THIRD CPSR CRYPTOGRAPHY AND PRIVACY CONFERENCE

June 7, 1993



EXCISE

Carnegie Endowment for International Peace

2400 N. Street, NW

Washington, DC

8:30 Coffee

9:00 Welcome and Introductions

9:30 Introduction to Cryptography

David Kahn, a noted historian of cryptography, will provide an overview of cryptography and discuss the current trend toward use in everyday activities.

10:00 Government Cryptography Policy

In the past several years, law enforcement and intelligence agencies have attempted to restrict the public development and implementation of cryptography. This panel will discuss recent developments including the Clipper Proposal, the Digital Signature Standard and the roles of NIST and the NSA under the Computer Security Act of 1987.

Moderator: Rick Weingarten, Executive Director, Computer Research Associates

Participants: John Podesta, Staff Secretary, The White House

David Sobel, Computer Professionals for Social Responsibility Ray Kammer, Acting Director, National Institute for Standards and

Technology

Dr. Steven Bryen, Secure Communications Technology

11:15 Break

11:30 The Digital Telephony Proposal

In 1992 the Federal Bureau of Investigation introduced a proposal to require that telecommunications manufacturers and service providers redesign their systems to facilitate wiretapping. This panel will discuss the implications of that proposal on privacy, security and the telecommunications network.

Moderator: David Flaherty, Wilson Center/University of Western Ontario

Participants: Janlori Goldman, Privacy and Technology Project, ACLU

James K. Kallstrom, Federal Bureau of Investigation Dr. Dorothy Denning, Georgetown University

William Murray, Deloitte and Touche

12:30 Lunch (provided)

SSIFIED

POIN Exemptions BS 87E

BO Clastions

<u>.</u>

UNCLASSIFIED

- 1:15 Debate - Encryption Policy, Privacy and Government Secrecy

Moderator: Professor Lance Hoffman, George Washington University

Participants: Whitfield Diffie, Sun Microsystems

Alan R. McDonald, Federal Bureau of Investigation

2:00 Export Controls

Currently, federal regulations restrict products that contain encryption from export. This panel will discuss the problems that these restrictions present and how they affect the use of cryptography within the United States.

Moderator: Roszel Thomsen, McKenney, Thomsen & Burke

Participants: Ilene Rosenthal, Software Publishers Association

Allan Suchinsky, Office of Defense Trade Controls, State Department

David Peyton, Information Technology Association of America

3:00 Cryptography in Everyday Use

This panel will look at the present and future applications of public key cryptography including Digital Cash, Privacy-Enhanced Mail, and Pretty Good Privacy.

Wayne Matson

Moderator: Mikki Barry, Intercon Systems

Presenters: Phil Zimmerman, Pretty Good Privacy

Steve Crocker, Trusted Information Systems

David Chaum, DigiCash

4:00-6:00 Reception at Carnegie

Marc Rotenberg, David Banisar CPSR Washington Office 202-544-9240 (voice), 202-547-5481 (fax) rotenberg@washofc.cpsr.org banisar@washofc.cpsr.org



LIII ASSIFIED

CPSR Cryptography and Privacy Conference June 7, 1993

Name Organization

John Adams IEEE Spectrum

Charlotte Adams FCW

Michael Autrey Privacy Times

Stewart Baker NSA

Brian Baker CUA Law School

James Bamford ABC World News Tonight

David Banisar CPSR

Mikki Barry Intercon Systems

Jerry Berman Electronic Frontier Foundation

Jim Bidzos RSA
Denis Bieber SecurTech

Jane Bortnick Congressional Research Service

Martina Bradford AT&T
Clint Brooks NSA

Reese Brown Jnl of Intel. and Counter-Intel.

Steven Bryen SecurTech
David Burnham TRAC
Jean Camp IEEE

Karen Casser

James Chandler.GWUDan CharlesNPRDavid ChaumDigiCash

John Cohen House Judiciary Committee

Sarah Comley

Dan Cook Department of State

Steven Crocker TIS

Colin Crowe House Telecomm

Jim DempseyHouse Judiciary CommitteeDorothy DenningGeorgetown UniversityWhitfield DiffieSun Microsystems

Mario Einaudi CPSR Woody Evans US West

David Farber University of Pennsylvania

Addison Fischer Fischer International

David Flaherty Wilson Center

Greg Frazier House Committee on Intelligence
Bob Gellman House Govt. Operations Comm

Frank Gilbert

John Gilmore Cygnus Support

Sol Glasner Mitre Janlori Goldman ACLU

Harry Goodman NPR

Tom Guidoboni

CPSR Cryptography and Privacy Conferen June 7, 1993

Name

Ann Harkins

Evan Hendricks

Ezra Herman

Lance Hoffman

Paul Hyland

David Johnson

David Kahn

Iim Kallstrom

Ray Kammer

Phil Karn

Stuart Kern

Jack King

Rob Kurz

Steven Levy

Herb Lin

Steve Lipner

Wayne Madsen

Fred Mailman

John Markoff

Kate Martin

Alan McDonald

Kate McGee

John McMullen

Lynn McNulty

Brock Meeks

Ken Mendelson

Ellen Messmer

John Mintz

William Murray

Mike Nelson

Juan Osuna

Bill Pauli

Beverly Peterson

David Y. Peyton

Harold Podell

Iohn Podesta **Bill Poulis**

Bob Rarog

Mitch Ratcliffe

Harold Relyea Jeff Richelson

Ilene Rosenthal

Marc Rotenberg

Organization

Senate Judiciary Committee

US Privacy Council

BNA

George Washington University

CPSR

Wilmer, Cutler & Pickering

Newsday

FBI

NIST

Qualcomm

Department of Treasury

BNA Legal Report

House Govt. Operations

MacWorld

National Acadamy of Sciences

Computer Sciences Corp

HP

NY Times

CNSS/ACLU

FBI

Oracle

Newsbytes

NIST

Communications Daily

House Judiciary Committee

Network World

Washington Post

Deloite and Touche

OSTP

CRA

Apple Computer

GAO

ITAA

General Accounting Office/OSI

The White House

Apple Computer

Digital Equipment Corp.

MacWeek

Congressional Research Service

National Security Archive

Software Publishers Association

CPSR

CPSR Cryptography and Privacy Conference June 7, 1993

Name Organization

Debbie Rudolph IEEE

Cathy Russell Senate Judiciary Committee

Jeff Schiller M

Wynn Schwartau Inter*Pak

John Schwartz Washington Post Bob Smith Privacy Journal

Olly Smoot CBEMA
David Sobel CPSR

John Sonderman Department of State

Ross Stapleton CIA
Gary Stern ACLU

Allan Suchinsky Department of State

Roszel Thomsen & Burke

Lee Tien

Peter Wayner Georgetown University

Rick Weingarten Computer Research Association
Danny Weitzner Electronic Frontier Foundation

William Whitehurst IBM Steven Wolff NSF

Phil Zimmermann Boulder Software Engineering

In a rock !!



MEMORANDUM

TO: The Files

FROM: PM/DTC/CED: John Sonderman

SUBJECT: CPSR Cryptography and Privacy Conference

June 7, 1993, Washington, DC

The first speaker was David Kahn, author of The Codebreakers. He gave an overview of cryptography. He claimed cryptographic growth follows communication growth, as communications expand, cryptography expands. Governments want to prevent the growth of cryptography to maintain order and security. The government feels it must know what is happening in society. The U.S. government is trying to control cryptography through export controls and introduction of the clipper chip. Both help maintain the status quo and prevent privacy from advancing.

Kahn went on to state that privacy is good. A balance must be made between national security and privacy/profit. He claimed if you outlaw good crypto only the outlaws will have good crypto. Further, while the government wants to hold back technology, it can't, the government can only delay technology. He pointed out that even Iran is on the BITNET. Philip Zimmermann then stated trying to stop cryptography was "...like trying to stop the wind."

Zimmermann went on to state that the government was on the "...wrong side of the power curve... it may not be a choice of are we going to live in a world of unbreakable crypto, we can't stop it, we must find a way to adjust." Zimmermann claimed that while outlawing drugs and alcohol may have merits, outlawing cryptography had no basis. He claimed "cryptography doesn't hurt people."

Kahn concluded that there are three government proposals currently: CCEP, DSS, and Clipper. Each alone is innocuous, but all three together are something else.





The next speaker was Ray Kammer, acting director of NIST. He addressed the Clipper initiative. He stated that Clipper is currently delayed do to problems finding key escrow agents and export control issues.

David Sobel, CPSR, spoke next on the Digital Signature Standard and the Computer Security Act of 1987. The act divided government cryptography into two categories, military controlled by NSA, and civilian controlled by NIST. Yet with DSS, of the documents CPSR obtained, 143 were from NIST and 1,138 were NSA. Sobel claimed NSA was running civilian cryptography, and that this was probably true in Clipper as well.

Dr. Steven Bryen, Secure Communications Technology, spoke on Clipper. He claimed Clipper was technology that will compete with his private sector products. Bryen stated that NIST/NSA had not identified the threat that clipper helps diminish. He also claimed Clipper was a domestic solution to an international problem. U.S. firms need secure communication abroad, and foreign governments might not allow Clipper in, or if they did demand the escrow keys.

Zimmermann then added a few comments. He said he was just back for Eurocrypt, and that he had learned that SHA hash algorithm was pretty good. He also stated:

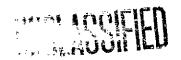
Clipper is voluntary for the moment until the other shoe drops... throw the baby out with the bath water, put the entire population at risk to catch a few criminals

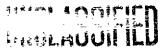
Zimmermann continued stating that "...someday the government may change to a bad government... government has a history of abuse, there is a crying need for cryptography... not to employ cryptographic technology..." helps a police state.

John Gilmore claimed the counter reaction to the clipper proposal could be far more wide spread use of non-clipper encryption. Gilmore questioned how the intel community would interface with the escrow system.

During a break, Stephen Crocker of Trusted Information Systems approached me and expressed his frustration with DTC. He claimed he had sent several letters requesting permission to put his TIS/PEM product on his FTP server. Having received no reply, he went ahead and did it anyway.

Several FBI agents spoke on the merits of the FBI Digital Telephony Proposal. The main criticism expressed by the audience was that the FBI hadn't justified the need for the proposal.





John Podesta of the White House spoke on the Clipper proposal. He claimed clipper addressed three issues: (1) providing a higher level of security, (2) takes advantage of advances in technology, and (3) takes into consideration the needs of law enforcement.

David Peyton, Information Technology Association of America spoke first on export controls. He claimed government policy needed to get in touch with reality. Cryptographic technology was available outside the U.S. and current policy was a "unilateral give away" to Britain and Finland. U.S. vendors are kept at a "policy disadvantage." He wanted the U.S. to decontrol cryptography over the Internet and to adopt the rules agreed to at COCOM. Exports should be allowed to legitimate end users in friendly countries.

Ilene Rosenthal, Software Publisher Association, also addressed foreign availability. She stated that increases in foreign sales meant more customers want cryptographic functions in the software. Sophisticated customers want the best security including DES. Foreign cryptographic products now dominate the market with 143 foreign software manufacturers from 13 countries. She also claimed the Internet made cryptography widely available including PGP which has become a standard in Europe.

Alan Suchinsky and Dan Cook of PM/DTC spoke on current export restrictions. Glenn S. Tenney of Fantasia Systems, Inc. asked how many investigations into export violations for cryptography were ongoing. Suchinsky said he did not know but would find out. During questions about criteria for export Zimmermann added "how about common sense?"

Steve Crocker, of Trusted Information Systems (TIME) spoke on his companies implementation of Privacy Enhanced Mail (PEM). TIS/PEM, as it is called, provides security, confidentiality and authentication. Crocker said he has mounted TIS/PEM on his Internet FTP server for anonymous access, but he had implemented some controls to reduce international distribution. TIS/PEM uses MD2, MD5, DES and RSA.

Philip Zimmermann spoke on his software program called Pretty Good Privacy (PGP). Zimmermann said PGP uses RSA/IDEA for encryption, RSA/MD5 to sign messages, plaintext compression, pass phrases with MD5 form IDEA keys and a grass roots trust model for public key certification. Zimmermann said he plans to change the signature mechanism from MD5 to IDEA after Zimmermann learned of weaknesses in MD5 while attending EUROCRYPT '93.

Zimmermann went on to state that PGP was published in June of 1991. Zimmermann claimed he did not know about the internet himself, but gave it to a friend that posted it onto netnews groups with a USA distribution set. He stated pgp was a "grass roots social phenomenon" and a matter of free speech. He claimed you "can't stop this."



DRAFT UNCLASSIFIED



MEMORANDUM

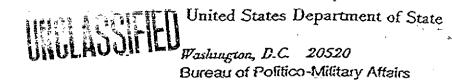
TO: ODUSD/DTSA/ML - Col. Richey

FROM: PM/DTC/CEB - Clyde G. Bryant, Jr.

UNCLASSIFIED

DRAFT





CENTER for DEFENSE TRADE

OFFICE OF DEFENSE TRADE CONTROLS PM/DTC

Only	UNCLASSIFIED	Information may be	transmitted by	FAX
------	---------------------	--------------------	----------------	-----

Only UNCLASSIFIED Information may be transmitted by FAX
TO: 5/A Robin Sterzer USCS 6/10/93 (Name) (Office) (Date)
FAX # 408-291-4151
TEL #: 408-291-4162
FROM: John Sonderman PM/DTC/CEB (Name) (Office)
FAX #: 703.875.5663
TEL# 703-875-5650
·
SUBJECT: CPSR Crypt & Priv. Gnf; Please call to clear on Memo to DTSA
to clear on Memo to DTSA
*

Number of Pages Transmitted in this FAX: 11 hel (Wer



--UNCLASSIFIED--