US006449723B1

(12) **United States Patent**
Elgressy et al.

(10) **Patent No.: US 6,449,723 B1**
(45) **Date of Patent: Sep. 10, 2002**

(54) **METHOD AND SYSTEM FOR PREVENTING THE DOWNLOADING AND EXECUTION OF EXECUTABLE OBJECTS**

(75) Inventors: **Doron Elgressy**, Haifa; **Asher Jospe**, Natanya, both of (IL)

(73) Assignee: **Computer Associates Think, Inc.**, Islandia, NY (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **09/183,690**

(22) Filed: **Oct. 30, 1998**

Related U.S. Application Data

(63) Continuation of application No. PCT/IL98/00083, filed on Feb. 23, 1998.

(30) **Foreign Application Priority Data**

Mar. 10, 1997 (IL) 120420

(51) **Int. Cl.**[7] **G06F 11/30**; G06F 15/173

(52) **U.S. Cl.** **713/201**; 709/224; 709/225

(58) **Field of Search** 713/200, 201; 370/389; 709/223, 224, 225, 226, 229, 331, 332; 714/38

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,414,833 A		5/1995	Hershey et al.	395/575
5,623,600 A	*	4/1997	Ji et al.	713/201
5,983,348 A	*	11/1999	Ji	713/200
6,092,194 A	*	7/2000	Touboul	713/200
6,098,173 A	*	8/2000	Elgressy et al.	713/201
6,125,390 A	*	9/2000	Touboul	709/223
6,154,844 A	*	11/2000	Touboul et al.	713/201
6,167,520 A	*	12/2000	Touboul	713/200
6,321,334 B1	*	11/2001	Jerger et al.	713/200
6,336,140 B1	*	1/2002	Elgressy et al.	709/224
6,345,361 B1	*	2/2002	Jerger et al.	713/200
2001/0049795 A1	*	12/2001	Elgressy et al.	713/200

FOREIGN PATENT DOCUMENTS

WO	WO 99/16225	* 4/1999	H04L/29/06
WO	WO 99/29082	* 6/1999	H04L/29/06

OTHER PUBLICATIONS

Giuri et al, "Role–Based Access Control in Java," May 1998, 3rd ACM Workshop on Role–Based Access, pp. 91–100.*

Kemmerer, Richard, "Security Issues in Distributed Software," 1997, Reliable Software Group, Department of Computer Science University of California, Santa Barbara, pp. 52–59.*

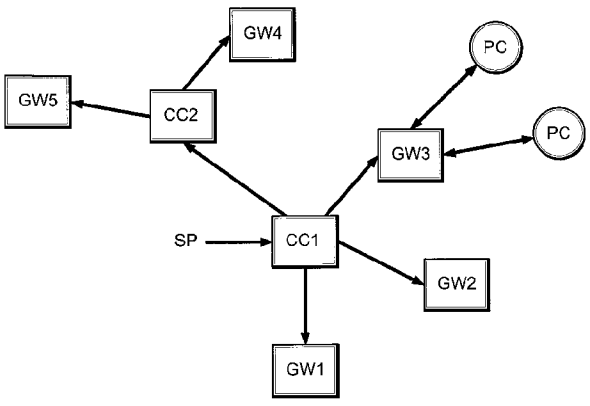
(List continued on next page.)

Primary Examiner—Gail Hayes
Assistant Examiner—Christopher A. Revak
(74) *Attorney, Agent, or Firm*—Cooper & Dunham LLP

(57) **ABSTRACT**

A method for selectively preventing the downloading and execution of undesired Executable Objects in a computer includes analyzing a header of a an Executable Object which is detected at a gateway, determining the resources of a computer that the Executable Object needs to utilize and comparing the resources of the computer that the Executable Object needs to utilize with a user's Security Policy representing the resources, or a combination of resources, that the user allows or does not allow an executable object to utilize within its network. The Executable Object is allowed to pass through the gateway and to reach the computer which has initiated its downloading, if the resources of the computer that the Executable Object needs to utilize are included in the list of the resources allowed for use by the Security Policy. The Executable Object is prevented from passing through the gateway, thereby preventing it from reaching the computer which has initiated its downloading, if the resources of the computer that the Executable Object needs to utilize are included in the list of the resources prohibited for use by the Security Policy.

17 Claims, 2 Drawing Sheets



OTHER PUBLICATIONS

"Security–7 Ltd. Announces Innovative Enterprise Internet Security System," Mar. 1997, PR Newswire, Dialog text search.*

Sharon Machlis: "Screening for Applets", Computerworld, vol. 31, No. 6, Feb. 10, 1997, USA, pp. 51–52.

Dean, D. et al.: "Java Security: From Hot Java to Netscape and Beyond", Proceedings of the 1996 IEEE Symposium on Security and Privacy, Oakland, CA, May 6–8, 1996, No. SYMP. 17, IEEE, pp. 190–200.

* cited by examiner

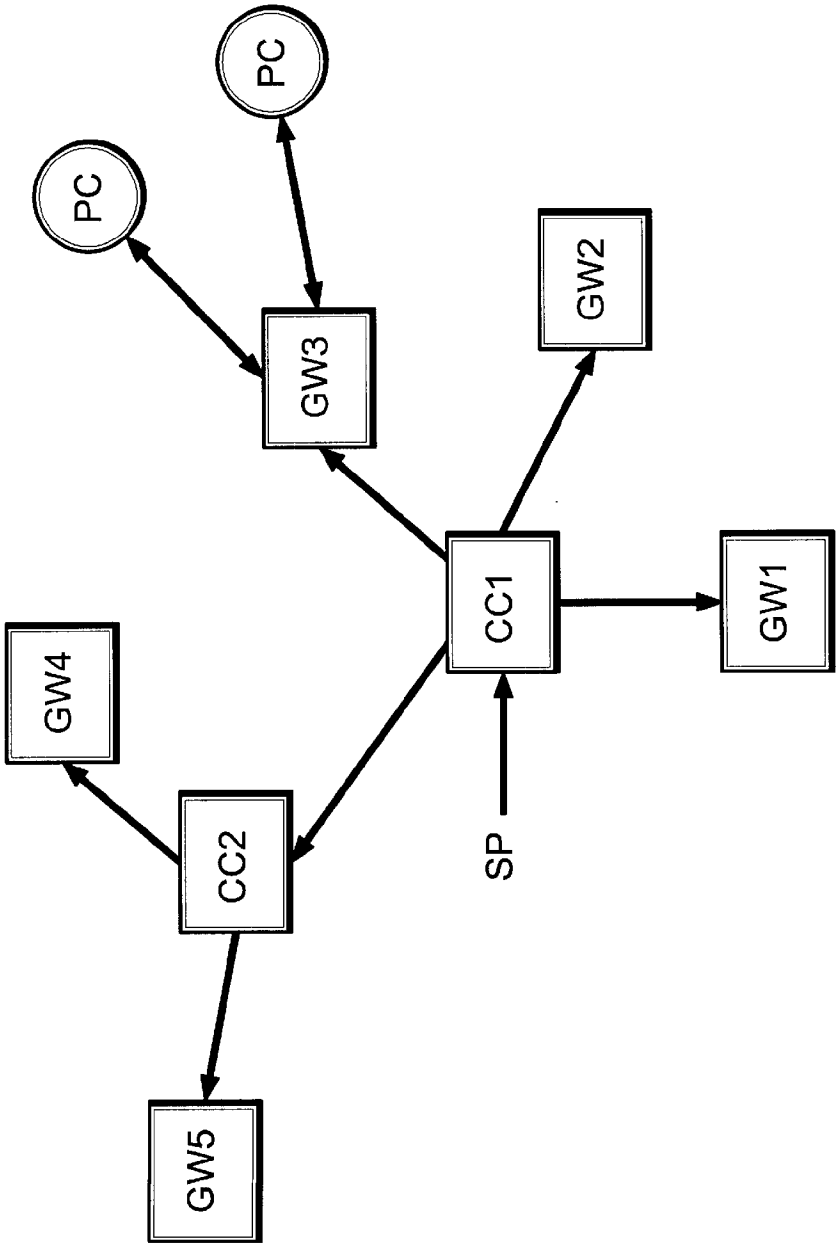


FIG. 1

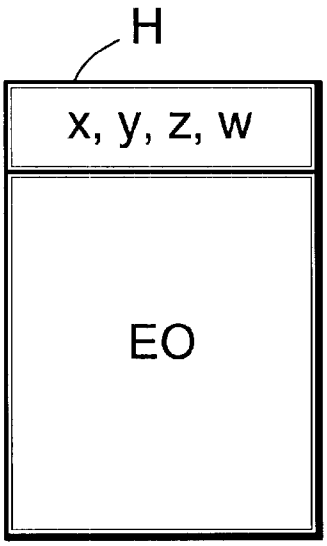


FIG. 2

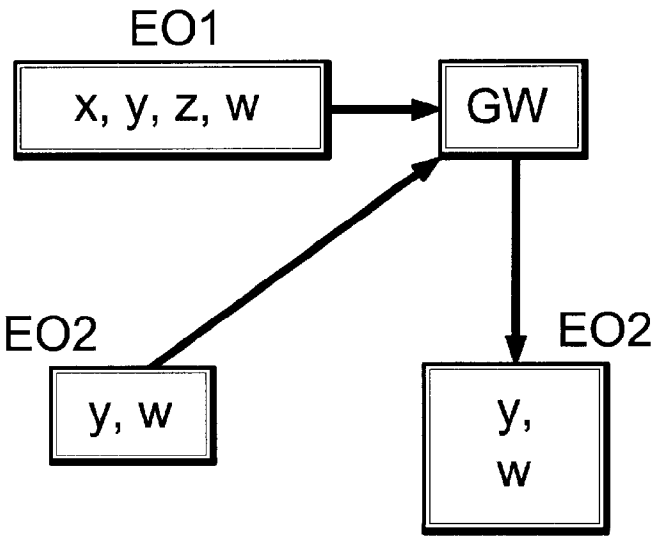


FIG. 3

METHOD AND SYSTEM FOR PREVENTING THE DOWNLOADING AND EXECUTION OF EXECUTABLE OBJECTS

CROSS-REFERENCED TO RELATED APPLICATION

This application is a continuation of co-pending application PCT/IL98/00083 filed Feb. 23, 1998 entitled "Method and System for Preventing the Downloading and Execution of Executable Objects".

FIELD OF THE INVENTION

The present invention relates to the security management of computer networks. More particularly, the invention relates to methods and systems for preventing the downloading and execution of undesirable Executable Objects in a workstation of a computer network.

BACKGROUND OF THE INVENTION

The Internet has developed very much both in respect of its contents and of the technology employed, since it began a few years ago. In the early days of the Internet, web sites included text only, and after a while graphics was introduced. As the Internet developed, many compressed standards, such as pictures, voice and video files, were developed and with them programs used to play them (called "players"). Initially, such files were downloaded to the user's workstation only upon his request, and extracted only by the appropriate player, and after a specific order from the user.

When, in the natural course of the development of the World Wide Web the search for a way to show nicer, interactive and animated Web Pages began, Sun Microsystems Inc. developed Java—a language that allows the webmaster to write a program, a list of commands—Network Executables— that will be downloaded to the user workstation without his knowledge, and executed by his browser at his workstation. The executables are used, e.g., to provide photographic animation and other graphics on the screen of the web surfer. Such executables have some ways approaching the user workstation's resources, which lead to a great security problem. Although some levels of security were defined in the Java language, it was very soon that a huge security hole was found in the language.

Since Java was developed, Microsoft developed ActiveX, which is another Network Executable format, also downloaded into the workstation. ActiveX has also security problems of the same kind.

The Internet has been flooded with "Network Executables" which may be downloaded—deliberately or without the knowledge of the users—into workstations within organizations. These codes. generally contain harmless functions. Although usually safe, they may not meet the required security policy of the organization.

Once executed, codes may jam the network, cause considerable irreversible damage to the local database, workstations and servers, or result in unauthorized retrieval of information from the servers/workstations. Such elements may appear on Java applets, ActiveX components, DLLs and other object codes, and their use is increasing at an unparalleled pace. The majority of these small programs are downloaded into the organization unsolicited and uncontrolled. The enterprise has no way of knowing about their existence or execution and there is no system in place for early detection and prevention of the codes from being executed.

The security problem was solved partially by the browser manufactures which allow the user to disable the use of executables. Of course this is not a reasonable solution, since all the electronic commerce and advertising are based on the use of executables. The security problem is much more serious once such an executable can approach the enterprise servers, databases and other workstations.

It is therefore clear that it is highly needed to be able to prevent undesirable Executable Objects from infiltrating the LAN/WAN in which we work and, ultimately, our workstation and server. However, so far the art has failed to provide comprehensive solutions which are safe and quick enough to be practically useful. Systems such as "Firewall" or "Finjan", distributed for use by Internet users, provide only partial solutions and, furthermore, are difficult to install and to update.

SUMMARY OF THE INVENTION

It is an object of the present invention to provide a comprehensive method for selectively preventing the downloading and execution of undesired Executable Objects in a computer, which overcomes the aforesaid drawbacks of prior art systems.

It is another object of the invention to provide such a system which is easy to install and which can be quickly and easily updated.

It is a further object of the invention to provide such a method which can be used with a large number of gateways, LAN's and workstations.

It is yet another object of the invention to provide such a security management system which is independent of the physical infrastructure and network layout.

It is a further object of the invention to provide a system which analyzes the executables "on the fly", and does not hinder the downloading and he operation of harmless executables.

It is yet a further object of the invention to provide a system of the kind described above, which operates as a central security system to which peripheral gateways may be added as needed, to provide a simple, dynamically growing security system.

It is furthermore an object of the invention to provide a central system which permits to define sub-groups of users. each group being subject to a different security policy.

Also encompassed by the invention is a computer system which utilizes the method of the invention.

Other advantages and objects of the invention will become apparent as the description proceeds.

The method for selectively preventing the downloading and execution of undesired Executable Objects in a computer, according to the invention, comprises the steps of:

(a) providing one or more Control Centers, each connected to one or more gateways located between a LAN and an external computer communication network;

(b) providing means coupled to each of said gateways, to detect Executable Objects reaching said gateway, to analyze the header of each of said Executable Objects, and to determine the resources of the computer that the Executable Object needs to utilize;

(c) providing means coupled to each of said gateways, to store a user's Security Policy representing the resources, or combination of resources, that the user allows or does not allow an Executable Object to utilize within its LAN, wherein the Security Policy is received from and/or stored in each of said one or more Control Centers;

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.