SecureBrain

WEB CONTENT SCANNER SDK

Web Content Inspection for PCs and Mobile

OVERVIEW

Web Content Scanner SDK is a multi-platform SDK that enables an application to filter websites based on web content at very high throughput as opposed to pure URL blacklisting. Our SDK can drastically help improve detection rates of cybercrime sites including regional phishing sites or websites injected with hostile JavaScript. It can also help reduce the cost involved in maintaining an ever-growing URL blacklist. Our SDK is available for Windows platform and mobile platforms.

REGIONAL THREATS COVERAGE

Today, most web browsers include security features that help protect users against cybercrime. For example, Internet Explorer includes a feature called “SmartScreen Filter” that is supposed to filter online phishing, fraud and spoofed malicious websites. Firefox and Chrome browsers include a service called “Google Safe Browsing” that checks pages against potential threats. While these technologies are helpful, they are often US centric or English-centric and tend to lack detection logic for regional threats.

For example, there is a category of cybercrime called “one-click fraud” in Japan. It is a form of money extortion fraud, and considered to be one of the top cybercrime incidents in the region. There are also traditional phishing attacks that target Japanese- specific brands in Japanese language. Unfortunately, such regional threats are not properly covered by the security features of most major web browsers. Thus, the need to provide additional coverage for regional specific cybercrime becomes critical.

Web Content Scanner SDK is a technology that has been designed to enable developers to integrate web content filtering into their apps to better improve regional threat coverage. Because it does not rely on pure URL blacklisting, it can also help improve overall detection rates and reduce daily maintenance costs.

TRADTIONAL URL WEB FILTERING

Traditional web content filtering technology relies on a set of URL blacklist or a list of known bad sites to filter hostile web content. This method is only effective if the number of new hostile web sites are small enough to allow maintaining the list easily. However, new hostile websites are increasing rapidly. Thus, the cost to maintain an effective URL blacklist will grow as well or else its protection level will decrease.

There are other factors that can make URL blacklists technology outdated. In yesterday's attacks, bad sites resided on independent web sites or domains making URL blacklists very effective. Today, we are now seeing a large number of "good" sites being injected with hostile code. This means that a good site yesterday could be a bad site today, and may be restored back to being a good site tomorrow. In the past, you only needed to add URLs of bad sites to a blacklist. But now, you must add and delete URLs to have an effective URL blacklist. This will cause an increase in costs to maintain a proper URL blacklist. New factors such as "short urls" making URLs dynamic will continue to make URL blacklist technology more outdated and costly to maintain effectively.

Our Web Content Scanner SDK is a technology that does not simply rely on a set of URL blacklists, and can inspect web content at very high speeds to make its determination. This enables your applications to provide better protection to your customers while keeping maintenance costs lower.

OUR WEB FILTERING TECHNOLOGY

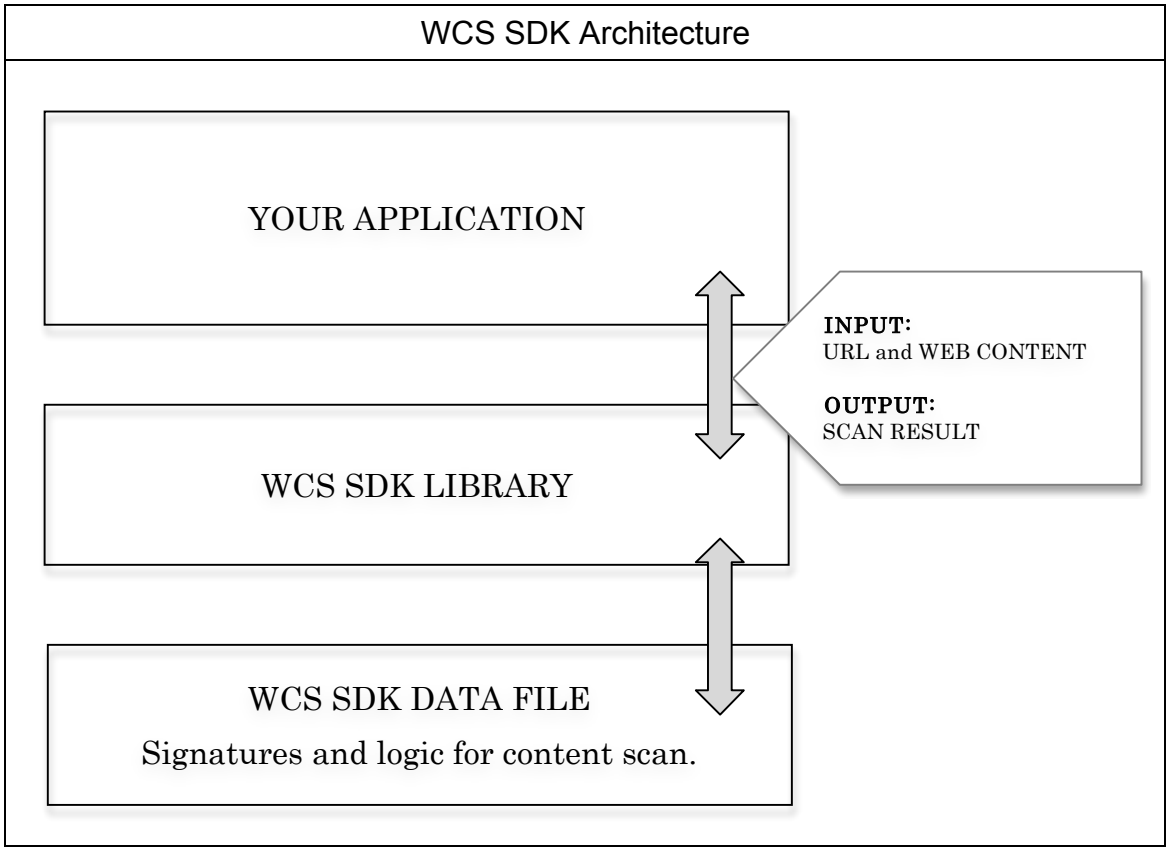
SecureBrain's Web Content Scanner SDK is a technology to filter web content and does not simply rely on a pure URL blacklist. Our technology enables applications to inspect the web content such as HTML and JavaScripts.

URL blacklist is often preferred because of its determination speeds. Typically, inspecting web content, meaning parsing HTML and JavaScript to look for specific signatures, can be very slow. As detection signatures increase for detection algorithm rules become more complex, it is perceived that determination speed will not scale because web content will need to be parsed multiple times as well.

However, SecureBrain's Web Content Scanner SDK provides a very high-speed web content inspection technology. Regardless of the number of detection

signatures or detection algorithm added, the web content only needs to be parsed once. This technology makes our content scanning performance very scalable as new threats evolve.

To ease deployment of new signatures or detection algorithm, the detection data is stored in separate files outside of the content scanning engine library. This means that to add new logic, you do not need to recompile and patch your program. You only need to deploy a new signature data file.



MAIN FEATURES OF WEB CONTENT SCANNER SDK

- High Speed Web Content Inspection Scanning Engine
  - Add detection signatures and logic based on web content
  - Signature and logic data stored in independent data files
- URL Blacklist via Cloud blacklist (http)
- URL Whitelist via Cloud whitelist (http)

INTEGRATING THE TECHNOLOGY

Depending on your target market and objective, there are four possible scenarios to integrate in our technology.

Scenario	Target Market	Objective	Solution
1	Japan	Want to quickly add support for Japanese threats.	Bundle ready-made application. Our partner offers “Internet SagiWall” application.
2	Japan	Want to integrate Japanese threat support into security application.	Integrate Web Content Scanner SDK into an application along with SecureBrain’s premade signatures for Japanese market.
3	Outside of Japan	Want to leverage technology for another regional market.	Integrate Web Content Scanner SDK into an application but will require customization of signatures to meet the needs of the regional market. Customization can be done either by SecureBrain or yourself.
4	Outside of Japan	Want to leverage technology for other regional market, but minimize development.	Bundle ready made application. Our partner offers “Internet SagiWall” application, but will require customization of signatures to meet regional market. Customization can be done by SecureBrain or yourself.

TRY OUR WEB CONTENT SCANNER TECHNOLOGY

If you want to try our technology, please try “Internet SagiWall” application. Internet SagiWall is a web content filtering application developed by SecureBrain’s partner called BB Softservice. Internet SagiWall utilizes SecureBrain’s Web Content Scanner SDK. Internet SagiWall trial versions are available at:

http://www.sagiwall.jp/product/demo.html

Internet SagiWall trial applications are available on Windows, Android, Modern UI and iOS platforms.

ABOUT SECUREBRAIN CORPORATION

Based in Tokyo, Japan, SecureBrain is a leader in providing high quality security software and services. Our software and services help protect our customers against Japanese specific cybercrime as well as global internet security threats such as online fraud, drive-by downloads and malware attacks. SecureBrain is also a government contractor specializing in cyber security and has consistently been awarded numerous contracts every year by the Japanese government.

CONTACT US

SecureBrain Corporation
Web: http://www.securebrain.co.jp/eng
Email: info.intl@securebrain.co.jp
Address: Kojimachi RK Building 4F, 2-6-7 Kojimachi, Chiyoda, Tokyo, JAPAN 102-0083