US005491752A

United States Patent [19]

Kaufman et al.

[11] **Patent Number: 5,491,752**

[45] **Date of Patent: Feb. 13, 1996**

[54] **SYSTEM FOR INCREASING THE DIFFICULTY OF PASSWORD GUESSING ATTACKS IN A DISTRIBUTED AUTHENTICATION SCHEME EMPLOYING AUTHENTICATION TOKENS**

[75] Inventors: **Charles W. Kaufman**, Northborough; **Radia J. Pearlman**, Acton; **Morrie Gasser**, Hopkinton, all of Mass.

[73] Assignee: **Digital Equipment Corporation, Patent Law Group**, Maynard, Mass.

[21] Appl. No.: **300,576**

[22] Filed: **Sep. 2, 1994**

Related U.S. Application Data

[63] Continuation of Ser. No. 34,225, Mar. 18, 1993, abandoned.

[51] **Int. Cl.**[6] **H04K 1/00**

[52] **U.S. Cl.** **380/30**; 380/25

[58] **Field of Search** 380/23, 24, 25, 380/30

[56] **References Cited**

U.S. PATENT DOCUMENTS

3,798,605	3/1974	Feistel	380/25
3,996,449	12/1976	Attanasio et al.	235/61.7 R
4,218,738	8/1980	Matyas et al.	380/25

(List continued on next page.)

OTHER PUBLICATIONS

1989, Mark, T., et al, "*Reducing Risks from Poorly Chosen Keys,*" University of Cambridge Computer Laboratory, from 12th Symposium On Operating System Principles.

Security Dynamics, Inc., "Kerberos and SecurID," approximately Apr. 1992, not published.

Lomas et al., "Reducing Risks from Poorly Chosen Keys," 12th Symposium on Operating System Principles, 1989, pp. 14–18, place of pub. unknown.

Tardo et al., "SPX: Global Authentication Using Public Key Certificates," Proceedings of IEEE Symposium Research in Security and Privacy, IEEE CS Press, 1991, pp. 232–244, place of publication unknown.

Abadi et al., "Authentication and Delegation with Smart–Cards," Oct. 22, 1990, pp. 1–24, place of publication unknown.

Woo et al., "Authentication for Distributed Systems," from Computer of IEEE Computer Society, Jan. 1992, pp. 49–51, place of pub. unknown.

U.S. application Ser. No. 07/875,050, filed Apr. 28, 1992, Kaufman et al.

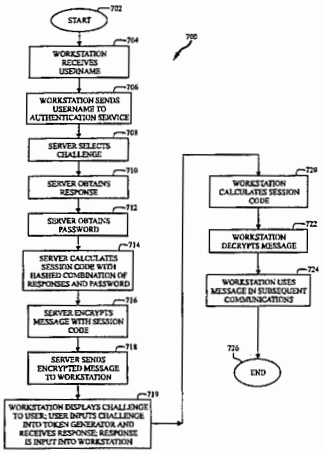
Primary Examiner—Tod R. Swann

Attorney, Agent, or Firm—A. Sidney Johnston

[57] **ABSTRACT**

An improved security system inhibits eavesdropping, dictionary attacks, and intrusion into stored password lists. In one implementation, the user provides a workstation with a "password", and a "token" obtained from a passive authentication token generator. The workstation calculates a "transmission code" by performing a first hashing algorithm upon the password and token. The workstation sends the transmission code to the server. Then, the server attempts to reproduce the transmission code by combining passwords from a stored list with tokens generated by a second identical passive authentication token generator just prior to receipt of the transmission code. If any password/token combination yields the transmission code, the workstation is provided with a message useful in communicating with a desired computing system; the message is encrypted with a session code calculated by applying a different hashing algorithm to the password and token. In another embodiment, the workstation transmits a user name to the authentication server. The server verifies the user name's validity, and uses an active authentication token generator to obtain a "response" to an arbitrarily selected challenge. The server generates a session code by performing a hashing algorithm upon the response and the password. The server sends the challenge and a message encrypted with the session code to the workstation. The workstation generates the session code by performing the hashing algorithm on the password and the received challenge, and uses the session code to decrypt the encrypted message. The message is useful in communicating with a desired computing system.

37 Claims, 7 Drawing Sheets



U.S. PATENT DOCUMENTS

4,227,253	10/1980	Ehrsam et al.	375/2
4,264,782	4/1981	Konheim	178/22
4,288,659	9/1981	Atalla	178/22.08
4,386,266	5/1983	Chesarek	235/380
4,399,323	8/1983	Henry	178/22.14
4,430,728	2/1984	Beitel et al.	340/825.31 X
4,626,845	12/1986	Ley	380/23 X
4,661,991	4/1987	Logemann	340/825.31 X
4,736,423	4/1988	Matyas	380/23
4,755,940	7/1988	Brachtl et al.	364/408
4,799,061	1/1989	Abraham et al.	340/825.34
4,815,031	3/1989	Furukawa	380/23 X
4,868,877	9/1989	Fischer	380/25
4,881,264	11/1989	Merkle	380/25
4,910,773	3/1990	Hazard et al.	380/21
4,919,545	4/1990	Yu	380/25
4,924,515	5/1990	Matyas et al.	380/25
4,932,056	6/1990	Shamir	380/23
4,965,568	10/1990	Atalla et al.	340/825.34
4,974,193	11/1990	Beutelspacher	364/900
4,993,068	2/1991	Piosenka et al.	380/23
5,023,908	6/1991	Weiss	380/23
5,029,208	7/1991	Tanaka	380/30 X
5,050,212	9/1991	Dyson	380/25
5,068,894	11/1991	Hoppe	380/23
5,081,678	1/1992	Kaufman et al.	380/21
5,109,152	4/1992	Takagi et al.	235/380
5,136,646	8/1992	Haber et al.	380/49
5,136,647	8/1992	Haber et al.	380/49
5,146,499	9/1992	Geffrotin	380/23
5,148,479	9/1992	Bird et al.	380/23
5,163,096	11/1992	Clark et al.	380/4
5,201,000	4/1993	Matyas et al.	380/30
5,204,966	4/1993	Wittenberg et al.	380/25 X
5,220,604	6/1993	Gasser et al.	380/23
5,224,163	6/1993	Gasser et al.	380/30
5,235,644	8/1993	Gupta et al.	380/48
5,297,206	3/1994	Orton	380/30
5,315,658	5/1994	Micali	380/30

FIG. 1
(Prior Art)

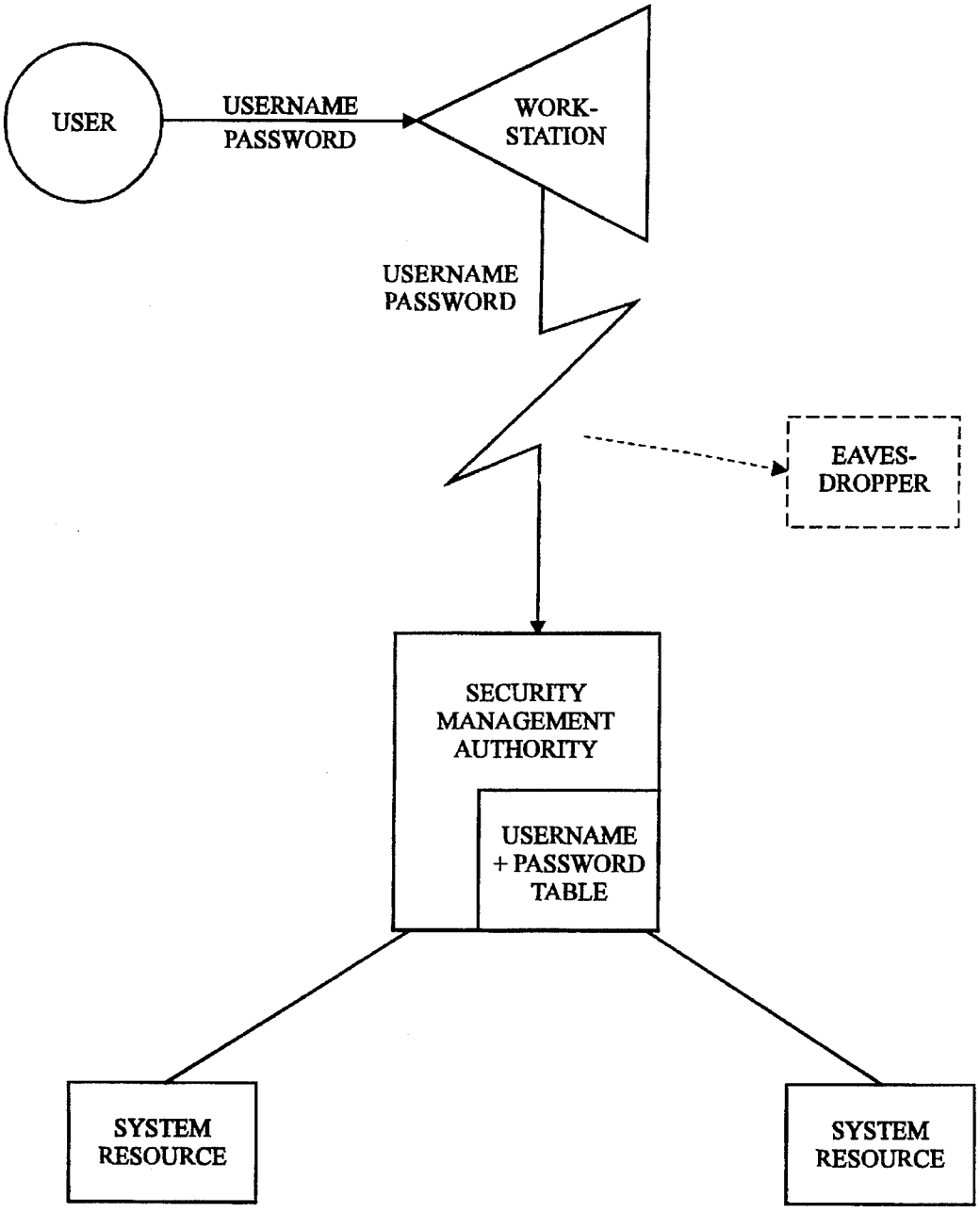


FIG. 2
(Prior Art)

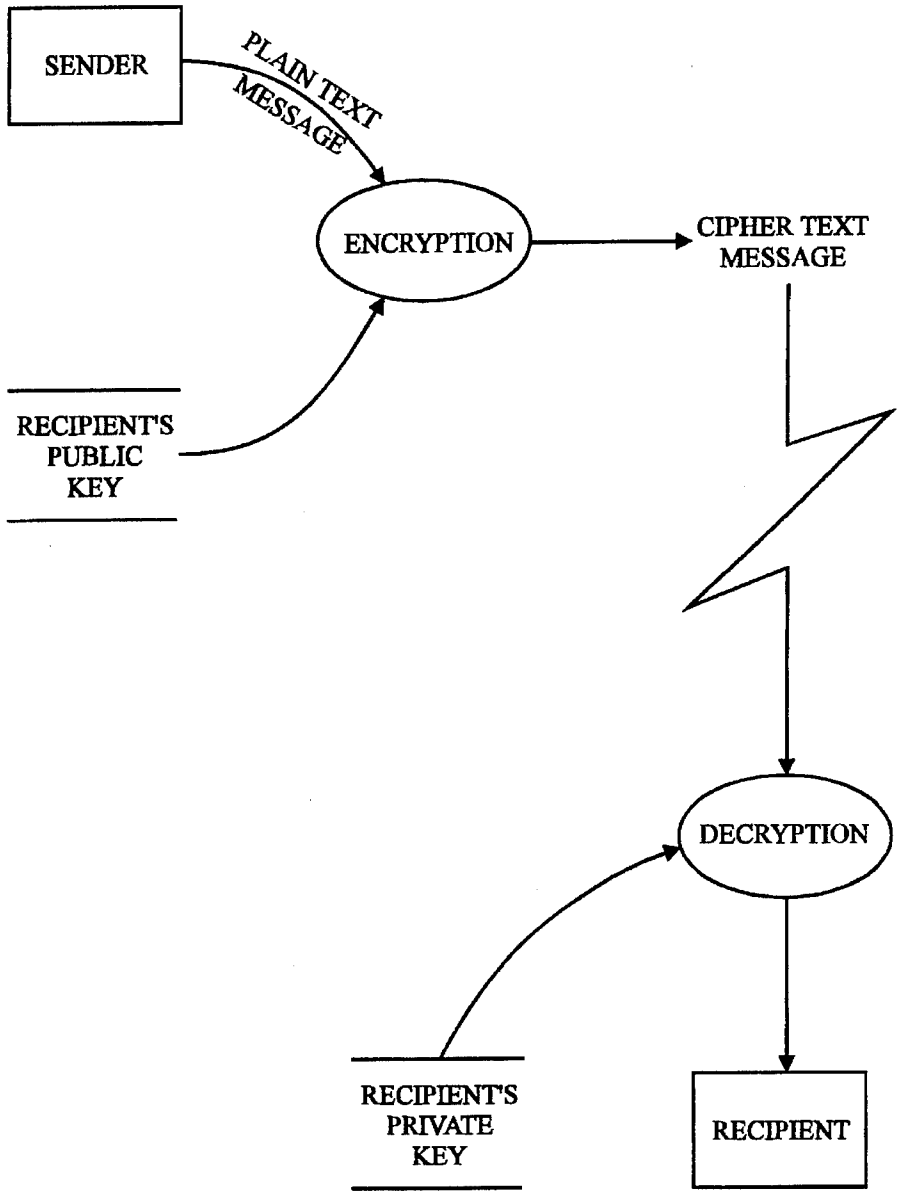
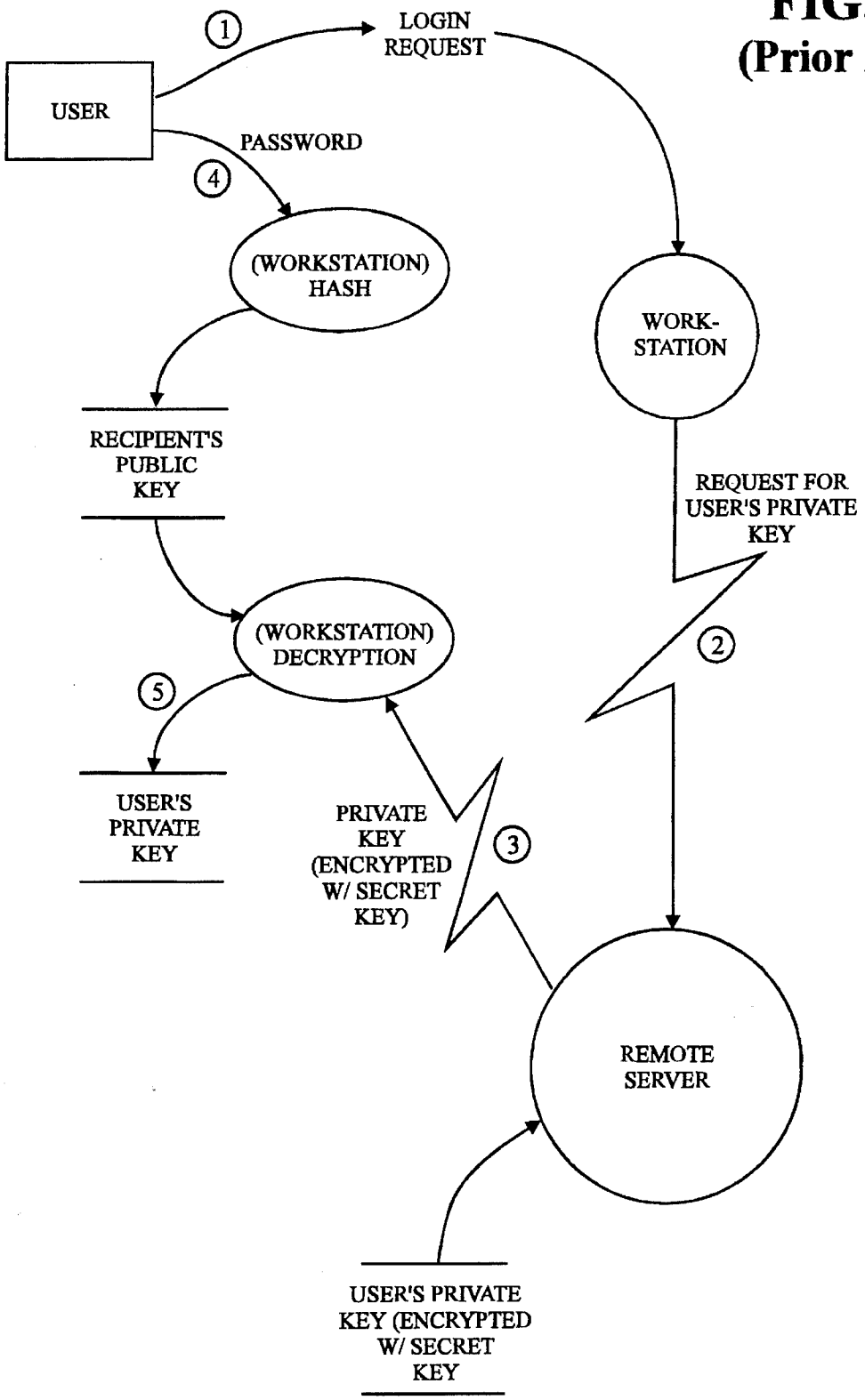


FIG. 3
(Prior Art)



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.