(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
23 October 2014 (23.10.2014)

WIPO | PCT

(10) International Publication Number
WO 2014/172205 A1

(51) International Patent Classification:
*G06F 21/00* (2013.01)

(21) International Application Number:
PCT/US2014/033882

(22) International Filing Date:
11 April 2014 (11.04.2014)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
13/862,923 15 April 2013 (15.04.2013) US
13/863,296 15 April 2013 (15.04.2013) US

(71) Applicant: **AMAZON TECHNOLOGIES, INC.** [US/US]; P.O. Box 8102, Reno, Nevada 89507 (US).

(72) Inventors: **POTLAPALLY, Nachiketh Rao**; 410 Terry Ave. North, Seattle, Washington 98109 (US). **CHAWLA, Rachit**; 410 Terry Ave. North, Seattle, Washington 98109 (US). **VOLKMAN, Jeremy Ryan**; 410 Terry Ave. North, Seattle, Washington 98109 (US). **MARR, Michael David**; 410 Terry Ave. North, Seattle, Washington 98109 (US).

(74) Agents: **LOHR, Jason D.** et al.; Novak Druce Connolly Bove + Quigg LLP, 1000 Louisiana Street, Fifty-Third Floor, Houston, Texas 77002 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ,

*[Continued on next page]*

(54) Title: HOST RECOVERY USING A SECURE STORE

(57) Abstract: Approaches are described for enabling a host computing device to store credentials and other security information useful for recovering the state of the host computing device in a secure store, such as a trusted platform module (TPM) on the host computing device. When recovering the host computing device in the event of a failure (e.g., power outage, network failure, etc.), the host computing device can obtain the necessary credentials from the secure store and use those credentials to boot various services, restore the state of the host and perform various other functions. In addition, the secure store (e.g., TPM) may provide boot firmware measurement and remote attestation of the host computing devices to other devices on a network, such as when the recovering host needs to communicate with the other devices on the network.

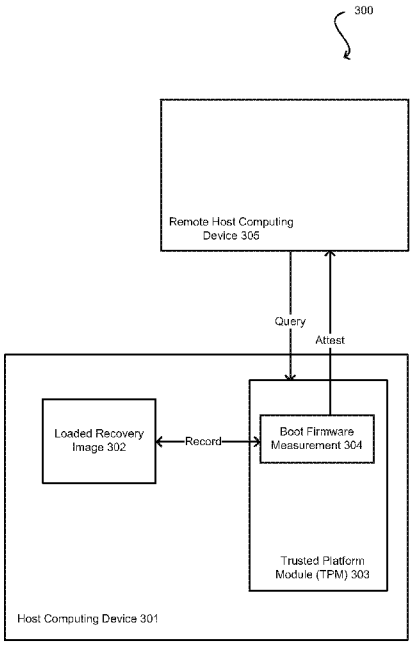


FIG. 3

WO 2014/172205 A1

UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

**Declarations under Rule 4.17**:

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*

— *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii))*

**Published**:

— *with international search report (Art. 21(3))*

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))*