Minutes of the Computer System Security and Privacy Advisory Board Meeting

June 8-10, 1999
National Institute of Standards and Technology
Gaithersburg, MD

Tuesday, June 8, 1999

Acting Chairman, Rick Weingarten, called the meeting to order at 9:20 a.m.. In addition to Mr. Weingarten, those members present were: Peter Browne, John Davis, Addison Fischer, John Sabo, Jim Wade and Karen Worstell.

Ed Roback, Board Secretariat, introduced and welcomed Mr. Peter Browne, who was recently appointed to membership on the Board. Mr. Browne is Senior Vice President and Division Head of Information Security Services at First Union Corporation.

Mr. Roback reviewed the meeting agenda and associated handout material. He also discussed the status of the membership appointments of the Board and those appointments to membership that were currently being processed.

As with all Board meetings, all sessions were open to the public. At the beginning of the meeting, there were nine members of the public in attendance.

The minutes of the March 1999 Board meeting were reviewed and unanimously approved.

Next, the Board members discussed the action items to be taken with regard to the correspondence that they had received from Ray Kammer, Director of the National Institute of Standards and Technology (NIST), in November 1998. The main content of the letter was separated into four unique segments: (1) security metrics and reference data sets; (2) identification of top IT security research issues; (3) federal agency improvement; and, (4) privacy in the system life-cycle. On the topic of security metrics, the Board discussed the possibility of co-hosting a security metrics workshop with NIST to call upon the IT industry to dialogue about the methods and requirements that would allow for development of better security products. In the area of identification of top IT security requirements, it was suggested that the Board hear from a representative of a White House Office of Science and Technology Policy research and development committee on their activities in the IT area. The National Research Council's recent Cyberspace Report was identified as a good example of security research issues. It would also be useful to obtain a list of federally-funded information and security projects currently underway.

After further discussion, it was decided that the Board would endeavor to develop a short discussion paper that would focus on all of the segments of the NIST request. Members Fischer, Worstell and Browne will work on the metrics issue; members Davis and Wade will work on the research issues; members Leo and Guida will work on the federal agency improvements issue; and members Trubow, Wade and Sabo will work on the privacy issue and members Fischer and

Browne will work on the system life-cycle issue. These topics will be added to the September Board meeting agenda and any output will be circulated to the membership prior to that meeting.

National Plan for Protecting the Infrastructure

Dr. Jeffery Hunker
Director
Critical Infrastructure Assurance Office

Dr. Hunker began his presentation by announcing that he was leaving the position of Director of the Critical Infrastructure Assurance Office (CIAO) to assume a new position with the National Security Council. The new Director of the CIAO will be Mr. John Tritak.

Dr. Hunker distributed copies of the May 1999 working draft of the National Plan for Information Systems Protection. He stated that the document was currently going thorough extensive interagency review and had not been widely circulated at this juncture. He requested that the Board review it and provide any comment to the CIAO within the next two weeks. While he apologized for the quick turn around request for comments, he felt that it was important to the CIAO to have the Board's reaction to the plan.

This draft was essentially the first version of the national plan and Dr. Hunker stressed that this plan would always be in an ongoing and revolutionary process state. It is divided into two component parts. One is actions that the Federal government have taken and the other deals with the actions that the private sector and local government can take. Its structure is that of a framework for action as opposed to a plan for action. It is designed around three objectives: prepare and prevent, detect and respond and build strong foundations. There are ten programs discussed. Each includes a list of milestones. Dr. Hunker stated that NIST has the action to establish standards for physical protection of critical federal computer systems. All programs are supported by requests in the President's FY2000 budget. Dr. Hunker stressed that from a policy coordination effort, this is an extremely difficult task and it does encompass all areas of the Federal government.

He closed his presentation by welcoming the comments of the Board, asking them to think in terms of what should be forthcoming as a result of this initial effort.

(1)Beyond Concern: Understanding Net Users' Attitudes about Online Privacy
(2) World Wide Web Consortium's Platform for Privacy Preferences Project

Lorrie Faith Cranor
AT&T Laboratories - Research

In her briefing on net users' attitudes about online privacy, Ms. Cranor discussed the problem that there needs to be a user interface designed for a tool that helps users manage the information they provide to web sites and that makes decisions based on web site privacy policies **[Ref. #1]**. This task is more difficult because while many surveys show high levels of public concern about internet privacy, there is little idea of how they perceive privacy and what their reaction is to the collection and use of personal information.

She reported that a web-based survey had been emailed to 1,500 DRI family panel members. Of that number, 523 surveys were returned with 381 of those respondents from the U.S. Those U.S. respondents tended to be more educated and had more internet experience and concern about internet privacy issues. Overall, statistically, 17% were extremely concerned about any use of data; 56% often had specific concerns and tactics for addressing them and, 27% reported that they were willing to provide data under most circumstances, but had mild general concern and some specific concerns. The completed report is available online at http://www.research.att.com/projects/privacystudy/.

Next, Ms. Cranor briefed the Board on the Platform for Privacy Preference Project (P3P). She identified some advantages and disadvantages of revealing personal information on line. Tools need to be developed to allow people to control the use and dissemination of their personal information. These empowerment tools can prevent your actions from being linked to you, allow you to develop persistent relationships not linked to each other or you, allow you to make informed choices about how your information will be used and know what assurances about information practices are trust worthy. Those with such tools include AT&T, Bell Labs, W3C and TRUSTe - Electronic Frontier Foundation and CommerceNet.

The guiding principles of the P3P working groups include information privacy, notice and communication, choice and control, fairness and integrity and security. They are proposing that a web site encode its privacy practices in the form of a P3P proposal, that automated tools be used to do the actual encoding and that user agents translate information in proposals into a more user friendly format.

For further information on P3P see: http;//www.w3.org/P3P.

CIO Security Committee Update

John Gilligan, Department of Energy
Fernando Burbano, Department of State
Co-Chairs of the CIO Security Committee

Mr. Gilligan **[Ref. #2]** began the briefing by explaining that the Committee's primary focus was to ensure implementation of security practices within the Federal government that gain public confidence and protect government services, privacy and sensitive and national security information. The Committee's annual budget is approximately $250K. Major thrusts include awareness and training, improvement of agency knowledge and use of security tools, improvement of security administrators' skills, improvement of effectiveness of agency computer security programs and the facilitation of implementing PDD-63. To enhance these efforts they also recommend partnering with agencies and the Critical Infrastructure Assurance Office (CIAO) to implement PDD-63 by reviewing agency plans, identifying priority focus areas, enhancing incident detection and response capabilities and being an advocate for funding to implement PDD-63. They also are behind the development of a National Information Assurance Plan.

As part of the CIO Council, they also work on the Education and Training Committee to help improve training of systems security personnel and are an advocate for the President's Cyber Corps Program. They also support the Interoperability Committee in its effort to establish common security guidelines.

Mr. Gilligan said that significant progress has already been accomplished in these work efforts, future initiatives have been aligned with key need areas and increased cyber security concerns will likely result in increased efforts.

The CIO Security Committee is looking to the Board for feedback on there proposed work efforts. They are interested in suggestions of where the Committee should be focusing and if there should be more proactive CIO participation. Gilligan believes that the CIOs need a more dynamic policy established.

Also, the funding for the CIO activity will soon be eliminated so they would welcome the Board's comments on that topic.

Mr. Burbano joined the discussion and emphasized the close ties between the CIO security committee and the implementation of PDD63's cyber security efforts. It was also his suggestion that the Administration treat this issue the same as it has the Y2K emergency issue. A security problem like computer hacking is a serious threat to the government. The problems, however, are so sophisticated that it is difficult at best to describe it sufficiently to those in the Administration or on the Hill so that they can understand the need for the funding to arrive at the solutions needed to thwart such hacker attacks. Mr. Burbano stated that it is imperative that the Hill, the Administration and the private sector come together on this issue.

Strategic Security Summit 2000

Karen Worstell
SRI Consulting, Inc.

Board Member, Karen Worstell, discussed an upcoming conference, Strategic Security Summit 2000 (SSS2K), which is being held in Helsinki, Finland on June 26-28, 2000. The focus will be on global strategic issues affecting information protection policy technology and business strategy. The format of the meeting will be invited speakers and keynotes, presentation of committee reviewed papers and exhibits of selected security companies. The mission of the conference is to address strategic issues affecting information protection for the third millennium in a forum of industry leaders around the world. The expected audience includes the attendance of 1000+ CIOs and senior managers, decision-makers, global industry, public and private sectors and multiple government representatives. It will provide the opportunity for the identification of the top ten issues in security and privacy on an international scale, for the draft of the SSS2K conference statement of direction and the fostering of understanding and partnership between the attending groups.

NIST Director's Request - Board Discussion

The Board discussed input for an appropriate reply to Director Kammer's letter. They returned to the discussion of the suggestion that the CSSPAB and NIST co-sponsor a security metrics workshop that would assist in the development of security metrics and reference data sets by bringing together both industry and government viewpoints. We will also work to hear from people who do information technology research. The Board Secretariat will look at the possibility of the Board and NIST hosting a workshop sometime in the March 2000 time period. More discussion will follow at the September Board meeting.

During this session, Ed Roback gave a short briefing on the feedback from the Advanced Encryption Standards conference that was held in Rome, Italy in April. The schedule is to announce the finalists this summer. At this time, the expectation is that there will be five finalists.

Public Participation Period

There being no public participation, the meeting was recessed at 4:50 p.m.

Wednesday, June 9, 1999

The meeting was reconvened at 9:10 a.m.

Information Technology Laboratory (ITL) Director Introduction

Dr. William O. Mehuron
Director

Dr. Mehuron was appointed Acting Director of the ITL in April 1999. He gave the Board a brief synopsis of his previous senior management and technical positions in the federal government. He most recently worked with the National Oceanic and Atmospheric Administration (NOAA) where he served as the Director of their Systems Acquisition Office and as the Acting Deputy Undersecretary of NOAA. Earlier in his career, Dr. Mehuron was Deputy Director for Research and Engineering at the National Security Agency. In addition to his federal service, he served for 20 years in the private sector.

Dr. Mehuron said that he is favorably impressed with the work going on in the ITL. He noted that 20% of the overall budget for the ITL goes to the Computer Security Division and that it was his intention to see the budget increased for this activity. NIST has proposed a very large initiative in electronic commerce to OMB and an important part of this initiative effort involves computer security. This proposal has been briefed to the Department of Commerce and the responses received have been valuable ones. There are plans for a Department of Commerce workshop/symposium on digital economy, and he again emphasized that information security is a very important part of this effort. Dr. Mehuron offered his endorsement of the letter that the Board had received from Director Kammer and encouraged them to continue to take an active role in responding to it.

The Board asked Dr. Mehuron how they could help further the electronic commerce effort for NIST. He responded that they should take advantage of the chain of command that the Board has to endorse the NIST effort to the Secretary of Commerce. He stated that he sees the ITL computer security role in the electronic commerce focusing on development of appropriate standards. The Board was pleased that Dr. Mehuron planned to push for increased support of ITL efforts at NIST.

The Board thanked Dr. Mehuron for his candor and invited him to return to future meetings to continue these discussions as events progress.

Update on GITS Security Committee Activities

Rich Guida, Chairman
GITS Committee
Department of the Treasury

Mr. Rich Guida, Chairman of the GITS Committee briefed the Board on the Federal Bridge Certification Authority **[Ref. #3]**. His presentation covered the Federal PKI policy authority overlay, technical boundary conditions, policy/political boundary conditions, potential architectures, current status and schedule. It supports four levels of assurance: rudimentary, basic, medium, high and is analogous to Canada CP. Currently they are working with several contractors as part of an EMA challenge to decide the approach. The tentative determination is cross certified CAs within membrane. Vendors will have to be on GSA schedule so that their products can be purchased. Entrust and GTE are the vendors offering initial products. The schedule is on target at this time. The prototype bridge is expected late in 1999 and will be located at NTIS. They expect to be operational sometime in early 2000.

Mr. Guida stated that the current draft CIAO plan contains no references to the PKI effort. He requested that the Board consider expressing this comment in their feedback to the CIAO on the draft. He indicated that he had provided comments to them earlier about this absence. However, there were no changes to the draft that reflected this.

Privacy Law Review: EU Data Directive and Bernstein v. DOJ

Marc Rotenberg
Executive Director
Electronic Privacy Information Center

Mr. Rotenberg, Executive Director of the Electronic Privacy Information Center, briefed the members on the European Data Directive, "Cryptography and Liberty 1999," and Bernstein v. DOJ and the Supreme Court and Privacy **[Ref. #4]**.

The EU Data Directive primary focus has been on the Safe Harbor proposal of the Department of Commerce that would allow U.S. companies that choose to adhere to certain privacy principles. The stated benefits for U.S. organizations for being in the safe harbor include:

- All 15 Member States (MS) will be bound by the European Commission's finding of adequacy;
- The understanding will create the presumption that companies within safe harbor provide adequate data protection and data flows to those companies will continue;
- MS requirements for prior approval of data transfers either will be waived or approval will be automatically granted;
- U.S. companies will have a transition period to implement safe harbor policies;
- Claims against U.S. organizations will for the most part be limited to claims of non-compliance with the principles, European consumers will be expected to exhaust their recourse within the U.S. organization first, and due process will be assured for U.S. organizations that are subject to complaints; and
- Generally, only the European Commission, acting with a committee of MS representatives will be able to interrupt personal data flows from an EU country to a U.S. organization.

This proposal has been a very contentious one with the Europeans, says Rotenberg. In response to a question as to how will non-EU/US countries respond to this issue, Rotenberg said that he believes that those countries will follow the EU solution as they are currently doing. There is an EU/US summit being held later in June at which time both parties hope to reach an agreement. He anticipates that there will be an agreement on the Safe Harbor proposal. There will be agreement on the principles but he expects there to be lingering questions as to the outcome. We may see some pressure to improve the privacy standards for the U.S. citizen and it is anticipated that the directive will leverage privacy technology such as encryption, anonymity, etc.

Mr. Rotenberg stated that the EPIC would soon release a world survey on privacy. He pointed the Board to the EPIC website for reference [www.epic.org].

Mr. Rotenberg's colleague, Wayne Madsen, briefed the Board EPIC's crypto survey. It was the second such survey to look at restrictions of controls on domestic use, export and key agency setting policy. The survey indicated that fewer countries restrict the use, manufacture or sale of encryption

Next, Mr. Rotenberg presented a brief overview of the Bernstein vs DOJ case, stating that Daniel J. Bernstein argued that the State had restricted his first amendment rights. What Mr. Rotenberg found significant was that there are over 6000 cases proposed to the Supreme Court each year and only approximately 150 of them are heard. He felt that this one was heard because of its security implications. He also mentioned another case, McIntire v Ohio where the issue was whether a person has the right to issue a political paper anonymously. The ruling of the Supreme Court was that the right to anonymous distribution of political information is the right of freedom of speech .

Mr. Rotenberg distributed copies to the Board of a recent EPIC publication, "Cryptography and Liberty 1999; an International Survey on Encryption Policy."

Information Security Risk Assessment of Leading Organizations

Ernest Doring
General Accounting Office (GAO)

Mr. Ernest Doring, General Accounting Office, briefed the Board on a new document that is a supplement to GAO's Executive Guide on Information Security Management. **[Ref. #5]** The document, "Information Security Risk Assessment; Practices of Leading Organizations," is being prepared as an exposure draft and will be released later this summer. Its objectives are to identify practical methods adopted by leading organizations and to identify critical success factors. Four organizations were studied: a multinational oil company, a financial services company, a government financial institution and a software engineering company. Risk assessment practices used covered critical success factors, processes, tools and related benefits. Mr. Doring encouraged the Board to review the exposure draft and submit any comments to GAO.

Board Discussion Period

The members exchanged copies of their comments on the draft CIAO national plan and the output will be sent to Board Chairman Ware with the request that he prepare an appropriate email response to Jeffery Hunker. Comments included :

- incorporate references to industry in milestones (ISAC, private sector liaison and information referrals);
- establish milestones for industry associations/advocates for investment and participation in the plan for information systems protection.;
- PKI is a critical element of e-commerce infrastructure and should be addressed as an action item(s);
- there is a lack of reference to "mission enabling" benefits;
- "Vulnerability Management" rather than "Vulnerability Assessment;"
- need a reference security model for critical infrastructure protection to include components such as firewalls, extranet, VPN, PKI, IDR, etc.;
- create employee awareness as an early milestone in support of the prepare and prevent objective;
- need for interoperable strong COTS encryption infrastructures that may cross national boundaries;
- Chapter 3 is unbalanced and confusing. The Department of Defense section is laden with acronyms.
- really like the front cover layout;
- impressive document overall; and
- a significant accomplishment to create the first draft.

There was discussion of the response to be prepared to the Secretary of Commerce on the Board's endorsement of NIST's proposed initiative on electronic commerce. The Board, without objection drafted a letter to be forwarded to the Chairman, who has editorial latitude, to send to the Secretary of Commerce on this subject.

The meeting was recessed at 4:50 p.m.

Thursday, June 10, 1999

The meeting was reconvened at 9:05 a.m.

Computer Security Act Revisited

Michael Quear
Professional Staff Member
Technology Subcommittee of the House Science Committee
U.S. House of Representatives

Mr. Quear's started his briefing by saying that he was here to tell the Board what was going on in Congress and to hear from the Board what they would like to see happening on the Hill.

The Gordon Bill has a high level of attention but a low level of understanding by the Congress. The Science Committee overview of legislation in the area of computer security started with the Computer Security Act of 1989 but has never been strongly enforced or implemented by NIST. The H.R. 1907, Computer Security Enhancement Act of 1997 provided general guidance to agencies on security. There is also another piece of legislation (Gordon) on electronic commerce that calls for the establishment of a national panel for the use of digital standards. The current version of the Computer Security Enhancement Act is expected to move later this summer and include the digital signature requirements of the Gordon Bill. The technology seems well developed but how do we get it organized is the problem. One technology is not favored over another but it should be sensitive to those kinds of things that apply to the federal establishment only. They encourage Federal agencies to buy commercial products in this area. They would also like to see NIST develop guidelines for agencies to use and list the technical guidelines and issues of operability. The goal is to create a level playing field so that people would know what the government at large is using. If they choose not to use COTS, agencies must address why they do not.

The Board was encouraged by Mr. Quear's remarks and asked his opinion on the probability of the passage of this newer version of the revision to the Computer Security Act. Mr. Quear responded that he felt the probability was high that the Bill would pass this Congressional session and encouraged the Board to check the legislative website for continuing updated.

Administration Privacy Update

Peter Swire
Chief Counselor for Privacy

Mr. Peter Swire is the newly appointed Chief Counselor for Privacy, appointed by OMB Director, Jacob Lew, to coordinate the federal government's response to privacy issues. He most recently was a Professor of Law at Ohio State University's College of Law. He's a lawyer and an economist and has worked in the cyperspace law and banking areas. He identified the privacy issue concerns of the public sector and they include financial, medical and internet privacy issues. He mentioned the Safe Harbor proposal by Ambassador Aaron and said that they are more optimistic than some of the press accounts may show. He also stated that there is ongoing dialogue with States regarding the public record review issue.

The Privacy Counselor position is located within the Office of Information and Regulatory Affairs at OMB, and has responsibility to oversee the implementation of the Privacy Act of 1974. The position will also encompass the Paperwork Reduction Act responsibilities and Federal government agency regulations in policies. He envisions that the low visibility of this position will allow for a more concentrated effort.

He distributed a copy of a June 2, 1999, memorandum to the Heads of Executive Departments and Agencies from Jacob J. Lew, Director, OMB, on the subject of privacy policies on Federal websites **[Ref. #6]**. This memo directs departments and agencies to post clear privacy policies on World Wide Web sites and provides guidance to do so. Mr. Swire welcomed the Boards comments on this directive.

As for the future outlook, Mr. Swire said that privacy policy has a new level of political commitment in this Administration and he expects this trend to continue.

On the political front, Mr. Swire said that policy development would likely continue in areas such as biometrics, where the possibility of scans being polluted exists. Therefore, rules and practices need to be in place sooner rather than later. Another privacy issue is how to work between privacy and authentication. There exists the potential tension between the good authentication that we need and the privacy that would be required to protect the data. Another significant issue is the use of government records and development and use of government databases. He believes that there is a need for standards to be developed for some of these major issues.

Mr. Swire is not currently involved in the cryptography policy arena and does not see the opportunity to become involved -in the near future.

Next, he solicited comments from the Board. A suggestion was made that perhaps there is a need for the development of a privacy department to address all of the issues Mr. Swire had raised. When asked how he was planning to handle the prioritization of these issues, he responded that he would call upon those from within OMB and other agencies on specific topics of interest as well as coordinate with others on the Hill. He suggested that the Board could help build a thoughtful process to interact between the Congress and the interagency groups and agencies on how to look at these issues. National discussion of these topics may bring the States into this arena as well.

The Board thanked Mr. Swire for his briefing and invited him to future Board meetings to continue this dialogue.

The next two scheduled presentations, OMB Updated by Glenn Schlarman, and Transatlantic Consumer Dialogue Privacy Coalition Briefing by Ed Mierzwinski did not take place because of unexpected schedule conflicts of the presenters. They will be rescheduled for a future Board meeting.

The Board moved on to further discussion of the correspondence being drafted to the Secretary of Commerce, the Director of NIST and the Director of CIAO.

There being no further business, the meeting was adjourned at 12:30 p.m.

References:

#1. Cranor presentation
#2. Gilligan/Burbano presentation
#3. Guida presentation
#4. Rotenberg presentation
#5. Doring presentation
#6. Jabob Lew June 2, 1999 letter

/S/

Edward Roback
Board Secretary

CERTIFIED as a true and accurate
summary of the meeting

/S/

Willis H. Ware
Chairman