



US007024555B2

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

(10) **Patent No.:** **US 7,024,555 B2**
(45) **Date of Patent:** **Apr. 4, 2006**

(54) **APPARATUS AND METHOD FOR UNILATERALLY LOADING A SECURE OPERATING SYSTEM WITHIN A MULTIPROCESSOR ENVIRONMENT**

3,996,449 A 12/1976 Attanasio et al.
4,037,214 A 7/1977 Birney et al.
4,162,536 A 7/1979 Morley
4,207,609 A 6/1980 Luiz et al.
4,247,905 A 1/1981 Yoshida et al.
4,276,594 A 6/1981 Morley
4,278,837 A 7/1981 Best

(75) Inventors: **Michael A. Kozuch**, Beaverton, OR (US); **James A. Sutton, II**, Portland, OR (US); **David Grawrock**, Aloha, OR (US); **Gilbert Neiger**, Portland, OR (US); **Richard A. Uhlig**, Hillsboro, OR (US); **Bradley G. Burgess**, Austin, TX (US); **David I. Poisner**, Folsom, CA (US); **Clifford D. Hall**, Orangevale, CA (US); **Andy Glew**, Portland, OR (US); **Lawrence O. Smith, III**, Beaverton, OR (US); **Robert George**, Austin, TX (US)

(Continued)

FOREIGN PATENT DOCUMENTS

DE 4217444 12/1992

(Continued)

OTHER PUBLICATIONS

Brands, Stefan, "Restrictive Blinding of Secret-Key Certificates", *Springer-Verlag XP002201306*, (1995), Chapter 3.

(Continued)

Primary Examiner—Thomas R. Peeso
(74) *Attorney, Agent, or Firm*—Blakely, Sokoloff, Taylor & Zafman LLP

(73) Assignee: **Intel Corporation**, Santa Clara, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 1003 days.

(57) **ABSTRACT**

An apparatus and method for unilaterally loading a secure operating system within a multiprocessor environment are described. The method includes disregarding a received load secure region instruction when a currently active load secure region operation is detected. Otherwise, a memory protection element is directed, in response to the received load secure region instruction, to form a secure memory environment. Once directed, unauthorized read/write access to one or more protected memory regions are prohibited. Finally, a cryptographic hash value of the one or more protected memory regions is stored within a digest information repository as a secure software identification value. Once stored, outside agents may request access to a digitally signed software identification value in order to establish security verification of secure software within the secure memory environment.

(21) Appl. No.: **10/043,843**

(22) Filed: **Nov. 1, 2001**

(65) **Prior Publication Data**

US 2003/0084346 A1 May 1, 2003

(51) **Int. Cl.**
G06F 1/26 (2006.01)

(52) **U.S. Cl.** **713/165**; 713/168; 713/189;
713/193; 713/200; 713/201

(58) **Field of Classification Search** 713/165,
713/168, 189, 193, 200, 201
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

3,699,532 A 10/1972 Schaffer et al.

38 Claims, 10 Drawing Sheets

