySpace account and pose as another teenager or even friend of another teenager, complete with pictures, friends (so called) and glowing profile. This then gives them unlimited access to the online profiles of every child, teenager and user of

that community site linked to that friend. Once they have found a potential target, they establish contact by posting messages and comments on the kid's blog and on their pictures.

Because the child has published a detailed profile of themselves, it is easy for the abuser to build up a relationship as they already know a lot of personal details and interests (favourite music, bands, hobbies, gripes and worries).

Kids and teenagers are very keen to add other people to the friends listing, to increase there perceived popularity. Thus the potential abuser is added and enters into a supposed network of trusted friends. Once a person is considered to be a friend, kids are then happy to exchange 'MSN 'addies' (addresses), if it is not already published on their profile. Thus the online predator or paedophile is introduced into the child's circle of trust and can begin grooming a potential victim.

2. **Internet messaging or chat clients** – all children and teens are using chat (internet messaging) based applications (MSN messenger, yahoo chat and AOL chat) to talk or rather type to their friends. It's cheaper and more convent than sitting on the phone all night and also allows an almost total degree of privacy from what the child thinks are simply nosy parents who don't understand.

Chat clients can also allow people to exchange files (i.e. homework notes or photos etc.) and use webcams to see and interact with each other. This produces a virtual private network that parents have little or no knowledge of and no means of controlling, monitoring or providing help and guidance when necessary.

In addition to this, the retail price of laptop computers had plummeted making them an attractive Christmas or birthday present. A lot of kids and teenagers now have their own laptop which means that they can sit in their bedrooms, with total privacy and communicate with whoever they like. This is also compounded by the use of Wi-Fi, as it is a simple matter to piggy back onto the neighbours' wireless network if the parents turn off their own system. So it is important if parental control software solutions are used they be installed on the kids' computer, not just the network access device (modem or router). Many parents have found their teenagers sitting on the laptop in the early hours of the morning, when they assumed they were safely asleep in bed.

The use of webcams (with chat clients) has often been considered to be a potentially sleazy thing because the media has reported several cases where paedophiles and online predators have encouraged children to perform sexual acts with them. However, the webcam can also act as a positive tool in the whole internet schema. It is very difficult for a potential child-abuser to mask their appearance when using webcams. The problem is that quite often, the abuser has already won the confidence of the child. Once the child trusts the person, regardless whether they know their true identity or not, all means of communication become potential areas of abuse i.e. phone, chat, mobile, webcam and actual physical meetings. It is a dangerous misconception to make that children who are victims of online abusers are necessarily unaware of their true identity.

There have been some situations where children have been lulled into meeting an abuser, paedophile or online predator who they think is their own age but there are equally as many cases where abusers win over their trust and then gradually reveal their true identity.

Once a child has released their chat address, they are open to communications and persuasion from others who often are not who they claim to be. The chat medium is not like a phone conversation – you can not deduce anything from a typed conversation and it is easy to masquerade as someone else. Teenagers love the attention that they often get from online friends and often thrive on the fact that they have someone to talk to who appears to understand them. This can make them especially vulnerable.

3. **Text Speech** - with the advent of mobile phone text messages, people started to abbreviate the words that they used, because they had limited space to type and a message was restricted to 140 characters. This habit has spilled over to online chat-clients as well. Most likely because it is quicker to type and easier to communicate without the difficulty of learning to spell and punctuate correctly.

   What this means is that children type and communicate in a semi-cryptic language that is often very difficult to understand, follow, and decipher.

   In addition to this, it is a simple matter to replace 'sensitive' words. For example, if you replace the word 'sex' with 'lemon', it changes the whole context and structure of the conversation making it almost impossible to determine its true content. This also combats software systems that scan for prohibitive words and phrases.

4. **Web Content** - as explained previously, inappropriate web content is possibly not as dangerous as the threat posed by online predators, paedophiles and potential abusers. Some parents and families have more stringent views on pornography and drugs than others. Within this section, there are two distinct classifications

   > i) accidental exposure,
   > ii) deliberate exposure.

   The first classification is where children are accidentally exposed to inappropriate material online either from e-mail or inadvertent web searches and advertising pop-ups. Almost any user of the internet can be exposed to this and most are on a daily basis.

   The second classification is where the child deliberately tries to find this inappropriate content. This is usually via web searches and could be regarded as a problem that is caused mainly by boys. Boys are more likely to search for pornographic or drug related content than teenage girls. Regardless of your opinion towards pornography or drugs, most people would agree that there is some sensitive topics and subject material that are inappropriate for teenagers and young minds to see and to view on a regular basis.

Some observations about Microsoft Windows Vista parental control features – the good and unfortunately the bad.

The Good features:
One of the great features of the Windows Vista operating system is the myriad of parental controls now built directly into it to help parents designate and control where kids go and what they do on online. The controls can monitor and restrict what games the kids can play and what programs they can access. Not only does Windows Vista control what the kids can do, it can also set what time of day they are allowed on the computer via profiles you can set up.

All the controls are centralized in one location. You can access them by going to the User Accounts page and looking for the Family and Parental Controls applet. Using this one control panel, you can set which websites your kids are allowed to access.
From the easily accessible menu, you can generate activity reports that show where your child has gone and what they've done whilst logged in. You can use these reports to see what they were doing, or you can use the information as a feedback system to see if your parental controls are working. Often, you'll set up a website filter that won't work exactly as planned, so you can use the activity report to fine tune your settings.

One of the great controls Vista allows parents is a time limiter. With so many kids today spending hours on the computer, it could be sensible to limit the amount of time your child or kids are looking at the screen. A graph showing time usage by day and hour across the whole week tells you when peak computer use is. All you have to do to restrict their use by time is pull up a grid of the days and hours of a week and click the times that you don't want your kids to use the computer. You can then be sure that the parental controls will work reliably even when you are not there to enforce the rule.

The limitations:
After carefully reading the above you would think Microsoft parental control features have all the problems covered. Unfortunately although they quite obviously have very good intentions it is very hard to keep your eyes on all the balls all the time. Microsoft makes a great operating system but their product range is truly huge. We are now going to outline a few possible problems with their as implemented approach to solving the problems of integrating parental control features into an operating system.

It has been suggested and argued that the Microsoft's Windows product family (Windows 2000, Window XP Home/Professional, Windows 2003 and Windows Vista) offers all the features needed to protect children, teenagers and families on the computer and the internet. We will look at the parental control features offered by the various Windows products and highlight where they and how fail to deliver as promised. It is a dangerous misconception to make that Microsoft Windows parental control features alone will protect children. Bill Gates himself stated this point in an interview. He made it clear that the only way to protect children online was for parents and families to give good, solid parental guidance, help and advice as and where necessary. Some parents may feel that it is not their business what their kids do online, but the reality is that kids are curious, and if their behavior is not monitored closely, they can find themselves in a world they do not understand, or places full of information that they don't need to know yet. Help, support and guidance are key when it comes to keeping your kids and

family safe and happy online or when using the computer. With a little time, knowledge and tools like KidSafe Total Control to help, you can give your kids a full experience of the Internet and the computer without cutting them off or alienating them at a time when they may need your help most.

This is a philosophy that the KidSafe Total Control software and secure USB key inventors and developers endorse and advocate strongly. We have never stated that any of the KidSafe products will keep children totally safe – they are merely a great tool they will 'help' parents keep their kids' safe online or when using the computer. We can however say that the KidSafe Total Control product suite has been professionally designed to fit a specific purpose, whereas the Microsoft Windows operating system is aimed at a wide range of users, from home users up to enterprise organisations. The technology used by Microsoft is the same across all these platforms and as a massive organisation they may not able to concentrate solely on one very important area.

The MS Windows Vista parental control features detailed:

Vista Parental Control
- Web Filtering
- Time limitation
- Games control
- Application Limitations

Password Access Control

Windows Firewall

User Groups & Account Restriction
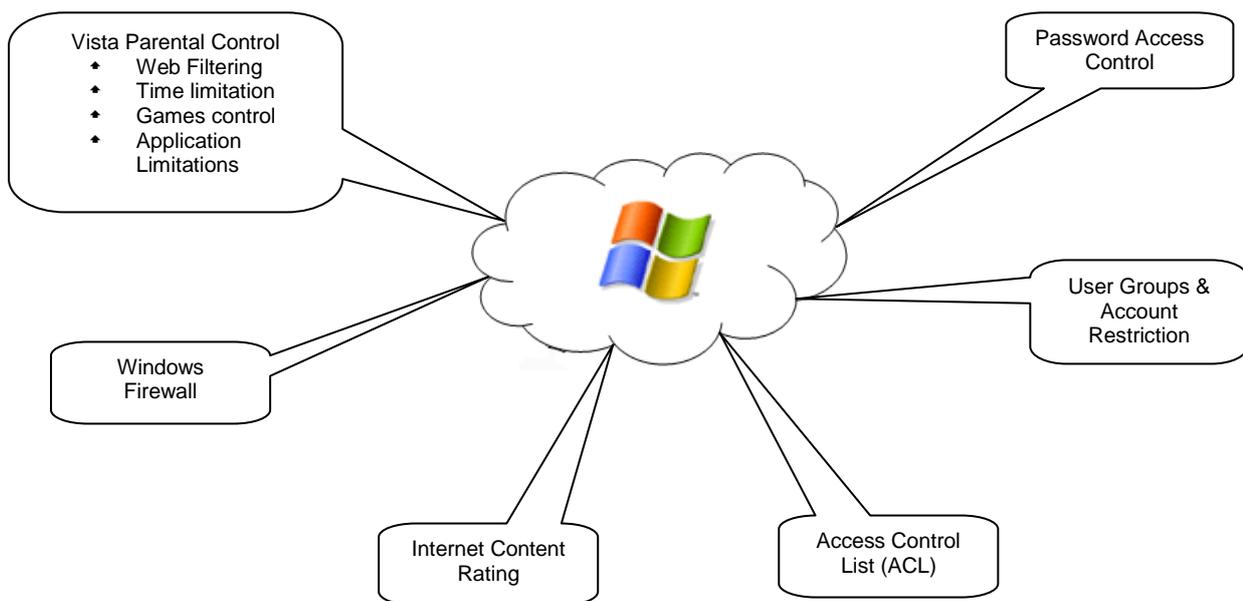
Internet Content Rating

Access Control List (ACL)

Fig 2 – Windows protection features

- **Password Access Control** – this forms the basis of access to a Windows platform. A user must logon to the system before they can use the computer or interact with the desktop. It is now commonly accepted that passwords are inherently weak and easy to circumvent. This can be done by a number of methods such as key board hooking (as described below) or simply 'shoulder surfing' (looking over the users shoulder whilst they type in the password).

   1) Most home and personal users do not have a good understanding of the importance of strong passwords. 45% of home users have passwords

which are based on personal information i.e. name, nickname, children's names etc. The remaining 55% do not have a password at all – it is a common feature in Windows XP Home and XP Professional to have auto-logon enabled, where the user does not have to enter any password. This is facilitated either by having no password set or by having the password stored in the registry in plain-text. A password stored in the registry is easy to access, read and bypass.   (see http://www.computerperformance.co.uk/Registry/registry_hacks_AutoAdminLogon.htm)

2) Windows offers programmers the ability to create what are known as 'hooking mechanisms' under the blanket of computer based training (CBT) systems. This was originally intended to allow companies to develop computer training systems, but it is now commonly used to create 'keyboard hooks'. These programmes are loaded by the operating system and allow the hooking application to preview and secretly save every key stroke. Keyboard hooks are a simple, effective and almost undetectable method of intercepting and capturing user passwords. Whilst this is not true for Windows logon password it is true for all application passwords and internet control passwords (see http://www.codeproject.com/dll/keyboardhook.asp?df=100&forumid=2388&exp=0&select=1941251 and http://www.codeproject.com/dll/Keyboardhook/Keyboardhook.zip).

3) Windows also allows the installation of GINA (Graphical Identification and Authentication) libraries. These libraries are used during the logon process and will intercept and store the user credentials (username, password and domain) in plain-text. There are hundreds of trojan GINA's available to download for free on the internet that are easily installed and will intercept and capture user logon details. Another interesting aspect of GINA libraries is their ability to elevate user permissions. A suitably tailored trojan-GINA can elevate a normal user to administration status which effectively means game over for any windows based parental control settings.

4) It is also possible to use specific hacking tools to break the encryption used on the SAM database (Windows password repository). The most well known of theses tools is *lophtcrack* which can break most password dumps within 24 hours. It also provides facilities to monitor network traffic for password data and to extract the password repository from Windows. (see http://sourceforge.net/projects/ophcrack/)

* **User Groups & Account Restrictions** – user groups and account restrictions form the basis of the control system enforced by the Windows operating system. Users of the computer are added to Groups, which are in turn given permissions to access various resources (files, program and peripherals) on that computer. Permissions (ACL) can be inherited by resources i.e. the files in a certain folder can inherit the folders permissions.

On the surface, user groups and account restrictions appear to be a solid and robust method of protecting and restricting access throughout the computer. However they become completely impractical and impossible to use for the following reasons:

1) Although user groups allow complex access profiles to be created, they

are also very complex to understand and use for a normal computer-user. Tailoring groups and accounts is a full time job for a network administrator and requires extensive training and knowledge, as well as third-party tools.

2) As with ALL aspects of Windows' control features, it relies on the premise that no user will have administration privileges. The protection mechanisms within Windows only work if you are not an administrator. Within a hardened domain this may be the case, but on home, personal and SMB (small medium business) computers this is not true. Based upon the complexity of setting up restrictions, most users opt to have administration privileges/accounts to allow them to simply use their computer.

3) In addition to this, on Windows XP Home edition, there is no facility to tailor user groups – a user is either and administrator or a standard user. The access permissions for the standard user group are so close to a guest account that it makes accounts under this group impossible to use. Most of the time, limited-users will not be able to access anything – from newly installed applications to simple sound card drivers.

4) Vista is faced with exactly the same problem. The system is so restrictive that the user either needs to be an administrator or is constantly clicking on prompts requesting access. This in it's self is a huge problem because users spend so much of their time clicking '*OK*' that when some really problematic happens, they just click '*OK*' anyway. Most users simply turn the extra 'security' features off to make the system useable.

5) Unless in a domain, user groups are practically impossible to setup and control. Again they require non-administrative permissions to be of any use.

6) Within your standard Windows installation, it is totally impractical to scroll through the whole system setting permissions on each and every application – there are 2500 executables on a clean Windows installation.

7) Because programs can be instructed to run under a different account, permissions can be bypassed using the Scheduling agent to launch process under its own context – which is that of LOCAL_SYSTEM. This account has full access to every aspect of the system and thus be easily used to bypass any application launching restrictions.

- **Internet Content Rating** – this forms the basis of the Microsoft attempt to tackle inappropriate web content and restrict access to sites. The content rating is based the ICRA / FOSI categorisation. In basic terms, website owners can voluntarily submit their website to ICRA for a categorisation. ICRA then creates an entry in their database that identifies what type of website it is. Whilst on paper this seems like a good idea, it practise it fails for many reasons:

  1) Primarily, the system is flawed because its voluntary. Webmasters simply cannot be bothered to submit their website. ICRA / FOSI only have 5000 sites categorised – of the 108 million sites on the internet, this only accounts for 0.0000462% which is entirely useless.

2) It is almost impossible to find a site classified or rated under ICRA.

3) Microsoft's implementation can work in two modes; the first is to block any prohibited sites or unrated sites. Based on the inability to find any sites classified by ICRA, this effectively blocks almost every site on the internet, including Microsoft's own site. This also includes Google and most other frequently used websites.

The second mode allows unrated sites to be viewed, whilst this makes the internet usable; it also means that you can access ANY sites that have not been rated by ICRA – which effectively means all sites barring the 5000 in their database.

Speaking simply system does not work at all!

4) Most importantly of all any internet options specified for the system only apply to Microsoft applications i.e. internet explorer. If a user were to install Firefox or one of the many other web browsers freely available it will function as normal with total disregard for any rating system.

5) The system for authorising blocked content is based on a password system – again this information can be captured using a simple keyboard hook.

6) This has no effect on chat applications or web-based chat clients

* **Vista's Parental Control, a summary:**
 The new features introduced into Vista in an attempt to address the concerns of parents appear great on the surface. Initially it looks like the control panel application offers many new features to help secure a computer user's experience. However upon closer inspection, there are little or no new working features in Vista's Parental Control. The applet is simply a wrapper for existing functionality that existed in Windows XP and we have already highlighted the flaws.

1) The web content rating system works exactly the same as in Windows XP and suffers exactly the same problems and un-workability.

2) The Gaming control is based on a voluntary rating system that the games developers can voluntarily conform to (or not).

3) The application restriction is based on white-listing which effectively means that the parent must specify every application that they wish their child to use. Analysis is currently being done to see how this listing may be bypassed using simple copy and paste methods and execution from removable devices such as a flash drive for example.

4) Finally, the overall access control system on which Vista is based - a password, which as we have seen is inherently insecure and easily circumvented when the users have physical access to the machine which of course they do in a home situation.

KidSafe software and secure USB key product suite and features:

This information is maintained and presented to show the logical progression that the KidSafe software product suite has made over the last three years and demonstrate the thinking behind the development of 'KidSafe Total Control' (KSTC).

'KSTC' has been made for use with windows Vista and Windows 7. We have taken KidSafe Parental Control, made improvements and built in many new features.

Based on the detailed analysis of the problem areas outlined in this document we have developed a software application which is specifically designed to address those areas.

Each product we have made is based and built upon the previous one. 'Total Control' was built upon 'Parental Control' and has all the functionality of the previous product with the additional features to differentiate it from the former.

We will now explain the features and function of each product.

'KidSafe Parental Control' (KSPC) software and secure USB key
Availability: Superseded by 'KidSafe Total Control'

KSPC is for parents who have little or no knowledge of how the computer works. If the kids know more about using the computer than you expect KSPC to fit your needs.

It is easy to install, use and is a simple concept to grasp. The token is like a key to the computer, when the parent has the key, they can be certain that their children are not using it, just like the keys to the car.

KSPC used a single key to control computer access. No key, no computer! The software fully integrated into the Windows operating system which meant it was very difficult to remove, stop or disable.

Features include:

- Two factor RSA authentication. The secure KidSafe USB key is something you have not just something you know – like the keys to your car. Keep is safe and you control access.

- One Key, one computer. The Key is linked directly to the computer and every key is unique.

- Windows administration accounts are allowed for all users without bypassing KidSafe protection systems

- Inbuilt online and manual update system with cryptographically signed verification.

- Software removal protection via 1024 bit RSA encrypted uninstall code received during the software installation and kept in a safe place by the parent.

- Lost key and lost uninstall code online support system.

- Removable media such as USB memory stick) uninstall code backup.

- Adult I.D. verification during online installation process.

- Software installation does not interfere with existing windows user accounts and passwords.

- System Restore protection. Software cannot be removed by setting a system restore point. Protect against System Restore roll-backs.

- Safe mode boot blocking, protection against safe boot mode.

- Low level registry key protection system, registry keys cannot be removed or changed.

- File modification protection, files cannot be deleted.

- Proc explorer protection, KidSafe processes and threads cannot be viewed or stopped by proc explorer or other low-level debugging tools.

- New operating system install protection, KidSafe will stop a new OS from being installed on top of itself.

- Fully configurable so the parent can control what happens when the key is removed.

- Skin-able to allow branding for other companies and re-distributors.

- Emergency fail-safe procedure in the unlikely even that KidSafe stops working.

- Inbuilt automatic software update system.

- Presently available in five different languages, French, German, Swedish, Dutch and English

KidSafe Total Control (KSTC) software and secure USB key
Availability: Presently in development, expected December 2009

KSTC is for parents who may be more computer literate or who have specific requirements in terms of restrictions. It is perfect for families where there is a wide range in ages between children. Because it offers the facility to easily create detailed profiles for each user, it is ideal for tailoring restrictions for different age groups. For example the parent may want to allow their younger children access to the computer to play games and use applications for homework but not to have any internet access. Conversely, they may wish to allow their older children access to the internet and chat clients.

KSTC contains all the features of KidSafe Parental Control but with an account restrictions sub-system. The parent key determines who is in charge. Token access can be more secure than password access alone. The windows administration accounts are based only on passwords. The parental key is kept safe by the adult and allows use of the computer without any policy restrictions. When the child logs on (existing user names and passwords are not affected) they will have restrictions enforced. Restrictions are controlled via a unique profile for each child. Profiles are created via an easy to use yet powerful wizard. Restrictions can be changed or viewed via the 'KidSafe control centre'. To access the control centre the unique parent key must be present.

Profile restrictions include time and date access control, computer usage quotas, true application restriction by black-listing, date and time or a combination of both, internet access restriction by white listing and date and time – meaning that children can only access sites authorised by the parent.

KSTC also contains an internet content filter system that can work in a number of different ways. Presently the system can be set up for white lists and intelligent filtering based on categories and key word analysis. We have designed this part of the software as a plugin system so you can choose how it should work now or in the future.

KidSafe Total Control (KSTC) Software Features:

- Choose blanket profiles or unique user profiles for each family member. All needs are not the same.

- Our easy to use yet still powerful profile wizard makes generating profiles as simple or complex as necessary. You decide.

- Profile controls are enforced when no key is present and overridden when parent key is inserted.

- Simply inserting the parent key allows easy access to the control centre and addition of controls or access to profiles. For example, if a child needs to access a particular web site that is not white-listed, the parent simply inserts their key, authorises it and then removes their key (the site is now added to the profile in question).

- Application launching restrictions by date, time and black list. This means that the parent can stipulate what applications are used and when. Application restriction is done by black-listing so that parent only needs to identify the applications that they wish to restrict, as opposed to the ones that they wish to allow.

  Application restriction means that parents can stipulate that they wish their children to use the computer during certain hours but only be able to use certain applications i.e. they could restrict the use of Internet Explorer and MSN Messenger between the 16:00 and 18:00 whilst they are not present to oversee their Childs use of these applications. This could also include control of any peer to peer file sharing applications.

- Software installation restrictions. Because KSTC black-lists applications, it must also assume that all applications installed after itself are automatically blocked unless otherwise stipulated. This means that children cannot simply install applications at there leisure. The applications installer will be prevented from running.

- Spy-ware and malware protection. In following with the application and software installation protection, KSTC will block the execution of applications that are run or installed after KSTC has been installed, this includes spyware and malware.

- Removable device restrictions. In following with the application and software installation restrictions, KSTC will block access to programmes on removable devices such as flash drives and CD-Rom, until authorised by their parent.

- Internet access by URL white-listing and date and time. KSTC allows parents to decide which websites they want their children to use and when. This is the opposite of other parental control applications where they adopt a black-listing policy. Black-listing is an unsustainable task that forces the policies and opinions of the software company onto the user. White-listing allows the parent to decide what they wish their children to see.

- Default profiling to allow parents to quickly enforce standard restrictions on their children.

- Restrictions are enforced regardless of administration status.

- Importation and exportation of profiles to allow parents and communities to share their profiles and knowledge.

- Logging of infringements to profiles. This allows parents to see what their children are trying to do, without actually spying on them. This also allows parents to easily authorise or block items without having to redefine entire profiles.

- Restrictions on ability to change system date and time, to prevent bypassing of date / time enforcement policies.

- Taskbar icon indicates control status and informs the users of any infringements via balloon tooltips. This allows the parent to easily authorise blocked items by inserting their parent key and clicking on the information tool tip.

KidSafe Intelligent Control (KSIC) –
Availability: will be available as part of KidSafe Total Control.

KSIC will help parents who possibly have already used KSTC white listing but find that they require their children to have access to a wider range of websites. The white-listing features of KSTC are perfectly suited to limiting access to a small-to-medium number of websites. However it does not allow complete access to the internet and so may present problems for older teenagers. The artificial intelligence engine of IC is designed specifically to filter content based on the existing knowledge that it has already learned. This is far superior to website rating, or simple word comparisons.

KSIC is now part of KSTC. It is able to actively and intelligently filter web content. KSIC allows parents to specify categories of content that they wish to restrict. KidSafe IC then uses an artificial intelligence engine to determine if the content falls within the restricted categories. Unacceptable content is transparently blocked without having to rely on voluntary categorisation systems such as ICRA or FOSI.

Features include (in addition to the features of KSTC):

- The ability to specify categories of content that the parent wishes to restrict.

- Categories include:
  - Adult
  - Chat
  - Drugs
  - Gambling
  - Hate
  - Job Search
  - Sport
  - Stock Quotes
  - Weapons

- Provides children with more freedom to '*surf*' with less parental intervention required.

- Allows parents 99% assurance that the children are not being exposed to the categories of information that they have flagged as being restricted.

- Same easy to use configuration profiling as in TC.

KidSafe Chat Control (KSCC)

KSCC is for parents who want to know who their kids are chatting with and when. It is an add-on for KSTC, it is used to encode/encrypt all data that is flowing out of the computer that is considered to be chat related (as determined by the target address/URL). A public/private key system is set up whereby users can only communicate with other users who also have a KidSafe key. Anyone without a KidSafe Key, who tries to chat with the child who does have one, will be blocked and presented with unintelligible data.

What this means is that we can say, with some degree of confidence, who any one particular user is chatting to. Each KidSafe Key is uniquely encoded and because the registration process requires a credit card, we can join a Key to a customer. Any chat that is deemed inappropriate can be reported and we can determine who was involved in the conversation. This is an entirely opt-in system.

Features include:
- All the features of the existing product suites
- Encrypted chat channels directly linked to the registered KidSafe users
- Chat audit trails - who, what when.

Competitive Product Reviews

We have been asked how KidSafe Total Control compares with existing parental control software applications. If you type parental control into Google, one of the first sites that may be found is:

Internet Filter Review 2007

http://internet-filter-review.toptenreviews.com/?ttreng=1&ttrkey=parental+control&gclid=CJC7mJHt-YwCFReRgQod2l-wCA

This site appears on the surface to be an independent review of internet filtering solutions. We believe however, the reality of this site is that it is intended to sell several of the products that they rate as being in the '*top-five'*. The other products are given a deliberately lowered rating as an attempt to promote the topmost who of course are owned by the reviewing site.

More importantly, it is not a simple matter to make a comparison between for example the KidSafe product(s) and the other products in this listing. This is due to several reasons that will be expanded upon and examined here:

1. Firstly, all of these products basically work in the same fashion – there is nothing new or innovative about anyone of them. One product is much the same as another, which is why it is easy for them to make feature comparisons.

   We believe these products do not have the '*right-idea'* about how to protect children when using a computer or online.

Because KidSafe is a totally unique and innovative product, it would be inaccurate to try and compare it against the features of these products. As an analogy, it would be like designing an aeroplane and comparing it with the features list of a car. The only similarity is that they both get your from one place to another. On the surface, the car has its alloy wheels, leather reclining seats, in-car entertainment system and air conditioning, whereas the aeroplane has an uncomfortable seat, and an in-flight magazine. But we all know that there is much more to it than that.

2. Secondly, these feature lists are mostly contrived and grossly inaccurate. We have tested the top 5 products and they do not work. They are easy to bypass and don't do what they purport to do.

   For example, if you have a product that can restrict programs from running, this feature would logically be referred to as '*application restriction*'. However, the ability to restrict applications/programs means that you they have the ability to restrict access to chat clients, internet clients, newsgroup reads, games etc. So is it accurate to say that you product has internet, chat, newsgroup and games protection or simply that it has application restriction? This is just marketing spin.

3. Thirdly, we would argue that KidSafe can be pitched on its own feature list, and the real control that it offers. I refer back to the interview that Bill Gates did for *The Sun* newspaper where he stated that the only real way to protect children is to get involved in what they do. The KidSafe products allow parents to do this.

   We have never and will never say that our product(s) will keep your kids safe – it is simply a tool to assist you. However it is a tool that has been professionally designed to fit a specific purpose. As we have shown, there are 30+ features that KidSafe has, that none of these other product have.

   These additional features are obviously not detailed on the sites feature-matrix because NONE of them have them. The most fundamental features that spring to mind are Safe-Boot protection and System Restore protection:

   > - the ability to allow users (kids) to boot into safe mode allows the user to bypass any protection previously offered and allows them to easily remove the software. No other products on the market protect against safe mood booting or enforce protection whilst in safe mode
   >
   > - System Restore allows users to roll-back there system to a point where the product was not installed, thereby removing the product and it's protection.

4. Finally, as we have shown it only takes 5 minutes on Google to find detailed information on how to bypass and circumvent the protection of most of these other products.

   The whole design concept of these products is flawed fundamentally, and as we have highlighted they all work in pretty much the same way. If you purchase one of these products and assume your kid will now be safe, you are being naive and burrowing your head in the sand.

   It is the nature of kids to break rules and push boundaries, this is all a

healthy part of growing up and discovering who they are. Some will try to break anything you put in their way to enforce these rules. This is exactly what we considered when designing the KidSafe product software suit and secure USB key implementation. Once again, we are trying to promote the idea that parents have to get involved in keeping their kids or family safe and sound when using the computer or doing stuff online. A parental control software suite alone (no matter how great it may or may not be) is not going to do the job by itself. KidSafe Total Control will help push the boundaries of control back in your favour and let you do what you do best, provide help and guidance where necessary and when it is most important to do so.

Summary:
If you have any questions or comment for the authors of the KidSafe Parental Control software whitepaper please do not hesitate to get in touch with us. All contact information can be found here:

http://kid-safe.tel

or directly:

mike@kid-safe.co.uk
stjohn@kid-safe.co.uk

We also recommend you have a look at our blog where we try to keep developments up to date:

http://www.kid-safe.co.uk/blog