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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
17 June 2004 (17.06.2004)

PCT

(10) International Publication Number
WO 2004/051585 A2

(51) International Patent Classification[7]: G07F 7/10

(21) International Application Number:
PCT/US2003/037928

(22) International Filing Date:
26 November 2003 (26.11.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/429,754 27 November 2002 (27.11.2002) US

(71) Applicant: **RSA SECURITY INC** [US/US]; 174 Middlesex Turnpike, Bedford, MA 01730 (US).

(72) Inventors: **JAKOBSSON, Markus**; 1203 Garden Street, Hoboken, NJ 07030 (US). **JUELS, Ari**; 131 Freeman Street, Brookline, MA 02446 (US). **KALISKI, Burton, S., Jr.**; 22 Pembroke Road, Wellesley, MA 02181 (US).

(74) Agent: **PRAHL, Eric, L.**; Hale and Dorr LLP, 60 State Street, Boston, MA 02109 (US).

(81) Designated States *(national)*: 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, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *without international search report and to be republished upon receipt of that 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.

WO 2004/051585 A2

(54) Title: IDENTITY AUTHENTICATION SYSTEM AND METHOD

(57) Abstract: A method and system for generating an authentication code that depends at least in part on a dynamic value that changes over time, an event state associated with the occurrence of an event, and a secret associated with an authentication device. By generating the authentication code responsive to an event state, an identity authentication code can be used to verify identity and to communicate event state information, and to do so in a secure manner.

IDENTITY AUTHENTICATION SYSTEM AND METHOD

Cross Reference to Related Applications

[0001] This application claims the benefit under 35 U.S.C. § 119(e) of U.S. Provisional Application No. 60/429,754, filed November 27, 2002.

Field of the Invention

[0002] The invention relates generally to the fields of cryptography and security. More specifically, the invention relates to the generation and verification of identity authentication codes.

Background of the Invention

[0003] Generally, security systems employ identity-based authentication schemes to verify the identity of an entity that is allowed access to a physical location or object, in the case of a physical security system, or electronic access to a computer system or data, in the case of a data security system. One goal of such security systems is to accurately determine identity so that an unauthorized party cannot gain access. Security systems can use one or more of several factors, alone or in combination, to authenticate entities. For example, identification systems can be based on something that the entity knows, something the entity is, or something that the entity has.

[0004] Examples of something an entity knows are a code word, password, personal identification number ("PIN") and the like. One exemplary computer-based authentication method involves the communication of a secret that is specific to a particular entity or user. The entity seeking authentication transmits the secret or a value derived from the secret to a verifier, which authenticates the identity of the entity. In a typical implementation, an entity

communicates both identifying information (e.g., a user name) and a secret (e.g., a password) to the verifier. The verifier typically possesses records that associate a secret with each entity. If the verifier receives the appropriate secret for the entity, the entity is successfully authenticated. If the verifier does receive the correct secret, the authentication fails.

[0005] Examples of something the entity is include characteristics that are unique to people, such as physical, biological, and psychological characteristics (referred to generally here as biological characteristics), such as fingerprints, handwriting, eye retina patterns, and face, body, and organ appearance, size and shape. Suitable biological characteristics typically are not under the control of the person, and are therefore difficult for anyone besides the intended person to present, because, in part, they are difficult to replicate. The verifier typically can observe the characteristic, and compare the characteristic to records that associate the characteristic with the entity. The observation of biological characteristics is referred to generally as biometric measurement.

[0006] An example of something an entity possesses is a physical or digital object, referred to generally as a token, that is unique, or relatively unique, to the user. A simple example is a conventional metal key for use in a door. Possession of the door key in effect authenticates the user to the lock and allows entry. Similarly, possession of a token such as a bank card having certain specific physical and electronic characteristics, for example containing a specific identification number that is revealed when the token is accessed in a particular manner, can be this type of factor. A token containing a computing device that performs encryption using an encryption key contained in the device would also be regarded as this type of factor. For example, a token could accept user input, which might include a PIN or a challenge value, and provide as output a result encrypted with a secret encryption key stored in the card. The verifier can then compare the output to an expected value in order to authenticate the entity.

[0007] A token might also, or alternatively, use additional input information, such as time, or a counter, for example, such that the result changes over time but is deterministic to an entity that possesses a secret (e.g., a value known only by the token and the verifier), but not predictable by an observer who does not possess the secret. These systems generally perform some computation using a stored secret as input to generate an authentication code that is used to authenticate the entity. Some systems are time-based, in that they use a time-based dynamic variable to calculate a non-predictable authentication code that ultimately authenticates the entity. Here, "non-predictable" means that the authentication code is not predictable by a party that does not know the associated secret, the algorithm for calculating the code, or both. One example, U.S. Patent No. 5,937,068 entitled "System and Method for User Authentication Employing Dynamic Encryption Variables," uses as input a combination or subset of three variables: the current time, the number of access requests made by the card, and a "secret dynamic encryption key" that is updated with each access request. The token, in this case, also verifies a PIN entered by the user before communicating an authentication code.

[0008] Although the dynamic nature of the authentication codes generated by such an approach avoids problems inherent with using fixed authentication codes, an unattended or stolen token remains vulnerable to attack. Would-be attackers who gain access to tokens can subject the tokens to sophisticated analysis intended to determine their methods of operation, and/or the secret(s) stored within. Attackers might inspect the token and conduct such analysis in order to determine the associated secret, the algorithm for calculating the authentication code, or both. The attacker might then be able to generate apparently valid authentication codes in order to illegally gain physical or electronic access to secured areas or systems. Many tamper-resistant hardware designs are available, however, new attacks are frequently developed to thwart tamper resistance. Further, current tamper resistant designs do not provide verifiers,

authentication systems, system administrators, or another relevant authority with any indication that the token has been tampered with.

[0009] One approach to detection of tampering is described in Johan Håstad, Jakob Jonsson, Ari Juels, Moti Yung, "funkspiel schemes: an alternative to conventional tamper resistance", ACM Conference on Computer and Communications Security 2000; 125-133. Håstad et al. describe several "funkspiel schemes" whereby a device can indicate to a verifier that tampering has occurred, without revealing to an adversary whether the tampering has been detected. The schemes are oriented toward the generation of a sequence of message authentication codes, where the message authentication may fail after tampering has been detected. In one example given, the message authentication code is embedded into a digital signature scheme, where the digital signature indicates whether a transaction has been approved by a device, while the message authentication code indicates whether the device has been tampered with. The message authentication code itself may not be suitable as an identity authentication code as it is oriented toward a sequence of message transactions rather than time-based identity authentication. In particular, Håstad et al does not provide any method for efficiently verifying a single authentication code among those over a very long period of time, without substantial computation by the verifier (e.g., a potentially long chain of function evaluations), substantial computation by both parties (e.g., asymmetric encryption) or substantial storage by both parties (e.g., many one-time bits).

Summary of the Invention

[0010] The invention addresses these shortcomings by including an indication of the occurrence of an event directly into the efficient computation of an identity authentication code, where the verifier may efficiently verify the authentication code and identify the signaling of an event state.

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.