Subject: Re: FW: Patent application - "System and method for the remote inspection of code"
From: Marc Berger <mberger@bezeqint.net>
Date: Tue, 06 Dec 2005 17:59:46 +0200
To: Yuval Ben-Itzhak <ybitzhak@finjan.com>

CONFIDENTIAL
ATTORNEY-CLIENT PRIVILEGED COMMUNICATION

Yuval, I'm reviewing the disclosure you sent me. It's extremely interesting and well-written!

COMMENTS

B'vracha,
Marc

Subject: FW: Patent application - "System and method for the remote inspection of code"
From: "Yuval Ben-Itzhak" <ybitzhak@finjan.com>
Date: Sun, 13 Nov 2005 08:37:44 +0200
To: "Marc Berger" <mberger@bezeqint.net>

FYI

From: Yuval Ben-Itzhak
Sent: 31 October, 2005 17:38
To: 'Marc Berger'
Subject: Patent application - "System and method for the remote inspection of code"

Hi Marc,

Please find attach my final draft for a patent application: "System and method for the remote inspection of code". In the past I sent you an earlier version.

I would appreciate if you can review it and move forward [redacted]

Regards,

Yuval Ben-Itzhak
CTO, Finjan Software

T: +972 (9) 864.8200 (x.243)
M: +972 (54) 49.44.929

http://www.finjan.com

System and Method for Inspecting Dynamically Generated Executable Code

FIELD OF THE INVENTION

The present invention relates to the field of securing computer applications, networks and services. More particularly, the present invention relates to a method and system for inspecting dynamically generated executable code using a remote process. In a most preferred embodiment of the invention, said inspecting is carried out in an automatic manner. Alternatively, semi-automatic, or manual methods are also within the scope of the invention.

BACKGROUND OF THE INVENTION

Connectivity, functionality and security are conflicting objectives in the application environment of organizations. Typical modern implementation of computer applications allows users to execute a wide range of applications, and offers various services, in order to meet the needs of a modern organization. Unfortunately, the need for such application by many users can lead to malicious content embedded by external entities, such as hackers, or untrusted entities, within these applications.

Currently, security measures and services involves the inspection of such applications for malicious code either on the user's machine (client inspection) or at a remote gateway,

just before the application reaches the user's machine for execution (gateway inspection). Examples of products providing such inspection method are: Microsoft Anti-spyware (client inspection) and Finjan Vital Security appliance (gateway inspection). Each of the inspection methods described above (client and gateway inspection) has its own advantages and disadvantages for assuring that an application is free from malicious code.

As hackers and other untrusted entities are also familiar with the security measures in place, new and advanced techniques were introduced to embed a malicious content in applications to bypass such inspection methods.

Common methods hackers are starting to use involve the dynamically creation of code. That is, the code (or part of it) is created and ready for execution on-the-fly, during execution of other parts of the applications. Using this method, hackers obscure the malicious code within applications. Generating executable code and make it execute on-the-fly or creating executable code and make it execute after all of the code is generated is a know art.

Having this method, gateway inspection methods will fail to identify the malicious code embedded within the application as they statically inspect the code (including the obscured malicious code) and do not execute it. On the other hand, it might be possible that client inspection method might identify the malicious code, when created, since this method runs on the user's machine while the application is executing. However, since the

hacker can have a client inspection method on his/her machine as well – it is more than likely that he/she will be able to reverse-engineer the inspection methods and refine the obscure code for undetection.

It is an object of the present invention to provide a system and method for inspecting applications for malicious code.

It is another object of the present invention to provide inspection methods that will inspect dynamically created executable code during execution in an automatic or semi-automatic manner.

It is another object of the present invention to provide inspection methods that will not disclose its inspection techniques by running on the user's desktop.

It is still another object of the present invention to provide means for dynamically inspecting and correcting each inspected application if malicious content was found.

It is still another object of the present invention to provide said tasks in a simple and efficient manner.

It is still another object of the invention to provide means which can effectively receive indications and reports of inspection results in an automatic or semi-automatic manner.

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.