

(19) World Intellectual Property
Organization
International Bureau



(43) International Publication Date
10 November 2005 (10.11.2005)

PCT

(10) International Publication Number
WO 2005/107130 A1

(51) International Patent Classification⁷: **H04L 9/00**,
G06F 13/14, 12/14

(21) International Application Number:
PCT/CA2004/002041

(22) International Filing Date:
26 November 2004 (26.11.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/568,119 4 May 2004 (04.05.2004) US

(71) Applicant (for all designated States except US): **RE-SEARCH IN MOTION LIMITED** [CA/CA]; 295 Phillip Street, Waterloo, Ontario N2L 3W8 (CA).

(72) Inventors; and

(75) Inventors/Applicants (for US only): **BROWN, Michael**,

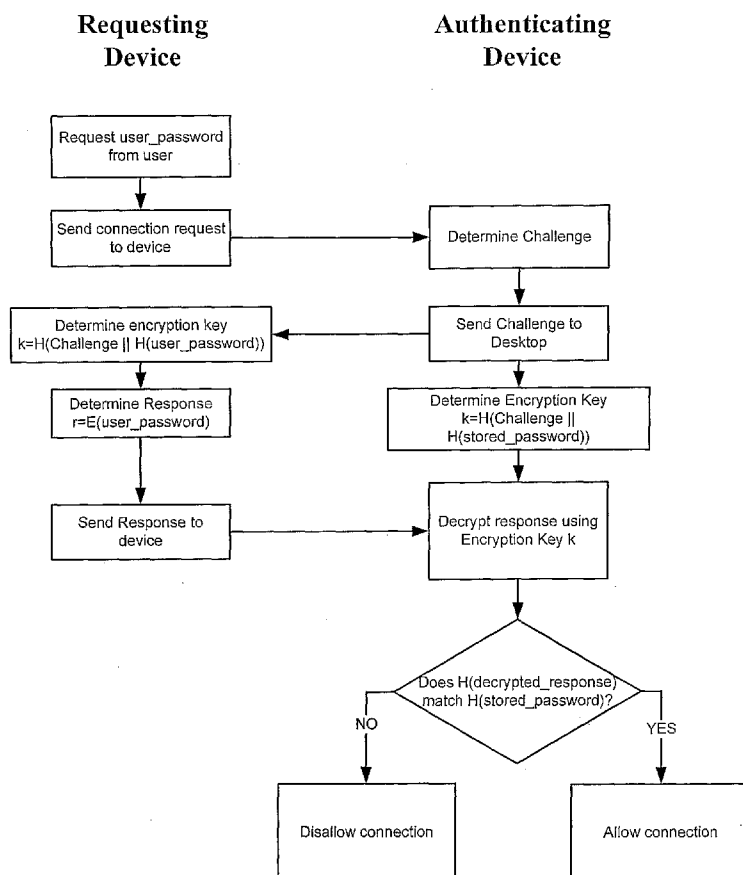
K. [CA/CA]; 8 Fernwood Place, Kitchener, Ontario N2M 2Z2 (CA). **BROWN, Michael, S.** [CA/CA]; 350 University Downs Cres., Waterloo, Ontario N2K 4B1 (CA). **KIRKUP, Michael, G.** [CA/CA]; 413 Exmoor Street, Waterloo, Ontario N2K 3X5 (CA). **LITTLE, Herbert, A.** [CA/CA]; 504 Old Oak Place, Waterloo, Ontario N2T 2V8 (CA).

(74) Agents: **WILSON, Jenna, L.** et al.; Dimock Stratton LLP, 20 Queen St. W., Suite 3202, Box 102, Toronto, Ontario M5H 3R3 (CA).

(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM,

[Continued on next page]

(54) Title: CHALLENGE RESPONSE SYSTEM AND METHOD



(57) Abstract: A challenge response scheme includes the authentication of a requesting device by an authenticating device. The authenticating device generates a challenge that is issued to the requesting device. The requesting device combines the challenge with a hash of a password provided by a user of the requesting device, and the combination of the hash of the password and the challenge is further hashed in order to generate a requesting encryption key that is used to encrypt the user supplied password. The encrypted user supplied password is sent to the authenticating device as a response to the issued challenge. The authenticating device generates an authenticating encryption key by generating the hash of a combination of the challenge and a stored hash of an authenticating device password. The authenticating encryption key is used to decrypt the response in order to retrieve the user-supplied password. If a hash of the user-supplied password matches the stored hash of the authenticating device password, then the requesting device has been authenticated and the authenticating device is in possession of the password.



TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

(84) Designated States (*unless otherwise indicated, for every kind of regional protection available*): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LU, MC, NL, PL, PT, RO, SE,

Published:

— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.