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

(10) **Patent No.:** **US 7,069,452 B1**
(45) **Date of Patent:** **Jun. 27, 2006**

(54) **METHODS, SYSTEMS AND COMPUTER PROGRAM PRODUCTS FOR SECURE FIRMWARE UPDATES**

(75) Inventors: **John R. Hind**, Raleigh, NC (US); **Marcia Lambert Peters**, Durham, NC (US)

(73) Assignee: **International Business Machines Corporation**, Armonk, NY (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 1207 days.

(21) Appl. No.: **09/614,982**

(22) Filed: **Jul. 12, 2000**

(51) **Int. Cl.**
G06F 17/00 (2006.01)
(52) **U.S. Cl.** **713/200**; 713/189; 713/1; 713/2
(58) **Field of Classification Search** 703/200; 713/1–2, 200–202, 189–194
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,022,077 A	*	6/1991	Bealkowski et al.	.... 711/163
5,293,424 A	*	3/1994	Holtey et al.	.... 713/193
5,579,522 A	*	11/1996	Christeson et al.	.... 713/2
5,844,986 A	*	12/1998	Davis	.... 713/187

OTHER PUBLICATIONS

"Introduction to Digtial Signal Processors", Jun. 15, 1999, [Retrieved from the Internet Apr. 29, 2004], "http://www.ece.utexas.edu/~bevans/hp-dsp-seminar/01__introduction/".*
ANSI Standard X9.31. Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry (rDSA), 1998.
Schneier, Bruce, *Applied Cryptography*, Dec. 1995, pp. 435-441 and 466-474.
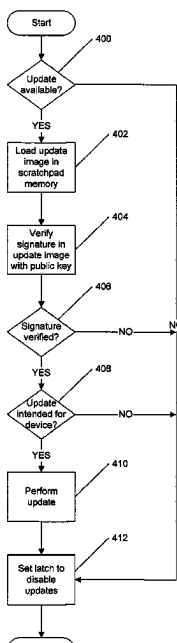
* cited by examiner

Primary Examiner—David Jung
(74) *Attorney, Agent, or Firm*—Myers Bigel Sibley & Sajovec

(57) **ABSTRACT**

Methods, systems and computer program products which provide secure updates of firmware (i.e. data stored in a programmable memory device of a processing system) are disclosed. Updates of a programmable memory of a device may be controlled by providing an update window of finite duration during which the programmable memory may be updated. Access to the programmable memory may be based on the state of an access latch. The access latch may be set to allow access after a hardware reset of the device. An update control program may be executed to control access to the programmable memory and the latch reset to prevent access upon completion of the update control program. Verification of the update may be provided through encryption techniques and rules incorporated in certificates for application of updates to provide for selectively updating devices. Also disclosed are methods of securely providing differing functionality to generic devices.
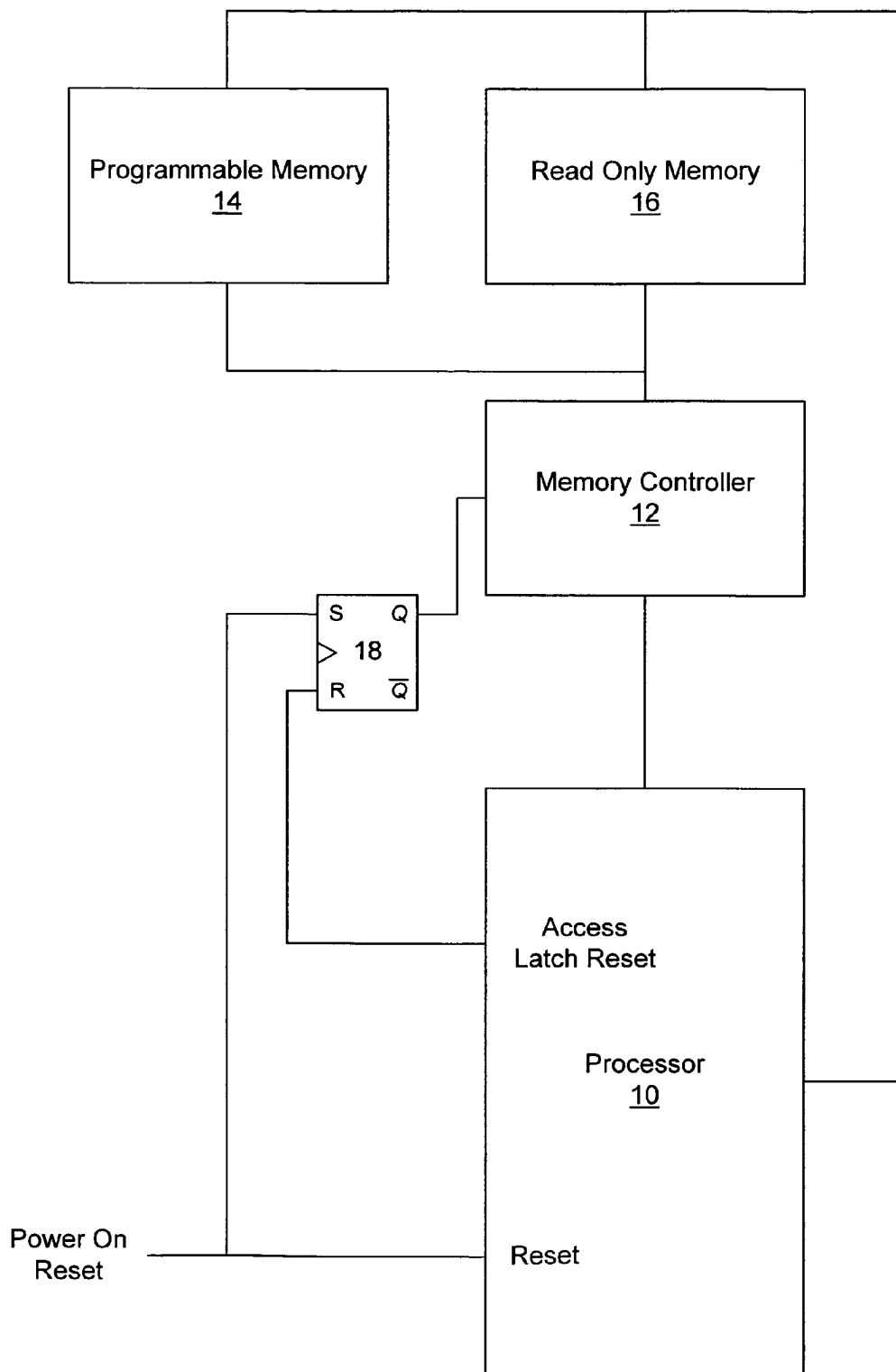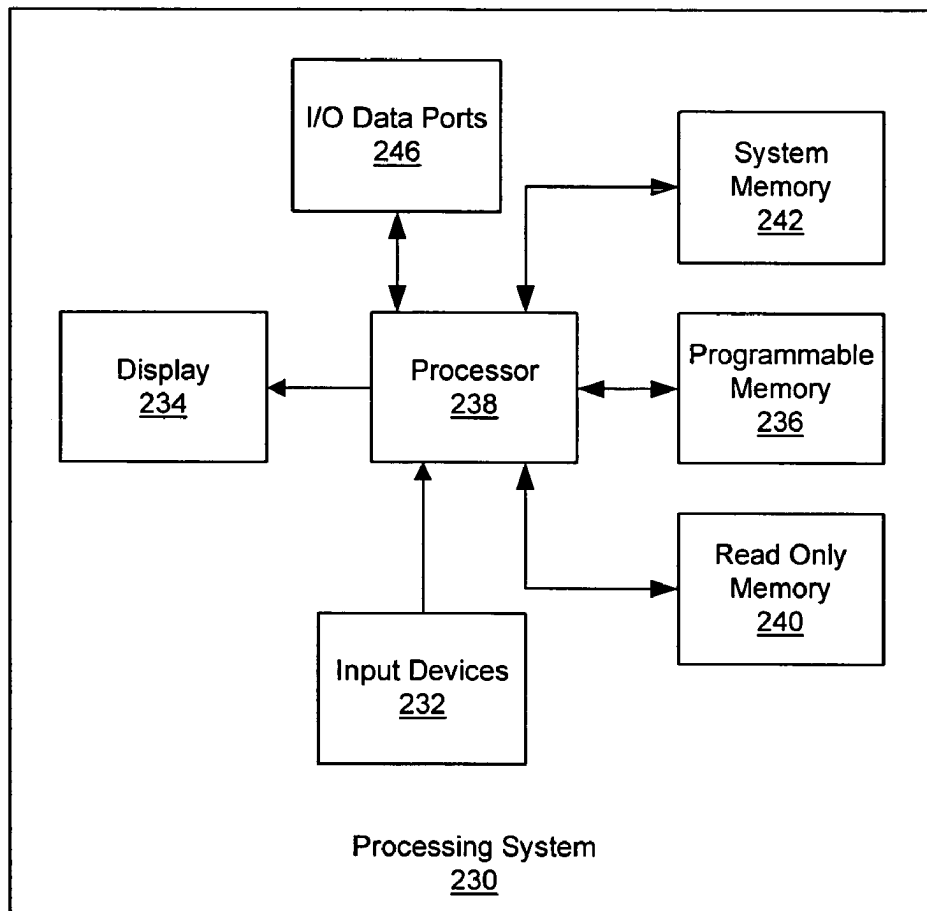
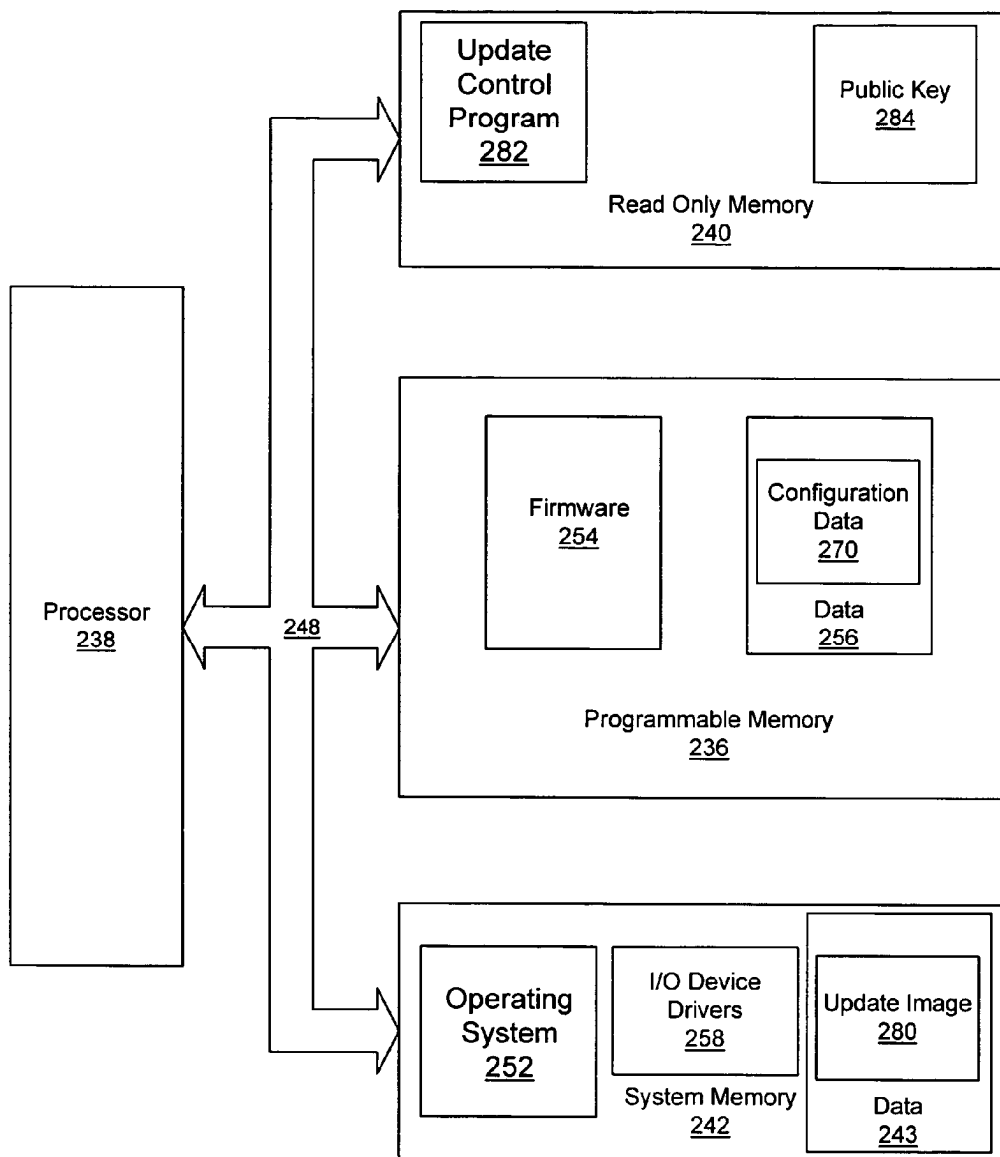**36 Claims, 12 Drawing Sheets**

Figure 1

Figure 2

Update Control Program 282

Public Key 284

Read Only Memory 240

Firmware 254

Configuration Data 270

Data 256

Programmable Memory 236

Processor 238

248

Operating System 252

I/O Device Drivers 258

Update Image 280

System Memory 242

Data 243

Figure 3

Figure 4A

DOCKET ALARM
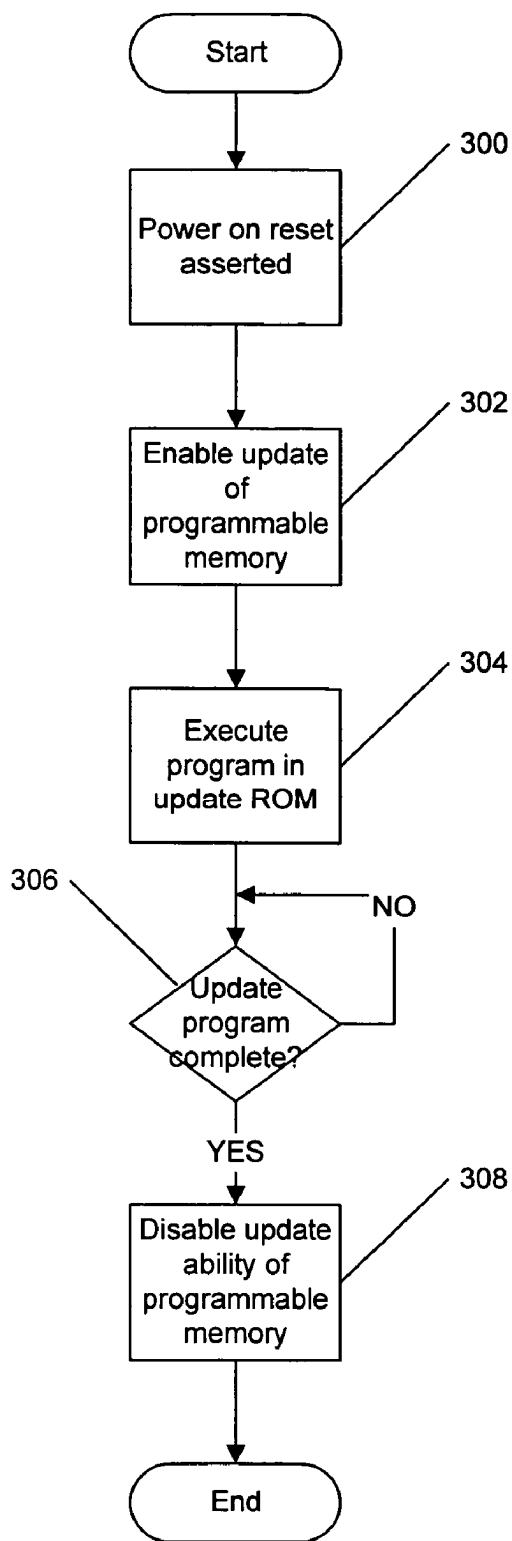
Explore Litigation Insights

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.