A View of The Task You Face

A Report to the NRC Committee on Cryptography

Ivan Sutherland

Perspectives 96-2
In an Essay Series Published by SunLabs

August 1996

For information regarding the SunLabs Perspectives Series, contact Jeanie Treichel, Editor-in-Chief <jeanie.treichel@eng.sun.com>.
For distribution issues, contact Amy Tashbook Hall, Assistant Editor <amy.hall@eng.sun.com>.

Editor's Notes

About the series—The *Perspectives* series is a collection of essays written by individuals from Sun Microsystems Laboratories. These essays express ideas and opinions held by the authors on subjects of general rather than technical interest. Sun Microsystems Laboratories publishes these essays as a courtesy to the authors to share their views with interested friends and colleagues. The opinions and views expressed herein are solely those of the authors, and do not in any way represent those of Sun Microsystems Laboratories, nor Sun Microsystems, Inc.

About the author—Dr. Ivan E. Sutherland recently won the prestigious Price Waterhouse Information Technology Leadership Award for Lifetime Achievement, as well as an honored place in the Smithsonian's Permanent Collection of Information Technology (IT) Innovation. The Lifetime Achievement Award "recognizes individuals who, over a lifetime and against great odds, have made an outstanding contribution to society through the use of information technology."

Ivan is widely known for his pioneering contributions in the field of computer graphics. His 1963 MIT Ph.D. thesis, *Sketchpad*, first demonstrated the potential of computer graphics. In his work on a head-mounted three-dimensional display at Harvard in the mid '60s, Ivan anticipated today's virtual reality by 25 years. He is co-founder of Evans and Sutherland, which produces the most advanced computer image generators now in use. As head of the Computer Science Department at Caltech, he helped make integrated circuit design an acceptable field of academic study. Dr. Sutherland is a member of both the National Academy of Engineering and the National Academy of Sciences. He received the ACM Turing Award in 1988 and holds several honorary degrees.

Presently, Dr. Sutherland is Vice President and Fellow of Sun Microsystems, Inc. He was previously with Sutherland, Sproull, and Associates, Inc. and Advanced Technology Ventures. He has worked on research projects at the U.S. Dept. of Defense, Harvard, MIT, and other leading institutions, and is the author of twelve patents and numerous publications.

—Ed.

Notes from the Author

In October 1994, the National Research Council (NRC) convened its "Committee to Study National Cryptography Policy." The committee was charged with understanding and reporting on the military, law enforcement, and commercial requirements for cryptography. Their report[1] came out in May 1996. It is available from the National Academy Press.

Their task was a challenging one. Until recently, cryptography was practiced mainly for military purposes and most cryptographic knowledge was held secret in military organizations. Recently, however, there has been a wider spread of cryptographic knowledge and a greatly increased demand to use it for commercial and personal privacy. I felt that this NRC Committee had a good chance to understand and balance the conflicting needs of commerce, individuals, and national security.

Their task was also very important. I feel strongly that two negative results may follow if the United States delays too long in commercializing cryptography. First, we will deny ourselves the security that cryptography offers, leaving our computers, computer networks, and communications systems open to exploitation by our international competitors and terrorism by our enemies. Second, if other nations offer suitable equipment before we do, they may dominate the market for security systems.

In the summer of 1995, I offered my views to the NRC Committee, emphasizing our nation's need for commercial cryptography. I offered a view of the committee's task as deciding in what year the commercial need for widespread cryptography exceeds the military and law enforcement needs to limit its spread.

This paper is the text of the talk I gave to the committee in Woods Hole, Massachusettes on July 19, 1995. I am especially fond of Michael Cobb's cartoons that I used as slides for my talk and that appear in this paper. I think they capture the essence of my points.

---

1. *Cryptography's Role in Securing the Information Society*, National Academy Press, Pre-publication edition, 30 May 1996. Publication version expected Fall 1996.

I offer this "Perspective" as my point of view on a topic that will no doubt remain controversial for some time. I hope you find these ideas provocative. I hope my paper will encourage you to form your own view of how our nation should treat cryptography.

Ivan Sutherland

Mountain View, CA
August 1996

A View of The Task You Face

A Report to the NRC Committee on Cryptography

Ivan Sutherland

Sun Microsystems Laboratories
2550 Garcia Avenue
Mountain View, CA 94043

1 Introduction

I believe that your panel on cryptography is the most important panel the National Research Council has convened in many years. We, as a nation, must choose whether or not to unleash the full power of cryptography for commercial gain. On the one hand, we may choose to keep cryptography under tight control and retain some ability to discover what our foreign and domestic enemies would prefer that we not know. On the other hand, we may choose to dominate the world market for commercial cryptographic equipment, gaining for ourselves both security and economic advantage. I believe that your panel must offer a judgment about which course to take. You are the only body in a position to do so.

I appreciate both sides of this argument. As a young man, I worked at the National Security Agency (NSA). I came to appreciate the enormity of its task, the strength of its technical base, and the great value to our nation of its successes. Some of the brightest people I've ever met, in or out of government, work at NSA, deeply dedicated to the national interest. I stand in awe of their accomplishments.

Figure 1.

More recently I have played a role in nurturing commerce. I have been an entrepreneur at Evans and Sutherland, a consultant at Sutherland, Sproull and Associates, a venture capitalist at Advanced Technology Ventures, and am now serving a technical role as a "Fellow" at Sun Microsystems, Inc. I recognize the dedication, skill, and luck it takes to build a successful commercial enterprise. I have shared the fruits of business success and paid the cost of failure. I have watched markets open and close. Commercial success comes only when the time is ripe. Once lost to competition, either domestic or foreign, market leadership is difficult to regain because customer habit, loyalty, and trust are easy to lose but hard to win.

With the close of the cold war, I see commercial competitiveness as our main national challenge. Our commercial competitors abroad compete well, and in several industries have stolen our markets. Figure 1, seen in Pittsburgh in the 70s, says it all.

I see in cryptography the potential for major U.S. commercial advantage. We could exploit it and become the first users and dominant supplier of secure information equipment to the world. I fear that we may shackle our information industry, preventing it from entering important new world markets and developing major new businesses. I fear that with such shackles we may kill it. I speak to you today because I want our information industry to lead what I see as an inevitable development.

2 The Players

I see three players in this controversy: Figures 2, 3, and 4.

Figure 2.

Individual: Our people presume personal privacy. They speak freely on the telephone. They use cash both for its convenience and for its anonymity. They want the privacy and freedom of speech guaranteed by the U.S. Constitution. Some claim that constitutional protection should cover electronic information. Some argue against government controls of cryptography on grounds of personal freedom. I also want personal freedom and privacy, but today with your group, I shall avoid arguing for or against them, concentrating instead on the commercial issue.

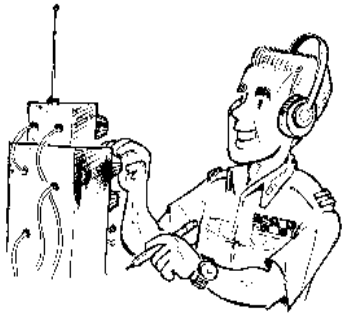

Figure 3.

Government: These people used their skill in cryptography to win World War II. Tapping communications remains an important tool for defense and law enforcement. For most of this century, military and law enforcement organizations have exploited lapses in their opponent's guard to advantage. Our Defense Department provides the world's best security devices and methods for use by our military and by our civilian government. They hold a national treasure of cryptographic know-how.

Figure 4.

Commercial: These people want to use cryptography in business. Some seek the opportunity to sell secure communications equipment and secure operating systems for computers. Some, fearing disastrous meddling in vital computers, emphasize its importance for commercial security. Some envision whole new industries for distributing software, information, news, and ideas—industries that will depend on cryptographic techniques to identify customers, to enforce copyrights, and to collect payments.

3 The Bombshell

In 1976 the world changed technically and politically when Diffie and Hellman published their ideas about Public Key Cryptosystems. (Whitfield Diffie and Martin Hellman, "New Directions in Cryptography," *IEEE Transactions on Information Theory,* Volume IT-22, 1976, pp. 644-645) Technically, the world changed forever because the new technique was so powerful. A major cost of cryptographic security, key distribution, no longer burdened its use. Politically, the world changed because Diffie and Hellman published in the open literature. Cryptography was no longer a state secret. I don't know, nor much care, whether our secret workers anticipated Public Key Cryptosystems. The essential fact is that with Diffie and Hellman's publication, a technically strong idea became public. The cat came out of the bag. See Figure 5.

Figure 5.

Public key cryptography promises strong security with small administrative cost. We now see how ordinary people might use secure telephones and electronic cash. We see how to make computer systems safe from hacker attack. We see how electronic commerce can flourish. Freedom from elaborate key distribution systems makes cryptography a tool rather than a burden. This presents a major opportunity.

The new cryptography offers major commercial opportunity for three reasons. First, it will let us secure electronic commerce from dangerous attack. Second, it opens a fresh market here and abroad for U.S. security products. Third, by protecting intellectual property and permitting electronic payment, as illustrated in Figure 6, it enables whole new information industries.

Figure 6.

4 Authentication vs. Encryption

I want to distinguish authentication from encryption. An authentication system defends against unauthorized entry. It adds credibility to the *bona fide* nature of the user or transaction. Authentication is important when I give instructions to the bank; it must be sure the instructions come from me. Everyday authentication relies on my social security number, my mother's maiden name, a picture identity card or driver's license, or the sound of my voice. Authentication falls short of making the transaction private; it certifies only that entry into the transaction is properly granted.

An encryption system, in contrast, conceals the content of the encrypted message, but may fall short of ensuring a proper origin. To access each separately encrypted document

one needs a separate key. Penetrating one document offers no special access to another.

There are many systems where authentication appears adequate, and where, were it foolproof, authentication might indeed be adequate. The trouble with authentication alone, of course, is that once fooled, a system that depends solely on authentication is vulnerable to major loss.

We use authentication widely in our computer systems today. We use passwords, personal identification numbers, card entry systems, and so forth. Nevertheless, our existing systems are all too vulnerable. In a few widely publicized cases, defenders have caught the perpetrators of attacks on computer systems. I suspect, however, that the public story reveals only the tip of this iceberg. Countless other attacks go unpublicized for fear of embarrassment to the system operator, for fear of loss of public confidence, because their perpetrators could not be caught, or simply because they went unnoticed. The fox is in our hen house as illustrated in Figure 7.

Figure 7.

Good security for computer systems requires both authentication and encryption. Authentication is essential to identify customers and employees, but authentication alone is not enough. Inside our computer systems, we must secure valuable data on a file by file and communication by communication basis for two reasons. First, without encryption we expose too much when authentication fails. Second, valid backup and maintenance tasks require access to files and data streams but should not expose content. Encrypted audit files can protect the nature and even the existence of audits, thus enhancing their ability to apprehend invaders.

5 The Changing Environment

For many years photographs bore reliable witness to events. They no longer do. Computer generated images of astonishing realism can fool the eye. Computers can put fresh faces seamlessly into scenes. Remember how realistic Tom Hanks looked speaking with Jack Kennedy in the movie *Forrest Gump*.

Digital cameras are already inexpensive and will soon be cheap. I predict that within ten years insurance companies will offer a reduction in premium to any automobile that carries continuously recording digital cameras. See Figure 8.

Figure 8.

After an accident such cameras may provide evidence of what happened. Their collective records will capture nearly everything that goes on in public streets. Video recordings have already had a marked effect on law enforcement from Rodney King to the Oklahoma City bombing. A new world of digital images awaits us. Will its product bear reliable witness through cryptography, or will digital images offer a new opportunity for fraud?

Everybody is “on the air” with cellular telephones. Sure, there are laws that forbid listening in to what other people say, but those laws violate physics. In effect, you shout across the miles when you talk by phone from your car. Of course others hear you, as illustrated in Figure 9.

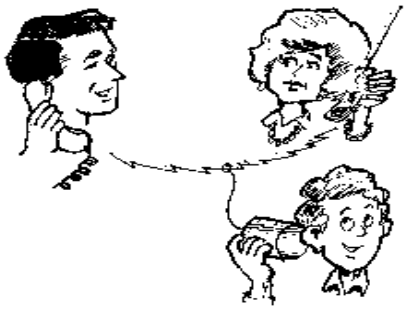

Figure 9.

Under existing law, your security options are silence and circumlocution. I favor laws that match physics. For security, I favor a law with two parts. First, my law would permit any listener to use any fact he or she picked up on the radio, or by tapping phones, for that matter. Second, my law would permit manufacture, sale, ownership, and use of any security device, cryptographic or otherwise. Such a pair of laws would replace the illusion of security with real security by creating an instant market for reliable commercial cryptosystems.

Secure radio telephony will offer new opportunities. There are obvious commercial uses like remote billing systems and remote load control for utilities, where very little use of radio spectrum can save miles of communication cable and millions of dollars in energy costs. There are obvious law enforcement values like routine use of cellular telephone service as an inexpensive substitute for today's special and insecure police radios. There are obvious consumer uses for mobile information services such as pay-per-play music, fast opinion polls, specialized news services, and so forth that depend on security both to prevent theft and to facilitate billing. Information security, generally, is an enabling technology that will make all kinds of new services possible.

Unfortunately, each such new service will offer new ways to invade personal privacy. We all hate solicitors who telephone at dinner time. We all despise uninvited advertising by FAX. Each commercial opportunity will present dilemmas requiring us to balance privacy against use. My current favorite dilemma follows from observing that the cellular phone system knows which cell my phone is in, thus locating my phone to within a few miles. Who owns that information and to what use may it be put?

Figure 10.

When my son borrows my car on Saturday night, as illustrated in Figure 10, I might like to know where it took him. It being my phone, am I entitled to that information, or is his privacy paramount? Of course, he can switch off the cellular phone, but does extinguishing the lights on its handset ensure that location tracking stops?

Your panel can't hope to resolve such conflicts. Nor can anyone prevent the growth of the new services that are to come. Your task, as I see it, is to decide when the United States will become a full participant in the new world of information. Even if we choose now to retain cryptography as a state monopoly, others will not. It is well to remember that we are only 5% of the world's population.

More and more of our commercial information travels as bits. Within a few years, my water heater and air conditioner will help bal-

ance loads by turning on or off upon digital instructions from my electric utility. Such digital communications need good security against the havoc penetration might yield. Imagine a hacker starting the Great Northeast Power Blackout at will, or the power available to terrorists by even making such a threat. The new world is upon us. How openly do we welcome it?

6 Investment Decisions

Why has U.S. industry failed to provide secure computer operating systems and secure communications devices? We have the technology. The chips that would be required could be made at low cost if built in commercial volume. The answer, I believe, rests in the confidence of management and financial investors. Today, no sensible commercial firm can invest more than superficially in information security.

Our investment failure follows from uncertainty of reward. Were a U.S. computer manufacturer to produce a secure computer operating system using top quality cryptography throughout, we would not now permit him to ship it abroad, and he could not even be certain of access to domestic markets, as illustrated in Figure 11. Today, firms face uncertain regulations that may or may not permit sales of advanced equipment. Faced with such uncertainty, commercial firms quite properly avoid serious investment in secure systems.

I believe that our failure to invest in security puts our U.S. information industry at risk. A foreign supplier will eventually offer good security. Ten years from now, Fujitsu may offer secure computers and Sony may offer secure cellular phones to the considerable peril of Intel, IBM, and Motorola. Ten years from now, new information services will be available worldwide.

Will we lead the development of those new services as we led color television, or follow as we did with VCRs and compact discs?

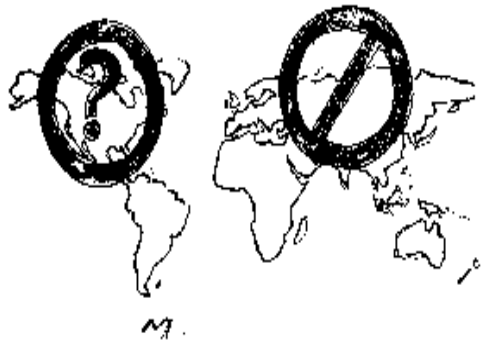

Figure 11.

7 Securing Our Economic Future

The future of U.S. economic security rests on timely commercial use of cryptographic technology. If we act too late, we will fail to make adequate commercial investment in security systems. If we act too late, we face national disasters as hackers or terrorists penetrate our information systems. If we act too late, new cryptographic industry will slip out of U.S. control to foreign suppliers. Our information industry may wither. We may become dependent on the Far East or Europe for the information equipment on which our economy depends.

Attacks on computer systems are a free enterprise activity. We need free enterprise working on computer defense too. Activating our free enterprise industry requires only a guarantee from government of an orderly market. Our information industry has plenty of private financial support. Its management, collectively, has demonstrated adequate courage. We have abundant technical knowledge.

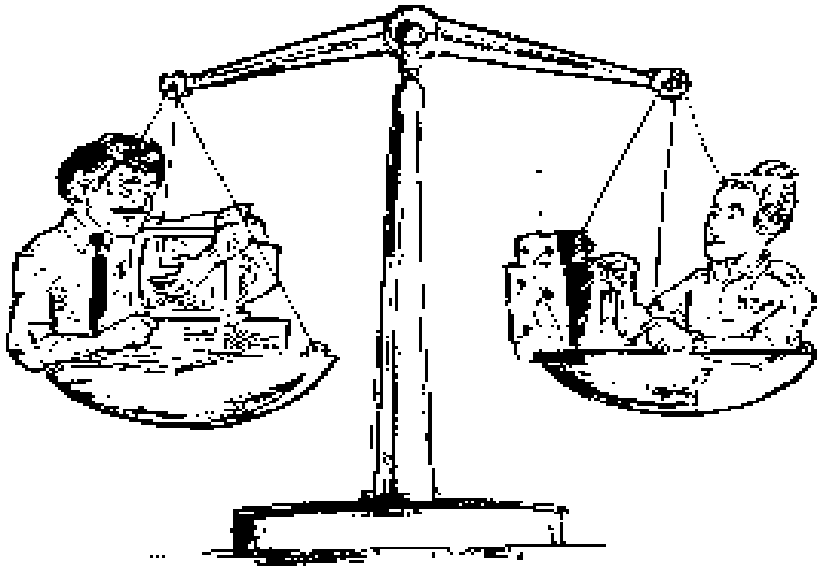

Figure 12.

All industry lacks is a clear charter permitting it to profit from this new activity. It needs a guarantee of understandable and stable government action. Industry needs a guarantee of freedom from the fetter of uncertainty.

Such a guarantee could come as a clear policy statement from the Executive Branch removing cryptographic equipment and software from export control and the threat of domestic control. Such a guarantee could come from Legislative action forbidding the Executive from regulating cryptography. Such a guarantee may come from a court case invalidating rules against cryptography. Any such guarantee will permit major commercial investment leading not only to domination of major world markets for U.S. equipment and secure systems for our own use, but also to new U.S. industries based on the new technology.

8 Your Job—Name The Year

In the past, the value of cryptography for military and law enforcement far exceeded its commercial value. The spread of cryptographic knowledge helps our foes cover their communications and so we rely more on other intelligence sources. Meanwhile, the commercial importance of cryptography increases for three reasons. First, a world market for new equipment waits. Second, the caliber of disaster possible by unauthorized penetration grows. Third, whole new industries will sprout from the new technology. We are entering an era where digital communications will dominate our commerce. We are already at the mercy of our computer systems. Are we to make our own security equipment or buy it abroad? Are we to remain with our systems unsecured? Will we

be the dominant players in the new information industries?

The winds of change are blowing. The commercial value of cryptography may have already or will soon outstrip its military and law enforcement value. A major world market awaits our entry. The risk to our economic system of unsecured commercial communications grows with their volume. New industry awaits the fresh ideas of entrepreneurs, ours or theirs. You are one of the few bodies with knowledge of both the government and the commercial utility of this emerging technology. Only you can assess their relative importance. See Figure 12.

I believe you can express your answer by nominating a particular year. It is the year when the commercial value of cryptography exceeds its value to government as illustrated in Figure 13.

Some think the year has already passed, some believe it yet to come. I have a private view, but I lack the knowledge for balanced judgment. You have that knowledge. You must make your judgment clearly and concisely, because as a nation, we must act promptly and properly on your judgment.

The investment required to use cryptography will take time. If the date you select is in the past, we are already behind and must hurry. If the date you select is in the future, we should plan now for the orderly change in rules that will make investment attractive. I believe that commercial use of cryptography is inevitable and will soon blossom. I hope you will help the United States to be a major player.

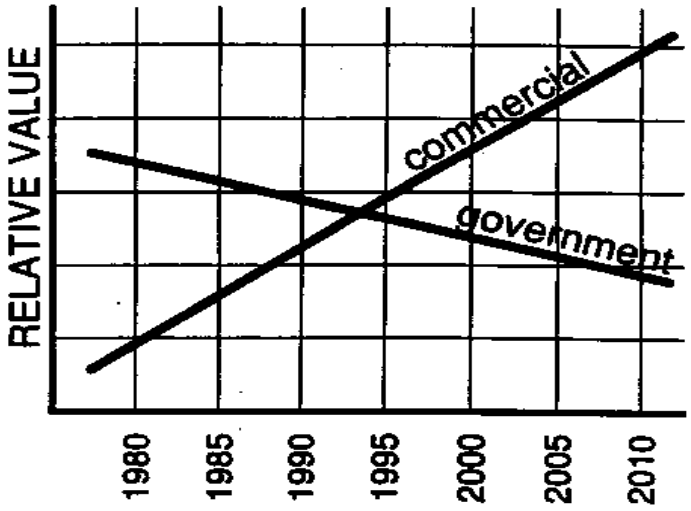

Figure 13. When does the value of commercial cryptography exceed its value as a government monopoly?