(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 3 401 824 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
14.11.2018 Bulletin 2018/46

(51) Int Cl.:
G06F 21/51 *(2013.01)*

(21) Application number: **18179497.5**

(22) Date of filing: **06.05.2009**

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO SE SI SK TR

(30) Priority: **08.05.2008 US 117634**

(62) Document number(s) of the earlier application(s) in accordance with Art. 76 EPC:
09743550.7 / 2 281 234

(71) Applicant: **Google LLC**
Mountain View, CA 94043 (US)

(72) Inventors:
- **Chen, J. Bradley**
  Mountain View, California 94043 (US)
- **Harren, Matthew T.**
  Mountain View, California 94043 (US)
- **Papakipos, Matthew**
  Mountain View, California 94043 (US)
- **Sehr, David C.**
  Mountain View, California 94043 (US)
- **Yee, Bennet S.**
  Mountain View, California 94043 (US)

(74) Representative: **Betten & Resch**
Patent- und Rechtsanwälte PartGmbB
Maximiliansplatz 14
80333 München (DE)

Remarks:
This application was filed on 25-06-2018 as a divisional application to the application mentioned under INID code 62.

(54) METHOD FOR VALIDATING AN UNTRUSTED NATIVE CODE MODULE

(57) A system that validates a native code module. During operation, the system receives a native code module comprised of untrusted native program code. The system validates the native code module by: (1) determining that code in the native code module does not include any restricted instructions and/or does not access restricted features of a computing device; and (2) determining that the instructions in the native code module are aligned along byte boundaries such that a specified set of byte boundaries always contain a valid instruction and control flow instructions have valid targets. The system allows successfully-validated native code modules to execute, and rejects native code modules that fail validation. By validating the native code module, the system facilitates safely executing the native code module in the secure runtime environment on the computing device, thereby achieving native code performance for untrusted program binaries without significant risk of unwanted side effects.

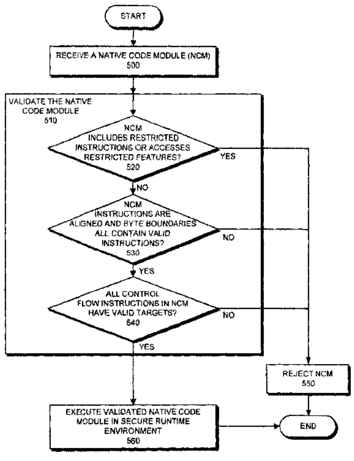
START
RECEIVE A NATIVE CODE MODULE (NCM)
500
VALIDATE THE NATIVE CODE MODULE
510
NCM INCLUDES RESTRICTED INSTRUCTIONS OR ACCESSES RESTRICTED FEATURES?
520
YES
NO
NCM INSTRUCTIONS ARE ALIGNED AND BYTE BOUNDARIES ALL CONTAIN VALID INSTRUCTIONS?
530
NO
YES
ALL CONTROL FLOW INSTRUCTIONS IN NCM HAVE VALID TARGETS?
540
NO
YES
REJECT NCM
550
EXECUTE VALIDATED NATIVE CODE MODULE IN SECURE RUNTIME ENVIRONMENT
560
END

FIG. 5

Printed by Jouve, 75001 PARIS (FR)