US006138236A

United States Patent [19]

Mirov et al.

[11] Patent Number: 6,138,236

[45] Date of Patent: *Oct. 24, 2000

[54] **METHOD AND APPARATUS FOR FIRMWARE AUTHENTICATION**

[75] Inventors: **Russell Norman Mirov**, Los Altos; **Gregory Charles Onufer**, Sunnyvale, both of Calif.

[73] Assignee: **Sun Microsystems, Inc.,** Palo Alto, Calif.

[*] Notice: This patent issued on a continued prosecution application filed under 37 CFR 1.53(d), and is subject to the twenty year patent term provisions of 35 U.S.C. 154(a)(2).

[21] Appl. No.: **08/674,026**

[22] Filed: **Jul. 1, 1996**

[51] **Int. Cl.^{7}** **G06F 11/30**; H04L 9/00
[52] **U.S. Cl.** **713/200**; 713/202
[58] **Field of Search** 713/200, 201, 713/202, 155, 161, 180; 380/282, 281

[56] **References Cited**

U.S. PATENT DOCUMENTS

5,448,045   9/1995   Clark 235/382

5,481,612	1/1996	Campana et al.	380/25
5,535,409	7/1996	Larvoire et al.	395/800
5,537,540	7/1996	Miller et al.	395/183.14
5,586,327	12/1996	Bealkowski et al.	395/652
5,621,796	4/1997	Davis et al.	380/24
5,633,930	5/1997	Davis et al.	380/24
5,643,086	7/1997	Alcorn et al.	380/25 X
5,768,382	6/1998	Schneier et al.	380/23

[57] **ABSTRACT**

An apparatus for firmware authentication and methods of operating the same result in software upgradability to firmware without compromising the integrity of the firmware. The apparatus for firmware authentication of a boot PROM comprises a software programmable data section having a plurality of micro-code. An authentication section having a hash generator configured to generate a data hash in response to the plurality of micro-code programmed in the software programmable data section to authorize execution of the plurality of micro-code of the data section.
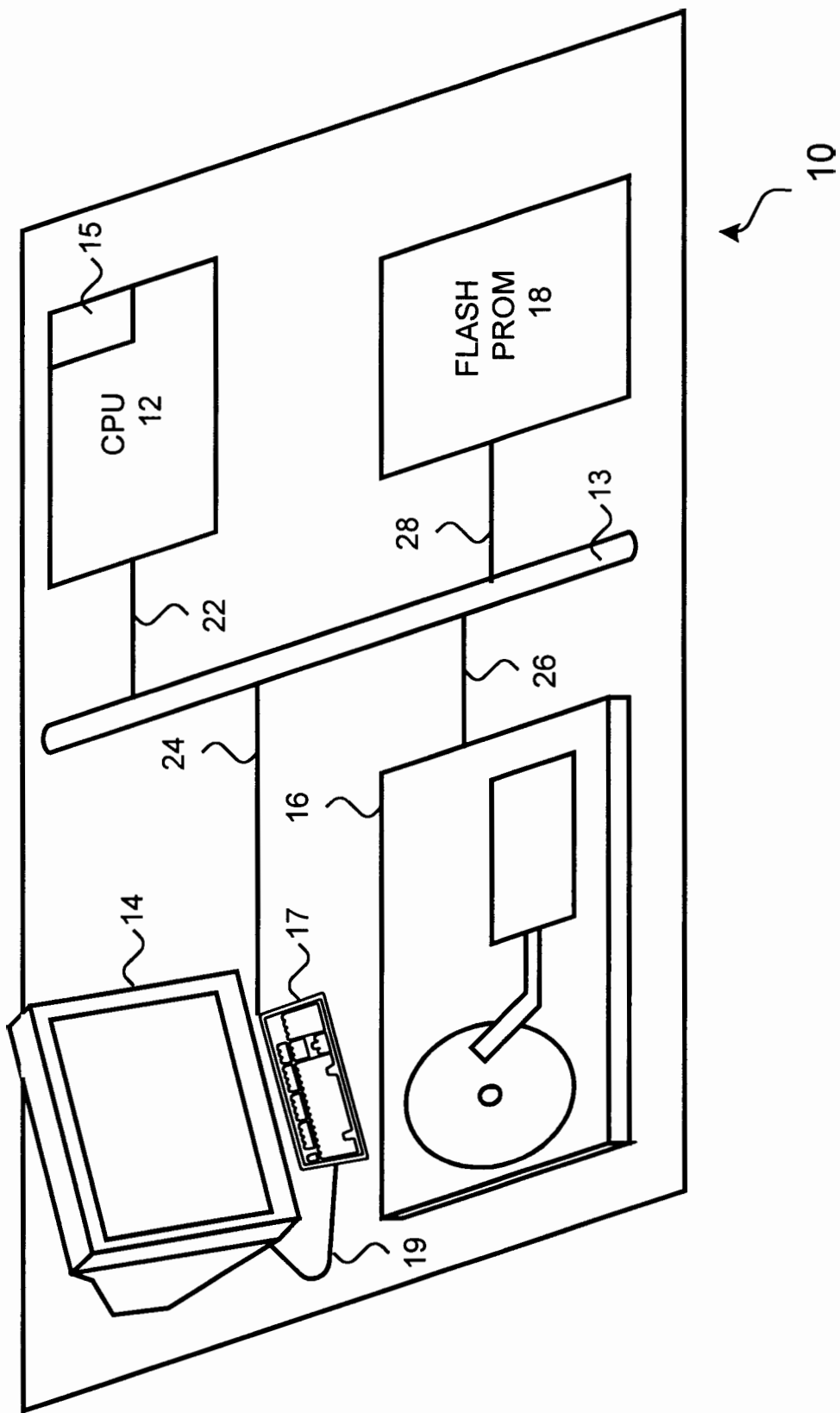
17 Claims, 4 Drawing Sheets

FIG. 1

18

PUBLIC KEY 56	SIGNATURE 57
DECRYPTOR 54	
HASH GENERATOR 53	UNSECURED MICRO-CODE 58
COMPARATOR 52	
SECURED MICRO-CODE 51	

45   55

FIG. 2

CALCULATE VERIFICATION
HASH FROM MICRO-CODE
62

OBTAIN PRIVATE KEY
64

ENCRYPT WITH PRIVATE KEY
AND VERIFICATION HASH TO
OBTAIN SIGNATURE
66

SAVE SIGNATURE
68

FIG. 3

```
┌─────────────────────────┐
│   GENERATE DATA HASH     │
│    FROM PROGRAMMED       │
│  UNSECURED MICRO-CODE    │
│           72             │
└─────────────────────────┘
             │
             ▼
┌─────────────────────────┐
│   DECRYPT VERIFICATION   │
│  HASH WITH PUBLIC KEY    │
│      AND SIGNATURE       │
│           73             │
└─────────────────────────┘
             │
             ▼
┌─────────────────────────┐
│   COMPARE VERIFICATION   │
│   HASH WITH DATA HASH    │
│           74             │
└─────────────────────────┘
             │
             ▼
```

```
               IF
NO        VERIFICATION        YES
   ◄── HASH MATCHES DATA ──►
               HASH
                75
```

┌─────────────────────────┐   ┌─────────────────────────┐
│   ALERT USER, PROVIDE   │   │ EXECUTE MICRO-CODE OF   │
│   RECOVERY OPTIONS   │   │ PROGRAMMABLE SECTION   │
│   78   │   │   77   │
└─────────────────────────┘   └─────────────────────────┘

FIG. 4

DOCKET ALARM
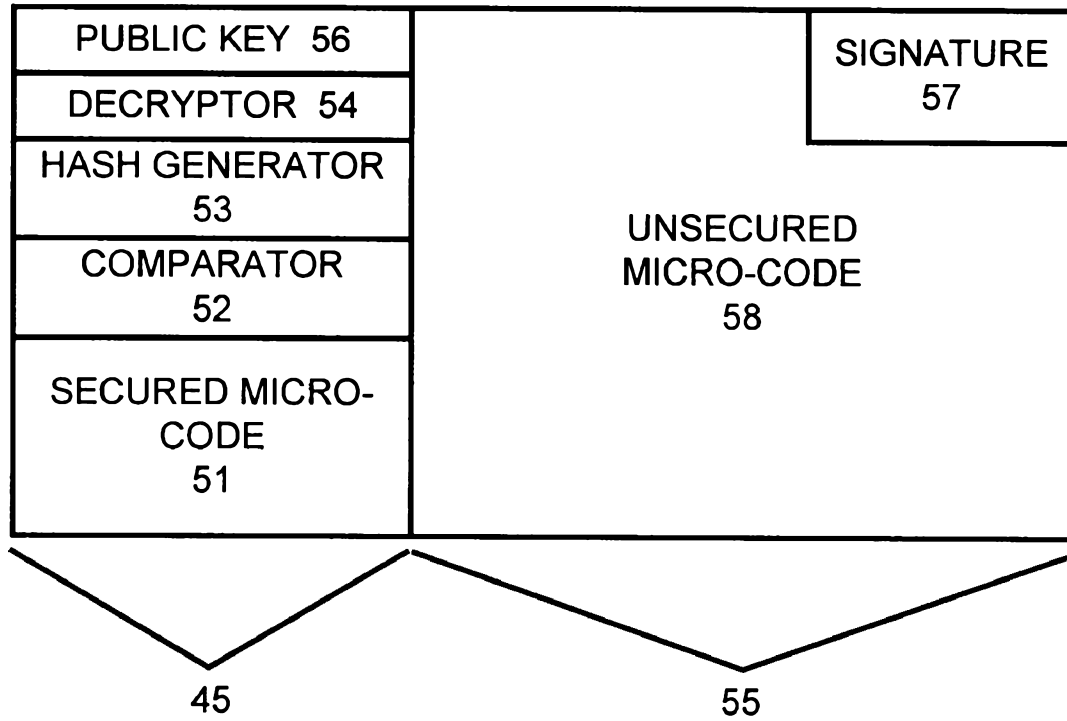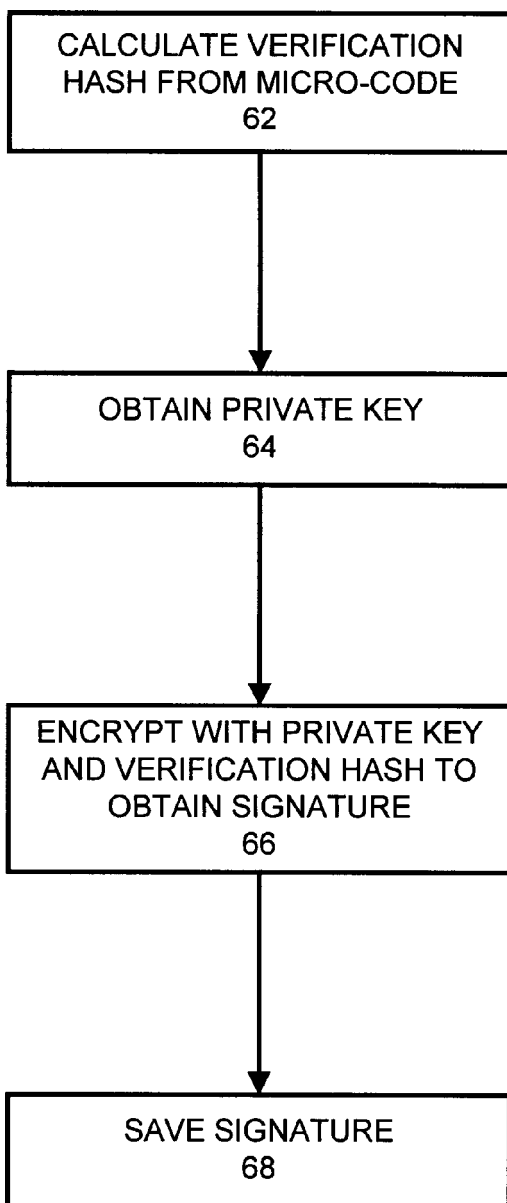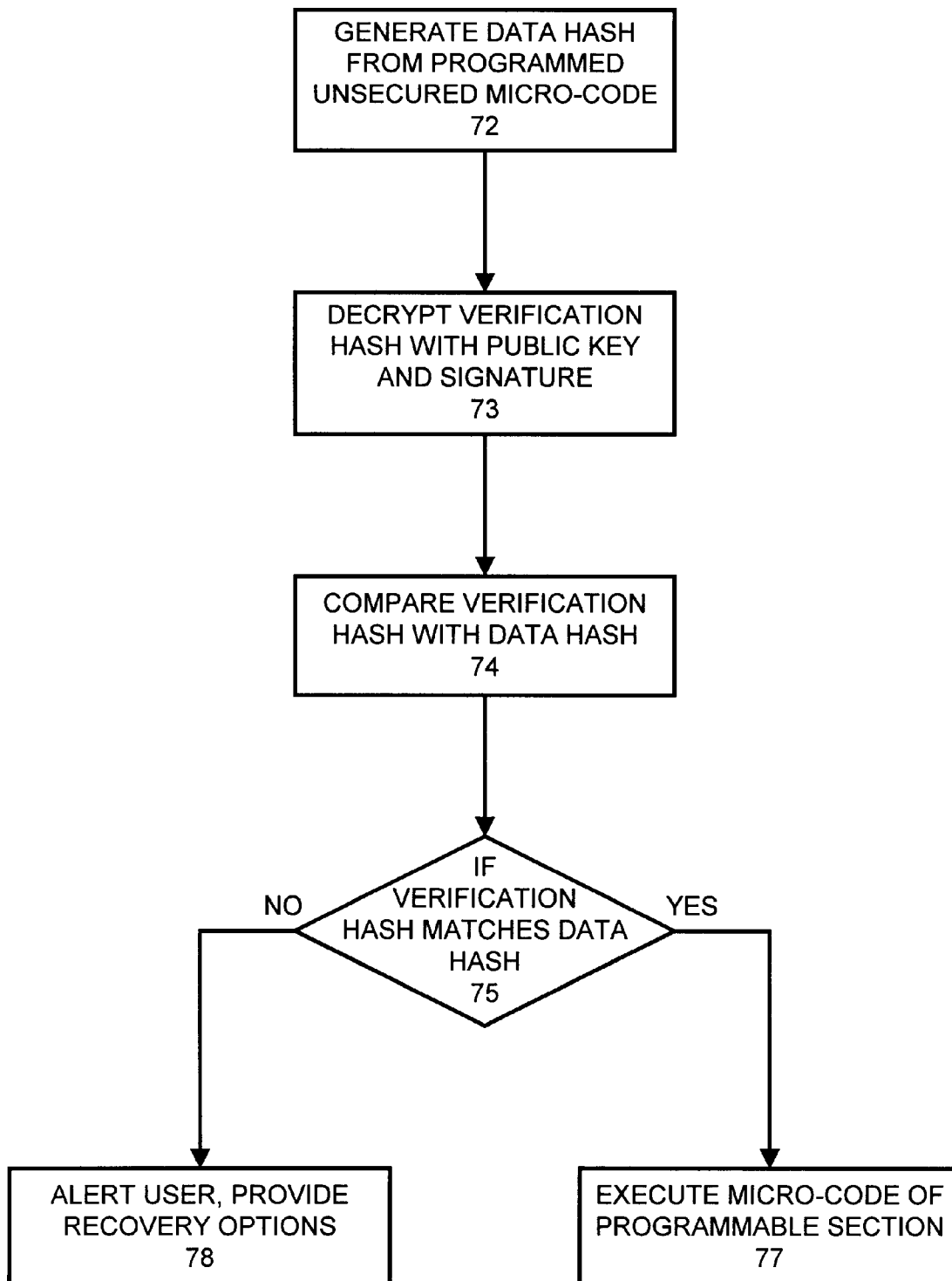
Explore Litigation Insights

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.

fastcase®
Smarter legal research.