07/29/99 jc674 U.S. PTO

PROVISIONAL PATENT APPLICATION cover sheet

A/PROV

This is a request for filing a PROVISIONAL APPLICATION under 37 C.F.R. § 1.53(c)

CERTIFICATE OF EXPRESS MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Services "Express Mail Post Office to Addressee" service under 37 CFR 1.10, in an envelope addressed to: Assistant Commissioner for Patents, Washington, D.C. 20231 on July 29, 1999.

Express Mail Label No. **EL133803643US**

Signed: Roger Yamamoto
Roger Yamamoto

EL133803643US

	Docket No.	07451.6005-00000	Type a plus sign (+) inside this box →	+

INVENTOR(S)/APPLICANT(S)

LAST NAME	FIRST NAME	MIDDLE INITIAL	RESIDENCE (City & Either State or Foreign Country)
SIBERT	W	OLIN	Lexington, MA

TITLE OF THE INVENTION ***(280 characters max.)***

SYSTEMS AND METHODS FOR USING CRYPTOGRAPHY TO PROTECT SECURE AND INSECURE COMPUTING ENVIRONMENTS

CORRESPONDENCE ADDRESS

FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER, L.L.P.
1300 I Street, N.W.
Washington, D.C. 20005
Telephone No.: (202) 408-4000

jc841 U.S. PTO 60/146426 07/29/99

ENCLOSED APPLICATION PARTS ***(check all that apply)***

- ☒ Specification consisting of 43 pages.
- ☐ Small Entity Statement
- ☒ Drawing(s)
  - Number of Sheets: 28 sheets of drawings (Figs. 1-22B)
- ☒ Other (specify): 17 pages of claims (71 claims) and 1 page of Abstract

METHOD OF PAYMENT ***(check one)***

☐ A check or money order is enclosed to cover the Provisional filing fees. ☒ The Commissioner is hereby authorized to charge filing fees and credit Deposit Account Number 06-0916.	PROVISIONAL FILING FEE ☒ $150.00

The invention was made by an agency of the United States Government or under a contract with an agency of the United States Government.

- ☒ No.
- ☐ Yes, the name of the U.S. Government agency and the Government contract number are:

Respectfully submitted,

SIGNATURE: _____ Date: July 29, 1999

Typed or Printed Name: C. Larry O'Rourke Registration No.: 26,014

☐ Additional inventors are being named on separately numbered sheets attached hereto.

PROVISIONAL APPLICATION FILING ONLY

SYSTEMS AND METHODS FOR USING CRYPTOGRAPHY TO PROTECT SECURE AND INSECURE COMPUTING ENVIRONMENTS

FIELD OF THE INVENTION

The present invention relates to computer security, and more particularly to secure and/or protected computer execution environments. Still more specifically, the present invention relates to computer security techniques based at least in part on cryptography, that protect a computer processing environment against potentially harmful computer executables, programs and/or data; and to techniques for certifying load modules such as executable computer programs or fragments thereof as being authorized for use by a protected or secure processing environment.

BACKGROUND AND SUMMARY OF THE INVENTION

Computers have become increasingly central to business, finance and other important aspects of our lives. It is now more important than ever to protect computers from "bad" or harmful computer programs. Unfortunately, since many of our most critical business, financial and governmental tasks now rely heavily on computers, dishonest people have a great incentive to use increasingly sophisticated and ingenious computer attacks.

Imagine, for example, if a dishonest customer of a major bank could reprogram the bank's computer so it adds to instead of subtracts from the customer's account — or diverts a penny to the customer's account from anyone else's bank deposit in excess of $10,000. If successful, such attacks would not only allow dishonest people to steal, but could also undermine society's confidence in the integrity and reliability of the banking system.

Terrorists can also try to attack us through our computers. We cannot afford to have harmful computer programs destroy the computers driving the greater San Francisco metropolitan air traffic controller network, the New York Stock Exchange, the life support systems of a major hospital, or the Northern Virginia metropolitan area fire and paramedic emergency dispatch service.

There are many different kinds of "bad" computer programs, which in general are termed "Trojan horses" — programs that cause a computer to act in a manner not intended by its operator, named after the famous wooden horse of Troy that delivered an attacking army disguised as an attractive gift. One of the most notorious kinds is so-called "computer viruses" — "diseases" that a computer can "catch" from another computer. A computer virus can be a computer program that instructs the computer to do harmful or spurious things instead of useful things — and can replicate itself to spread from one computer to another. Since the computer does whatever its instructions tell it to do, it will carry out the bad intent of a malicious human programmer who wrote the computer virus program — unless the computer is protected from the computer virus program. Special "anti-virus" protection software exists, but it unfortunately is only partially effective — for example, because new viruses can escape detection until they become widely known and recognized, and because sophisticated viruses can escape detection by masquerading as tasks the computer is supposed to be performing.

Computer security risks of all sorts — including the risks from computer viruses — have increased dramatically as computers have become increasingly connected to one another over the Internet and by other means. Increased computer connectivity provides increased capabilities, but also creates a host of computer security problems that haven't been fully solved. For example, electronic networks are an obvious path for spreading computer viruses. In October 1988, a university student used the Internet (a network of computer networks connected to millions of computers worldwide) to infect thousands of university and business computers with a self-replicating "worm" virus that took over the infected computers and caused them to execute the computer virus instead of performing

the tasks they were supposed to perform. This computer virus outbreak (which resulted in a criminal prosecution) caused widespread panic throughout the electronic community.

Computer viruses are by no means the only computer security risk made even more significant by increased computer connectivity. For example, a significant percentage of the online electronic community has recently become committed to a new "portable" computer language called Java™ developed by Sun Microsystems of Mountain View, California. Java was designed to allow computers to interactively and dynamically download computer program code fragments (called "applets") over an electronic network such as the internet, and execute the downloaded code fragments locally. The Java programming language's "download and execute" capability is valuable because it allows certain tasks to be performed locally on local equipment using local resources. For example, a user's computer could run a particularly computationally or data-intensive routine — relieving the provider's computer from having to run the task and/or eliminating the need to transmit large amounts of data over the communications path.

While Java's "download and execute" capability has great potential, it raises significant computer security concerns. For example, Java applets could be written to damage hardware, software or information on the recipient computer, make the computer unstable by depleting its resources, and/or access confidential information on the computer and send it to someone else without first getting the computer owner's permission. People have expended large amounts of time and effort trying to solve Java's security problems. To alleviate some of these concerns, Sun Microsystems has developed a Java interpreter providing certain built-in security features such as:

- a Java verifier that will not let an applet execute until the verifier verifies the applet doesn't violate certain rules,
- a Java class loader that treats applets originating remotely differently from those originating locally,
- a Java security manager that controls access to resources such as files and network access, and

In addition, Sun has indicated that in the future the Java interpreter may use digital signatures to authenticate applets.

Numerous security flaws have been found despite these techniques. Moreover, a philosophy underlying this overall security design is that a user will have no incentive to compromise the security of her own locally installed Java interpreter — and that any such compromise is inconsequential from a system security standpoint because only the user's own computer (and its contents) are at risk. This philosophy — which is typical of many security system designs — is seriously flawed in many useful electronic commerce contexts.

Load modules may contain algorithms, data, cryptographic keys, shared secrets, and/or other information that permits a load module to interact with other system components (e.g., other load modules and/or computer programs operating in the same or different protected processing environment). For a load module to operate and interact as intended, it should execute without unauthorized modification and its contents may need to be protected from disclosure.

Unlike many other computer security scenarios, there may be a significant incentive for an owner of a protected processing environment to attack his or her own protected processing environment. For example:

- the owner may wish to "turn off" payment mechanisms necessary to ensure that people delivering content and other value receive adequate compensation; or
- the owner may wish to defeat other electronic controls preventing him or her from performing certain tasks (for example, copying content without authorization); or
- the owner may wish to access someone else's confidential information embodied within electronic controls present in the owner's protected processing environment; or

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.