US005935246A

United States Patent [19]

Benson

[11] **Patent Number: 5,935,246**

[45] **Date of Patent: Aug. 10, 1999**

[54] **ELECTRONIC COPY PROTECTION MECHANISM USING CHALLENGE AND RESPONSE TO PREVENT UNAUTHORIZED EXECUTION OF SOFTWARE**

[75] Inventor: **Glenn Stuart Benson**, Munich, Germany

[73] Assignee: **International Computers Limited**, London, United Kingdom

[21] Appl. No.: **08/838,620**

[22] Filed: **Apr. 11, 1997**

[30] **Foreign Application Priority Data**

Apr. 26, 1996 [GB] United Kingdom 9608696

[51] **Int. Cl.**[6] **G06F 12/14**

[52] **U.S. Cl.** **713/200**; 713/201; 713/202

[58] **Field of Search** 395/186, 387, 395/860, 187.01; 380/25, 4, 21, 23, 30; 713/200

[56] **References Cited**

U.S. PATENT DOCUMENTS

4,558,176	12/1985	Arnold et al.	178/22.08
4,926,480	5/1990	Chuam	380/23
4,947,430	8/1990	Chaum	380/25
5,109,413	4/1992	Comerford et al.	380/4
5,146,575	9/1992	Nolan, Jr.	395/425
5,224,163	6/1993	Gasser et al.	380/30
5,315,657	5/1994	Abadi et al.	380/25
5,371,794	12/1994	Diffie et al.	380/21
5,436,972	7/1995	Fischer	380/25
5,568,552	10/1996	Davis	380/4
5,724,425	3/1998	Chang et al.	380/25

FOREIGN PATENT DOCUMENTS

WO 88/05941 8/1988 WIPO .

OTHER PUBLICATIONS

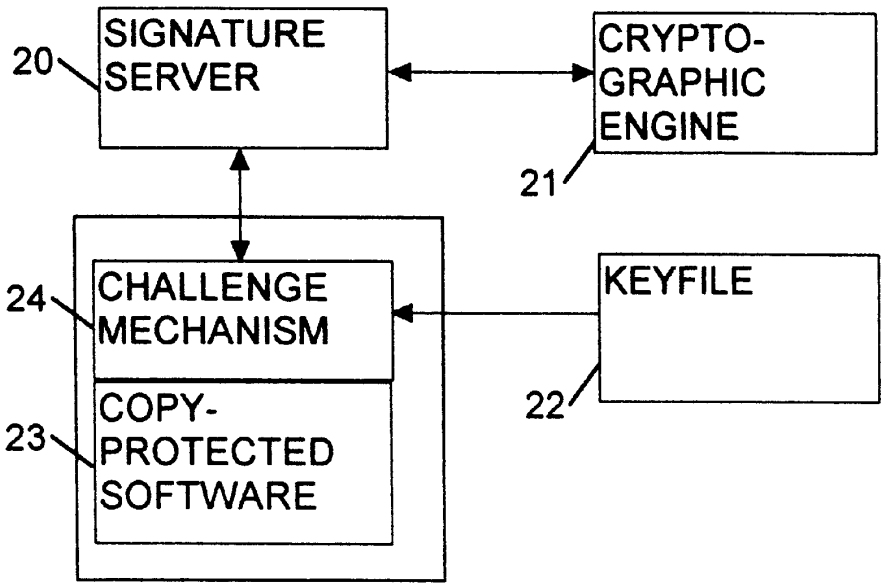
Davis, "Cryptographic Randomnes From Air Turbulence In Disk Driver", Advances in Cryptology, Conference 14, Aug. 21, 1994, pp. 114–120.

Primary Examiner—Hassan Kizou
Assistant Examiner—Rijue Mai
Attorney, Agent, or Firm—Lee, Mann, Smith, McWilliams, Sweeney & Ohlson

[57] **ABSTRACT**

A copy protection mechanism for protecting software against copying, consists of a challenge mechanism embedded in each protected item of software. The challenge mechanism has no access to the customer's private keying material. In operation, the challenge mechanism sends a random challenge to the customer's signature server. The signature server signs the challenge, using the customer's private keying material and then returns the signed challenge to the challenge mechanism. The challenge mechanism then verifies the signed challenge, using the customer's public keying material, and prohibits the customer from using some or all of the protected item of software unless the verification is successful. The mechanism permits every customer to receive an identical copy of the copy protected program with the embedded challenge mechanism.

25 Claims, 3 Drawing Sheets



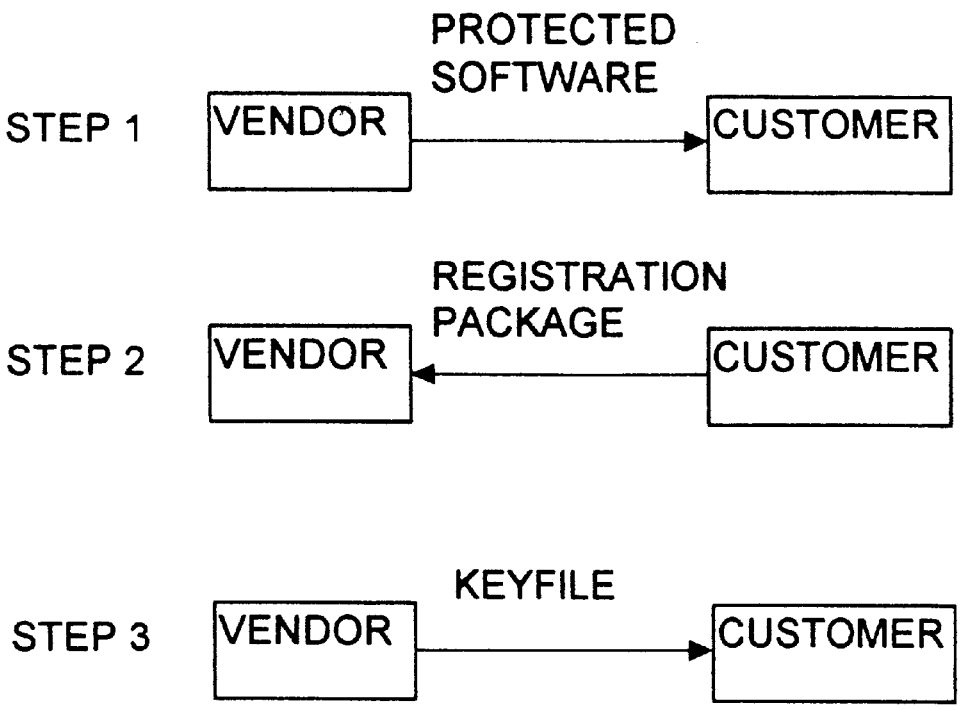


FIG. 1

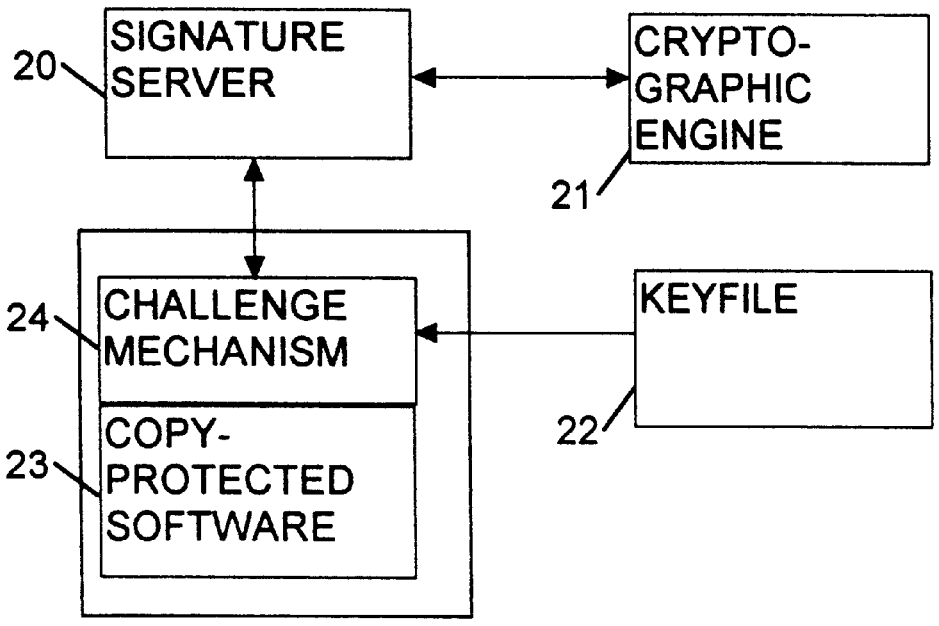


FIG. 2

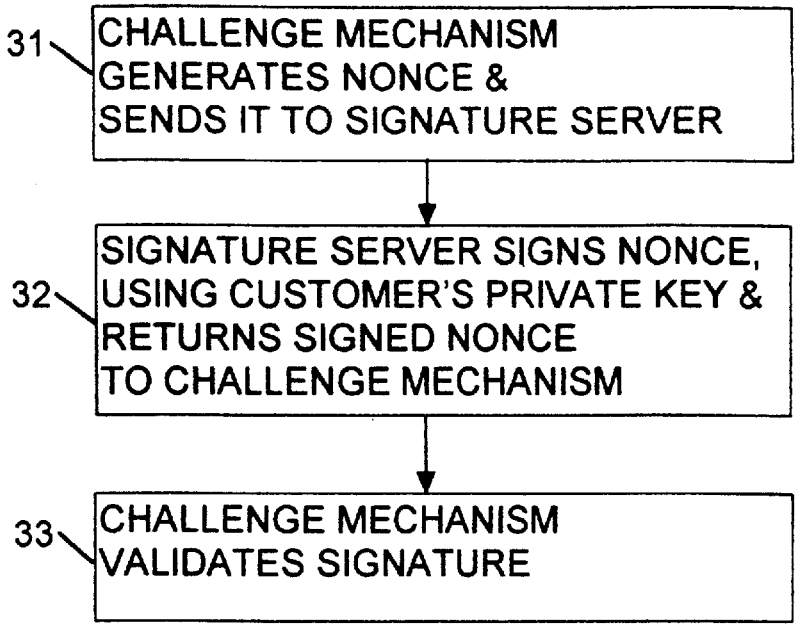


FIG. 3

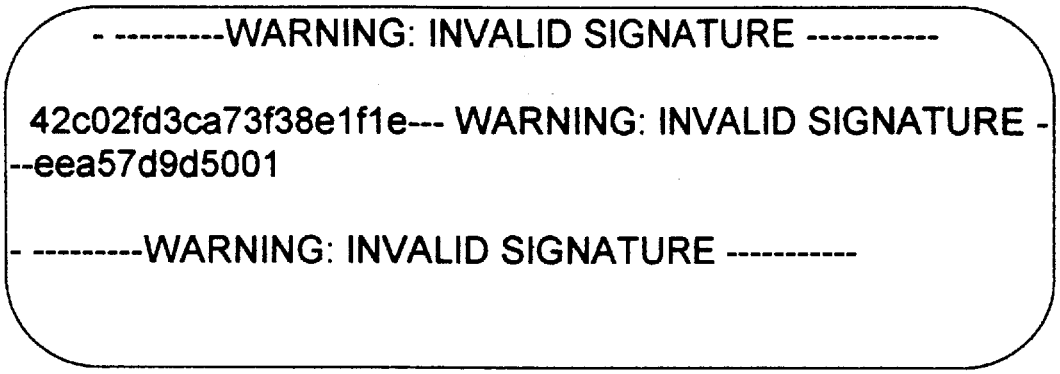


FIG. 4

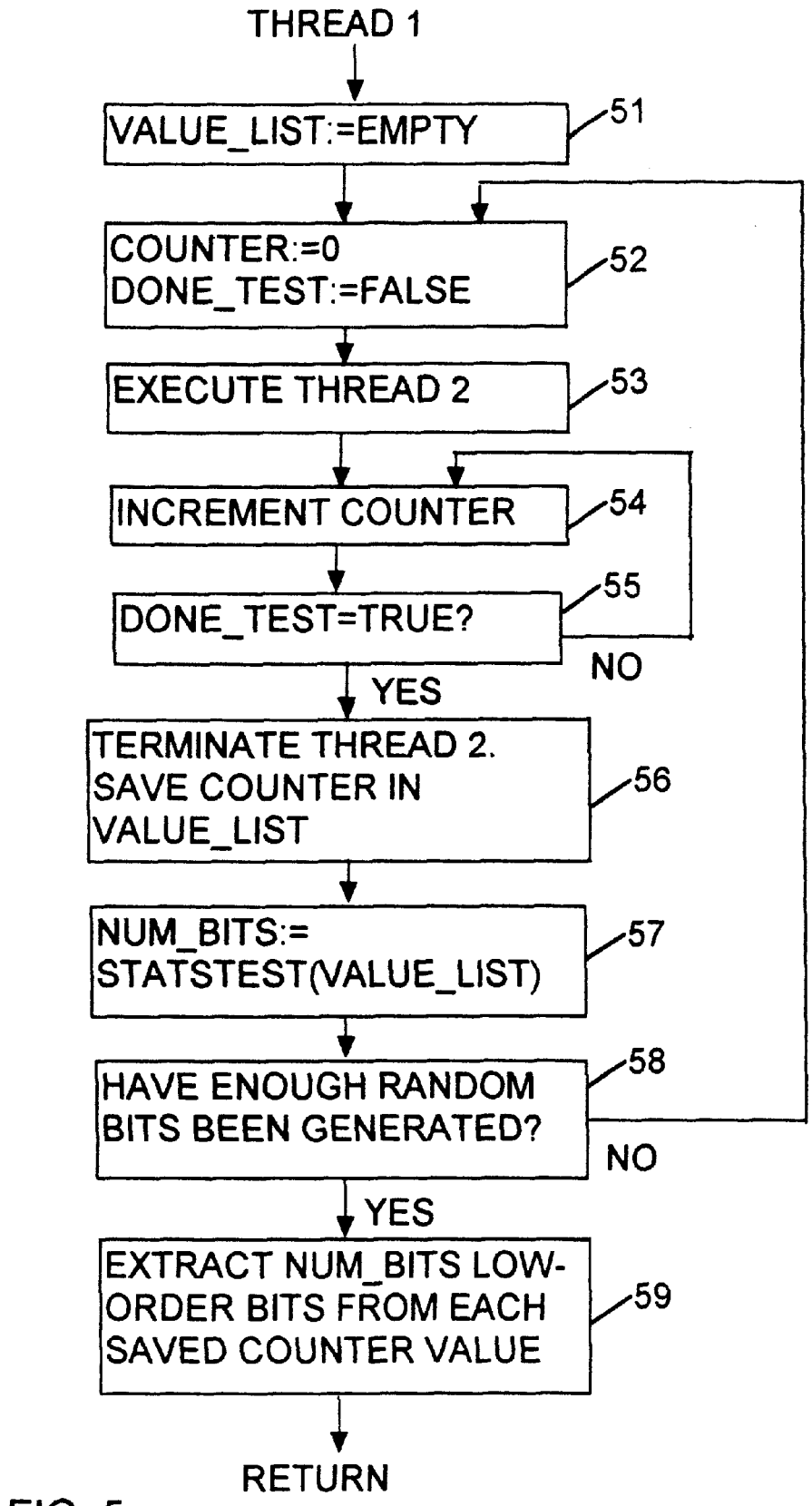


FIG. 5

ELECTRONIC COPY PROTECTION MECHANISM USING CHALLENGE AND RESPONSE TO PREVENT UNAUTHORIZED EXECUTION OF SOFTWARE

BACKGROUND TO THE INVVENTION

This invention relates to electronic copy protection mechanisms for protecting software against unauthorized copying.

The Business Software Alliance estimates the 1995 financial losses attributed to software piracy as US$8.1 Billion for business application software and US$15.2 Billion for all software. Solutions have been proposed in two areas: (i) improved Intellectual Property Rights (IPR) legislation, and (ii) enhanced electronic copy protection (ECP) mechanisms. IPR legislation and enforcement are improving in many countries, but there are still significant difficulties in other parts of the world. As a result, some vendors are currently reassessing ECP.

It is desirable for any ECP mechanism to satisfy the following requirements.

The ECP mechanism should prohibit unauthorized users from executing copy protected software.

The ECP mechanism should not prohibit the user from making backups.

The ECP mechanism should make only standard hardware and software assumptions. For example, although hardware dongles provide excellent copy protection services, many vendors do not wish to limit the sale of the software to the collection of users who own or are willing to install a dongle.

The ECP mechanism should have minimal impact upon the user interface. The visible impact should be limited to the customer's initial login to the operating system and/or smart card. Subsequent impact upon the user interface should be relegated to relatively minor performance concerns.

The ECP mechanism should not limit execution of the copy protected software to a limited collection of machines. When a customer legitimately purchases software, the customer should be able to execute the software on any machine regardless of ownership. The customer should optionally be able to authorize simultaneous execution of the software on multiple machines.

The ECP mechanism should have no required network dependencies in order to execute an already purchased copy protected program.

The vendor should be permitted to distribute an identical version of the copy protected software to all users. This requirement permits the copy protected software to be distributed through normal channels such as, for example, CD-ROMs, floppy disks, or network bulletin boards.

It should be excessively difficult and/or computationally infeasible for a potential software pirate to circumvent the copy protection mechanism without modifying the copy protected program. This requirement serves as an important virus-protection measure because a digital signature supplied by the vendor would not validate if a pirate distributes a modified version of the original program.

The ECP mechanism should not compromise any of the customer's private keying material. In particular, the ECP mechanism should not disclose the customer's private keying material to the vendor, any program produced by the vendor, or any simple Trojan horse program. While the primary functionality of copy protection is to protect the software vendor, one must not do so at the expense of the customer.

The ECP mechanism should be available in either a software-only version or a hardware-assisted (smart card) version, to assure widespread market acceptance.

The least time consuming attack by a potential software pirate should be byte-code disassembly of the copy protected software. In order to thwart the copy protection mechanism, the pirate must remove or change the ECP. Choudhury et al. ["Copyright Protection for Electronic Publishing over Computer Networks", available as at Mar. 27, 1996 on Word Wide Web at http://ftp.research.att.com/dist/anoncc/copyright.epub.ps.Z] propose a mechanism in which a protected document can be viewed only via a specially configured viewer program, which allows a user to view the document only if the user supplies the viewer with the user's private keying material. This deters the user from distributing unauthorized copies of the viewer program, since that would require the user to divulge his or her private keying material to others. However, because Choudhury's mechanism requires that the viewer program obtain access to the customer's private keying material, it breaks one of the requirements listed above. Furthermore, Choudhury's mechanism may not be used in conjunction with a smart card that is configured to avoid releasing private keying material.

The object of the present invention is to provide an improved ECP mechanism that is able to satisfy the above requirements.

The ECP mechanism of the present invention makes use of asymmetric cryptography, also known as public key cryptography. In asymmetric cryptography, each user has public keying material and private keying material. Each user may post his or her public keying material to a publicly accessed directory without compromising the corresponding private keying material. Normally, the user guards the private keying material as a close secret. Using the RSA asymmetric encryption algorithm, for example, a pair of users may encrypt and then subsequently decrypt a message using either of two methods: (i) encrypt using the public keying material and decrypt using the private keying material; or (ii) encrypt using the private keying material and decrypt using the public keying material. Two examples are presented below.

Secret message: A user, Alice, posts her public keying material to a well-known directory or bulletin board. A second user, Bob, wishes to send a confidential message to Alice. Bob encrypts the message using Alice's public keying material and sends the encrypted message to Alice. Since Alice is the only user with access to the corresponding private keying material, only Alice may decrypt the message to discover its original content.

Digital signature: A digital signature is an electronic analog of a handwritten signature. After posting her public keying material, Alice encrypts a message using the private keying material. Since anyone may access the public keying material, there is no message secrecy. However, since Alice is the only user with access to the private keying material, no one else can "forge Alice's signature" by performing the encryption. Any user may validate Alice's signature using the public keying material.

Both examples depend upon the fact that Alice closely guards her private keying material. Otherwise, the crypto-

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.