US008495372B2

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

(10) **Patent No.: US 8,495,372 B2**
(45) **Date of Patent: Jul. 23, 2013**

(54) **AUTHENTICATION METHODS AND APPARATUS USING PAIRING PROTOCOLS AND OTHER TECHNIQUES**

(75) Inventors: **Daniel Vernon Bailey**, Pepperell, MA (US); **John G. Brainard**, Sudbury, MA (US); **Ari Juels**, Brookline, MA (US); **Burton S. Kaliski, Jr.**, Wellesley, MA (US)

(73) Assignee: **EMC Corporation**, Hopkinton, MA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 1582 days.

(21) Appl. No.: **11/939,232**

(22) Filed: **Nov. 13, 2007**

(65) **Prior Publication Data**

US 2008/0065892 A1 Mar. 13, 2008

Related U.S. Application Data

(63) Continuation of application No. 11/671,264, filed on Feb. 5, 2007.

(60) Provisional application No. 60/764,826, filed on Feb. 3, 2006.

(51) **Int. Cl.**
H04L 9/32 (2006.01)
H04L 9/00 (2006.01)

(52) **U.S. Cl.**
USPC **713/171**; 713/172; 380/277

(58) **Field of Classification Search**
USPC 713/171, 168, 172, 155, 159; 380/277; 726/5, 9
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,347,580	A *	9/1994	Molva et al.	713/159
5,600,722	A *	2/1997	Yamaguchi et al.	713/155
5,657,388	A	8/1997	Weiss	
6,085,320	A *	7/2000	Kaliski, Jr.	713/168
6,996,722	B1 *	2/2006	Fairman et al.	713/192
7,039,021	B1	5/2006	Kokudo	
7,080,259	B1 *	7/2006	Nakanishi et al.	713/193
7,181,015	B2 *	2/2007	Matt	380/279
7,266,695	B2 *	9/2007	Nakayama	713/172
7,464,865	B2 *	12/2008	Brown et al.	235/380

(Continued)

OTHER PUBLICATIONS

J. Zheng et al., "Will IEEE 802.15.4 Make Ubiquitous Networking a Reality?: A Discussion on a Potential Low Power, Low Bit Rate Standard," IEEE Communications Magazine, Topics in Emerging Technologies, Jun. 2004, pp. 140-146.

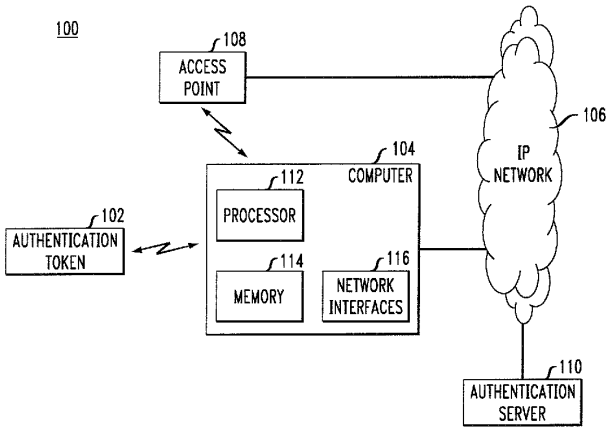
(Continued)

Primary Examiner — Zachary A Davis
(74) *Attorney, Agent, or Firm* — Ryan, Mason & Lewis, LLP

(57) **ABSTRACT**

In one aspect, a first processing device, which may be an authentication token, establishes a shared key through a pairing protocol carried out between the first processing device and a second processing device. The pairing protocol also involves communication between the second processing device and an authentication server. As part of the pairing protocol, the first processing device sends identifying information to the second processing device, and the second processing device utilizes the identifying information to obtain the shared key from the authentication server. The first processing device encrypts authentication information utilizing the shared key, and transmits the encrypted authentication information from the first processing device to the second processing device. The second processing device utilizes the shared key to decrypt the encrypted authentication information.

12 Claims, 2 Drawing Sheets



U.S. PATENT DOCUMENTS

7,571,489	B2 *	8/2009	Ong et al.	726/29
7,597,250	B2 *	10/2009	Finn	235/380
7,672,459	B2 *	3/2010	O'Hara et al.	380/278
7,774,611	B2 *	8/2010	Muntz et al.	713/182
7,822,209	B2 *	10/2010	Fu et al.	380/284
7,827,409	B2 *	11/2010	Fascenda	713/171
7,934,005	B2 *	4/2011	Fascenda	709/229
2004/0222878	A1	11/2004	Juels	
2007/0250712	A1 *	10/2007	Salgado et al.	713/171

OTHER PUBLICATIONS

J-H. Hoepman, "The Ephemeral Pairing Problem," Financial Cryptography '04, Lecture Notes in Computer Science, 2004, pp. 1-15, Springer-Verlag.

F. Stajano et al., "The Resurrecting Duckling: Security Issues for Ad-hoc Wireless Networks," 7th International Workshop Proceedings on Security Protocols, Lecture Notes in Computer Science, 1999, pp. 1-11, vol. 1796, Springer-Verlag.

G. Itkis et al., "Intrusion-Resilient Signatures, or Towards Obsoletion of Certificate Revocation," Advances in Cryptology—CRYPTO '02, 2002, pp. 1-16, Springer-Verlag.

M. Jakobsson, "Fractal Hash Sequence Representation and Traversal," Proceedings of the 2002 IEEE International Symposium on Information Theory (ISIT '02), 2002, pp. 1-8.

D. Boneh et al., "Identity-Based Encryption from the Weil Pairing," Lecture Notes in Computer Science: Advances in Cryptology—CRYPTO 2001, 2001, pp. 1-27.

J. Hastad et al., "Funkspiel Schemes: An Alternative to Conventional Tamper Resistance," Seventh ACM Conference on Computer and Communications Security, 2000, 9 pages.

Microsoft Corporation, "Scanning 802.11 Networks," Microsoft Developer Network Library, 2007, pp. 1-3.

Ensure Technologies, "XyLoc for the Healthcare Industry," www.ensuretech.com, 2004, 5 pages.

Privaris, "plusID Universal Biometric Device," www.privaris.com, 2006, 2 pages.

Privaris, "Achieving Universal Secure Identity Verification with Convenience and Personal Privacy," A Privaris Business White Paper, Dec. 11, 2006, 9 pages, Version 0.1.

M. Comer, "Transient Authentication for Mobile Devices," PhD Thesis, University of Michigan, 2003, 111 pages.

IEEE Standard 802.11, Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, 1999 Edition, 528 pages.

A.J. Menezes et al., Handbook of Applied Cryptography, CRC Press, 1997, pp. 1-780.

"RAWether for Windows, Windows Networking Architecture," PCAUSA—Introduction to the Windows Networking Architecture, http://www.rawether.net/product/tour01.htm, 2007, 2 pages.

* cited by examiner

FIG. 1

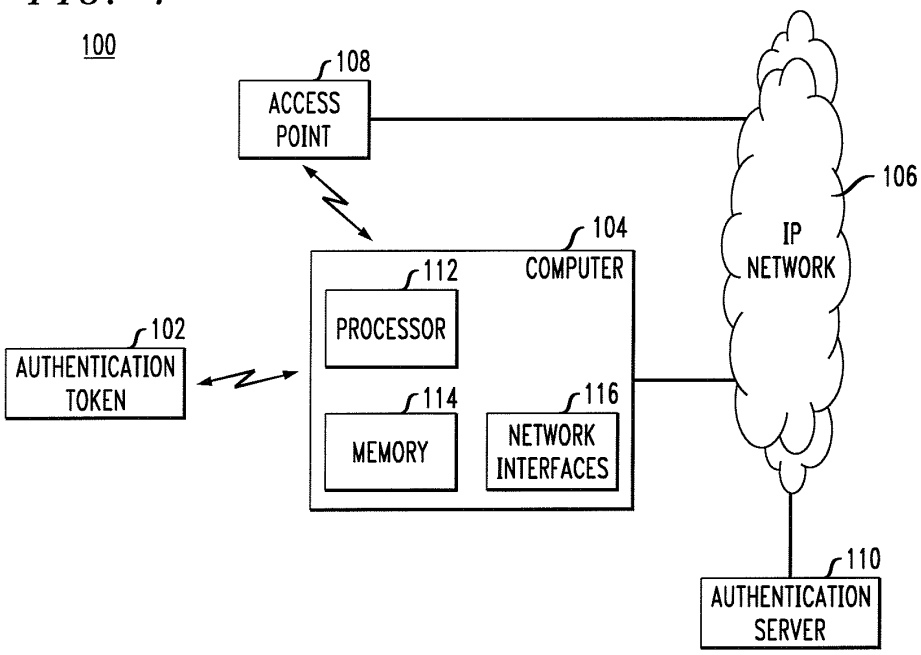


FIG. 2

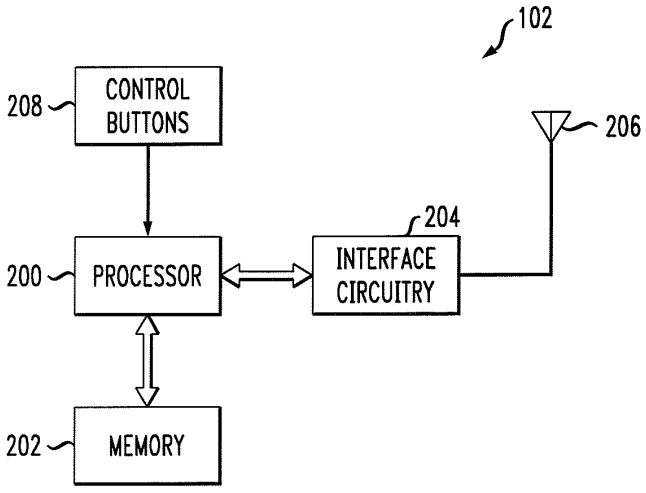
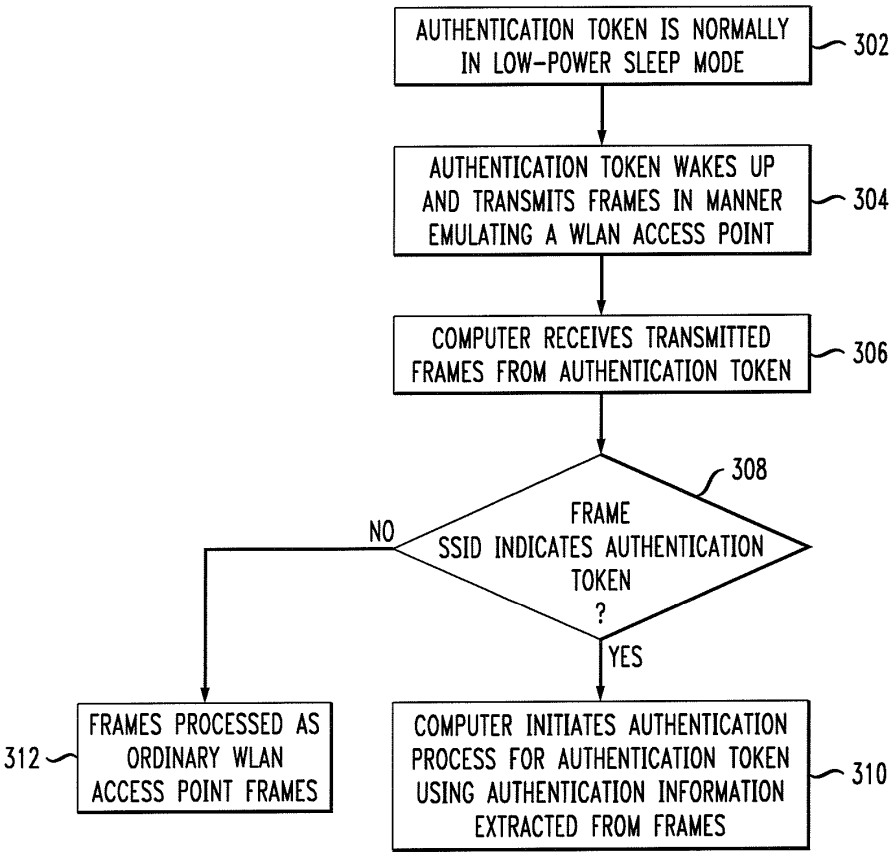


FIG. 3



AUTHENTICATION METHODS AND APPARATUS USING PAIRING PROTOCOLS AND OTHER TECHNIQUES

RELATED APPLICATION(S)

The present application is a continuation of U.S. patent application Ser. No. 11/671,264, filed Feb. 5, 2007, and entitled "Wireless Authentication Methods and Apparatus," which claims the priority of U.S. Provisional Patent Application Ser. No. 60/764,826, filed Feb. 3, 2006 and entitled "The RFID Authenticator," both of which are incorporated by reference herein. Another related application is U.S. patent application Ser. No. 11/768,608, entitled "Authentication Methods and Apparatus Utilizing Hash Chains," which is also a continuation of above-noted U.S. patent application Ser. No. 11/671,264, and is incorporated by reference herein.

FIELD OF THE INVENTION

The present invention relates generally to techniques for authentication, and more particularly to authentication tokens or other processing devices utilized in authentication operations.

BACKGROUND OF THE INVENTION

The growing need for better user authentication is drawing increased attention to technologies such as one-time passwords. In a one-time password system, a user typically carries a device or "token" that generates and displays a series of passwords over time. The user reads the currently displayed password and enters it into a personal computer, e.g., via a Web browser, as part of an authentication operation. Such a system offers a significant improvement over conventional password-based authentication since the password is dynamic and random. Previously misappropriated one-time passwords are of no help to an attacker in determining the current password, which remains hard to guess.

One particular example of a one-time password device of the type described above is the RSA SecurID® user authentication token, commercially available from RSA, The Security Division of EMC Corporation, of Bedford, Mass., U.S.A. For a number of years, SecurID® has been the dominant solution in two factor authentication. Its relative simplicity combined with its independence from client-side software has contributed in no small measure to its success in many large enterprises. In a typical embodiment, a SecurID® authentication token may comprise a small handheld device with an LCD screen that displays a new one-time tokencode consisting of six to eight decimal digits every 60 seconds. An ordinary user would utilize this tokencode, possibly in combination with a personal identification number (PIN) with the resulting combination called a passcode, instead of a static password to access secure resources. Each displayed tokencode is based on a secret seed and the current time of day. Any verifier with access to the seed and a time of day clock can verify that the presented tokencode is valid.

A wireless authentication token, that is, a token that transmits authentication information over the air rather than via the user, can offer many attractions. Such a token can alleviate much of the burden on users in manually entering tokencodes or other authentication information. It can also achieve considerably higher transmission bandwidth, opening up a range of new functions beyond simple authentication, such as encryption. Wireless tokens can offer several other potential advantages as well, such as hands-free authentication for physically demanding environments like hospitals and factory floors, and rapid fire authentication for temporally demanding situations, such as online auctions.

Conventional aspects of wireless authentication tokens are described in, for example, M. Corner, "Transient Authentication for Mobile Devices," PhD Thesis, University of Michigan, 2003. The approach disclosed therein is designed to protect information on mobile devices such as laptops from exposure in the event of theft or loss. Its authentication protocol utilizes bidirectional communication between mobile devices and authentication tokens. Such an approach is problematic, however, in that authentication tokens that accept input in their authentication protocols can be vulnerable to active attacks.

Accordingly, a need exists for improvements in wireless authentication tokens and other processing devices utilized in authentication operations.

SUMMARY OF THE INVENTION

Illustrative embodiments of the present invention meet the above-identified need by providing improved techniques for authentication utilizing authentication tokens or other processing devices.

In accordance with one aspect of the invention, a first processing device, which may be, for example, a wireless authentication token or an RFID tag, establishes a shared key through a pairing protocol that is carried out between the first processing device and a second processing device and involves communication between the second processing device and an authentication server. As part of the pairing protocol, the first processing device sends identifying information to the second processing device, and the second processing device utilizes the identifying information to obtain the shared key from the authentication server. The first processing device encrypts authentication information utilizing the shared key, and transmits the encrypted authentication information from the first processing device to the second processing device. The second processing device utilizes the shared key to decrypt the encrypted authentication information.

In a given illustrative embodiment, the identifying information may comprise a MAC address of the first processing device. The first processing device may generate the shared key using a key derivation function applied to a secret seed, where the secret seed is known to the first processing device and the authentication server but not known to the second processing device. As part of the pairing protocol the first processing device further sends a tokencode to the second processing device, and the second processing device utilizes the identifying information and the tokencode to obtain the shared key from the authentication server. Also as part of the pairing protocol, the second processing device may send information to the first processing device indicating that the second processing device is authorized by the authentication server to pair with the first processing device. The first processing device may generate the shared key using a key derivation function applied to at least part of the information sent to the first processing device by the second processing device.

In accordance with another aspect of the invention, a base point on an elliptic curve is derived in a first processing device. Authentication information is generated in the first processing device utilizing the base point and a private key of the first processing device, and the authentication information is transmitted from the first processing device to a second processing device. The base point on the elliptic curve may be derived, for example, by applying a one-way function to a

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.