Internet Safety Technical Task Force

Online Predators Early Detection - The Multi-Dimensional Approach

Hanan Lavy, CEO Credint, Inc. (hanan.l@credint.com)

Dr. Dror Zernik, CTO Credint, Inc. (dror.z@credint.com)

July, 2008

ABSTRACT

As a personal communication media the Internet is unsafe. The Web 2.0 revolution has sharpened the need to provide anonymity, yet maintain trust.

A very painful example is the activity of online-predators who exploit the trust of kids, and hide behind the anonymity curtain.

Credint's protection service uses a patented *multi-dimensional* approach to analyze the relations between the protected kids and their chat-buddies. The different dimensions of the analysis create an interference effect, that result earlier detection of pedophile-kid relations as well as lower the false alarms.

Keywords

Parental controls, criminological profiling, community protection, relations tracking, multi-dimensional.

Functional Goals

X **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

As a personal communication media the Internet is unsafe. The Web 2.0 revolution has sharpened the need to provide anonymity, yet maintain trust.

One painful example is the activity of online-predators who exploit the trust of kids, and hide behind the anonymity curtain. A similar phenomenon is observed in dating sites, where anonymity is often abused.

Understanding the nature of the relations over its developed period of time is critical in deciding whether relations cross any safety boundaries. In addition, as predators interact with dozens of kids concurrently, it is equally important to have a quick knowledge transfer between the preyed kids once a predator is detected. Further, the network analysis of such behavior empowers any detection hints.

PROPOSED SOLUTION

Credint developed a service, ***TeenSafe***™, which implies a multi-dimensional approach in determining the nature of the relations between kids and their chat-buddies.

As a part of the service, TeenSafe measures a few dozens of parameters that change over the *course of the relations.* Using these parameters the TeenSafe engine identifies risky relations in which any of the protected kids are involved. Such parameters include content-related parameters as well as contextual ones (which we refer to as meta-content).

The content-related parameters detect the atmosphere of the chat sessions, the topics that are being discussed, information that is being passed between the parties (including sometime their ages), initiating part of the chat and such.

Meta content includes the length of each chat session, time of day of the sessions, their frequency and such.

Building an *over-time* profile of every one of the measured parameters creates a long-term pattern, or profile, of the relations. This profile describes best the characteristics of the relations between the parties.

This profile is then matched to known pedophilic pattern, which is well studied and has been published in several criminological studies [1]. A good match indicates a high likelihood of pedophilic relations.

Another dimension that is being looked at is the *potential vulnerability of the protected kid*. Kids that use the Internet a lot, create lots of new chat buddies and so forth are more vulnerable to pedophile attacks than other kids. Moreover, kids that are new in their physical environment (relocated lately, for instance) or are in any sort of personal crisis, are also an easier target for predators.

On top of these dimensions Credint uses the information it collected on a predator to alert other relations in which the predator participates. This approach allows the TeenSafe to form the ***Global Child Protection Network***™. This networked dimension creates a *community synergy effect*: the total strength of the community is much bigger than the sum of its members' protection strength.

In order to be absolutely positive about the predator virtual identity, and to be immune to nick-name changes, the TeenSafe system extracts a technical *fingerprint of the predator.* This fingerprint enables detecting the predator's consistent virtual identity and blocking the predator to access the protected kids.

Features and Functionality

The solution includes a data collector (DC) component and a main processing component (PC). The DC collects all the chat sessions content (and later will also gather interactions in chat rooms and emails) and passes it to the PC. The DC is not necessarily located on the kid's machine. Accordingly, this method may also be relevant for smart-phone device, as protection is provided through the "Internet Cloud".

In the PC the relation pattern and profile is built and matched to known pedophilic relations patterns. The Kids' information is taken into account before alert triggering.

The relations between chatters are also managed in the PC and are the basis for alert triggering based on the ***Global Child Protection Network***™.

Use Cases

Assume two TeenSafe subscribers: Nancy13, who is a 13 years old girl and Anna14 who is a 14 years old girl. Assume JohnSmith is a predator chatter that interacts with both Nancy13 and Anna14.

Assume that JohnSmith is in contact with Nancy13 for 3 weeks and with Anna14 for 2 days. Hence the relations with Nancy13 are past the grooming stage and are into a desensitization stage: JohnSmith tries to get Nancy13 to be used to sexual content. With Anna14 JohnSmith is in the early "getting-to-know each other" stage.

Once the system identifies that JohnSmith is a predator, due to the content of the recent chat sessions with Nancy13, using all the information from previous chat sessions collected in the past 3 weeks of interactions, the guardians of Nancy13 will be notified by SMS or email.

In addition, the guardians of Anna14 might be notified that she is in an interaction with JohnSmith, who seems to be a predator, based on his relations with other kids in the network.

Effectiveness

The proposed solution is effective when the solicitation between the predator and the prey takes at least 1-2 days. In case of "morning chat; evening meeting" the proposed solution has the same effectiveness as other known solutions (the various word spotting tools).

The longer the solicitation process, the more effective the proposed solution is as the contextual analysis of the over-time pattern can allow for early detection of unwanted relations.

Moreover, the larger the community using the solution is, the effectiveness of the ***Global Child Protection Network***™ is bigger.

Measuring the effectiveness of the solution will be done statistically. We expect to trigger the guardians of kids protected by Credint's solution in more than 98% of the pedophilic relations cases. We expect to have at most 2% false-negative cases (i.e. pedophilic cases we did not alert on) and up to 5% false positive (i.e. alerts that were triggered on non-pedophilic cases).

Strengths - Weaknesses Analysis

Strengths:

Since the TeenSafe system is multi-dimensional, it gains its power as more information is available on each of the dimensions.

- This ensures a very low false alarm ratio.
- Another immediate impact of the multi-dimensional approach is the ability to provide very early alerting. This allows for reducing the child's damage. The capability to provide such early alerts is also a result of the community synergy effect.
- Since the system relies on networked computing, it may be deployed in several configurations, which do not necessarily involve installation on kid's machine. Consequently, it can also provide protection for IM communication to other hand-held devices.

Weaknesses:

- The challenge of protecting children from online predators is huge. Accordingly, short relations (few hours) with an eventual meeting can hardly be detected.
- Backend support system is more complex than any standalone product.

Implementation Requirements

Backend

In order to implement the solution a supporting backend system is being developed. Such a system needs to be able to support millions of subscribers. For a million subscribers it requires:

- 4 strong server machines (2 of them as backup for high availability) with Linux OS.
- 1TB of disk space for database.
- Distributed-enabled database.

Data collector component

There are four different possibilities for this component. For simplicity of the discussion here we assume that the DC selected configuration is that it resides on the kid's machine. This requires the parent to simply install the DC on the kid's machine. The DC is transparent to the kid and it is very hard to remove it.

Other alternatives are:

- DC in Internet Service Provider (ISP).
- DC in IM vendor.
- DC in the Internet cloud.

Viability of Technology

The TeenSafe solution is viable in the US and any other English speaking country in the world. Its core is almost language-independent and requires a basic Natural Language Processing (NLP) adaptation to non-English speaking countries. The full solution requires a longer language adaptation to non-English countries.

EXPERTISE

The CTO of Credint is a PhD in CS and an expert in NLP, as well as veteran technologist that served as CTO in number of companies.

In addition, Credint's extended team includes a top criminologist (PhD and a senior staff member in Bar-Ilan University) with special expertise in sex-crimes and pedophiles. The company also enjoys the design partnership of both police forces and commercial partners.

COMPANY OVERVIEW

Credint was established in 2008 after a long study of the problem, and when the founding team was convinced the solution is viable. Immediately upon its founding the product development began, design partnerships were formed, and an integration of an early version with a major ISP in Europe is expected before the end of the year. The Company will unveil its first kids' safety product in a few months timeframe.

Founders

Hanan Lavy (CEO) – Hanan has over 18 years in R&D management positions, in both startups and large corporate. Most recently, Hanan was a Director of R&D at Mercury/HP Software, managing a worldwide group of development teams in its Enterprise Monitoring product line. Hanan holds a B.Sc. in Computer Science and Business Administration (cum laude) from the Hebrew University, Jerusalem.

Dr. Dror Zernik, (CTO, VP of Engineering) – Dror has over 20 years in leading software projects in distributed and Internet-based environments. Most recently, Dror was the CTO of e-Glue, a company that provides solutions for real-time customer interaction management. Prior to that Dror was co-founder of several startups, serving as CEO and VP R&D. Dror also accumulated intensive R&D experience with leading enterprises such as IBM and Tandem. Dror holds a Ph.D. in Computer Science from the Hebrew University. Dror also holds a BA from Bezalel Art Academy.

Advisors

Dale Fuller – strategist. Former CEO/President/BOD of McAfee, Borland and WhoWhere (acquired by Lycos); Currently Dale is on the BOD of Krugle and Phoenix Technologies.

Dr. Yael Idisis – criminologist. Yael is the Deputy Head of clinical division, Department of Criminology, Bar Ilan University and is an expert in sex-crimes and pedophiles.

Ronny Gorlicki –market/sales executive. Ronny is currently serving as EVP of Sales at Comsys Mobile and held marketing and sales positions at Wizcom, and National Semiconductors.

Uriel Maimon –forensic technology expert. Uriel is a senior forensic and fraud detection expert, serving as a security advisor to RSA (EMC).

BUSINESS MODEL OVERVIEW

"Protecting Every Child" Vision

Credint's social vision is to allow every child in the world, that is using the Internet, enjoy it without the fear of being abused by online-predators. Hence, Credint intends to offer *TeenSafe Basic Protection* service at a very low price.

TeenSafe Basic Protection distribution will also help Credint build its ***Global Child Protection Network***™ fast and hence enhance the effectiveness of the protection as described above.

Credint will also offer *TeenSafe Advanced Protection* service to parents through distribution channels.

CONTACT INFORMATION

Hanan Lavy, hanan.l@credint.com.
Phone: +972 52 530 6057

REFERENCES

1. Wolak, J., Finkelhor, D., Mitchell, K. J. & Ybarra, M. L. (2008). Online "Predators" and Their Victims: Myths, Realities, and Implications for Prevention and Treatment. American Psychologist, February-March 2008 edition, Volume 63, No. 2, 111-128.

CERTIFICATION

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