Sentinel Kid SAFE

Sentinel Tech Holding Corp / Eschel Hamel
http://www.senttech.com

ABSTRACT

Tracking children's activities on websites is a very challenging task for parents, made all the more difficult by modern children who are Internet savvy may have knowledge as to how they can mask their identity.

Sentinel Kid SAFE is a tool that will be offered to parents as a means of registering their children's email addresses and their unique devices, providing a central registry in which websites could check their existing and new users to block the accounts and/or notify parents of the children's activity.

Keywords

Filtering, identification, verification, parental controls, notification, safety, and security

Functional Goals

Please indicate the functional goals of the submitted technology by checking the relevant box(es):

☑ Limit harmful contact between adults and minors
☐ Limit harmful contact between minors
☑ Limit/prevent minors from accessing inappropriate content on the Internet
☑ Limit/prevent minors from creating inappropriate content on the Internet
☐ Limit the availability of illegal content on the Internet
☑ Prevent minors from accessing particular sites without parental consent
☑ Prevent harassment, unwanted solicitation, and bullying of minors on the Internet
☐ Other – please specify

PROBLEM INTRODUCTION

Parents want to have full control over their kids' online experiences. Additionally, social networks and other websites don't want children who are underage, or whose parents prohibit them from accessing their sites.

Identity verification (IV) techniques alone are ineffective and easily defeated. Moreover, they are cost prohibitive in very large social networking environments. IV is a 20th century solution to a 21st century problem, and should only be used during the adjudication process for both cost effectiveness and efficacy.

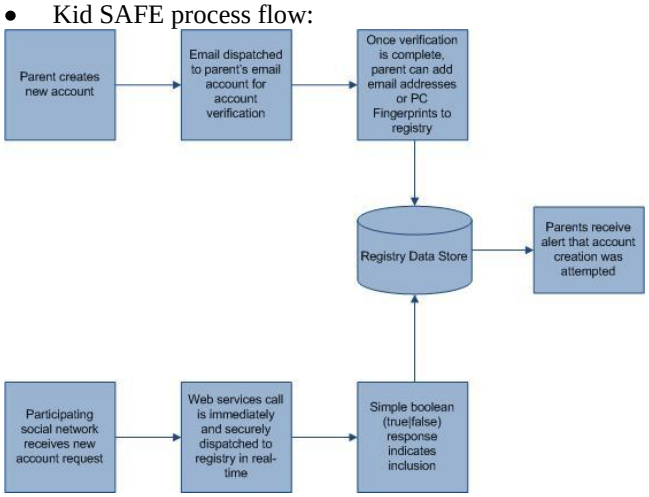
PROPOSED SOLUTION

Sentinel Kid SAFE offers registration by parents into a central registry, of their children's email addresses they wish to have blocked by social networks, which can then be accessed by social networks and other websites at point of registration, and compared historically, so that these sites can block access.

Additionally, Kid SAFE offers registration of the children's device IDs into a similar central registry that can be accessed and utilized in the same manner.

The Sentinel Kid SAFE registry provides parents the ability to decide and control whether or not their children access certain social networking sites and online communities

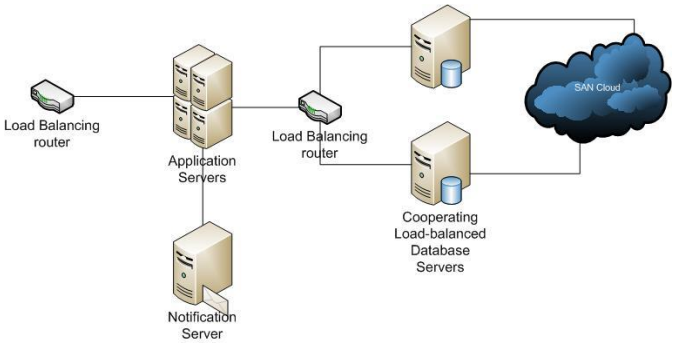
- Parental two-phase email validation
  - Email dispatched to parent's email address to for account activation
- Activated account can add email addresses to blacklist
- Activated account can add computers to blacklist
  - Use of Sentinel A.D.A.P.T. PC Fingerprinting Technology
- Provides a granular blocking design
  - Offers the ability to block use of some networks while allowing others
- Email/SMS Alert Mechanism
- Kid SAFE process flow:



Kid SAFE Process

- Technology Platform
  - Microsoft .NET Technology and Windows Servers
  - Full parental user interface
  - Full SOAP-based web services for ease of integration
  - Simple Web Services for ease of integration

- Basic Design:



Kid SAFE Design

- User Interface:

Kid SAFE Login Screen

Kid SAFE Registration

Kid SAFE Parental Options

- Core Design Principles:
  - Privacy
    - Limited data collection, collecting only minimum amount of data from parents needed
    - Hashing of children's emails to ensure privacy
  - Data Security
    - Full end-user-to-persistence encryption
    - Hashing of private data completely prevents disclosure
    - Network design limits attack vectors
    - Data security audits by a reputable, third-party data security auditor
  - Performance
    - Three-tier design
  - Scalability
    - Linear scaling allows for modular, effortless performance upgrades
  - Reliability
    - 99.999% uptime
    - Fully redundant through all three tiers.
  - Resiliency
    - Collocation facility offering triple redundancy on bandwidth and power
    - Multiple DNS geographical locations
- The web application will be built using Microsoft's .NET technology (ASP.NET, C#) and hosted on Microsoft's Windows Server 2003. The data store will either be Oracle or Microsoft SQL Server. This service will also expose a SOAP-based web services interface for submission of candidate email addresses (as well as candidate PC Fingerprints) at registration time. A Boolean value of True or False will be returned to indicate whether or not the email address or PC Fingerprint is present in the system and should be excluded. The technology used to uniquely identify a blacklisted client's fingerprint can be a "zero-residue" technology. This means that cookies or other client-

persisted data will be not solely be used to compute this value as such technology is easily defeated.

- **Usage of Sentinel A.D.A.P.T.**
  Sentinel recently debuted Sentinel A.D.A.P.T., which is the result of a partnership with an anti-online fraud organization. The core technology of A.D.A.P.T. is the "PC Fingerprint" technology, which is an online method to compute a unique "fingerprint" of a PC using just the data that is already available to the browser. It uses no client-side code, ActiveX, Flash or cookie-based methods.
  Sentinel proposes to use Sentinel A.D.A.P.T.'s technology to voluntarily collect the PC Fingerprints of the computers that parents specify and add that information to the registry. A simple integration with the registration pages of participating social networks would allow for an additional check to make sure that the email registry was not being defeated by simply acquiring another email address from one of the many web-based free email providers.
  The underlying technology of A.D.A.P.T. is a proven technology and is in wide use in the financial and retail anti-fraud space.
- **Economics**
  - Short time to delivery because most elements exist within Sentinel's infrastructure
  - The industry would pay subscription fee for access to database
  - The registry should be no or very low cost to parents to encourage participation and assist with potential NGO and government concerns.
- Application and usage of Sentinel Kid SAFE is not limited to the United States, and will function equally well if offered to parents and websites located outside of the country.
- Potential concerns and how they are addressed:
  (1) Email Adjudication Process
  In the event that there are questions raised due to the registration of a given email address, there will be a customer support process (for which Sentinel currently has an active and fully scalable customer service infrastructure in place.) to assist in resolving these issues:
    1. User calls 800 number and notifies Sentinel that their email address and/or machine ID shouldn't be blocked
    2. Sentinel operator verifies user's personal information via standard ID verification practices
    3. If user passes the verification, Sentinel will adjudicate and unblock their information. If user fails, information remains blocked.
    4. Message generated to user notifying them of pass/update or fail.
    5. Sentinel logs record of dispute and recording of call.
    6. Passed/Updated users can now access social networking sites which utilize our registry database.

  (2) Cyber-Bully Denial of Service (DOS) attack
  - Use of both parental notification engine and Sentinel's PC Fingerprint technology alleviates problem
  - Parents will be encouraged to register both their child's email address and child's PC Fingerprint.
  - Participating social networks will be encouraged to actively block ONLY when both criteria are present.
  - The Parental Notification Engine will fire a notification on either an email or PC Fingerprint hit, so parents are aware of successful access.
  - A Cyber Bully would need both the email address AND physical access to the victim's device to successfully perform DOS.
  - Additionally, a small fee could be assessed to use service, which could potentially mitigate CyberBully attacks, but this is not the preferred solution

  (3) Participating Social Network Policies
  - How the information in the registry is used is dictated solely by the requesting social network.
  - Sentinel provides simple yes/no answer to the inclusion question.
  - Sentinel provides PC Fingerprint registration
  - Sentinel provides parental notification for registered email or PC Fingerprint hit

EXPERTISE

John Cardillo, Sentinel's CEO, is a former New York city Police office and is leading in the efforts on several levels to improve the safety and security of internet users, especially children who can be easy targets for sexual predators

Sentinel SAFE is currently used by social networks and online communities with a total membership of more than 300 million users worldwide. Additionally, it is currently utilized by the National Center for Missing and Exploited Children.

COMPANY OVERVIEW

Sentinel, the leader in online verification is dedicated to enabling safer social interaction on the Internet – more secure social networking, online dating, and e-marketplace experiences.

MORE INFORMATION

Sentinel is the premier provider of online safety and security services as well as the leading provider of Sexual Predator tracking and detection services. Sentinel is committed to promoting safety throughout the Internet and beyond. With its Kid SAFE technology, Sentinel has positioned its products to cover identity-related security end-to-end.

CONTACT INFORMATION

Eschel Hamel
ehamel@senttech.com
(305) 599-6325
8550 NW 33rd St
Suite 100
Doral, Florida 33122
USA

CERTIFICATION

I certify that I have read and agree to the terms of the Internet Safety Technical Task Force Intellectual Property Policy