US007243236B1

(12) **United States Patent**
Sibert

(10) **Patent No.: US 7,243,236 B1**
(45) **Date of Patent: Jul. 10, 2007**

(54) **SYSTEMS AND METHODS FOR USING CRYPTOGRAPHY TO PROTECT SECURE AND INSECURE COMPUTING ENVIRONMENTS**

(75) Inventor: **W. Olin Sibert**, Lexington, MA (US)

(73) Assignee: **Intertrust Technologies Corp.**, Sunnyvale, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 544 days.

(21) Appl. No.: **09/628,692**

(22) Filed: **Jul. 28, 2000**

Related U.S. Application Data

(60) Provisional application No. 60/146,426, filed on Jul. 29, 1999.

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

(52) **U.S. Cl.** **713/179**; 713/168; 713/169; 726/2; 380/255; 702/35

(58) **Field of Classification Search** 719/331; 713/201, 179; 62/259.2; 324/760
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

3,573,747	A	4/1971	Adams et al.
3,609,697	A	9/1971	Blevins
3,796,830	A	3/1974	Smith
3,798,359	A	3/1974	Feistel
3,798,360	A	3/1974	Feistel
3,798,605	A	3/1974	Feistel
3,806,882	A	4/1974	Clarke

(Continued)

FOREIGN PATENT DOCUMENTS

AU	A-36815/97	2/1998

(Continued)

OTHER PUBLICATIONS

Shimshon Berkovits, et al., *Authentication of Mobile Agents*, Mobile Agents and Security, Springer-Verlag, Giovanni Vigna, Ed., 1998, pp. 114-136.

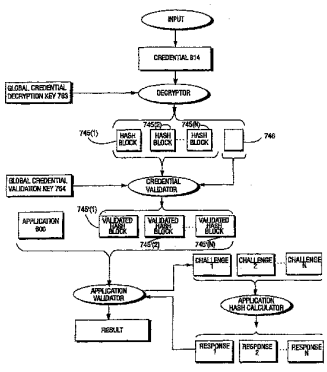
(Continued)

Primary Examiner—Nasser Moazzami
Assistant Examiner—Carl Colin
(74) *Attorney, Agent, or Firm*—Finnegan, Henderson, Farabow, Garrett & Dunner LLP

(57) **ABSTRACT**

Computation environments are protected from bogus or rogue load modules, executables, and other data elements through use of digital signatures, seals, and certificates issued by a verifying authority. A verifying authority—which may be a trusted independent third party—tests the load modules and/or other items to verify that their corresponding specifications are accurate and complete, and then digitally signs them based on a tamper resistance work factor classification. Secure computation environments with different tamper resistance work factors use different digital signature authentication techniques (e.g., different signature algorithms and/or signature verification keys), allowing one tamper resistance work factor environment to protect itself against load modules from another tamper resistance work factor environment. The verifying authority can provide an application intended for insecure environments with a credential having multiple elements covering different parts of the application. To verify the application, a trusted element can issue challenges based on different parts of the authenticated credential that the trusted element selects in an unpredictable (e.g., random) way, and deny service (or take other appropriate action) if the responses do not match the authenticated credential.

27 Claims, 28 Drawing Sheets



EXAMPLE CREDENTIAL VALIDATION

U.S. PATENT DOCUMENTS

3,829,833 A 8/1974 Freeny, Jr.
3,906,448 A 9/1975 Henriques
3,911,397 A 10/1975 Freeny, Jr.
3,924,065 A 12/1975 Freeny, Jr.
3,931,504 A 1/1976 Jacoby
3,946,220 A 3/1976 Brobeck et al.
3,956,615 A 5/1976 Anderson et al.
3,958,081 A 5/1976 Ehrsam et al.
3,970,992 A 7/1976 Boothroyd et al.
4,048,619 A 9/1977 Forman et al.
4,071,911 A 1/1978 Mazur
4,112,421 A 9/1978 Freeny, Jr.
4,120,030 A 10/1978 Johnstone
4,163,280 A 7/1979 Mori et al.
4,168,396 A 9/1979 Best
4,196,310 A 4/1980 Forman et al.
4,200,913 A 4/1980 Kuhar et al.
4,209,787 A 6/1980 Freeny, Jr.
4,217,588 A 8/1980 Freeny, Jr.
4,220,991 A 9/1980 Hamano et al.
4,232,193 A 11/1980 Gerard
4,232,317 A 11/1980 Freeny, Jr.
4,236,217 A 11/1980 Kennedy
4,253,157 A 2/1981 Kirschner et al.
4,262,329 A 4/1981 Bright et al.
4,265,371 A 5/1981 Desai et al.
4,270,182 A 5/1981 Asija
4,278,837 A 7/1981 Best
4,305,131 A 12/1981 Best
4,306,289 A 12/1981 Lumley
4,309,569 A 1/1982 Merkle
4,319,079 A 3/1982 Best
4,323,921 A 4/1982 Guillou
4,328,544 A 5/1982 Baldwin et al.
4,337,483 A 6/1982 Guillou
4,361,877 A 11/1982 Dyer et al.
4,375,579 A 3/1983 Davida et al.
4,433,207 A 2/1984 Best
4,434,464 A 2/1984 Suzuki et al.
4,442,486 A 4/1984 Mayer
4,446,519 A 5/1984 Thomas
4,454,594 A 6/1984 Heffron et al.
4,458,315 A 7/1984 Uchenick
4,462,076 A 7/1984 Smith, III
4,462,078 A 7/1984 Ross
4,465,901 A 8/1984 Best
4,471,163 A 9/1984 Donald et al.
4,484,217 A 11/1984 Block et al.
4,494,156 A 1/1985 Kadison et al.
4,513,174 A 4/1985 Herman
4,528,588 A 7/1985 Löfberg
4,528,643 A 7/1985 Freeny, Jr.
4,553,252 A 11/1985 Egendorf
4,558,176 A 12/1985 Arnold et al.
4,558,413 A 12/1985 Schmidt et al.
4,562,306 A 12/1985 Chou et al.
4,562,495 A 12/1985 Bond et al.
4,577,289 A 3/1986 Comerford et al.
4,584,641 A 4/1986 Guglielmino
4,588,991 A 5/1986 Atalla
4,589,064 A 5/1986 Chiba et al.
4,593,353 A 6/1986 Pickholtz
4,593,376 A 6/1986 Volk
4,595,950 A 6/1986 Löfberg
4,597,058 A 6/1986 Izumi et al.
4,634,807 A 1/1987 Chorley et al.
4,644,493 A 2/1987 Chandra et al.
4,646,234 A 2/1987 Tolman et al.
4,652,990 A 3/1987 Pailen et al.
4,658,093 A 4/1987 Hellman
4,670,857 A 6/1987 Rackman
4,672,572 A 6/1987 Alsberg
4,677,434 A 6/1987 Fascenda
4,680,731 A 7/1987 Izumi et al.
4,683,553 A 7/1987 Mollier
4,685,056 A 8/1987 Barnsdale et al.
4,688,169 A 8/1987 Joshi
4,691,350 A 9/1987 Kleijne et al.
4,696,034 A 9/1987 Wiedemer
4,701,846 A 10/1987 Ikeda et al.
4,712,238 A 12/1987 Gilhousen et al.
4,713,753 A 12/1987 Boebert et al.
4,740,890 A 4/1988 William
4,747,139 A 5/1988 Taaffe
4,757,533 A 7/1988 Allen et al.
4,757,534 A 7/1988 Matyas et al.
4,768,087 A 8/1988 Taub et al.
4,791,565 A 12/1988 Dunham et al.
4,796,181 A 1/1989 Wiedemer
4,799,156 A 1/1989 Shavit et al.
4,807,288 A 2/1989 Ugon et al.
4,817,140 A 3/1989 Chandra et al.
4,823,264 A 4/1989 Deming
4,827,508 A 5/1989 Shear
4,858,121 A 8/1989 Barber et al.
4,864,494 A 9/1989 Kobus
4,868,877 A 9/1989 Fischer
4,903,296 A 2/1990 Chandra et al.
4,924,378 A 5/1990 Hershey et al.
4,930,073 A 5/1990 Cina, Jr.
4,949,187 A 8/1990 Cohen
4,977,594 A 12/1990 Shear
4,999,806 A 3/1991 Chernow et al.
5,001,752 A 3/1991 Fischer
5,005,122 A 4/1991 Griffin et al.
5,005,200 A 4/1991 Fischer
5,010,571 A 4/1991 Katznelson
5,023,907 A 6/1991 Johnson et al.
5,047,928 A 9/1991 Wiedemer
5,048,085 A 9/1991 Abraham et al.
5,050,213 A 9/1991 Shear
5,091,966 A 2/1992 Bloomberg et al.
5,103,392 A 4/1992 Mori
5,103,476 A 4/1992 Waite et al.
5,111,390 A 5/1992 Ketcham
5,119,493 A 6/1992 Janis et al.
5,128,525 A 7/1992 Stearns et al.
5,136,643 A 8/1992 Fischer
5,136,646 A 8/1992 Haber et al.
5,136,647 A 8/1992 Haber et al.
5,136,716 A 8/1992 Harvey et al.
5,146,575 A 9/1992 Nolan, Jr.
5,148,481 A 9/1992 Abraham et al.
5,155,680 A 10/1992 Wiedemer
5,163,091 A 11/1992 Graziano
5,168,147 A 12/1992 Bloomberg
5,185,717 A 2/1993 Mori
5,187,787 A 2/1993 Skeen et al.
5,201,046 A 4/1993 Goldberg et al.
5,201,047 A 4/1993 Maki et al.
5,208,748 A 5/1993 Flores et al.
5,214,702 A 5/1993 Fischer
5,216,603 A 6/1993 Flores et al.
5,221,833 A 6/1993 Hecht
5,222,134 A 6/1993 Waite et al.
5,224,160 A 6/1993 Paulini et al.
5,224,163 A 6/1993 Gasser et al.
5,235,642 A 8/1993 Wobber et al.
5,245,165 A 9/1993 Zhang
5,247,575 A 9/1993 Sprague et al.
5,257,369 A 10/1993 Skeen et al.
5,260,999 A 11/1993 Wyman
5,263,158 A 11/1993 Janis
5,265,164 A 11/1993 Matyas et al.

5,276,735	A	1/1994	Boebert et al.	5,633,932	A	5/1997	Davis et al.
5,280,479	A	1/1994	Mary	5,634,012	A	5/1997	Stefik et al.
5,285,494	A	2/1994	Sprecher et al.	5,636,276	A	6/1997	Brugger
5,301,231	A	4/1994	Abraham et al.	5,636,292	A	6/1997	Rhoads
5,311,591	A	5/1994	Fischer	5,638,443	A	6/1997	Stefik et al.
5,319,705	A	6/1994	Halter et al.	5,638,504	A	6/1997	Scott et al.
5,337,360	A	8/1994	Fischer	5,640,546	A	6/1997	Gopinath et al.
5,341,429	A	8/1994	Stringer et al.	5,655,077	A	8/1997	Jones et al.
5,343,527	A	8/1994	Moore	5,687,236	A	11/1997	Moskowitz et al.
5,347,579	A	9/1994	Blandford	5,689,587	A	11/1997	Bender et al.
5,351,293	A	9/1994	Michener et al.	5,692,047	A	11/1997	McManis
5,355,474	A	10/1994	Thurasingham et al.	5,692,180	A	11/1997	Lee
5,373,561	A	12/1994	Haber et al.	5,710,834	A	1/1998	Rhoads
5,388,211	A	2/1995	Hornbuckle	5,715,403	A	2/1998	Stefik
5,390,247	A	2/1995	Fischer	5,717,923	A	2/1998	Dedrick
5,390,330	A	2/1995	Talati	5,724,425	A	3/1998	Chang et al.
5,392,220	A	2/1995	Van den Hamer et al.	5,740,549	A	4/1998	Reilly et al.
5,392,390	A	2/1995	Crozier	5,745,569	A	4/1998	Moskowitz et al.
5,394,469	A	2/1995	Nagel et al.	5,745,604	A	4/1998	Rhoads
5,410,598	A	4/1995	Shear	5,745,678	A *	4/1998	Herzberg et al. 713/200
5,412,717	A	5/1995	Fischer	5,748,763	A	5/1998	Rhoads
5,421,006	A	5/1995	Jablon	5,748,783	A	5/1998	Rhoads
5,422,953	A	6/1995	Fischer	5,748,960	A	5/1998	Fischer
5,428,606	A	6/1995	Moskowitz	5,754,849	A	5/1998	Dyer et al.
5,432,950	A	7/1995	Sibigtroth	5,757,914	A	5/1998	McManis
5,438,508	A	8/1995	Wyman	5,758,152	A	5/1998	LeTourneau
5,442,645	A	8/1995	Ugon	5,765,152	A	6/1998	Erickson
5,444,779	A	8/1995	Daniele	5,768,426	A	6/1998	Rhoads
5,449,895	A	9/1995	Hecht et al.	5,819,263	A	10/1998	Bromley et al.
5,449,896	A	9/1995	Hecht et al.	5,842,173	A	11/1998	Strum et al.
5,450,493	A	9/1995	Maher	5,892,900	A	4/1999	Ginter et al.
5,453,601	A	9/1995	Rosen	5,896,454	A	4/1999	Cookson et al.
5,453,605	A	9/1995	Hecht et al.	5,910,987	A	6/1999	Ginter et al.
5,455,407	A	10/1995	Rosen	5,915,019	A	6/1999	Ginter et al.
5,455,861	A	10/1995	Faucher et al.	5,917,912	A	6/1999	Ginter et al.
5,455,953	A	10/1995	Russell	5,920,861	A	7/1999	Hall et al.
5,457,746	A	10/1995	Dolphin	5,940,504	A	8/1999	Griswold
5,463,565	A	10/1995	Cookson et al.	5,940,505	A	8/1999	Kanamaru
5,473,687	A	12/1995	Lipscomb et al.	5,943,422	A	8/1999	Van Wie et al.
5,473,692	A	12/1995	Davis	5,949,876	A	9/1999	Ginter et al.
5,479,509	A	12/1995	Ugon	5,970,145	A *	10/1999	McManis 713/187
5,485,622	A	1/1996	Yamaki	5,982,891	A	11/1999	Ginter et al.
5,491,800	A	2/1996	Goldsmith et al.	5,991,399	A *	11/1999	Graunke et al. 380/279
5,497,479	A	3/1996	Hornbuckle	5,999,949	A	12/1999	Crandall
5,497,491	A	3/1996	Mitchell et al.	6,009,170	A	12/1999	Sako et al.
5,499,298	A	3/1996	Narasimhalu et al.	6,009,543	A *	12/1999	Shavit 712/200
5,504,757	A	4/1996	Cook et al.	6,016,393	A	1/2000	White et al.
5,504,818	A	4/1996	Okano	6,047,242	A *	4/2000	Benson 702/35
5,504,837	A	4/1996	Griffeth et al.	6,112,181	A	8/2000	Shear et al.
5,508,913	A	4/1996	Yamamoto et al.	6,138,119	A	10/2000	Hall et al.
5,509,070	A	4/1996	Schull	6,148,083	A *	11/2000	Fieres et al. 380/255
5,513,261	A	4/1996	Maher	6,157,721	A	12/2000	Shear et al.
5,517,518	A	5/1996	Morson et al.	6,185,683	B1	2/2001	Ginter et al.
5,530,235	A	6/1996	Stefik et al.	6,237,786	B1	5/2001	Ginter et al.
5,530,752	A	6/1996	Rubin	6,240,185	B1	5/2001	Van Wie et al.
5,533,123	A	7/1996	Force et al.	6,253,193	B1	6/2001	Ginter et al.
5,534,975	A	7/1996	Stefik et al.	6,292,569	B1	9/2001	Shear et al.
5,537,526	A	7/1996	Anderson et al.	6,820,200	B2 *	11/2004	Takeuchi et al. 713/179
5,539,735	A	7/1996	Moskowitz				
5,539,828	A	7/1996	Davis				
5,550,971	A	8/1996	Brunner et al.				
5,553,282	A	9/1996	Parrish et al.				
5,557,518	A	9/1996	Rosen				
5,557,798	A	9/1996	Skeen et al.				
5,563,946	A	10/1996	Cooper et al.				
5,568,552	A	10/1996	Davis				
5,572,673	A	11/1996	Shurts				
5,592,549	A	1/1997	Nagel et al.				
5,603,031	A	2/1997	White et al.				
5,606,609	A	2/1997	Houser et al.				
5,613,004	A	3/1997	Cooperman et al.				
5,621,797	A	4/1997	Rosen				
5,629,980	A	5/1997	Stefik et al.				

FOREIGN PATENT DOCUMENTS

AU	A-36816/97		2/1998
AU	A-36840/97		2/1998
BE	9 004 79		12/1984
DE	3803982	A1	1/1990
EP	0128672	A1	12/1980
EP	0 084 441	A1	7/1983
EP	0 135 422	A1	3/1985
EP	0 180 460	A1	5/1986
EP	0 370 146	A1	5/1990
EP	0 398 645	B1	11/1990
EP	0399822	A2	11/1990
EP	0421409	A2	4/1991

EP	0 456 386 A2	11/1991
EP	0 469 864 A2	2/1992
EP	0565314 B1	10/1993
EP	0 570 123 B1	11/1993
EP	0 593 305 A2	4/1994
EP	0 651 554 A1	5/1995
EP	0 668 695 A2	8/1995
EP	0 695 985 A1	2/1996
EP	0 696 798 A1	2/1996
EP	0 714 204 A2	5/1996
EP	0 715 243 A1	6/1996
EP	0 715 244 A1	6/1996
EP	0 715 245 A1	6/1996
EP	0 715 246 A1	6/1996
EP	0 715 247 A1	6/1996
EP	0 749 081 A1	6/1996
EP	0 725 376 A2	8/1996
EP	0 763 936 A2	9/1996
EP	0 778 513 A2	6/1997
EP	0 795 873 A2	9/1997
EP	0 800 312 A1	10/1997
EP	0 913 757 A2	5/1999
GB	2 136 175 A	9/1984
GB	2264796 A	9/1993
GB	2 294 348 A	4/1996
GB	2 295 947 A	6/1996
JP	57-000726	1/1982
JP	62-225059	10/1987
JP	62-241061	10/1987
JP	01-068835	3/1989
JP	64-068835	3/1989
JP	02-242352	9/1990
JP	02-247763	10/1990
JP	02-294855	12/1990
JP	04-369068	12/1992
JP	05-181734	7/1993
JP	05-257783	10/1993
JP	05-268415	10/1993
JP	06-175794	6/1994
JP	06-215010	8/1994
JP	06-225059	8/1994
JP	07-056794	3/1995
JP	07-084852	3/1995
JP	07-141138	6/1995
JP	07-200317	8/1995
JP	07-200492	8/1995
JP	07-244639	9/1995
JP	08-137795	5/1996
JP	08-152990	6/1996
JP	08-185292	7/1996
JP	08-185298	7/1996
WO	WO 85/02310	5/1985
WO	WO 85/03584	8/1985
WO	WO 90/02382	3/1990
WO	WO 92/06438	4/1992
WO	WO 92/22870	12/1992
WO	WO 93/01550	1/1993
WO	WO 94/01821	1/1994
WO	WO 94/03859	2/1994
WO	WO 94/06103	3/1994
WO	WO 94/16395	7/1994
WO	WO 94/18620	8/1994
WO	WO 94/22266	9/1994
WO	WO 94/27406	11/1994
WO	WO 95/14289	5/1995
WO	WO 96/00963	1/1996
WO	WO 96/03835	2/1996
WO	WO 96/05698	2/1996
WO	WO 96/06503	2/1996
WO	WO 96/13013	5/1996
WO	WO 96/21192	7/1996
WO	WO 96/24092	8/1996
WO	WO 96/27155	9/1996
WO	WO 97/03423	1/1997
WO	WO 97/07656	3/1997
WO	WO 97/25816	7/1997
WO	WO 97/32251	9/1997
WO	WO 97/43761	11/1997
WO	WO 97/48203	12/1997
WO	WO 98/09209	3/1998
WO	WO 98/10381	3/1998
WO	WO 98/37481	8/1998
WO	WO 98/45768	10/1998
WO	WO 99/01815	1/1999
WO	WO 99/24928	5/1999
WO	WO 99/48296	9/1999

OTHER PUBLICATIONS

M. Blaze, et al., *Decentralized Trust Management*, Proc. IEEE Conference on Security and Privacy, 1996, pp. 164-173.

David Chess, *Security Issues in Mobile Code Systems*, Mobile Agents and Security, Springer-Verlag, Giovanni Vigna, Ed., 1998, pp. 1-14.

C. Ellison, et al., *SPKI Certificate Theory*, Internet Engineering Task Force (IETF) RFC 2693 —Sep. 1999, pp. 1-38, available at http://www.ietf.org/rfc/rfc2693.txt?number=2693.

Fritz Hohl, *Time Limited Blackbox Security: Protecting Mobile Agents from Malicious Hosts*, Lecture Notes in Computer Science, vol. 1419: Mobile Agents and Security, Springer-Verlag, 1998, G. Vigna, Ed., pp. 90-111.

Li Gong, et al., *Signing, Sealing and Guarding Java Objects*, Mobile Agents and Security, G. Vigna, editor, Springer-Verlag, 1998, vol. 1419 of LNCS, pp. 206-216.

Tomas Sander et al., *Towards Mobile Cryptography*, IEEE Proceedings of Security and Privacy, 1998, pp. 1-10.

Tomas Sander et al., *Protecting Mobile Agents Against Malicious Hosts*, Mobile Agents and Security: Lecture Notes in Computer Science, Springer-Verlag, G. Vigna, Ed., vol. 1419, 1998, pp. 1-16.

Steve R. White, *ABYSS: A Trusted Architecture for Software Protection*, IBM Thomas J. Watson Research Center, Yorktown Heights, New York 10598, 1987, pp. 38-51.

"Microsoft Authenticode Technology", Microsoft Corporation, Oct. 1996.

Abadi, M. et al., "Authentication and Delegation with Smart-cards," Technical Report 67, DEC Systems Research Center, available as of Oct. 1990 at <http://citeseer.nj.nec.com/article/abadi92authentication.html>, pp. 1-22.

Ameke, D. et al., "AT&T Encryption System Protects Information Services," Jan. 9, 1995, 1 page.

Baggett, D., "Cable's Emerging Role in the Information Superhighway," Cable Labs, undated, 13 slides.

Barassi, T.S., "The Cybernotary: Public Key Registration and Certification and Authentication of International Legal Transactions," undated, prior to 1997, 4 pages.

Barnes, H., memo to H. LaMuth, subject: George Gilder articles, May 31, 1994, 2 pages.

Bart, D., "Comments in the Matter of Public Hearing and Request for Comments on the International Aspects of the National Information Infrastructure," Aug. 12, 1994, 17 pages.

Baum, M., "Worldwide Electronic Commerce: Law, Policy and Controls Conference," Nov. 11, 1993, 18 pages.

Best, R.M., "Preventing Software Piracy With Crypto-Microprocessors," Digest of Papers, VLSI: New Architectural Horizons, Feb. 1980, pp. 466-469.

Bisbey II, R.L. et al., "Encapsulation: An Approach to Operating System Security," USC/Information Science Institute, Marina Del Rey, CA, Oct. 1973, pp. 666-675.

Blaze, M., "A Cryptographic File System for Unix," pre-print of paper for First ACM Conference on Computer and Communications Security, Fairfax, Virginia, Nov. 3-5, 1993, 8 pages.

Blaze, M., "Key Management in an Encrypting File System," available as of Aug. 23, 2002 at <http://www.usenix.org/publicaitons/libratry/proceedings/bos94/full_papers/blaze.asp>, pp. 1-12.

Blom, R. et al., "Encryption Methods in Data Networks," Ericsson Technics, No. 2, Stockholm, Sweden, 1978, pp. 72-105.
Bruner, R.E., "Power Agent, NetBot Help Advertisers Reach Internet Shoppers," visited on Aug. 13, 1997, 2 pages.
Caruso, D., "Technology, Digital Commerce: 2 Plans for Watermarks, Which Can Bind Proof of Authorship to Electronic Works," N.Y. Times, Aug. 7, 1995, p. D5.
Castano, S. et al., *Database Security*, Addison-Wesley & Acm Press, 1995.
Champine, G., *MIT Project Athena: A Model for Distributed Campus Computing*, Digital Equipment Corporation, 1991.
Chaum, D., "Achieving Electronic Privacy," Scientific American, Aug. 1992, pp. 96-101.
Chaum, D., et al. "Wallet databases with observers," Ernest F. Brickell, editor, Advances in Cryptology —CRYPTO '92, 12th Annual International Cryptology Conference, Santa Barbara, CA, Aug. 16-20, 1992, Proceedings, pp. 89-105.
Chaum, D., "Security Without Identification Card Computers to Make Big Brother Obsolete," available at <http://www.chaum.com/articles/Security_Without_Identification.htm, visited on Aug. 23, 2002, 24 pages.
"List of Articles," <http://www.chaum.com/articles/list-of-articles.htm>, visited on Aug. 23, 2002, 4 pages.
Choudhury, A.K., et al., "Copyright Protection for Electronic Publishing Over Computer Networks," AT&T Bell Laboratories, Murray Hill, NJ, Jun. 1994, 18 pages.
Clark, T., "Ad Service Gives Cash Back," <http://www.news.com/News/Item/0,4,13050,00.html>, visited Aug. 13, 1997, 2 pages.
Cohen, F.B., "Operating System Protection Through Program Evolution," 8246 Computers & Security, No. 6, (Oxford, Great Britain) Oct. 1993, available at <http://all.net/books/IP/evolve.html, visited on May 31, 2002, 22 pages.
Cox, B., "What If There is a Silver Bullet and the competition gets it first?" Journal of Object-Oriented Programming, Jun. 1992, available at <http://www.virtualschool.edu/cox/CoxWhatIfSilverBullet.html>, pp.1-5, visited on Aug. 23, 2002.
Cunningham, D., et al., "AT&T, VLSI Technology Join To Improve Info Highway Security,"(News Release) Jan. 31, 1995, 3 pages.
CUPID Protocols and Services (Version 1): "An Architectural Overview,"Nov. 1992, available at <http://www.cni.org/projects/CUPID>, 25 pages.
Custer, H. *Inside Windows NT*, Microsoft Press, Redmond WA, 1993.
Davies, D. et al., *Security for Computer Networks*, John Wiley & Sons, 1989.
Dempsey L.., "The Warwick Metadata Workshop: A Framework for the Deployment of Resource Description," D-Lib Magazine, Jul./Aug. 1996, 8 pages.
Denning, D.E., *Cryptography and Data Security*, Addison-Wesley, Reading MA. 1983.
Denning, D.E. et al., Data Security, 11 Computing Surveys No. 3, Sep. 1979, pp. 227-249.
Denning, D.E., "Secure Personal Computing in an Insecure Network," Communications of the ACM, Aug. 1979, vol. 22, No. 8, pp. 476-482.
Diffie, W. et al., "New Directions in Cryptography," IEEE Transactions on Information Theory, vol. 22, No. 6, Nov. 1976, pp. 644-651.
Diffie, W. et al., "Privacy and Authentication: An Introduction to Cryptography," Proceedings of the IEEE, vol. 67, No. 3, Mar. 1979, pp. 397-427.
Dusse, S.R. et al., "A Cryptographic Library for the Motorola DSP 56000," Advances in Cryptology-Proceedings of Eurocrypt 90, (I.M. Damgard, ed., Springer-Verlag) 1991, pp. 230-244.
Dyson, E., "Intellectual Value," WIRED Magazine, Jul. 1995, pp. 136-141 and 182-184.
Garcia, D.L., "Before a Hearing on Science, Space and Technology," Subcommittee on Technology, Environment, and Aviation, May 26, 1994, pp. 97-108.
Gleick, J., "Dead as a Dollar," The New York Times Magazine, Jun. 16, 1996, Sect. 6, pp. 26-30, 35, 42, 50, 54.
Greguras, F., "Softic Symposium '95, Copyright Clearances and Moral Rights, " Dec. 11, 1995, 3 pages.
Guillou, L.C., "Smart Cards and Conditional Access," Advances in Cryptography—Proceedings of EuroCrypt 84 (T. Beth et al, ed., Springer-Verlag, 1985) 10 pages.
Haar, S.V., "PowerAgent Launches Commercial Service," Interactive Week, Aug. 4, 1997, 1 page.
Harman, H., *Modern Factor Analysis*, Third Edition Revised, University of Chicago Press, Chicago and London, 1976, table of contents, 5 pages.
Hearst, M.A., "Interfaces for Searching The Web," Scientific American, Mar. 1997, pp. 68-72.
Herzberg, A. et al., "Public Protection of Software," ACM Transactions on Computer Systems, vol. 5, No. 4, Nov. 1987, pp. 371-393.
Hofmann, J., "Interfacing the NII to User Homes," Consumer Electronic Bus. Committee Presentation, NIST, Jul. 1994, 14 slides, missing slide 14.
Holt, S., "Start-Up Promises User Confidentiality in Web Marketing Service," InfoWorld Electric News, viewed Aug. 13, 1997, 2 pages.
Ioannidis, J., et al. "The Architecture and Implementation of Network-Layer Security Under Unix," Fourth USENIX Security Symposium Proceedings (Oct.), USENIX, Berkeley, Calif. 1993, 11 pages.
Jiang, J.J. et al., "A Concept-based Approach to Retrieval from an Electronic Industrial Directory," International Journal of Electronic Commerce, vol. 1, No. 1 (Fall 1996) pp. 51-72.
Jones, D., "Top Tech Stories, PowerAgent Introduces First Internet 'Informediary' to Empower and Protect Consumers," viewed Aug. 13, 1997, 3 pages.
Kelly, K., "E-Money," Whole Earth Review, Summer 1993, pp. 40-59.
Kent, S. T., *Protecting Externally Supplied Software in Small Computers*, Sep. 1980, 254 pages.
Kohl, J. et al., "The Kerberos Network Authentication Service (V5)," Network Working Group Request for Comments RFC-1510, Sep. 1993, pp. 1-104.
Kohl, U, et al., "Safeguarding Digital Library Contents and Users Protecting Documents Rather Than Channels," In *D-lib Magazine*, Sep. 1997, available at <http://www.dlib.org/dlib/september97/ibm/09lotspiech.html>, visited Oct. 30, 2002, pp. 1-9.
Kristol, D.M. et al., "Anonymous Internet Mercantile Protocol," AT&T Bell Laboratories, Murray Hill, NJ, Mar. 17, 1994, pp. 1-16.
Lagoze, C., "The Warwick Framework, A Container Architecture for Diverse Sets of Metadata," D-Lib Magazine, Jul./Aug. 1996, 7 pages.
Lanza, M., "George Gilder's Fifth Article-Digital Darkhorse," Newspapers, Feb. 21, 1994, 2 pages.
Lampson, B. et al., "Authentication in Distributed Systems: Theory and Practice," ACM Trans. Computer Systems, vol. 10, No. 4 (Nov. 1992), pp. 1-46.
Lehman, B., "Intellectual Property and the National Information Infrastructure, a Preliminary Draft of the Report of the Working Group on Intellectual Property Rights," Jul. 1994, 141 pages.
Levy, S., "E-Money, That's What I Want," WIRED, Dec. 1994, 14 pages.
Low, S.H. et al., "Anonymous Credit Cards," AT&T Bell Laboratories, Proceedings of the 2nd ACM Conference on Computer and Communication Security, Fairfax, VA, Nov. 2-4, 1994, 10 pages.
Low, S.H. et al., "Anonymous Credit Cards and Its Collusion Analysis" AT&T Bell Laboratories, Murray Hill, NJ, Oct. 10, 1994, 18 pages.
Low, S.H. et al., "Document Marking and Identification Using both Line and Word Shifting" AT&T Bell Laboratories, Murray Hill, NJ, Jul. 29, 1994, 22 pages.
Lynch, C., "Searching The Internet," Scientific American, Mar. 1997, pp. 52-56.
Maclachlan, M., "PowerAgent Debuts Spam-Free Marketing," TechWire, Aug. 13, 1997, 3 pages.
Maxemchuk, N.F., "Electronic Document Distribution," AT&T Bell Laboratories, Murray Hill, NJ, Sep./Oct. 1994, 11 pages.
Milbrandt, E., "Steganography Info and Archive," 1996, 2 pages.
Mori, R. et al., "Superdistribution: The Concept and the Architecture," The Transactons of the EIEICE, V, E73, No. 7, Tokyo, Japan, Jul. 1990, pp. 1133-1146.

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.