Sentinel Advanced Detection Analysis & Predator Tracking (A.D.A.P.T.)

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

ABSTRACT
Identifying and tracking legitimate users on websites is a challenging task, made all the more difficult by those who do not wish to be identified due to illicit activity..

Sentinel Advanced Detection Analysis & Predator Tracking (A.D.A.P.T.) is a covert device fingerprinting technology in association with risk management engines. It helps identify and separate legitimate devices visiting a website from those which are suspect, thus supplementing standard user identification with computer identification.

Keywords
Filtering, identification, verification, pattern recognition, forensics, registered sexual offender, predator, social networks, dating websites, 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 – Provides websites with ability to validate legitimate users from those not permitted or those using false identities.

PROBLEM INTRODUCTION
Separating legitimate users from those using false identities is a common issue that virtually all websites have to deal with in one form or another. Risk management based solely on user entered information and IP address contains an inherent risk because validation is dependent on data elements that are easily changed, disguised or stolen This becomes particularly concerning if the individual attempting to mask their identity is a Registered Sex Offender or Predator.

One way to alleviate this issue is to identify and track the computer/s the fraudulent party is using, but doing so in a way that is transparent to the general user community.

PROPOSED SOLUTION
A.D.A.P.T. is a covert fingerprinting technology (Clientless Device Identification), which works with real time authentication and risk management engines. It helps detect and prevent fraudulent account access and openings as well as other suspect behavior.

A.D.A.P.T. identifies legitimate vs. suspect devices visiting a given website by invisibly generating a device fingerprint. By doing so, it can differentiate individual devices despite past registration, the credentials presented, or the Internet connection (IP address). A.D.A.P.T. has the capability of differentiating between 1.461 quindecillion (10^{48th}) unique device fingerprints.

All of this is accomplished without the need to collect any personally identifying information (name, address, etc.) or details about a specific individual (behavior, purchasing patterns, etc.)

- A.D.A.P.T. is a web service which computes an identity from the raw HTTP + JavaScript Collector (JSC) data
  - Uses JavaScript to ask the browsing device additional questions
  - Makes use of CGI parameters already included within the protocol
- A.D.A.P.T. takes into account numerous device parameters in order to create a very accurate "fingerprint" of the device
- By evaluating the nuances of dozens of operating system, browser, and PC characteristics, it generates a unique string to represent the device
- A.D.A.P.T. has the following features:
  - **Non-intrusive**, causing no change to the end-user, allowing for seamless deployment
  - **Completely covert**, providing no visible mechanism for fraudsters to exploit, and is simply passive observation or a given device
  - **Has no tagging**, making no use of cookies, Flash objects, or certificates. No enrollment is necessary so there is no possibility of stolen credentials.
  - **Leaves no residue**, because there is nothing placed on the user's device.
- The A.D.A.P.T. API also includes the following two features:
- (1) **A.D.A.P.T. Diff™**
  - Performs a comparison between two PC fingerprints at the raw data level

- If there are slight differences, it can calculate a proximity match, providing a "Percentage of Match" between devices
- The risk engine can then use a threshold to determine if the inbound device is a new device or a modification of a known device.
- The following is an example of an A.D.A.P.T. Diff comparison:

	PC 1	PC 2
Language	en-us	en-us
Doc Charset	windows-1252	windows-1252
Browser ID	Mozilla/4.0 (compatible; MSIE 7.0)	Mozilla/4.0 (compatible; MSIE 7.0)
CPU Class	x86	x86
Flash Version	WIN 9,0,16,0	WIN 9,0,28,0

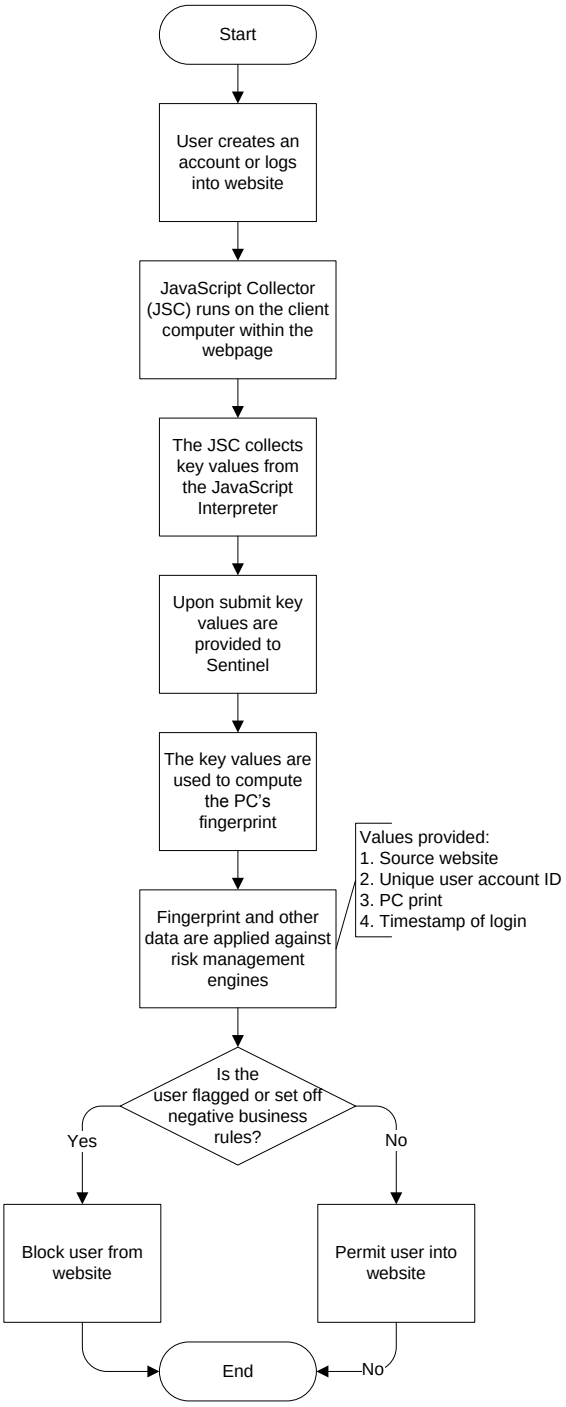
A.D.A.P.T. Diff Compare

- (2) **TimeDiff Linking ™ (TDL)**
  - Calculated by measuring the Time Difference between the device and the server with which it connects
  - TDL is used to augment A.D.A.P.T. and is a patent-pending technology unique to Sentinel's partner, 41st Parameter
  - The following example demonstrates how logins to multiple accounts, using different account IDs, different IP addresses, but having the same A.D.A.P.T. and TDL reveals the same device/individual

Account ID	IP Address	A.D.A.P.T.	TDL in Minutes
23nndwowe3j3o3k5nn56	220.68.139.147	933A7BF8077C0852C7FEED729249BE149EFB3CFE	132
34l4k6j6h72j23k6j36l2j	122.203.118.132	933A7BF8077C0852C7FEED729249BE149EFB3CFE	132
3k67jj9s0344yug99t83g	210.118.104.84	933A7BF8077C0852C7FEED729249BE149EFB3CFE	132

TimeDiff Compare

- The combined A.D.A.P.T. technologies offer the following benefits:
  - Forensic clientless device identification (CDI technology)
  - Covertly gathers numerous parameters about a device to provide a unique "fingerprint"
  - Combines device parameters with user entered information (80+ data elements) into over 350 rules and algorithms to accurately and covertly pinpoint and ID
  - Creates a time-diff and PC-diff comparison litmus tests
  - Calculates a recommended action and risk score
  - Provides user defined risk models
  - Provides investigators with a comprehensive set of prioritized investigation tools to analyze suspect transactions on a single screen
  - Conducts link analysis on seemingly unrelated data against both user entered information and device harvested information
  - Links all activities to the device used, regardless of the identity assumed or IP address claimed
  - Verifies and validates the authenticity of both existing customers as well as new customers with no account history
- The following is the simplified process flow:



Sentinel A.D.A.P.T. Process Flow

- Implementation Requirements
  - Simple integration with existing website
  - Simple web services based calls
  - No end-user experience
- Technical Standards

    - Web Services
- Application and usage of this technology is not limited to the United States, and will function equally well when applied against devices located outside of the country.
- Currently, this technology is in wide use in the financial and retail anti-fraud space.

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

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 A.D.A.P.T. 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.